Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85577Neubiberg

Modulhandbuch des Studiengangs

Cyber - Sicherheit
(Master of Science)

an der
Universität der Bundeswehr München

(Version 2025)

Stand: 11. Dezember 2024

Inhaltsverzeichnis

Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulname	Modulnummer
Netzsicherheit	5502

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gabi Dreo Rodosek	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10102	VÜ	Netzsicherheit	Pflicht	3
10103	P	Praktikum Netzsicherheit	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Rechnernetzen, wie sie z.B. in der Bachelor-Vorlesung Einführung in Rechnernetze vermittelt werden.

Qualifikationsziele

Die Studierenden lernen in der Vorlesung Netzsicherheit die Gefährdungsaspekte von Netzen und deren Entwicklung detailliert kennen. Nach erfolgreichem Abschluss des Moduls sind die Studierenden befähigt, sicherheitsrelevante Aspekte in vernetzten Strukturen zu erkennen und Betrachtungen von Netzen in Bezug auf Sicherheitsaspekte durchzuführen. Sie werden in die Lage versetzt, Verfahren zum Schutz und der Absicherung der jeweiligen Netze zu identifizieren. Mittels der Vorstellung von aktuellen Geräten und neuer Verfahren werden die Studierenden zusätzlich befähigt, Abschätzungen von Sicherheitsgefährdungen durch neue Technologien zu geben.

Nach dem Praktikum Netzsicherheit sind die Studierenden in der Lage, Maßnahmen zur Abwehr von gängigen Bedrohungen und zur Absicherung von IT-Systemen zu implementieren und deren Wirksamkeit zu verifizieren. Durch die eigenständige Bearbeitung von angeleiteten, praktischen Aufgaben vertiefen und festigen die Studierenden ihre Kenntnisse im Bereich Cyber-Sicherheit.

Inhalt

In der Vorlesung Netzsicherheit erhalten Studierende einen vertieften Einblick in Fragestellungen der Netzsicherheit. Hierbei werden zunächst die Sicherheitsbedrohungen im Wandel von klassischen Angriffen hin zum Cyber War mit Schadsoftware und deren Verbreitung betrachtet, sowie u.a. aktive und passive Angriffe, Blended Attacks, Web Hacking, Spam, Botnetze und Aspekte der Internet-Kriminalität behandelt.

Im weiteren Verlauf stehen sowohl Firewall-Architekturen, -konzepte, -Systeme als auch Intrusion Detection und Prevention Systeme, Honeypots (Low- und High-Interaction), Honeynets sowie Early Warning Systeme im Fokus. Eine vertiefende Auseinandersetzung mit sicherheitsrelevanten Protokollen wie IPsec und den Auswirkungen der breitbandigen Nutzung von IPv6 auf die Netzsicherheit ist ebenso Bestandteil der Vorlesung. Wesentliche Techniken und Besonderheiten neuer Verfahren und Ansätze zur Angriffserkennung im Bereich der mobilen Endgeräte wie Smartphones und Tablet-PCs sowie des Cloud Computings schließen die Thematik ab.

Schwerpunkt im Praktikum Netzsicherheit ist die selbstständige Durchführung von praktischen Aufgaben zu aktuellen Themen und Fragestellungen der Absicherung von IT-Systemen. Zu Beginn werden einfache Angriffe auf den Ebenen 2 bis 4 sowie 7 des ISO/OSI-Referenzmodells vorgestellt, bspw. durch die Manipulation von ARP, Subnetting oder Angriffe gegen Webseiten auf Applikationsebene (z.B. XSS). Entsprechende Gegenmaßnahmen werden untersucht und integriert (z.B. Einrichtung und Betrieb einer Firewall, Absicherung von Webservern, Aufbau und Betrieb von Tunneln). Darauf aufbauend werden weitere, aktuelle Angriffsverfahren behandelt, bspw. Bot-Netz-Attacken oder spezialisierte Angriffe wie z.B. zielgerichtete Angriffe. Hierzu werden ebenfalls geeignete Gegenmaßnahmen entwickelt und praktisch implementiert (z.B. Intrusion Detection/Prevention Systeme, low/high interaction Honeypots/Honeynets).

Literatur

William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, ISBN-10 0134444280, 2016

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 20 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

- Pflichtmodul im Masterstudiengang CYB
- Wahlpflichtmodul im Masterstudiengang ME, Wahlpflichtgruppe ITSK

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Hardwaresicherheit	5503

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Ph.D. M.S. (OSU) Klaus Buchenrieder	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
25381	VL	Eingebettete Systeme	Pflicht	2
25382	UE	Eingebettete Systeme	Pflicht	1
55031	VÜ	Embedded Systems Security	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Voraussetzung für alle Modulbestandteile sind Kenntnisse in Rechnerarchitektur. Für Eingebettete Systeme sind zusätzlich Kenntnisse zu Rechnerorganisation notwendig, wie sie im Bachelor-Modul Rechnerorganisation vermittelt werden.

Qualifikationsziele

Die Studierenden vertiefen die Kompetenz, das grundlegende Verhalten und die wesentlichen Aufgaben von hardwarenahen Rechnersystemen in der Praxis zu verstehen und zu bewerten. Sie können Eigenschaften von hardwarenahen Rechnersystemen fachwissenschaftlich einordnen und haben damit die Grundlage, die Verwendbarkeit dieser Konzepte für bestimmte praktische Anwendungen zu bewerten. Die Studierenden wissen, wie eingebettete Systeme hinsichtlich der Übertragung, Verarbeitung und Speicherung von Daten abzusichern sind. Sie kennen technische und physische Angriffsvarianten wie Seitenkanalangriffe und wissen, wie Software-Implementierungen dagegen gehärtet werden können.

Inhalt

In der Vorlesung und Übung Eingebettete Systeme erhalten die Studierenden einen umfassenden Überblick über die wesentlichen Grundlagen und Konzepte, die zum Entwurf eingebetteter Systeme notwendig sind. Zu Beginn werden die Kenntnisse über Hardware-Konzepte aus dem Modul "Rechnerorganisation" vertieft und darauf aufbauend Mikro- und spezielle Architekturen entwickelt. Neben den gängigen Prozessorarchitekturen werden digitale Signalprozessoren (DSP) und System-on-Chip Architekturen eingeführt. Zu Themen der maschinennahen Programmierung von Mikroprozessoren und Mikrokontrollern werden Konzepte und Probleme der Verarbeitung von Events und Daten unter Echtzeitbedingungen behandelt. Nach der Einführung asynchroner Ereignisse und den dazu gehörenden Zeitbedingungen werden grundlegende Verfahren zur Ereignissynchronisation beschrieben und

Prozessplanungsverfahren vorgestellt. Im dritten Abschnitt des Modulbestandteils wird auf die Entwurfsmethodik für die Konstruktion leistungsfähiger Eingebetteter Systeme eingegangen. In der Übung zur Vorlesung wird hardwarenahe Software in Kleingruppen entwickelt, in Betrieb genommen und getestet.

In der Vorlesung Embedded Systems Security wird nach einem Überblick über typische Architekturen und Eigenschaften von zeitgemäßen eingebetteten Systemen ein Schwerpunkt auf mögliche Angreifer auf solche Systeme gelegt. Ausgehend davon, dass typische Angreifer Hardware-Zugriff haben, werden verschiedene Angriffsmöglichkeiten erläutert und zueinander in Kontext gesetzt. Anhand von typischen Hardware-Chips werden Sicherheitsmechanismen und dedizierte Sicherheitschips besprochen. Danach wird ein Schwerpunkt auf kryptographische Algorithmen und deren Implementierung in eingebetteten Systemen gelegt. Dabei werden die schwerwiegenden sogenannten Seitenkanalangriffe behandelt. Danach wird die Implementierung von Sicherheitsmechanismen gegen vorgestellte Angriffe thematisiert. FPGA Zielplattformen sind in speziellen Einsatzbereichen sehr relevant. Die Informationssicherheit von Systemen auf deren Basis wird eigens behandelt. Schlußendlich wird noch die Kommunikationssicherheit von eingebetteten Systemen erläutert. In der Übung wird ein beispielhaftes eingebettetes µC-System anhand der in der Chip-HW vorhandenen Sicherheitsmechanismen gehärtet. Danach wird eine kryptographische Implementierung auf diesen µC portiert und ein Seitenkanalangriff durchgeführt.

Literatur

Wird im Skriptum angegeben. Zusatzmaterial für die jeweilige Veranstaltung wird in ILIAS bereitgestellt.

Leistungsnachweis

Portfolio, das zu jeder der beiden Lehrveranstaltungen eine schriftliche Klausur von 45 Minuten umfasst.

Die Leistungen für das Modul Hardwaresicherheit gehen wie folgt in die Note ein:

- schriftliche Klausur (Eingebettete Systeme): 30%;
- verpflichtende praktische Übung mit Ausarbeitung (Eingebettete Systeme): 20%;
- schriftliche Klausur (Embedded System Security): 30%;
- verpflichtende praktische Übung mit Ausarbeitung (Embedded System Security): 20%.

Verwendbarkeit

- Pflichtmodul im Masterstudiengang CYB
- Wahlpflichtmodul im Masterstudiengang ME, Wahlpflichtgruppe ITSK

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Datenschutz und Privacy	5504

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55041	VÜ	Datenschutz	Pflicht	3
55042	VÜ	Privacy Enhancing Technologies	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse der Informatik, wie sie im Bachelor-Studium vermittelt werden.

Qualifikationsziele

Die Studierenden kennen die Ziele und Grundbegriffe des Datenschutzes. Sie können erkennen, welche Vorgänge datenschutzrelevant sind und welche gesetzlichen und branchenspezifischen Regelungen dabei berücksichtigt werden müssen. Sie können Folgeabschätzungen für neue Technologien und Verfahren vornehmen und aktuelle technische Schutzmaßnahmen anwenden. Die Studierenden können die Datenschutzrelevanz passiver und aktiver Angriffe wie Verkehrsanalysen beurteilen und Abwägungen zwischen hoher Schutzwirkung und anderen Merkmalen wie Kosten, Bandbreite und Latenz treffen. Sie kennen Ansätze wie Differential Privacy, Multi-Party-Computation und Homomorphe Verschlüsselung und können deren Anwendungsgebiete voneinander abgrenzen

Inhalt

Das Ziel der Vorlesung "Datenschutz" ist es, das Verständnis und die Bedeutung von Privacy für Einzelpersonen und demokratische Gesellschaften zu vermitteln. Es wird ein Überblick über die historische Entwicklung der Privatsphäre und die aktuelle rechtliche Situation, insbesondere in Deutschland und der EU, gegeben, wobei der Fokus auf der Datenschutz-Grundverordnung (DSGVO) liegt. Des Weiteren werden Grundbegriffe des Datenschutzes und die Datenschutz-Grundsätze erläutert, wobei der Schwerpunkt auf verschiedenen technischen Maßnahmen zur Datenschutzumsetzung liegt, wie beispielsweise der technischen Realisierung des Rechts auf Löschung.

In der Vorlesung "Privacy Enhancing Technologies" (PETs) liegt der Schwerpunkt auf der technischen Unterstützung und Umsetzung von Datenschutz und Privatsphäre. Es werden zunächst die Prinzipien von PETs sowie grundlegende Umsetzungsansätze wie z.B. Privacy by Design, Kryptographie oder Multi-Party Computation vorgestellt und

analysiert. Anschließend werden sowohl theoretische Konzepte als auch praktische Anwendungen, Methoden und Werkzeuge der PETs betrachtet, z.B. Funktionsweise und Einsatzgebiete von Blockchain und ePass. Zur anschaulichen Vermittlung des Wissens über Datenschutz im gesamten Datenlebenszyklus werden Daten in sechs Bereiche unterteilt und separat behandelt: (1) Authentifizierung, (2) Daten auf lokalen Systemen (Data-at-Rest), (3) Daten in Übertragung (Data-in-Motion), (4) Daten Online/im Web, (5) Anonymes Bezahlen, (6) Privatsphäre auf mobilen Geräten. Für jeden Bereich werden die Risiken für die Privatsphäre analysiert und mögliche Schutzmethoden und -techniken vorgestellt und diskutiert.

Literatur

- Petrlic, R., Sorge, Ch., and Ziebarth, W.: Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie. Wiesbaden: Springer Fachmedien Wiesbaden, 2023
- Th. Kranig, A. Sachs und M. Gierschmann: Datenschutz-Compliance nach der DS-GVO, Bundesanzeiger Verlag, 2019
- M.-T. Tinnefeld, B. Buchner, and Th. Petri. Einführung in das Datenschutzrecht 5. A. Datenschutz und Informationsfreiheit in europäischer Sicht. De Gruyter Oldenbourg, 2019
- Roßnagel, A.: Datenschutz in einem informatisierten Alltag. Berlin Friedich-Ebert-Stiftung, 2007

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer.

Verwendbarkeit

- Pflichtmodul im Masterstudiengang CYB
- Wahlpflicht im Masterstudiengang ME, Wahlpflichtgruppe ITSK

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Systemsicherheit	5505

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gunnar Teege	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10104	VÜ	IT-Forensik	Pflicht	3
55051	VÜ	Betriebssystemsicherheit	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Betriebssystemen, wie sie z.B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden lernen die wesentliche Rolle kennen, die das Betriebssystem für die Absicherung von Computersystemen spielt und die dabei verwendeten Vorgehensweisen und nötigen Hardware-Voraussetzungen, aber auch die Grenzen rein technischer Maßnahmen. Damit sind sie in der Lage, die Wirksamkeit von Sicherheitsmaßnahmen einzuordnen und Sicherheitseigenschaften von Betriebssystemen abhängig von der Einsatzumgebung zu bewerten. Sie erhalten eine erste Orientierung zum Vorgehen bei der Absicherung von IT-Systemen durch Auswahl und Konfiguration des Betriebssystems und den Einsatz spezieller Sicherheitsmechanismen.

Die Studierenden entwickeln ein Verständnis für die Prinzipien und Vorgehensweisen bei der Untersuchung von Sicherheitsvorfällen. Sie kennen die grundlegenden Schritte eines Computerforensikers und können diese auf konkrete Angriffsszenarien anwenden. Insbesondere verstehen sie die verschiedenen Analysemethoden und sind in der Lage, diese in Form einer gerichtsverwertbaren Aufarbeitung anwenden zu können. Ferner beherrschen sie die forensische Analyse einer Festplatte mittels Open-Source-Tools sowie die Erarbeitung von Konzepten zur Sicherheitsüberprüfung komplexer Systeme.

Inhalt

Zu den Sicherheitsaspekten von IT-Systemen, die typischerweise durch das Betriebssystem implementiert werden, gehören klassischerweise die Zugangs- und Zugriffskontrolle und die Bildung verschiedener Schutzbereiche zur Ausführung von Anwendungen. In der Veranstaltung Betriebssystemsicherheit werden zuerst die wesentlichen Mechanismen zur Absicherung von Software, insbesondere des Betriebssystems selbst vorgestellt (secure boot, Festplattenverschlüsselung,

Hauptspeicherverschlüsselung). Anschließend werden Maßnahmen zur Herstellung von Vertraulichkeit innerhalb eines Rechners betrachtet und Angriffe darauf (Verdeckte Kanäle, Seitenkanäle). Im zweiten Teil der Veranstaltung werden Autorisierungssysteme vorgestellt. Dabei wird ihre Struktur betrachtet, allgemeine Eigenschaften und Grenzen (Safety-Problem) und der Umgang mit diesen Systemen (Sicherheitsmodelle, mandatory / discretionary access control). Abschließend werden Bewertungskriterien für die Sicherheit von Rechensystemen behandelt mit Schwerpunkt auf dem Common Criteria Standard.

IT-Forensik beschäftigt sich mit der Untersuchung von Vorfällen (Incidents) von IT-Systemen. Durch Erfassung, Analyse und Auswertung digitaler Spuren in Computersystemen werden nach Möglichkeit sowohl der Tatbestand als auch der oder die Täter festgestellt. Im Rahmen der Veranstaltung erhalten die Studenten zunächst einen grundlegenden Überblick über die Thematik IT-Forensik. Im nächsten Schritt erfolgt ein vertiefender Einblick in den Aufbau von Speichermedien (Festplatten, Flashspeicher, Magnetbänder) sowie Arten, Standards, Schnittstellen (Aufbau und Analyse von Standarddateisystemen, bspw. FAT, NTFS, ext4fs). Darauf aufbauend erfolgt eine Klassifikation von Datenträgern, Partitionierungsverfahren sowie prinzipiellen Analysemöglichkeiten (z.B. vor dem Hintergrund einer Verschlüsselung von Dateien). Als nächstes werden typische Angriffsmethoden untersucht, bevor am praktischen Beispiel einer forensischen Post-Mortem-Analyse ein konkretes Szenario bearbeitet wird. Hierbei wird u.a. ein spezieller Fokus auf die Einbeziehung von Behörden im Sinne einer gerichtsverwertbaren Auswertung gelegt.

Literatur

Zur Vorlesung Betriebssystemsicherheit: Es gibt kein Lehrbuch, das genau den Vorlesungs-Inhalt abdeckt. In den folgenden Büchern werden Themen aus der Vorlesung behandelt, sie sind als vertiefende Literatur verwendbar:

- Andrew S. Tanenbaum: Moderne Betriebssysteme, Pearson Studium, 3. Auflage, 2009
- Claudia Eckert: IT-Sicherheit, DeGruyter, Oldenbourg, 9. Auflage, 2014
- Trent Jaeger: Operating Systems Security, Morgan & Claypool, 2008
- Joachim Biskup: Security in Computing Systems, Springer, 2009.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer.

Verwendbarkeit

- Pflichtmodul im Masterstudiengang CYB
- Wahlpflichtmodul im Masterstudiengang ME, Wahlpflichtgruppe ITSK
- Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfeld Technische Informatik

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Kryptologie	5506

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55061	VÜ	Einführung in die Kryptographie	Pflicht	3
55062	VÜ	Kryptoanalyse	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse in Mathematik, im Algorithmenentwurf und in der Algorithmenanalyse, wie sie in einführenden Lehrveranstaltungen zur Mathematik (Mathematische Strukturen, Lineare Algebra, Analysis) und zur Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden kennen die wichtigsten grundlegenden kryptographischen Verfahren. Sie kennen ihre Vor- und Nachteile und ihre Stärken und Schwächen und können beurteilen, in welchen Situationen welche Verfahren eingesetzt werden können.
Sie kennen verschiedene Anwendungsgebiete kryptographischer Verfahren wie Geheimhaltung, Authentizität von Nachrichten und digitale Signaturen. Ferner kennen Sie die wichtigsten Methoden der Kryptoanalyse.

Inhalt

Die Grundbegriffe der Kryptographie sollen zuerst an klassischen symmetrischen Verschlüsselungsverfahren erläutert werden. Es werden zum Beispiel Stromchiffren und Blockchiffren (DES - Data Encryption Standard, AES - Advanced Encryption Standard) behandelt. Ein Schwerpunkt der einführenden Lehrveranstaltung werden allerdings asymmetrische Public-Key-Verschlüsselungsverfahren sein, zum Beispiel das RSA-Verfahren, die Diffie-Hellman-Schlüsselvereinbarung, El-Gamal-Systeme und weitere Verfahren. Auch Zero-Knowledge-Protokolle sollen behandelt werden. Neben der reinen Nachrichtenverschlüsselung sollen auch andere Anwendungen behandelt werden, zum Beispiel Signatur-Verfahren, Authentizität von Nachrichten sowie Authentifikation von Kommunikationsteilnehmern.

Unter Kryptoanalyse versteht man die Analyse von kryptographischen Verfahren mit dem Ziel, ihre Sicherheit zu beweisen und zu quantifizieren, oder mit dem Ziel, Schwachstellen

aufzudecken und ggf. Gegenmaßnahmen zu ergreifen. In der Vorlesung "Kryptoanalyse" wird die Kryptoanalyse hauptsächlich von den Verfahren behandelt, mit denen die Studierenden in der Vorlesung "Kryptographie" bereits vertraut gemacht wurden:

- Kryptoanalyse der Enigma als Beispiel zur historischen Kryptographie;
- Kryptoanalyse von RSA (Low-Exponent-Angriffe, Common-Modulus-Angriffe, Angriffe auf das Padding, Faktorisierungsalgorithmen/quadratisches Sieb)
- Kryptoanalyse von Verfahren, die auf dem diskreten Logarithmus in der multiplikativen Gruppe eines endlichen Körpers oder in einer elliptischen Kurve beruhen (Algorithmus von Silver-Polig-Hellman, Rho-Verfahren von Pollard, Baby-Step-Giant-Step-Verfahren von Shanks, Indexcalculus in der multiplikativen Gruppe);
- Die Algorithmen von Shor zur Kryptoanalyse mit dem Quantencomputer;
- Kryptoanalyse von Verfahren, die immun gegen Angriffe mit dem Quanten-Computer zu sein scheinen. Als Beispiel wird das auf linearen Codes beruhende McEliece-Verfahren behandelt.

Neben der Diskussion der theoretischen Grundlagen wird auch auf ganz praxisnahe und konkrete Angriffsszenarien, wie zum Beispiel Logjam oder den Heartbleed-Bug, eingegangen.

Literatur

- B. Schneier: Angewandte Kryptographie. Pearson Studium, 2005
- M. Stamp and R. M. Low: Applied cryptanalysis. Breaking ciphers in the real world. John Wiley & Sons, 2007
- Buchmann, J.: Einführung in die Kryptographie, 6. Auflage, Springer Spektrum, 2016
- Forster, O.: Algorithmische Zahlentheorie, 2. Auflage, Springer-Verlag, 2015
- Hoffstein, J.; Pipher, J.; Silverman, Joseph H.: An Introduction to Mathematical Cryptography, Springer-Verlag, 2010
- Beutelspacher, A.; Neumann, Heike B.; Schwarzpaul, T.: Kryptographie in Theorie und Praxis, 2. Auflage, Vieweg+Teubner, 2010
- Paar, C.; Pelzl, J.: Kryptographie verständlich, Springer Vieweg, 2016

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer.

Verwendbarkeit

- Pflichtmodul im Masterstudiengang CYB
- Wahlpflicht im Masterstudiengang ME, Wahlpflichtgruppe ITSK

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Anwendungssicherheit	5507

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10107	VÜ	Sichere vernetzte Anwendungen	Pflicht	3
55071	VL	Language-based Security	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Gute Kenntnisse in den Bereichen Programmiersprachen, Compiler und systemnahe Programmierung werden vorausgesetzt.

Qualifikationsziele

Es wird die Kompetenz vermittelt, grundlegende Designfehler, weit verbreitete Sicherheitslücken und typische Implementierungsfehler auf Quelltextebene zu erkennen und zu vermeiden. Studierende lernen praxisrelevante Penetration-Testing-Ansätze, ausgewählte wichtige Software-Härtungsmaßnahmen und Bausteine sicherer vernetzter Anwendungen samt ihren betrieblichen Aspekten kennen.

Studierende erwerben fundierte Kenntnisse zu aktuellen Angriffen und Verteidigungstechniken. Behandelte Techniken werden sowohl theoretisch als auch praktisch behandelt, sodass Studierende neben Faktenwissen zu den jeweiligen Techniken auch jene Methodenkompetenzen erwerben, die es ihnen erlaubt, Sicherheitsfragestellungen aus Programmiersprachen-Sicht kompetent zu beantworten.

Inhalt

Die Vorlesung Entwicklung und Betrieb sicherer vernetzter Anwendungen betrachtet Methoden, Konzepte und Werkzeuge zur Absicherung von verteilten Systemen über deren gesamten Lebenszyklus. Anhand von Webanwendungen und anderen serverbasierten Netzdiensten werden zunächst Angreifer-, Bedrohungs- und Trustmodelle sowie typische Design-, Implementierungs- und Konfigurationsfehler und deren Zustandekommen analysiert. Auf Basis dieser Grundlagen wird ein systematisches Vorgehen bei der Entwicklung möglichst sicherer vernetzter Anwendungen erarbeitet. Nach einem Überblick über die Besonderheiten der auf IT-Sicherheitsaspekte angepassten Entwicklungsprozesse werden ausgewählte Methoden und Werkzeuge, u.a. zur statischen bzw. dynamischen Code-Analyse und für Penetration Tests, und ihr Einsatz in den einzelnen Phasen des Softwarelebenszyklus mit den Schwerpunkten

Implementierung und operativer Einsatz vertieft. Am Beispiel von Authentifizierungs- und Autorisierungsverfahren u.a. auf Basis von LDAP, SAML, XACML und OAuth wird die Integration klassischer und moderner Access-Control-Modelle in neu entwickelte Systeme und Legacy-Anwendungen mit ihren betrieblichen Aspekten, u.a. Management und Skalierbarkeit, diskutiert. Nach einem Überblick über aktuelle Härtungs- und Präventionsansätze in Compilern, Betriebssystemen und Libraries werden ausgewählte Ansätze zur Analyse von Exploits und Malware behandelt. Unter dem Stichwort Ethical Hacking werden abschließend Vorgehensweisen bei der Responsible Disclosure identifizierter Schwachstellen diskutiert, die zu einer kontinuierlichen Verbesserung der Sicherheitseigenschaften komplexer Anwendungen führen.

Ziel der Vorlesung Language-based Security ist es, Grundlagen aus der sprach-basierten Sicherheit aus praktischer und theoretischer Sicht zu vermitteln. Konkret wird fundamentales Wissen zu aktuellen Angriffstechniken, z.B. Code-Injection und Code-Reuse Angriffe, vermittelt. Die jeweiligen Angriffstechniken werden danach sukzessive in ihre Bestandteile zerlegt und aus der Perspektive der sprach-basierten Transformationen beleuchtet. Themen der Vorlesung sind:

- Laufzeitstruktur von Programmen auf Maschinenebene
- Angriffe durch Injektion malignen Codes (“code injection attacks”) und deren Abwehr
  - Buffer Overflows und Stack Canaries
  - Control-Flow Hijacking und Control-Flow Integrity
- Angriffe durch Wiederverwendung bereits existierenden Codes (“code re-use attacks”) und deren Abwehr
  - Return-Oriented Programming und Software Diversity
- Angriffe durch Daten
  - Non-Control Data Attacks und Data-Flow Integrity bzw. Data Randomization
- Aktuelle Resultate
  - Theoretische Sicherheit von Control-Flow Integrity
  - Trends in Software Diversity

Literatur

- Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, 3. Auflage, Wiley, 2021
- Loren Kohnfelder: Designing Secure Software, No Starch Press, 2021
- Daniel Deogun, Dan Bergh Johnsson, Daniel Sawano: Secure by Design, Manning, 2019
- Sachar Paulus: Basiswissen Sichere Software, dpunkt-Verlag, 2011
- Michael Howard, David LeBlanc, John Viega: 24 Deadly Sins of Software Security, McGraw-Hill, 2009

Leistungsnachweis

Schriftliche Prüfung mit 120 Minuten Dauer.

Verwendbarkeit
Die im Modul behandelten Inhalte finden in den MCYB-Wahlpflichtmodulen zu Language-based Security, Compilerbau (auch in MINF) sowie Identitätsmanagement Anwendung und sind bei eigenen Implementierungen, z.B. im Rahmen der Masterarbeit, zu berücksichtigen.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Security- und IT- Management	5508

Konto	Pflichtmodule - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Ulrike Lechner	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
240	84	156	8

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10106	VÜ	Sicherheitsmanagement	Pflicht	3
10471	VÜ	IT-Governance	Pflicht	4
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Grundlegende Kenntnisse über die Anwendungsbereiche und Methoden der IT-Sicherheit, wie sie z.B. im Modul Grundlagen der Informationssicherheit vermittelt werden.

Qualifikationsziele

Die Studierenden lernen zentrale Fragestellungen und wichtige Instrumente der Organisation, Steuerung und Kontrolle der IT und der IT-Prozesse von Organisationen kennen, in die auch sämtliche operativen Aspekte der Informationssicherheit zu integrieren sind. Sie lernen Fragestellungen und Methoden der Praxis im IT-Management kennen. Sie werden befähigt, Methoden des IT-Managements zu gestalten und zu evaluieren.

Die Vorlesung Sicherheitsmanagement vermittelt die Kompetenz, den Themenkomplex Informationssicherheit in seiner Breite strukturiert und nach technischen und organisatorischen Aspekten differenziert anzugehen und je nach Einsatzszenario systematisch Schwerpunkte im operativen Sicherheitsmanagement zu setzen. Studierende werden in die Lage versetzt, in realistischen Anwendungsbeispielen den Erfüllungsgrad von Anforderungen durch internationale Normen und branchenspezifische Vorgaben zu beurteilen und Maßnahmen zu planen, um identifizierte Defizite zu beseitigen.

Inhalt

Wie kann die IT-Landschaft einer Organisation gestaltet werden? Informationssysteme spielen eine zentrale Rolle für Organisationen und die Gesellschaft als Ganzes.
Thema dieser Veranstaltung ist die Steuerung der IT in einer Organisation mit den Themenfeldern Strategie, Personal, Prozesse, Compliance und Risikomanagement. Weitere Themen sind Outsourcing und Cloud Computing sowie wichtige Ansätze in der Regulierung und Standardisierung.

IT-Governance ist ein vergleichsweise neues Gebiet der Informatik und Wirtschaftsinformatik, das der zentralen Rolle der IT in Organisationen Rechnung trägt. Die IT mit ihren Prozessen ist so zu gestalten, dass sie die gesetzlichen Anforderungen erfüllt und die Geschäftsstrategie umsetzt. Weitere Aufgaben sind die Wertschöpfung durch IT und die Minimierung von IT-Risiken. IT-Governance soll den Rahmen schaffen, um IT-Leistungen effektiv und effizient zu erbringen.

Die Vorlesung Sicherheitsmanagement führt in die organisatorischen und technischen Aspekte des Umgangs mit dem Thema Informationssicherheit in komplexen Umgebungen ein, beispielsweise in Konzernen mit mehreren Standorten und bei organisationsübergreifenden Kooperationen wie Zulieferpyramiden oder internationalen Forschungsprojekten. Auf Basis der internationalen Normenreihe ISO/IEC 27000, die u.a. im Rahmen des IT-Sicherheitsgesetzes auch national stark an Bedeutung gewinnt, und weiterer Frameworks wie COBIT werden die Bestandteile so genannter Informationssicherheits-Managementsysteme (ISMS) analysiert und Varianten ihrer Umsetzung mit den damit verbundenen Stärken und Risiken diskutiert. Neben der Integration vorhandener technischer Sicherheitsmaßnahmen in ein ISMS werden auch die Schnittstellen zu branchenspezifischen Vorgaben, beispielsweise dem Data Security Standard der Payment Card Industry, zum professionellen IT Service Management bei IT-Dienstleistern und zu gesetzlichen Auflagen betrachtet.

Literatur

- Michael Klotz, Matthias Goeken, Martin Fröhlich. IT-Governance: Ordnungsrahmen und Handlungsfelder für eine erfolgreiche Steuerung der Unternehmens-IT, dpunkt-Verlag, 2023.
- Andreas Rüter, Jürgen Schröder, Axel Göldner, Jens Niebuhr. IT-Governance in der Praxis: Erfolgreiche Positionierung der IT im Unternehmen. Anleitung zur erfolgreichen Umsetzung regulatorischer und wettbewerbsbedingter Anforderungen (Xpert.press), 2010.
- Michael Brenner et al., Praxisbuch ISO/IEC 27001, Hanser Verlag, 4. Auflage 2022
- Thomas Harich, IT-Sicherheitsmanagement, mitp Professional Verlag, 3. Auflage 2021

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen. Für die VÜ IT-Governance sind die folgenden Leistungen zu erbringen: Vortrag von 20-30 Minuten Dauer und Bearbeitungszeit von 2-4 Wochen in Gruppenarbeit und Bearbeitung eines Praxisproblems mit Präsentation von 20-30 Minuten Dauer in Gruppenarbeit und 6-12 Wochen Bearbeitungszeit. Zu der VÜ IT-Sicherheitsmanagement ist eine schriftliche Klausur von 30 Minuten Dauer zu absolvieren. In die Note gehen die Leistung zu IT-Sicherheitsmanagement zu 3/7 ein, die Leistung aus IT-Governance zu 4/7. In die Note zu IT-Governance gehen der Vortrag zu 40% und die Bearbeitung eines Praxisproblems zu 60% ein.

Verwendbarkeit

Die Inhalte des Moduls sind Grundlage vertiefender Wahlpflichtmodule wie Enterprise Architecture und IT Service Management, IT-Governance (MWIN) sowie Staatliche IT-Sicherheit und können in die Konzeption eigener technischer und organisatorischer Sicherheitsmaßnahmen und Prozesse, z.B. im Rahmen einer Masterarbeit, einfließen.

Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Grundlagen der Informationssicherheit	1651

Konto	Überkonto Wahlpflicht - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Pflicht	6

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10101	VÜ	Ausgewählte Kapitel der IT-Sicherheit	Pflicht	3
11432	VÜ	Sicherheit in der Informationstechnik	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für das Modul werden grundlegende Kenntnisse in folgenden Bereichen benötigt:

- Programmieren und Software Engineering, wie z.B. in den Bachelormodulen "Einführung in die Informatik 1/2" und "Objektorientierte Programmierung" vermittelt.
- Rechnernetze, wie z.B. in "Einführung in Rechnernetze" vermittelt.

Qualifikationsziele

Das Absolvieren des Moduls wird Studierenden im Bachelor-Studium, die den Master-Studiengang Cyber-Sicherheit (MCYB) studieren möchten, **dringend** empfohlen. MCYB-Studierende, die das Modul nicht bereits im Bachelor-Studium absolviert haben, müssen es zu Beginn des Master-Studiengangs verpflichtend belegen.

Studierende erhalten einen Einblick in die verschiedenen Aspekte der IT-Sicherheit und sind in der Lage, die Bedeutung und Zusammenhänge verschiedener technischer und organisatorischer Einflussfaktoren auf die IT-Sicherheit zu verstehen. Mit den erworbenen Kenntnissen können die Studierenden systematische Bewertungen des Schutzbedarfs und des Sicherheitsniveaus moderner IT-Systeme und IT-Infrastrukturen vornehmen, in die auch in der Praxis häufig noch unterschätzte nicht-technische Faktoren einfließen.

Inhalt

Das Modul führt in die Grundlagen der Informations- und IT-Sicherheit ein und gibt dabei einen breiten Überblick über die Teildisziplinen der Informationssicherheit.

Die Lehrveranstaltung "Sicherheit in der Informationstechnik" umfasst klassische Methoden der technischen und organisatorischen Informationssicherheit, u.a.

- Bedrohungen und Gefährdungen, Risikoanalysen
- Security Engineering
- Grundlagen der angewandten Kryptographie
- Sicherheitsmodelle

- Grundlagen von
  - Netzsicherheit
  - komponentenorientierter Sicherheit
  - Systemsicherheit
  - Anwendungssicherheit
  - Softwaresicherheit

Die Lehrveranstaltung "Ausgewählte Kapitel der IT-Sicherheit" vertieft einige Aspekte der Informationssicherheit mit hoher praktischer Relevanz u.a. anhand von Fallbeispielen und Lösungsansätzen aus der Forschung; die behandelten Themen umfassen u.a.:

- Security Incident Response mit Breach- und Malware-Analyse
- Social Engineering: Faktor Mensch in der Informationssicherheit
- Stolperfallen bei angewandter Kryptographie

Literatur

- Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle. De Gruyter Oldenbourg 2018 (10. Auflage).
- Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley 2021 (3. Auflage).
- Christof Paar, Jan Pelzl: Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender. Springer Vieweg 2016.
- Sharon Conheady: Social Engineering in IT Security — Tools, Tactics, and Techniques. McGrawHill 2014.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer, in der beide Lehrveranstaltungen des Moduls in gleichem Umfang geprüft werden.

Verwendbarkeit

Das Modul vermittelt Grundlagen und Begriffe der IT-Sicherheit, die u.a. in der Softwareentwicklung und beim praktischen Betrieb von IT-Diensten benötigt werden. Seine Inhalte werden in den meisten Modulen im Masterstudiengang Cyber-Sicherheit vorausgesetzt und sind für die IT-sicherheitsbezogenen Module in den Masterstudiengängen Informatik, Wirtschaftsinformatik und Mathematical Engineering (Wahlpflichtgruppe IT-Sicherheit und Kommunikation) relevant.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird jeweils im WT für Master-Studierende und im FT für Bachelor-Studierende angeboten.

Sonstige Bemerkungen

Das Modul wird derzeit üblicherweise inhaltsgleich zweimal pro Jahr, im WT und im FT, angeboten. Es ist dabei im WT für Masterstudierende (zum Beginn des Masterstudiums) und im FT für Bachelorstudierende (BINF-/WINF-Wahlpflichtmodul gemäß Musterstudienplan im FT des zweiten Studienjahres) gedacht. Die Teilnahme ist selbstverständlich auch im jeweils anderen Trimester möglich, allerdings kann bei der Termin- und Raumplanung keine Rücksicht auf Überschneidungen mit anderen Mastermodulen (im FT) bzw. Bachelormodulen (im WT) genommen werden.

Modulname	Modulnummer
Erweiterte Digitale Forensik	1162

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11621	VL	Erweiterte Digitale Forensik (Vorlesung)	Pflicht	3
11622	UE	Erweiterte Digitale Forensik (Übung)	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Voraussetzungen laut Prüfungsordnung
Das Modul 5505 muss bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.
Empfohlene Voraussetzungen
Das Modul 1551 soll bestanden sein.
Qualifikationsziele
Die Studierenden erwerben fortgeschrittene Kenntnisse und Fähigkeiten zur Durchführung einer IT-forensischen Untersuchung. Dazu gehören weitergehende Themen wie Hashfunktionen und Approximate Matching zur Erkennung bzw. Wiedererkennung von Artefakten, fortgeschrittene Dateisystemanalyse am Beispiel ext4, Linux-Analyse und fortgeschrittene Hauptspeicheranalyse.
Inhalt
Die Studierenden lernen fortgeschrittene Betriebssystemforensik am Beispiel von Linux kennen und arbeiten insbesondere mit Linux-Artefakten. Weiterführende Betrachtungen zur Sicherung und Analyse des Hauptspeichers werden mittels des Linux-Betriebssystems und des Frameworks Volatility behandelt. Weiterhin wird der Einsatz von kryptographischen sowie ähnlichkeitserhaltenden Hashfunktionen zur automatisierten (Wieder-)erkennung von Datenstrukturen betrachtet. Im Kontext der Dateisystemforensik wird ein aktuelles Dateisystem analysiert, beispielsweise ext4 wegen seiner Bedeutung für Android. Weiterhin wird ein aktuelles Themengiebt (z.B. Mobilfunkforensik, Netzwerkforensik, Automotive Forensik) bearbeitet.
Literatur
• Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.

- Breitinger, Frank, et al. Approximate matching: definition and terminology. US Department of Commerce, National Institute of Standards and Technology, 2014.
- Baier, Harald. "Towards automated preprocessing of bulk data in digital forensic investigations using hash functions." it-Information Technology 57.6 (2015): 347-356.
- Kornblum, Jesse. "Identifying almost identical files using context triggered piecewise hashing." Digital investigation 3 (2006): 91-97.
- Baier, Harald, and Frank Breitinger. "Security aspects of piecewise hashing in computer forensics." 2011 Sixth International Conference on IT Security Incident Management and IT Forensics. IEEE, 2011.
- Carrier, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.
- Linux Ext4 Kernel Wiki. https://ext4.wiki.kernel.org/index.php/Main_Page
- Casey, Eoghan, Cameron H. Malin, and James M. Aquilina. Malware forensics: investigating and analyzing malicious code. Syngress, 2008.

Leistungsnachweis

Portfolio: Es sind die Lösungen aller 7 Übungsblätter schriftlich auf 5 Seiten zum Übungstermin via Ilias im pdf-Format abzugeben. Die Bearbeitungszeit beträgt je 1 Woche. Im Prüfungszeitraum des Wintertrimesters findet ein individuelles Fachgespräch der Dauer 30 Minuten statt. Die Modulnote ist zu 100% das Ergebnis des Fachgesprächs

Verwendbarkeit

Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Vernetzte Operationsführung und Digitale Streitkräfte	1169

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11691	VL	Vernetzte Operationsführung und Digitale Streitkräfte	Pflicht	3
11692	UE	Vernetzte Operationsführung und Digitale Streitkräfte	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Wünschenswert aber nicht notwendig sind Kenntnisse im Bereich Unternehmensstrukturen und Middleware-Technologien, wie sie in Modulen für "Projektmanagement", "Enterprise Architecture und IT Service Management" und „Middleware und mobile Cloud Computing“ vermittelt werden.

Qualifikationsziele

Die Digitalisierung auf der Basis aktueller Informations- und Kommunikations-technologien dominiert zunehmend alle wirtschaftlichen, gesellschaftlichen und privaten Bereiche. Sie wird auch im sicherheitsrelevanten Kontext von (Cyber-) Verteidigung zunehmend zum Schlüsselfaktor und zentralen Gestaltungselement für alle involvierten Player. Klassisches Militär muss sich in hohem Tempo auf allen Ebenen den digitalen Herausforderungen stellen und wird so im Verbund mit Partnern und Verbündeten immer mehr zur „Digitalen Streitkraft“. Zukünftige Führungskräfte gilt es entsprechend auf diese Herausforderungen vorzubereiten.

Das Modul vermittelt die entsprechenden Grundlagen und Fähigkeiten zur Planung, Durchführung, Überwachung und Auswertung von Vernetzten Operationen (Stichwort Network Centric Warfare) auf der Basis der heute zur Verfügung stehenden Methoden, Werkzeuge und digitalen Technologien. Zunächst wird die zugrunde liegende Begriffswelt eingeführt und darauf aufbauend ein kritisches Gesamtverständnis der domänen-spezifischen Anforderungen einerseits sowie vertiefte Kenntnisse über Aufbau und Funktion der eingesetzten Applikationen und Standardsysteme andererseits vermittelt. Neben entsprechenden Anwendungsgrundlagen und wissenschaftlichen Ansätzen, werden Methoden zur eigenständigen Konzeption und Gestaltung angepasster IT-Lösungen unter Nutzung von Interoperabilitätsstandards und Sicherheitskonzepten für die Zusammenarbeit im multinationalen Umfeld vermittelt. Die Teilnehmer werden

so in die Lage versetzt, in einer späteren Verwendung strukturiert, eigenständig und methodisch fundiert gemeinsam mit anderen „Stakeholdern“ verantwortlich an der ständigen Weiterentwicklung der Digitalen Transformation von Streitkräften mitzuwirken.

Inhalt

Im gegenwärtigen Digital-Zeitalter wird unsere VUCA-Welt (Volatility, Uncertainty, Complexity, Ambiguity) vorwiegend durch Informationstechnologie geprägt. Mit der Globalisierung von Informationsflüssen in nahezu Lichtgeschwindigkeit nehmen Informationen die zentrale Bedeutung als „Rohstoff und Ware“ in den digitalen Wertschöpfungsketten des 21. Jahrhunderts ein. Für eine moderne Digitale Armee bilden Daten und Informationen die essenzielle Grundlage für Planung, Ausrichtung, Architektur, Operationsdurchführung sowie die permanente Weiterentwicklung gemäß der sich ständig ändernden Anforderungen. Hierfür müssen Entscheidern relevante Informationen zur richtigen Zeit am erforderlichen Ort in angemessener Qualität und Quantität zur Verfügung gestellt werden. Im Rahmen der gesamten, partnerübergreifenden Wertschöpfungskette sind relevante Daten und Informationen entsprechend interoperational, digital, schneller, besser etc. innerhalb der jeweiligen Verteidigungsallianz zur Verfügung zu stellen. Der Informationsverarbeitungsprozess umfasst dabei im Wesentlichen die Planung mittels formalisierter Modelle, die Umsetzung in geeignete IT-Systeme und Applikationen sowie deren fortlaufende Integration sowohl auf technischer als auch organisatorischer Ebene und zwar gemeinsam und abgestimmt mit den Schlüsselparametern Zielbezug, Fähigkeitsorientierung sowie Schutzbedarfen.

Die Wissenschaft und die „Defence Community“ stellen hierfür entsprechende Werkzeuge, Methoden und Standards zur Verfügung, um sowohl national als auch international im Kontext des NATO-Bündnisses für die sog. *Multi-Domain Operations (MDO)* die Voraussetzungen für eine Vernetzte Operationsführung zu schaffen. Entscheidungsgrundlage und zentrales verbindendes Element bildet hierbei das *Gemeinsame Rollenorientiertes Einsatzlagebild* (GREL) mit multi-dimensionalen Betrachtungsebenen, welches es zu generieren und ständig anzupassen gilt. Neben der klassischen *Red- and Blue-Perspektive* gilt es, immer weitere Dimensionen und Ebenen wie beispielsweise *Cyber Threat*, *Space* oder *Environmental* einzubinden.

Ohne eine systematische und ganzheitliche Entwicklungsstrategie für die Streitkräfte lässt sich die ständig zunehmende Komplexität dieser Systeme und Prozesse nicht mehr beherrschen. Der stetige Zuwachs an spezifischen Fähigkeiten und spezialisierten Diensten stellt ein „Moving Target“ dar. Die Problematik besteht zudem in der Erreichung von Anwendungs- und Datenkompatibilität unter den verschiedenen Systemen und Sicherheitsleveln sowie in der korrekten Interpretation der Semantik von Informationen unter strikter Einhaltung von Datenschutz und Vertraulichkeit. Das Modul bereitet die zukünftigen Führungskräfte auf diese Herausforderungen vor und vermittelt die entsprechenden Grundlagen, Methoden und Anwendungskenntnisse.

Zunächst erfolgt eine grundlegende Einführung in die Begriffswelt, die komplexen Anforderungen und den zu erfüllenden Anspruch einer NetOpFü im trägernahen Kontext. Dies beinhaltet die mit der digitalen Transformation verbundenen Anwendungssysteme sowie die im Zusammenhang stehenden Wissens- und Informationsstrukturen.

Anschließend erfolgt eine vertiefte Auseinandersetzung mit den aktuellen und im Rahmen der NATO-Streitkräfte unterstützenden Systemen und Integrationskonzepten des sog. *Federated Mission Networking (FMN*). Dies umfasst die zentralen Aspekte der Kompatibilität hinsichtlich integraler Interoperabilität und Sicherheit mit dem Ziel einer gemeinsamen multinationalen, streitkräfteübergreifenden Fähigkeitsweiterentwicklung.

Einblicke in den aktuellen Stand von Wissenschaft, Forschung und Technik werden an konkreten Beispielen vermittelt: *C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance)* und *Network Centric Warfare (NCW)*. An Fallbeispielen wird die Anwendung des zentralen Konzeptes *des Effects-based Approach to Operations (EBAO)* diskutiert. Weiterhin wird anhand ausgewählter Studien der zentrale Ansatz *des Concept Development & Experimentation (CD&E)* vorgestellt, der für die Gestaltung, Validierung und Einführung von IT-gestützten Verfahren und Methoden eine zentrale Bedeutung hat. Die dabei notwendigen administrativen und logistischen Prozesse zur Unterstützung der Führungsaufgaben runden die digitale Weiterentwicklungsstrategie ab.

Darüber hinaus vermittelt das Modul wichtige Grundlagen und Konzepte des *Knowledge Management* zur wissensbasierten Entscheidungsunterstützung in komplexen, vernetzten Operationen. Mittels der architekturbasierten Gestaltung auf der Basis von entsprechenden Rahmenwerken (*NATO Architecture Framework NAF*) wird *Enterprise Architecture* als systematischer Ansatz zur fähigkeitszentrierten Weiterentwicklung von Digitalen Streitkräften vorgestellt und vertieft. Dabei wird auch der gesamtplanerische Zusammenhang zur NATO und dem FMN aufgegriffen unter Berücksichtigung von Multi-Layer-Defence und -Security-Ansätzen.

In der begleitenden Übung haben die Teilnehmer Gelegenheit, einzelne Aspekte anhand von Standards, Best Practices und Beispielen aus Forschung und Praxis eigenständig zu vertiefen und so erste Anwendungserfahrungen zu sammeln. Abgerundet wird das Modul durch den Einbezug externer Experten, die Einblicke in ihre unmittelbaren praxisnahen Erfahrungen mit Lösungsansätzen im Kontext der Vernetzten Operationsführung geben.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Literatur

1. Sebastian Schäfer: Vernetzte Operationsführung – Eine Einführung, Luftwaffenamt, 2005
2. David S. Alberts, John J. Garstka, Frederick P. Stein: Network Centric Warfare, CCRP Publication Series, 2000
3. Michael-Günther Lux: Effects-Based Approach to Operations (EBAO), Luftwaffenamt, 2007
4. Dr. Lee Whitt: SmartCOP – the fusion of collaborative workspaces and the Common Operational Picture, International Command and Control Research and Technology Symposium, 2005
5. Edward A. Smith: Effects Based Operations (EBO) – Applying Network Centric Warfare in Peace, Crisis and War, Washington, 2002
6. Edward A. Smith: Complexity, Networking and Effects-Based Approaches to Operations, Washington, 2006

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Das Wahlpflichtmodul ist die Grundlage für weiterführende und vertiefende Veranstaltungen sowie wissenschaftliche Arbeiten im Kontext der Vernetzten Operationsführung. Es stellt Basiswissen für die Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/Cyber Sicherheit dar. Es stellt zudem eine gute Ergänzung mit den Wahlpflichtmodulen für "Projektmanagement" sowie "Enterprise Architecture und IT Service Management", die einen eher querschnittlichen, aber ebenso zentralen Blickwinkel etablieren.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im HT.

Modulname	Modulnummer
Middleware und mobile Cloud Computing	1398

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
13981	VL	Middleware und mobile Cloud Computing	Pflicht	3
13982	UE	Middleware und mobile Cloud Computing	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden Kenntnisse aus dem Bereich des Software Engineering, insbesondere der Objektorientierung (Modul Objektorientierte Programmierung). Wünschenswert sind Grundkenntnisse in der XML-Technologien sowie in einer der objektorientierten Programmiersprache, wie z. B. Java, Scala, C++.

Qualifikationsziele

Das *Modul Middleware und mobile Cloud Computing* zielt darauf ab, den Studierenden

vertiefend die Bedeutung der Integration als Kernaufgabe der Angewandten Informatik

näher zu bringen. Die Teilnehmer erhalten neben einem grundlegenden Verständnis für die Anforderungen an eine Middleware-basierte Integration theoretische und praktische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middleware-Konzepte und serviceorientierter Schnittstellen. In diesem Zusammenhang werden wissenschaftliche Methoden vermittelt, die die Teilnehmer in die Lage versetzen, in komplexen Anwendungssystemlandschaften eigenständig und systematisch einen höheren Integrationsgrad zu erreichen. Zudem werden grundlegende Aspekte von *Verteilten Systemen* wie Kommunikationsprotokolle, Austauschformate und Sicherheitsaspekte betrachtet. Die so vermittelten IT-technischen Kenntnisse befähigen die Teilnehmer darüber hinaus aus einer Cyber-Bedrohungsperspektive betrachtet, eine fundierte Analyse hinsichtlich möglicher Leistungsengpässe und Schwachstellen zu konzipieren sowie in der gegebenen IT-Landschaft zu implementieren. Ohne diese Kenntnisse und Fähigkeiten kann de-facto auf potenzielle Bedrohungsszenarien beim Betrieb komplexer IT-Systeme kaum geeignet begegnet werden. Die im Modul vermittelten Grundlagen versetzen die Teilnehmer in die Lage, geeignete Maßnahmen zur Cyber-Abwehr in Middleware-/ Cloud-Strukturen zu integrieren (Stichwort: *Security-as-a-Service*).

Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang

mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. Durch eigenständige Anwendung von Technologien wie *Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), .NET, Simple Object Access Protocol (SOAP) oder Representational State Transfer (REST)* erhalten die Teilnehmer Methoden-, Fach- und Umsetzungskompetenz im Umgang mit grundlegenden Middleware-Konzepten und deren Basistechnologien. In der Kombination aus theoretischer Behandlung und praktischer Vertiefung versetzt das Modul die Teilnehmer in die Lage, verteilte Anwendungen auf der Basis von Middleware zu entwerfen und systematisch in die Praxis umzusetzen.

Inhalt

Im heutigen Digitalzeitalter mit *Industrie 4.0, Digital Governance* und *Künstlicher Intelligenz* etc. agieren fast alle Systeme als vernetzte Fähigkeitsträger. Moderne Enterprise Anwendungen basieren auf Standard-Middleware-Architekturen, wo Funktionalität zunehmend über Cloud-basierte Dienste plattformübergreifend den Clients – insbesondere zunehmend mobilen Endgeräten – zur Verfügung gestellt wird. Das Modul bietet einen fundierten Einstieg in die aktuellen Middleware-Basistechnologien. Auf den Grundlagenkenntnissen der Objektorientierten Programmierung aufbauend werden entlang der Entwicklungslinie Schritt für Schritt aktuelle Middleware-Konzepte und -Technologien eingeführt. Das Modul etabliert dazu zunächst die Basisabstraktion und das Grundverständnis Middleware-basierter Systeme. Dabei werden grundlegende Fähigkeiten zur Beherrschung heterogener Anwendungslandschaften und deren Komplexitätsparameter vermittelt. Diese berücksichtigen die Dimensionen der *Kommunikation* und *Transaktion* sowie Zugriffsmöglichkeiten und Schutzaspekte in *Schichtarchitekturen*. Unabhängig von der jeweils eingesetzten Technologie nimmt das Abstraktionskonzept der *Schnittstellen-Basierung* eine zentrale Rolle beim Design verteilter Anwendungen und somit im gesamten Modul ein.

Im Folgenden wird tiefer auf die unterschiedlichen Integrationsparadigmen und -technologien mit ihren jeweiligen spezifischen Stärken und Schwächen (Fähigkeiten, Schwachstellen, Angriffspunkte usw.) eingegangen. Aktuelle Middleware-Dienste und Architekturkonzepte wie *Verteilte Objektmodelle*, *Komponentenmodelle* und *Service Oriented Middleware (SOA)* bilden den Schwerpunkt des zweiten Teils des Moduls. Hier werden jeweils zunächst die allgemeinen Prinzipien erläutert und dann anhand konkreter Beispiele Standard-Middleware-Technologien und deren zugrunde liegenden Konzepte und Prinzipien vertieft.

Der dritte Teil stellt das *Cloud-Konzept* in den Mittelpunkt und zeigt Schritt für Schritt an einfachen Beispielen die Entwicklung Cloud-basierter Dienste und deren Zugriff über mobile Clients (Apps). Zudem werden erste Einblicke in aktuelle Trends wie *Mirco-Service-Architekturen* oder *Containerisierung* gegeben.

Die begleitende Übung bietet die Gelegenheit, aktuelle Technologien anhand einfacher Beispiele kennen zu lernen und erste praktische Erfahrung im Umgang mit Middleware und mobilen, Cloud-basierten Anwendungen zu sammeln.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Literatur

1. Alexander Schill, Thomas Springer: Verteilte Systeme, Springer Vieweg, 2012
2. Chris Britton, Peter Bye: IT Architectures and Middleware: Strategies for Building Large, Integrated Systems; Addison-Wesley, 2004
3. Dieter Masak: Moderne Enterprise Architekturen, Springer, 2005
4. Binildas Christudas: Practical Microservices Architectural Patterns, Apress, 2019
5. Die Beauftragte der Bundesregierung für Informationstechnik: SAGA-Modul Technische Spezifikationen, Version 5.0.0, 2011

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informationssystemen und stellen somit eine Grundlage für Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/ Cyber Sicherheit dar.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Identitätsmanagement	1446

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Dr. rer. nat. Daniela Pöhn	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
14461	VÜ	Identitätsmanagement	Pflicht	3
14462	SE	Seminar Identitätsmanagement	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für das Modul werden grundlegende Kenntnisse in den folgenden Bereichen benötigt:

- Funktionsweise von Webanwendungen, wie sie z.B. in der Lehrveranstaltung Sichere vernetzte Anwendungen behandelt werden.
- IT-Sicherheit, wie sie z.B. in Modul 3459 vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten einen Überblick über Protokolle, Anwendungsbeispiele und Sicherheitsaspekte des Identitätsmanagements. Sie verstehen unterschiedliche Methoden und können die Modelle des Identitätsmanagements anwenden sowie die Protokolle vergleichen. Dadurch sind sie in der Lage, Bedeutung und Zusammenhänge verschiedener Einflussfaktoren auf die IT-Sicherheit und damit der Sicherheit der Identitäten zu analysieren. Mit dem erworbenen Wissen werden die Studierenden in die Lage versetzt, sich tiefergehend selbstständig einzuarbeiten und den Einsatz von Protokollen in verschiedenen Anwendungen zu bewerten.

Inhalt

Das Modul führt in die Grundlagen des Identitätsmanagements und deren Zusammenhang mit IT-Sicherheit ein. Darauf aufbauend bietet es einen breiten Überblick über verschiedene Protokolle des Identitätsmanagements im Webbereich, deren Sicherheit und Anwendungsgebiete. Dieser Überblick wird als Basis für die weitere Betrachtung der Sicherheit, des Security Managements und angrenzende Gebiete verwendet.

Die Vorlesung Identitätsmanagement betrachtet unterschiedliche Protokolle für Identitätsmanagement im Web-Bereich und deren Zusammenspiel mit der Sicherheit. Anhand unterschiedlicher Modelle des Identitätsmanagements werden

die darin enthaltenen Protokollen, u.a. SAML, OAuth, OpenID Connect und User Managed Access, mit deren Rollen, Architekturen, Austauschformaten und mit Hilfe von Verwendungsbeispielen erklärt. Darauf aufbauend wird deren Sicherheit und das Vertrauen in die gesendeten Benutzerinformationen analysiert. Dies beinhaltet typische Design-, Implementierungs- und Konfigurationsfehler sowie Fehler im Design der Protokolle selbst. Nach diesem Grundstock werden unter Einbeziehung von IT-Sicherheit und Security Management Normen, Guidelines, wie NIST SP 800-63, und praktischen Anwendungen, u.a. Vectors of Trust, dessen betrachtet. Abschließend wird ein Überblick über angrenzende Themen, wie Identitäten bei IoT, DNS und IEEE 802.1X, gegeben.

Das Seminar Identitätsmanagement vertieft einige Aspekte der Vorlesung mit hoher praktischer Relevanz. Die behandelten Themen umfassen u.a. Security Management beim Identitätsmanagement, Angriffe und Abwehrmechanismen und neue Protokoll-Entwicklungen.

Literatur

- Claudia Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle. 10. Auflage, 2018, De Gruyter Oldenburg Verlag, ISBN-10: 978-9-352-86653-3
- Elisa Bertino, Kenji Takahashi: Identity Management – Concepts, Technologies, and Systems, 2010, Artech House, ISBN-10: 978-1-608-07040-4
- Shimon K. Modi: Biometrics in Identity Management – Concepts to Applications, 2011, Artech House, ISBN-10: 978-1-608-07018-3
- Morey J. Haber, Darran Rolls: Identity Attack Vectors, 2019, Apress, ISBN-10: 978-1-484-25164-5
- Yvonne Wilson, Abhishek Hingnikar: Solving Identity Management in Modern Applications – Demystifying OAuth 2.0, OpenID Connect, and SAML 2.0, 2019, Apress, ISBN-10: 978-1-484-25095-2

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen:

VÜ: Schriftliche Klausur von 30 Minuten Dauer oder Fachgespräch von 15 Minuten Dauer. Zu Beginn der Veranstaltung wird bekannt gegeben, welche dieser beiden Leistungen zu erbringen ist.

SE: Schriftliche Ausarbeitung (Wahl aus Seminartemplate mit 15-25 Seiten und ACM Sigconf-Format mit 8-10 Seiten), die innerhalb des Trimesters (Bearbeitungszeit acht bis sechzehn Wochen) angefertigt werden soll, und eine anschließende Präsentation (20 Minuten Vortrag + 10 Minuten Diskussion). Die konkrete Dauer sowie der konkrete Umfang werden zu Beginn der Veranstaltung bekannt gegeben.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 50 zu 50 in die Note ein

Verwendbarkeit

Digitale Identitäten sind aus dem heutigen Leben nicht mehr wegzudenken und stellen zugleich einen wichtigen Baustein für die IT-Sicherheit dar. Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die Gestaltung von sicheren

(Web-)anwendungen. Die Inhalte ergänzen die Ausbildung um einen Aspekt von hoher praktischer Bedeutung. Somit kann das Modul folgende Module ergänzen:

- Datenschutz und Privacy (5504)
- Anwendungssicherheit (5507)
- Web Technologies (1306)
- Benutzbare Sicherheit (3919) und Benutzbare Sicherheit (erweitert) (3918)

Dauer und Häufigkeit
Das Modul dauert zwei Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Enterprise Architecture und IT Service Management	1507

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15071	VL	Enterprise Architecture und IT Service Management	Pflicht	3
15072	UE	Enterprise Architecture und IT Service Management	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Empfehlenswert aber nicht zwingend erforderlich sind Grundkenntnisse der Service-orientierten Architektur (SOA).

Qualifikationsziele

Die Regierbarkeit komplexer IT-Landschaften (IT Governance) wird zunehmend zentraler, strategischer Wettbewerbsfaktor für Unternehmen, Organisationen und nicht zuletzt auch Armeen wie die Bundeswehr. Enterprise Architecture & IT Service Management bilden die beiden zentralen Säulen zur Beherrschung dieser komplexen Aufgabenstellung. Die Teilnehmer werden durch das Modul mit breiter Methodenkompetenz und Fachkenntnis in die Lage versetzt, in dem noch relativ jungen Forschungsgebiet auf dem aktuellen Stand und seiner Bedeutung an der Gestaltung komplexer IT-Landschaften mitzuwirken. Dies umfasst die Aspekte der Planung, des Betriebs und der Wartung über den gesamt Lebenszyklus inklusive der Beachtung von leistungsbezogenen Parametern und der Informationssicherheit sowohl organisatorisch als auch technisch. Zudem werden Fähigkeiten zur Identifizierung und Beseitigung von Engpassen und Schwachstellen vermittelt. In der Vertiefung werden heute dominierende Standards und Best Practices, wie TOGAF, ITIL, UAF und ArchiMate, in Aufbau, Struktur und Domänenbezug verankert und die Grundkenntnisse zu ihrer Anwendung vermittelt. Anhand konkreter Fallbeispiele und Diskussionen mit externen Fachleuten erlangen die Teilnehmer zudem die notwendigen Fähigkeiten zur eigenständigen Anwendung und Übertragung der Methoden und Ansätze in Domänenkontexte.

Inhalt

Das Service-basierte Architekturkonzept (Service Oriented Architecture, SOA) bildet seit geraumer Zeit einen wichtigen Grundpfeiler für die Gestaltung und Anpassung komplexer IT-Landschaften an die sich fortlaufend verändernden Anforderungen aus dem

Geschäftsprozessumfeld einer Unternehmung oder Organisation. Es gilt, Anforderungen aus den Geschäftsprozessen strukturiert, zielgerichtet und sicher abzubilden. Dies hat unter Berücksichtigung aktueller und moderner Technologien möglichst effektiv und effizient auf Basisdienste einer unterliegenden IT Service-Schicht zu erfolgen. Diese sind zum Beispiel in Form von Cloud-basierten Diensten orts- und technologieübergreifend der Anwendungsebene zur Verfügung zu stellen. Hierbei werden unter anderem die Dimensionen wie Fähigkeiten, Kollaboration und Sicherheit abgedeckt. Rahmenwerke zur Beschreibung der für einen Unternehmenstyp bzw. einen Anwendungsbereich typischen Architekturbestandteile und Zusammenhänge zwischen den „Building Blocks“ (Enterprise Architecture Frameworks) bilden eine immer wichtiger werdende Grundlage hierfür.

Das Modul führt die Studierenden in die Thematik der architekturbasierten Gestaltung von komplexen IT-Landschaften ein. Im ersten Teil der Veranstaltung werden zunächst die Entwicklungsgeschichte und die zentrale Grundidee von Unternehmens-rahmenwerken vorgestellt und an einführenden Beispielen diskutiert sowie ein Überblick über entsprechende Standards gegeben. Anhand einzelner ausgewählter Standards wie beispielsweise The Open Group Architecture Framework (TOGAF) werden dann einzelne Aspekte der Anwendung von Enterprise Architecture selbstständig an Fallbeispielen vertieft. Hierzu gehört die Nutzung von Referenzmodelle mit Fokus auf Business, Applikation, Infrastruktur und Sicherheit.

Im zweiten Teil des Moduls steht das Management komplexer IT-Landschaften auf Basis der Service-orientierten Architektur im Mittelpunkt. IT Service Management als Überbegriff aller Ansätze und Methoden zur Unterstützung bei der Abbildung von Geschäftsprozessen auf sichere und verlässliche IT-Basisdienste bildet einerseits ein wichtiges Fundament heutiger IT-Governance. Andererseits stellt dieses Paradigma Unternehmen und Anwender vor die Herausforderung einer fortwährenden, systematischen und möglichst optimalen Abbildung der Unternehmensprozesse auf IT-Bausteine und Standard- Anwendungssysteme - auch als Business-IT-Alignement bezeichnet. Hierbei spielen Standards und Rahmenwerke - allen voran die IT Infrastructure Library (ITIL) - eine zentrale Rolle. Neben der Verankerung der grundlegenden Konzepte und Methoden des IT Service Managements wird den Studierenden anhand von Praxisbeispielen gespiegelte Anwendung der Rahmenwerke vermittelt. Die praktische Anwendung dieser zu erlernenden Fähigkeiten steht im Mittelpunkt des Moduls. Anwendungsexperten aus unterschiedlichen Bereichen, z. B. aus Automobilkonzernen, werden zusätzlich tiefere Einblicke in den aktuellen Stand der Handhabung geben.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Literatur
1. Mathias Weber: Enterprise Architecture Management – neue Disziplin für die ganzheitliche Unternehmensentwicklung, Bundesverband Informationswirtschaft, 2011 2. Marc Lankhorst: Enterprise Architecture at Work, Springer, 2009 3. Scott A. Bernard: An Introduction to Holistic Enterprise Architecture, AuthorHouse, 2020 4. The Open Group: The Open Group Architecture Framework (TOGAF) Standard, Version 10, 2022 5. Bundesministerium des Innern: Leitfaden für Entwickler von Prozess- und Datenmodellen, Koordinierungs- und Beratungsstellen der Bundesregierung für Informationstechnik in der Bundesverwaltung 2007 6. Dirk Matthes: Enterprise Architecture Frameworks Kompendium, Springer 2011
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Das Wahlpflichtmodul ist die Grundlage für weiterführende und vertiefende Veranstaltungen sowie wissenschaftliche Arbeiten im Kontext der Gestaltung und Anpassung komplexer IT-Landschaften. Es stellt Basiswissen für den Masterstudiengänge Wirtschaftsinformatik, aber auch im Bereich Informatik/ Ingenieurinformatik/Cyber Sicherheit dar und ergänzt sich mit den Wahlpflichtmodulen für "Middleware und mobile Cloud Computing".
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Digitale Forensik	1551

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15511	VL	Digitale Forensik (VL)	Pflicht	3
15512	UE	Digitale Forensik (UE)	Pflicht	3
15513	SE	Seminar zur IT-forensischen Gutachtenerstellung	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Voraussetzungen laut Prüfungsordnung
Das Modul 5505 muss bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.

Qualifikationsziele
Die Studierenden kennen die allgemeine IT-forensische Vorgehensweise und können diese bei der Durchführung IT-forensischer Analysen anwenden sowie in einem Gutachten dokumentieren. Sie kennen wichtige Spurenquellen im Betriebssystem Windows und können diese auswerten. Die Studierenden kennen Datenformate von verbreiteten Anwendungen und können diese analysieren. Sie wissen Sicherungs- und Analyseverfahren des Hauptspeichers und können diese anwenden. Wesentliche Anti-Forensik-Ansätze sind den Studierenden bekannt, und sie können diese bewerten. Weiterhin können die Studierenden Speichertechnologien erklären und digitale Spuren eingebetteter Systeme IT-forensisch sichern und auswerten.

Inhalt
Die Studierenden lernen die Betriebssystemforensik am Beispiel von Windows kennen und arbeiten insbesondere mit der Windows-Registry sowie Windows-Artefakten. Im Kontext der Anwendungsforensik wird das SQLite Datenbankformat behandelt und für Anwendungen wie Firefox, Thunderbird, Skype analysiert. Die Sicherung und Analyse des Hauptspeichers wird mittels des Windows-Betriebssystems und des Frameworks Volatility behandelt. Auf dem Gebiet der Anti-Forensik lernen die Studierenden die gängigen Kategorien von antiforensischen Maßnahmen kennen und bewerten. Flashbasierte Speichertechnologien sowie der direkte Zugriff auf einen Datenträger und die zugehörige Auswertung sind low-level Fertigkeiten, die die Studierenden einsetzen.

An Hand der Erstellung eines Gutachtens für ein Fallbeispiel werden im Rahmen des Seminars die gelernten Inhalte umfassend angewendet.

Literatur

- Carvey, Harlan. Windows registry forensics: Advanced digital forensic analysis of the windows registry. Elsevier, 2011.
- Carrier, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.
- Casey, Eoghan, Cameron H. Malin, and James M. Aquilina. Malware forensics: investigating and analyzing malicious code. Syngress, 2008.
- Hummert, Christian, and Dirk Pawlaszczyk, eds. Mobile Forensics-The File Format Handbook: Common File Formats and File Systems Used in Mobile Devices. Springer Nature, 2022.
- Solomon, David A., Mark E. Russinovich, and Alex Ionescu. Windows internals. Microsoft Press, 2009.
- Russinovich, Mark E., David A. Solomon, and Alex Ionescu. Windows internals, part 2. Pearson Education, 2012.
- Sanderson, Paul, et al. SQLite Forensics. Independently published, 2018.

Leistungsnachweis

Portfolio: Es sind die Lösungen von 6 der 8 Übungsblätter schriftlich auf 5 Seiten zum Übungstermin via Ilias im pdf-Format abzugeben und im zugehörigen Übungstermin aktiv zu erläutern. Die Bearbeitungszeit beträgt je 1 Woche. Im Rahmen des Seminars ist eine 15-seitige Ausarbeitung als exemplarisches Gutachten zu einer vorgegebenen Zweifelsfrage anzufertigen, die Bearbeitungszeit für die Ausarbeitung beträgt 10 Wochen im Zeitraum Mitte Dezember bis Ende Februar des Folgejahres. Über alle drei Lehrveranstaltungen wird ein 30-minütiges individuelles Fachgespräch durchgeführt, dessen Ergebnis zu 100% die Modulnote ist.

Verwendbarkeit

Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Einführung in die Quanteninformationsverarbeitung	3010

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Dr. Dipl.-Phys. Sabine Tornow	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
30101	VÜ	Einführung in die Quanteninformationsverarbeitung	Pflicht	3
30102	P	Praktikum Quantenschlüsselaustausch	Wahlpflicht	3
30103	SE	Seminar Quantentechnologien	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in linearer Algebra. Vorkenntnisse in Quantenmechanik und Kryptographie sind hilfreich, aber nicht erforderlich.

Qualifikationsziele

Studierende verstehen Konzepte der Quanteninformationsverarbeitung (Quantenkommunikation, Quantenkryptographie, Quantenkodierungstheorie, Quantenalgorithmen und Quantenfehlerkorrektur) und können weitere Entwicklungen zu Quantenkryptographie, Algorithmen, Fehlerkorrektur und Quantenkommunikation einordnen und bewerten. Studierende können Experimente, z.B. zur Quantenkommunikation und Fehlerkorrekur implementieren und auf einem Quantencomputer testen und die praktische Realisierung des Quantenschlüsselaustausches experimentell umsetzen (siehe Praktikum).

Am Ende des Kurses sind die Studierenden in der Lage, den grundlegenden mathematischen Formalismus (z.B. Zustände, Kanäle) und die Schlüsselkonzepte zu erklären. Sie sind in der Lage, diese Konzepte und Methoden anzupassen und anzuwenden, um Probleme der Quanteninformationsverarbeitung zu lösen.

Inhalt

Vorlesung: Quanteninformation ist eine Synthese von Informatik, Quantentheorie und Informationstheorie. Quantensysteme werden zur Speicherung von Information und die Gesetze der Quantenmechanik zur Verarbeitung von Information verwendet. Die in diesen Systemen vorhandene Information kann nicht mit den Gesetzen der klassischen Informationstheorie beschrieben werden. Diese wird zur Quanteninformationstheorie erweitert. Die Quanteninformation ermöglicht eine fundamental neue Art der Informationsverarbeitung wie die Quantenteleportation, Quantenkryptographie und

Quanten-Algorithmen. Es werden folgende Themengebiete behandelt: Grundlagen der Quantentheorie, Quantenverschränkung, Quanten-Shannon-Theorie, effiziente Quantenalgorithmen, Quantenkryptographie, Quantenkanäle, Quantenfehlerkorrektur, Quantennetzwerke und Quantenkommunikation.

Praktikum:

- Durchführung eines QKD-Modellversuchs, der das BB84-Protokoll mit polarisiertem Licht in der Praxis umsetzt
- Detailliertes Wissen über die Schritte, die für ein QKD-Protokoll erforderlich sind
- Experimentelle Durchführung des Protokolls in Teams bestehend aus zwei Personen, die die Rolle von Sender und Empfänger übernehmen
- Versenden einer mit Quantenschlüsseln verschlüsselten Nachricht
- Verfassen eines Versuchsprotokolls

Seminar: Aktuelle Themen in den Bereichen der Quantentechnologie:

Quantensensorik, Quantum Memory, Quantum Repeater, Quantum Computing, Quantenkommunikation, Post-Quantum Kryprographie, Quantenmetrologie, Quantenbildgebung, usw.

Literatur

- Riccardo Manenti and Mario Motta: Quantum Information Science, Oxford University Press
- Thomas Vidick and Stephanie Wehner: Introduction to Quantum Cryptography, Cambridge University Press
- Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

- als Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit (MCYB)
- in Modul 5506 Kryptologie im Studiengang MCYB
- in Modul 3491 Algorithmen und Komplexität im Studiengang MINF
- in Modul 3820 Quantencomputer in Theorie und Praxis im Studiengang MCYB
- in Modul 1037 Informations- und Codierungstheorie im Studiengang MCYB
- in Modul 1289 Nachrichtentheorie und Übertragungssicherheit im Studiengang MCYB
- in Modul 5548 Modern Cryptography im Studiengang im Studiengang MCYB
- in Modul 2994 Ausgewählte Kapitel des OR: Data-driven Optimization MINF

Dauer und Häufigkeit

Das Modul wird jedes Jahr ab dem WT angeboten und dauert zwei Trimester. Die Vorlesung wird im WT angeboten, das Praktikum oder das Seminar im FT.

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	3396

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
33961	VÜ	Data Mining und IT-basierte Entscheidungsunterstützung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Grundkenntnisse zu mathematischen Methoden des Operations Research und der Statistik wie sie z.B. im Bachelor Informatik bzw. Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Insbesondere ist es das Ziel, IT-basierte Entscheidungsunterstützung unter der speziellen Cyberperspektive zu betrachten: Wie können Angriffe schneller erkannt, wie kann man sich optimal dagegen schützen und wie können Entscheidungsunterstützungssysteme gegenüber Cyberangriffen optimiert werden. Das Modul gibt einen Überblick über aktuelle Modelle und Verfahren sowie relevante Bedrohungsszenarien.

Inhalt

Die Studierenden sollen in dieser Veranstaltung mit den IT-basierten und entscheidungstheoretischen Grundlagen im Bereich der modernen Datenanalyse vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von geeigneten Analyseverfahren zur Erforschung von komplexen datenbasierten Zusammenhängen ("Exploratory Analysis").

Data Mining bedeutet dabei das Extrahieren von impliziten, noch unbekannten Informationen aus Rohdaten. Dazu sollten IT-Systeme in die Lage versetzt werden, Datenbanken und Datenansammlungen (z.B. im Bereich der Geoinformatik) automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert. Insbesondere das heutige maschinelle Lernen und das Verfahren des "Datafarming" stellen dafür die Werkzeuge und Techniken zur Verfügung, die in den Bereich des modernen Wissensmanagements (bis zur Begriffsanalyse) und "Datamining" hineinführen.

Literatur

- Decision Support Systems Developing Web-Enabled Decision Support Systems, Abhijit A. Pol and Ravindra K. Ahuja. Dynamic Ideas 2007.
- Exploratory Data Analysis Making Sense of Data: A Practical Guide to Exploratory Data Analysis and Data Mining, Glenn J. Myatt. John Wiley, 2006.
- Spatial Data Analysis Spatial Data Analysis - Theory and Practice, Robert Haining, Cambridge University Press 2003.
- Data Mining Data Mining: Practical Machine Learning Tools and Techniques (Second Edition) Ian H. Witten, Eibe Frank. Morgan Kaufmann 2005.
- Data Mining: A Knowledge Discovery, K. Cios, W. Pedrycz, R. Swiniarski Springer, 2007.
- Data Mining Introductery and Advanced Topics, Margaret Dunham, Prentice Hall, 2003.
- Advances in Knowledge Discovery and Data Mining, U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, editors , MIT Press, 1996.
- Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber. Morgan Kaufmann, 2006.
- Principles of Data Mining, David J. Hand, Heikki Mannila and Padhraic Smyth. MIT Press, 2000. Daniel T. Larose,
- Discovering Knowledge in Data: An Introduction to Data Mining, John Wiley 2004. Robert Nisbet, John Elder, IV and Gary Miner.
- Handbook of Statistical Analysis and Data Mining Applications. Elsevier 2009.
- Statistical Learning - Machine Learning Trevor Hastie, Robert Tibshirani, Jerome Friedman,
- The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Verlag, 2001. Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, Wiley-IEEE Press, 2002.

Weiterführende Literatur:

- Zeitreihenanalyse Time Series Analysis. Hamilton 1994.
- Reinforcement Lernen und Spieltheorie Reinforcement Learning: An Introduction. Sutton and Barto: MIT Press 1998.
- Fun and Games: A Text on Game Theory. Binmore, Linster, Houghton Mifflin 2000.
- Statistik Bayesian Data Analysis. Gelman, Carlin, Stern, Rubin: Chapman 1995. Introduction to Mathematical Statistics. Hogg, Craig: Prentice Hall 2004.
- Principles of Statistics. Bulmer: Dover 1979.
- Probability, Random Variables and Stochastic Proc., Papoulis, McGraw, Hill 2002.

Leistungsnachweis

Portfolio auf der Basis der folgenden vier Teilleistungen, je mit 25% gewichtet, für deren Bearbeitung die Studierenden einen Bearbeitungszeitraum von je 2 Wochen haben:

1. Analysebericht "Pre-Processing" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)
2. Analysebericht "Clustering" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)
3. Analysebericht "Classification" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)

4. Analysebericht "Outlier Detection" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)

Verwendbarkeit

Die Vorlesung kann durch weiterführende Veranstaltungen im Bereich der Datenanalyse fortgeführt werden, z.B. im Bereich der modernen Begriffsanalyse, des Algorithmic Engineering, im Rahmen von Spezialvorlesungen der Numerik und Statistik sowie der Geoinformatik. Ebenfalls bestehen enge Bezüge zu wissenschaftlichen Forschungsgebieten im Bereich der Künstlichen Intelligenz.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Language-based Security	3584

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
35841	P	Praktikum Language-based Security	Pflicht	4
35842	SE	Seminar Language-based Security	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung und in sprachbasierter Sicherheit vorausgesetzt, wie sie z.B. in den gleichnamigen Bachelor- und Master-Veranstaltungen vermittelt werden.

Qualifikationsziele

Die Studierenden erwerben die Fähigkeit, Probleme der sprachbasierten Sicherheit in der Praxis zu analysieren und sich durch geeignete Implementierungen von Prototypen kritisch mit der Materie auseinanderzusetzen. Dabei sollen die Studenten durch mehrere Varianten verschiedene "Härtegrade" der Verteidigungstechniken illustriert und dadurch Kompetenz bei der Bewertung der relativen Vor- und Nachteile in der Anwendung der Techniken erworben werden.

Inhalt

Im Rahmen des Praktikums werden zu den jeweiligen Themengebieten der Vorlesung "Language-based Security" konkrete Implementierungen von Prototypen in einem kleinen, aber repräsentativen Compiler durchgeführt. Um die Effizienz der Verteidigungstechniken zu messen, werden bei Bedarf vorher Angriffe implementiert und diese dann mit Hilfe der implementierten Verteidigungen abgewehrt. Studenten sollen dabei auch den Effekt der Verteidigung für den Angreifer verstehen und abschätzen lernen.

Beispielsweise werden folgende Verteidigungstechniken implementiert:

1. Stack Canaries in verschiedenen Varianten, plus Code Injection via Buffer Overflows.
2. Bounds Checking in verschiedenen Varianten.

3. Code-Reuse Angriffe und Verteidigungen:
   1. Software Diversity in voller Breite und Tiefe:
      - NOP Insertion
      - Equivalent Instruction Substitution
      - Register Assignment Randomization
      - Basic Block Randomization
      - Function Permutation
      - Data Randomization

   2. Control-Flow Integrity in verschiedenen Varianten.

4. Spectre Angriffe und Verteidigungen.

Das Seminar widmet sich aktuellen Themen der sprachbasierten Sicherheit und je nach Interesse auch dem weiteren Gebiet der Software- und Systemsicherheit.

Literatur

- Automated Software Diversity (Synthesis Lectures on Information Security, Privacy, and Trust). Morgan & Claypool Publishers, Per Larsen, Stefan Brunthaler, Lucas Davi, Ahmad-Reza Sadeghi, Michael Franz
- Software Security: Principles, Policies, and Protection. Mathias Payer, EPFL, https://nebelwelt.net/SS3P/

Leistungsnachweis

Portfolio. Der Leistungsnachweis setzt sich aus der Absolvierung des Praktikums und dem Erstellen einer schriftlichen Ausarbeitung, sowie der zugehörigen Präsentation zusammen.

Im Rahmen des Praktikums müssen 4 von 5 Übungen in einem kleinen, für Praktikumszwecke geeigneten Compiler (QBE) implementiert werden. Sollten Studenten vorher schon das Modul "Compilerbau (erweitert)" abgeschlossen haben, können diese ihren eigenen Compiler zur Implementierung der Übungen verwenden. Eine Übung bedarf einer schriftlichen Ausarbeitung einer Industriestudie, sowie einer Analyse der Sicherheit eines wissenschaftlichen Artikels. Die Bearbeitungszeit der Übungen beträgt sechs bis zwölf Wochen. Der Implementierungsumfang pro Übung richtet sich primär an den verwendenden Compiler und den individuellen Lösungsansatz, bedarf zwischen 100 und 200 Zeilen.

Die zu erbringende schriftliche Ausarbeitung umfasst zwischen 10 und 20 Seiten, die zugehörige Präsentation zwischen 20 und 40 Minuten.

In einem nachfolgenden Gespräch werden Verständnisfragen zu den Praktikumsabgaben und der Literatur gestellt, die Dauer dieses Gesprächs ist zwischen 20 und 40 Minuten.

Die Note wird wie folgt berechnet:
- 1/4: Schriftliche Ausarbeitung der Seminararbeit.
- 1/4: Mündliche Präsentation der Seminararbeit.
- 1/4: Implementierung der Praktikumsarbeit.

• 1/4: Mündliche Prüfung zum Thema der Praktikumsimplementierung.
Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfeld Enterprise Security
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Compilerbau	3647

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau studiert die systematische Konstruktion von Compilern in allen Phasen, mithin der lexikalischen, syntaktischen und semantischen Analyse mit gängigen Verfahren. Die Vorlesung startet mit einer kleinen Untermenge der C Programmiersprache und vergrößert diese Menge schrittweise wie folgt:

- Unterstützung mehrerer skalarer Datentypen, z.B. Bool'sche Variablen
- Unterstützung mehrerer zusammengesetzter Datentypen, z.B. Records
- Unterstützung von komplexeren lokalen Variablen
- Unterstützung von Funktionen

Innerhalb der wachsenden Programmiersprache werden verschiedene Konzepte erörtert:

- Typüberprüfung
- Feldgrenzenüberprüfung
- Direkte Erzeugung von Maschinencode
- Optimierungen (Register Allokation, Peephole Optimization, etc.)
- Virtuelle Maschinen, Konstruktion und Optimierung.

Literatur
• Engineering a Compiler, Cooper & Torczon. • Modern Compiler Implementation in ML, Andrew Appel. • Modern Compiler Design, Grune et al. • Principles of Program Analysis, Fleming et al. • Compiler Construction, Waite und Goos. • Übersetzerbau: Band 1: Virtuelle Maschinen; Wilhelm, Seidl. • Übersetzerbau: Band 2: Syntaktische und semantische Analyse; Wilhelm, Seidl, Hack. • Übersetzerbau: Band 3: Analyse und Transformation; Seidl, Wilhelm, Hack. • Structure and Interpretation of Computer Programs; Abelson und Sussman. • How to Design Programs, Matthias Felleisen, Robert Bruce Findler, Matthew Flatt, Shriram Krishnamurthi. • Schreibe Dein Programm!; Herbert Klaeren, Michael Sperber. • The Little Schemer, Friedman, Felleisen.
Leistungsnachweis
Schriftliche Prüfung von 120 Minuten Dauer.
Verwendbarkeit
• Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfeld Software- und Informationsmanagement • Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Enterprise Security und Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Compilerbau (erweitert)	3648

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
36481	P	Praktikum Compilerbau	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau studiert die systematische Konstruktion von Compilern in allen Phasen, mithin der lexikalischen, syntaktischen und semantischen Analyse mit gängigen Verfahren. Die Vorlesung startet mit einer kleinen Untermenge der C Programmiersprache und vergrößert diese Menge schrittweise wie folgt:

- Unterstützung mehrerer skalarer Datentypen, z.B. Bool'sche Variablen
- Unterstützung mehrerer zusammengesetzter Datentypen, z.B. Records
- Unterstützung von komplexeren lokalen Variablen
- Unterstützung von Funktionen

Innerhalb der wachsenden Programmiersprache werden verschiedene Konzepte erörtert:

- Typüberprüfung
- Feldgrenzenüberprüfung
- Direkte Erzeugung von Maschinencode
- Optimierungen (Register Allokation, Peephole Optimization, etc.)
- Virtuelle Maschinen, Konstruktion und Optimierung.

Das Praktikum Compilerbau vertieft die Kenntnisse des Compilerbaus in verschiedene Richtungen (siehe Leistungsnachweis). Im Praktikum gibt es einen spezifischen Fokus auf Sicherheit-basierte Themen, es besteht z.B. die Moeglichkeit Control-Flow Integrity oder Software Diversity im eigenen Compiler aus dem vorhergehenden Trimester (also WT oder FT) zu implementieren.

Literatur

- Engineering a Compiler, Cooper & Torczon.
- Modern Compiler Implementation in ML, Andrew Appel.
- Modern Compiler Design, Grune et al.
- Principles of Program Analysis, Fleming et al.
- Compiler Construction, Waite und Goos.
- Übersetzerbau: Band 1: Virtuelle Maschinen; Wilhelm, Seidl.
- Übersetzerbau: Band 2: Syntaktische und semantische Analyse; Wilhelm, Seidl, Hack.
- Übersetzerbau: Band 3: Analyse und Transformation; Seidl, Wilhelm, Hack.
- Structure and Interpretation of Computer Programs; Abelson und Sussman.
- How to Design Programs, Matthias Felleisen, Robert Bruce Findler, Matthew Flatt, Shriram Krishnamurthi.
- Schreibe Dein Programm!; Herbert Klaeren, Michael Sperber.
- The Little Schemer, Friedman, Felleisen.

Leistungsnachweis

Der Leistungsnachweis ist ein Portfolio und besteht aus einer praktischen Ausarbeitung eines komplexeren Teilgebiets des Compilerbaus in dem eigenen, in der Compilerbau Übung erstellten Compiler. Die Teilgebiete umfassen folgende Aufgaben:

- Design und Implementierung eines einfachen Python Frontends für den erstellten Beispielcompiler.
- Design und Implementierung komplexer Datentypen, Unterstützung für Klassen, Objekte und dynamische Bindung von Methodenaufrufen.
- Backend-Optimierungen: Design und Implementierung eines automatischen Befehlsauswahlverfahrens auf Grundlage von Bottom-Up Rewriting Systems (BURS).
- Backend: Unterstützung einer zusätzlichen Backend-Architektur, z.B. RISC-V oder ARM.
- Sprachbasierte Sicherheit: Implementierung verschiedener Compiler-gestützter Verteidigungstechniken

Es kann nur ein Thema gewählt werden, die Bearbeitungszeit umfasst 6 bis 12 Wochen. Die Bearbeitung wird durch eine Präsentation mit einer Dauer von 20 - 40 Minuten, durch die Abgabe des Quelltextes der erbrachten Lösung (Umfang: 1000 - 2000 Codezeilen) und durch ein Fachgespräch mit zugehörigen Verständnisfragen, ebenfalls im Umfang von 20 - 40 Minuten, abgeschlossen.

Die Note wird wie folgt berechnet:

- 1/3: Implementierung zu Compilerbau Uebung
- 1/3: Implementierung des Praktikums

• 1/3: Muendliche Pruefung zum Thema der Praktikumsimplementierung
Verwendbarkeit
• Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfeld Software- und Informationsmanagement • Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Enterprise Security und Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Post-Quantum Cryptography	3931

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
39311	VÜ	Introduction to Post-Quantum Cryptography	Pflicht	4
39312	VÜ	Selected Topics in Post-Quantum Cryptography	Pflicht	4
39313	SE	Post-Quantum Cryptography in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Grundkenntnisse in Mathematik (Diskrete Strukturen, Lineare Algebra, Wahrscheinlichkeitstheorie) und in Informatik (Algorithmenentwurf und -analyse) sowie in der Kryptographie (Basiskonzepte) vorausgesetzt. Notwendige (minimale) Grundlagen des Quantencomputings werden in den Lehrveranstaltungen eingeführt.

Qualifikationsziele

Die Studierenden kennen den Einfluss von Quantencomputern auf die Kryptographie (Shor, Grover) und deren Implikationen. Sie kennen quantenresistente mathematische Problemklassen, deren Sicherheit und Verwendung dieser zur Konstruktion kryptographischer Basismechnismen. Die Studierenden kennen Designprinzipien von aktuellen Post-Quanten Verfahren und deren Funktionsweise und haben einen Einblick in die aktuellen praktischen und theoretischen Herausforderungen der Post-Quanten Kryptographie. Sie sind in der Lage kryptographische Verfahren zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um die Post-Quanten Kryptographie und ihre Anwendungen.

Inhalt

Introduction to Post-Quantum Cryptography - In dieser Vorlesung werden die Gundlagen der Post-Quanten (oder quantensicheren) Kryptographie behandelt.
Es wird die Notwendigkeit der Neubetrachtung der Kryptographie aufgrund von Quantencomputern und relevanter Quantenalgorithmen (Shor, Grover) sowohl im Kontext symmetrischer als auch asymmetrischer Kryptographie diskutiert. Danach werden die Unterschiede zwischen klassischen Angreifern und Quantenangreifern sowie die Auswirkungen auf die beweisbare Sicherheit veranschaulicht. Der Hauptteil

der Vorlesung umfasst dann einen Überblick über relevante Klassen mathematischer Probleme die zur Konstruktion quantensicherer Kryptographie herangezogen werden. Dies umfasst hash-basierte Signaturen, multivariate Kryptographie, Kryptographie basierend auf fehlerkorrigierenden Codes, gitterbasierte Kryptographie sowie isogeniebasierte Kryptographie. In den Übungen werden die Kenntnisse aus der Vorlesung vertieft sowie konkrete Beispiele und Beweise betrachtet.

Selected Topics in Post-Quantum Cryptography - In dieser Vorlesung werden zuerst, aufbauend auf den in der ersten Vorlesung erarbeiteten Grundlagen, moderne Konstruktionsprinzipien aktueller beweisbar sicherer quantenresistenter kryprographischer Basismechanismen (asymmetrische Verschlüsselung bzw. KEMs und Signaturen) betrachtet. Dies umfasst sowohl generische Prinzipien wie auch spezifische Aspekte für ausgewählte Verfahren verschiedener Problemklassen. Danach werden ausgewählte und aktuell relevante Themen aus dem Bereich der Post-Quanten Kryptographie betrachtet: Dies umfasst sowohl praktische als auch theoretisch und stärker forschungsbezogene Aspekte. Beispielsweise die Standardisierung von und Migration zu Post-Quanten Kryptographie (z.B. Hybridisierung), die Integration von Post-Quanten Kryptographie (in Sicherheitsprotokolle oder aktuelle Anwendungen) wie auch die Konstruktion fortgeschrittener kryptographischer Verfahren basierend auf Post-Quanten Annahmen und damit in Verbindung stehende Herausforderungen. In den Übungen werden die Kenntnisse aus der Vorlsung vertieft sowie konkrete Beispiele und Beweise betrachtet.

Post-Quantum Cryptography in Practice - In diesem praxisorientierten Seminar geht es um den praktischen Einsatz von quantensicheren kryptographischen Verfahren.
In Bezug auf das ausgewählte Thema wird von den Studierenden eine weitgehend selbständig gefertigte prototypische Umsetzung eines Miniprojektes unter Verwendung von geeigneten open-source Softwarebibliotheken bzw. Technologien erwartet. Die Ergebnisse der Implementierungsarbeit sollen dann in einem Bericht beschrieben und während der Präsentation demonstriert werden.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen können zum Teil auch in englischer Sprache gehalten werden.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio:

Zu den Vorlesungen mit Übungen: ein mündliches Fachgespräch von 30 Minuten oder eine schriftliche Klausur von 60 Minuten über die Inhalte aus beiden Veranstaltungen; die Form des Leistungsnachweises wird zu Beginn des Moduls festgelegt.

Zum Seminar: Erstellung und Abgabe einer Präsentation zur Demonstration von Ergebnissen des Miniprojektes (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.
Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfelder Enterprise Security, Public Security, Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im Frühjahrstrimester.

Modulname	Modulnummer
Biometric Recognition	4211

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
42111	VL	Biometric Recognition	Pflicht	4
42112	SE	Selected topics in Biometric Recognition	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Grundkenntnisse in den Bereichen Machine Learning, Kryptologie, IT-Sicherheit. Gute Programmierkenntnisse (Python).

Qualifikationsziele
Vorlesung: Die Studierenden sollen das Verständnis für die Prinzipien und Verfahren in der Biometrie entwickeln und die wichtigsten biometrischen Verfahren kennenlernen. Darüber hinaus sollen sie die Sicherheitseigenschaften eines biometrischen Systems und komplexe Beziehungen zwischen Verfahren und Umgebungseinflüssen (z.B. Beleuchtungssituationen, Posenvariation etc.) herstellen und deren Auswirkung auf die Erkennungsleistung von Systemen bewerten können. Die Studierenden sollen für einen vorgegebenen Anwendungsbereich geeignete Verfahren auswählen können und eine ausgewogene Balance zwischen Technologie und Grundprinzipien des Datenschutzes entwickeln. Seminar: Die Studierenden können aktuelle Einsatz-Szenarien von biometrischen Systemen implementieren und evaluieren. Die Studierenden sind in der Lage, aktuelle Herausforderungen biometrischer Systeme zu verstehen, zu analysieren, zu evaluieren und zu diskutieren, um neue Lösungen zu finden. Darüber hinaus können sie fachliche Literatur und aktuelle Veröffentlichungen recherchieren, um Methoden zu finden, welche ihnen bei der Entwicklung neuer Lösungen helfen können. Die Studierenden können ihre Arbeit im Team präsentieren und Herausforderungen diskutieren. Des Weiteren können

die Studierenden Fragen zu den anderen Vorträgen formulieren und mit Ideen beitragen, um die Herausforderungen zusammen zu lösen.

Inhalt

Vorlesung:

- Mechanismen der wichtigsten biometrischen Verfahren, die heute in kommerziellen Systemen zum Einsatz kommen (Fingerbilderkennug, Gesichtserkennung, Iriserkennung)
- Die Methoden der Sensorik, Signalverarbeitung, Merkmalsextraktion und Klassifikation
- Bewertungskriterien zur Auswahl von biometrischen Systemen: Erkennungsleistung vs. Sicherheitseigenschaften
- Grundzüge der im Kontext von biometrischen Systemen relevanten Datenschutzprinzipien

Seminar:

Die Studierenden wählen ein Projekt aus der Liste der angebotenen Projekte aus. Am Ende des Trimesters sollten die Studierenden eine Ausarbeitung und ggf. Code abliefern und ihre Arbeit in einer 20- bis 40-minütigen Präsentation (inkl. Q&A-Slot) vorstellen.

Literatur

- S. Li, A.K. Jain, Handbook of Face Recognition, Springer, (2011)
- D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, (2009)
- J. Wayman, A. Jain, D. Maltoni, D. Maio, Biometric Systems, Springer, (2005)
- Forschungsartikel in peer-reviewed Konferenzen oder Journalen

Leistungsnachweis

Portfolio: zur Vorlesung ein 60-minütige schriftliche Klausur und zum Seminar eine Ausarbeitung (6 bis 10 Seiten), ggf. Code und eine 20- bis 40-minütige Präsentation (inkl Q&A-Slot). Die Bearbeitungsdauer für die Ausarbeitung und die Vorbereitung der Präsentation beträgt 4 bis 6 Wochen. Die Leistungen in der Klausur und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit um maschinelles Lernens um die wichtigen technologischen Aspekte des Authentisierens, der Privatheit und entsprechenden Methoden und Verfahren. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet der Biometrischen Erkennung.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im FT.

Modulname	Modulnummer
Deep Learning for IT-Security	4212

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
42121	VL	Deep Learning	Pflicht	4
42122	SE	Selected Topics in Deep Learning for IT-Security	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse in den Bereichen Machine Learning, Algorithmen. Gute Programmierkenntnisse (Python).

Qualifikationsziele

Vorlesung:

Die Studierenden verstehen die Grundprinzipien von Deep Learning Methoden, welche heutzutage weit verbreitet in der Künstlichen Intelligenz sind, insbesondere für Muster Erkennung oder Biometrie. Sie werden nicht nur mit linearen Netzen arbeiten, sondern auch mit Convolutional Neural Networks (CNN) für Bildverarbeitung und Long Short-Term Memory (LSTM) Networks fu#r die Verarbeitung von Sequenzen. Die Studierenden können verschiedene Ansätze vergleichen, ihre Vorteile und Nachteile besprechen, und entscheiden, welches der beste Ansatz zur Bewältigung der anstehenden Herausforderungen ist. Seminar:

Die Studierenden können aktuelle deep learning Architekturen implementieren und evaluieren. Die Studierenden sind in der Lage, aktuelle Herausforderungen des deep learnings und ihrer Anwendungen in der IT-Sicherheit zu verstehen, zu analysieren, zu evaluieren und zu diskutieren, um neue Lösungen zu finden. Darüber hinaus können sie fachliche Literatur und aktuelle Veröffentlichungen recherchieren, um Methoden zu finden, welche ihnen bei der Entwicklung neuer Lösungen helfen können. Die Studierenden können ihre Arbeit im Team präsentieren und Herausforderungen diskutieren. Des Weiteren können die Studierenden Fragen zu den anderen Vorträgen formulieren und mit Ideen beitragen, um die Herausforderungen zusammen zu lösen.

Inhalt

Vorlesung:

- Grundlagen der deep learning
- Convolutional Neural Networks
- Long Short-Term Memory (LSTM) Networks
- Generative Adversarial Networks (GAN) und Autoencoders (AE)
- Biometrische Erkennung und deep learning
- Angriffserkennug in der Biometrie: Presentation Attack Detection (PAD) und deep learning

Seminar:

Die Studierenden wählen ein Projekt aus der Liste der angebotenen Projekte aus.
Die Projekte werden Anwendungen der gelernten Algorithmen in der Cybersicherheit bearbeiten. Am Ende des Trimesters sollten die Studierenden eine Ausarbeitung und ggf. Code abliefern und ihre Arbeit in einer 20- bis 40-minütigen Präsentation (inkl. Q&A-Slot) vorstellen.

Literatur

- I. Goodfellow, Y. Bengio, A. Courville: Deep Learning (Adaptive Computation and Machine Learning series), The MIT Press; Illustrated Edition (18. November 2016), ISBN: 978-0262035613
- F. Chollet: Deep Learning with Python, Manning Publications, 2017, ISBN: 978-1617294433
- B. Bhanu, A. Kumar: Deep Learning for Biometrics, Springer, 2017, ISBN: 978-3319616568
- Forschungsartikel in peer-reviewed Konferenzen oder Journalen

Leistungsnachweis

Portfolio: zur Vorlesung ein 60-minütige schriftliche Klausur und zum Seminar eine Ausarbeitung (6 bis 10 Seiten), ggf. Code und eine 20- bis 40-minütige Präsentation (inkl Q&A-Slot). Die Bearbeitungsdauer für die Ausarbeitung und die Vorbereitung der Präsentation beträgt 4 bis 6 Wochen. Die Leistungen in der Klausur und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten vermitteln tiefes Verständnis von modernen Verfahren des deep learnings. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet der Biometrischen Erkennung.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im FT.

Modulname	Modulnummer
Privacy Preserving Machine Learning	4213

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
42131	VL	Privacy Preserving Machine Learning	Pflicht	4
42132	SE	Selected topics in Privacy Preserving Machine Learning	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Grundkenntnisse in den Bereichen Machine Learning, Kryptologie, Datenschutz und Privacy. Gute Programmierkenntnisse (Python).

Qualifikationsziele
Vorlesung: Die Studierenden lernen und können die mathematische Definition von differential privacy verstehen und ihre wichtigsten Eigenschaften analysieren. Darüber hinaus werden Sie wichtige algorithmische Werkzeuge für die private Beantwortung einfacher numerischer und nicht-numerischer Abfragen kennenlernen, sowie ihre Garantien für den Schutz der Privatsphäre. Diese Mechanismen dienen als Bausteine zur Konstruktion privater Algorithmen für maschinelles Lernen. Wir werden uns insbesondere auf die private empirische Risikominimierung mit Techniken konzentrieren. Schließlich werden wir das dezentralisierte Modell der differentiellen Privatsphäre betrachten. Die Studierenden können am Ende verschiedene Ansätze vergleichen, ihre Vorteile und Nachteile besprechen, und entscheiden, welches der beste Ansatz zur Bewältigung der anstehenden Herausforderungen ist. Seminar: Die Studierenden können aktuelle differential privacy und federated learning Architekturen implementieren und evaluieren. Die Studierenden sind in der Lage, aktuelle Herausforderungen des datenschutzgerechten maschinellen Lernens zu verstehen, zu analysieren, zu evaluieren und zu diskutieren, um neue Lösungen zu finden. Darüber hinaus können sie fachliche Literatur und aktuelle Veröffentlichungen recherchieren, um Methoden zu finden, welche ihnen bei der Entwicklung neuer Lösungen helfen können. Die Studierenden können ihre Arbeit im Team präsentieren und Herausforderungen

diskutieren. Des Weiteren können die Studierenden Fragen zu den anderen Vorträgen formulieren und mit Ideen beitragen, um die Herausforderungen zusammen zu lösen.

Inhalt

Vorlesung:

- Einführung in differential privacy
- Der exponentielle Mechanismus & erweiterte Komposition
- Differentiell private empirische Risikominimierung
- Differentiell privater stochastischer Gradientenabstieg
- Federated learning

Seminar:

Die Studierenden wählen ein Projekt aus der Liste der angebotenen Projekte aus. Am Ende des Trimesters sollten die Studierenden eine Ausarbeitung und ggf. Code abliefern und ihre Arbeit in einer 20- bis 40-minütigen Präsentation (inkl. Q&A-Slot) vorstellen.

Literatur

- C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, 2014
- K. Nissim et al., Differential Privacy: A Primer for a Non-technical Audience, Journal of Entertainment & Technology Law, 2018
- S. Vadhan, The Complexity of Differential Privacy, Tutorials on the Foundations of Cryptography, 2017
- P. Kairouz et al., Advances and Open Problems in Federated Learning, 2019

Leistungsnachweis

Portfolio: Zur Vorlesung ein 60-minütige schriftliche Klausur und zum Seminar eine Ausarbeitung (6 bis 10 Seiten), ggf. Code und eine 20- bis 40-minütige Präsentation (inkl Q&A-Slot). Die Bearbeitungsdauer für die Ausarbeitung und die Vorbereitung der Präsentation beträgt 4 bis 6 Wochen. Die Leistungen in der Klausur und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit und Kryptograhie, und vermitteln tiefes Verständnis von modernen Verfahren des Schutzes der Privatsphäre. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet des Schutzes der Privatsphäre durch biometrische Systeme.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Foundations of Distributed Systems and Blockchains	5118

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
51181	VÜ	Foundations of Distributed Systems and Blockchains	Pflicht	4
51182	SE	Research Topics in Security for Decentralized Systems	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Grundkenntnisse in Mathematik (Diskrete Strukturen, Lineare Algebra, Wahrscheinlichkeitstheorie) und in Informatik (Algorithmenentwurf und -analyse) vorausgesetzt. Basiswissen in der Kryptographie (Basiskonzepte) ist hilfreich, aber nicht notwendig (alle verwendeten Konzepte werden im Modul eingeführt).

Qualifikationsziele

Die Studierenden kennen grundlegende Konzepte in dezentralen Systemen (z.B. Fehlertoleranz und Konsensus) und lernen grundlegende kryptographische Mechanismen kennen, die zur Realisierung dieser Eigenschaften notwendig sind (z.B. Hashfunktionen, MACs und Signaturen). Diese Konzepte werden dann anhand von Blockchains und Kryptowährungen betrachtet und es werden weitere wichtige Konzepte im Kontext von Blockchains eingeführt (z.B. Proof-of-Work, Proof-of-Stake, Proof-of-Space). Die Studierenden lernen relevante kryptographische Mechanismen wie das Generieren von verteilten und verifizierbaren Zufallszahlen sowie das Feld der Threshold-Kryptographie und deren Anwendungen kennen. Darüber hinaus bekommen die Studierenden einen Einblick in Privatheits- und Skalierungsprobleme in Blockchains sowie in kryptographische Konzepte, mit denen diese Probleme gelöst werden können. Im Speziellen wird das Konzept des Verifiable Computing und so genannter Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) behandelt. Studierende sind in der Lage Herausforderungen in dezentralen Systemen (im Speziellen Blockchains) zu erkennen und zu analysieren sowie die Einsatzmöglichkeiten relevanter kryptographischer Mechanismen zur Lösung dieser Herausforderungen zu verstehen. Darüber hinaus kennen die Studierenden den aktuellen Stand der Forschung in diesem Feld.

Inhalt
Foundations of Distributed Systems and Blockchains - In dieser Vorlesung werden die Grundlagen von dezentralen Systemen sowie in diesem Kontext relevanter Kryptographie behandelt. Ein Schwerpunkt der Vorlesung liegt auf Blockchains und Kryptowährungen, insbesondere auf deren Grundlagen und Funktionsweise. Hier werden Mechanismen wie Proof-of-Work, Proof-of-Stake sowie Proof-of Space, Transaktionen sowie notwendige kryptographische Mechanismen (z.B. Merkle Trees) und deren Abstraktionen und Varianten behandelt. Es wird auch die Unveränderlichkeit von Blockchains kritisch hinterfragt und Konzepte zur „Aufweichung“ dieser Eigenschaft werden präsentiert. Als wichtiges kryptographisches Konzept wird die so genannte Threshold-Kryptographie eingeführt, die es ermöglicht kryptographische Funktionalität (z.B. das Erstellen einer Signatur) auf mehrere Parteien zu verteilen. Als verwandtes Thema wird auch die verteilte und verifizierbare Erzeugung von Zufallszahlen behandelt. Bei all diesen kryptographischen Konzepten wird immer der Bezug zu Anwendungen im Blockchain-Kontext veranschaulicht. Als ein weiteres wichtiges Konzept wird so genanntes Verifiable Computing und so genannte Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) behandelt. Diese Techniken ermöglichen das Lösen von Skalierbarkeits- und Privatheitsproblemen in Blockchains. In den Übungen werden die Kenntnisse aus der Vorlesung vertieft sowie konkrete Beispiele betrachtet. **Research Topics in Security for Decentralized Systems** - In diesem Seminar bekommen Studierende einen Einblick in aktuelle Forschungsthemen an der Schnittstelle zwischen dezentralen Systemen und Sicherheit mit Fokus auf Einsatz von Kryptographie. Die Schwerpunkte liegen auf neuen kryptographischen Verfahren und Konzepten sowie deren Anwendungen in dezentralen Systemen und Blockchains im Speziellen. Zu Beginn des Seminars wird eine Themenauswahl vorgestellt, die von Studierenden über die Dauer des Seminars bearbeitet und am Ende präsentiert werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikel aus führenden wissenschaftlichen Konferenzen stützen. In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Vorlesung wird in deutscher Sprache gehalten, Teile der Übungen und des Seminars können auch in englischer Sprache gehalten werden.
Literatur
Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.
Leistungsnachweis
Portfolio auf der Basis der folgenden Leistungen: 51181: Ein mündliches Fachgespräch von 20 Minuten oder eine schriftliche Klausur von 45 Minuten; die Form des Leistungsnachweises wird zu Beginn des Moduls festgelegt. In 51182: Erstellung und Abgabe einer schriftlichen Ausarbeitung (10 bis 20 Seiten) und eine Präsentation (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen. Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfelder Enterprise Security, Public Security, Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und beginnt jedes Jahr in WT. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Offensive Sicherheitsüberprüfungen	5523

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55091	VÜ	Penetration Testing	Pflicht	6
55093	P	Penetration Testing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Gute Kenntnisse in den Bereichen Netzsicherheit und Systemsicherheit, wie in den gleichnamigen beiden Modulen vermittelt.

Qualifikationsziele

Die Studierenden können organisationsinterne Überprüfungen der IT-Sicherheitseigenschaften von Systemen, Diensten und Netzen planen und durchführen. Sie beherrschen Testmethoden auf Netz-, Anwendungs- und Systemebene und haben ausgewählte aktuelle Werkzeuge für diesen Zweck kennengelernt. Sie kennen die Aufgabenbereiche und Randbedingungen von Red Teams und Pentesting-Dienstleistern.

Inhalt

Die Vorlesung Penetration Testing führt in die Aufgabengebiete von Pentesting- bzw. Red-Teams ein. Für verschiedene Anwendungsgebiete wie das Sicherheitstesten einzelner Systeme, komplexerer IT-Dienste und ganzer Rechnernetze und IT-Infrastrukturen werden die Vor- und Nachteile verschiedener Testvarianten wie Whitebox- und Blackbox-Tests analysiert. Unter Orientierung an bewährten Good-Practice-Dokumentationen wie OWASP und OSSTMM werden praxisrelevante Angriffsvarianten von der Reconnaissance-Phase bis zum Einbringen von Exploit-Payloads behandelt. Ebenso werden die strukturierte Erstellung von Pentesting-Berichten und deren Auswertung durch die auftraggebende Organisation betrachtet.

Das Praktikum Penetration Testing stellt auf Basis einer Praktikumsinfrastruktur (abgeschottete Laborumgebung) Aufgaben, in denen die Studierenden als fiktiver Auftragnehmer eines technischen Penetrationstests fungieren. Mithilfe ausgewählter bereitgestellter Softwarewerkzeuge müssen die für Pentests ausgewählten Systeme, Dienste und Subnetze erkundet und auf verschiedenste Verwundbarkeiten untersucht werden, ohne den Betrieb der übrigen Infrastruktur zu beeinträchtigen. Für einige Überprüfungen müssen eigene Werkzeuge bzw. Skripte/Payloads konzipiert und

implementiert werden. Über die gewählte Vorgehensweise, die einzelnen Schritte der Durchführung und die zu priorisierenden Ergebnisse ist eine Ausarbeitung zu erstellen, die vom Stil her an Pentest-Berichte angelehnt ist.

Literatur

- M. Kofler et al.: Hacking & Security. Rheinwerk Verlag, 2022
- P. Calderon: Nmap Network Exploration and Security Auditing Cookbook. Packt Publishing Ltd, 2021
- P. Kim and J.Faircloth: The Hacker Playbook 3. Secure Planet LLC, 2015
- V. K. Velu: Mastering Kali Linux for advanced penetration testing. Packt Publishing Ltd, 2017

Leistungsnachweis

Portfolio. Der Leistungsnachweis besteht aus zwei Teilen: (1) schriftliche Klausur von 60 Minuten Dauer; (2) praktischer Leistungsnachweis in Form eines Penetrationstests (Pentests), einschließlich der Anfertigung eines schriftlichen Berichts. Für den Pentest wird eine Labor-Umgebung bereitgestellt, die ein mittelständisches Unternehmen simuliert. Der Zugang zum Labor erfolgt per VPN, was die Durchführung des Pentests ortsunabhängig ermöglicht. Die Bearbeitung erfolgt nach Ausgabe der Aufgabenstellung und muss innerhalb von 10 Wochen abgeschlossen sein. Der Pentest-Bericht muss einen Manager-Teil und einen Admin-Teil enthalten und zwischen 30 und 60 Seiten umfassen.

Die Leistungen in der schriftlichen Klausur und im Praktikum gehen im Verhältnis 50 zu 50 in die Note ein.

Verwendbarkeit

- Wahlpflicht für das Vertiefungsfeld Cyber Network Capabilities (CNC) im Studiengang MCYB
- Wahlpflicht für das Vertiefungsfeld Enterprise Security (ES) im Studiengang MCYB
- Wahlpflicht im Studiengang MME, Wahlpflichtgruppe ITSK
- Wahlpflicht im Studiengang MCAE

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Modern Cryptography	5548

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Manulis	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55481	VÜ	Modern Cryptography	Pflicht	4
55482	SE	Seminar Research Trends in Cryptography	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende mathematischen Kenntnisse sowie ein generelles Interesse an moderner Kryptographie vorausgesetzt.

Qualifikationsziele

Die Studierenden kennen Designprinzipien und Funktionsweise von modernen kryptographischen Verfahren und Protokollen und beherrschen den Umgang mit entsprechender Sicherheitsmodellierung und -beweisführung. Sie sind in der Lage kryptographische Verfahren zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um Kryptographie und ihren Anwendungen.

Inhalt

- **Modern Cryptography** - In dieser Vorlesung werden moderne Methoden der Kryptographie sowie weiterführende kryptographische Verfahren und Protokolle detailliert vorgestellt und analysiert. Neben der allgemeinen Funktionsweise wird auf die Sicherheitsmodellierung und beweisbare Sicherheit eingegangen. Dazu werden, z.B., moderne Beweisführungsmethoden wie kryptographische Reduktionen eingeführt. Zu den Themen der Veranstaltung gehören unterschiedliche kryptographische Funktionalitäten, darunter Einwegfunktionen, Pseudozufallszahlengeneratoren, Hashfunktionen, Blockchiffren, message authentication codes, digitale Signaturen und Verschlüsselungsverfahren, sowie weiterführende Techniken wie Identifikationsverfahren und zero-knowledge Beweise. Neben den weit verbreiteten auf diskreten Logarithmen oder Integer Faktorisierung basierenden Verfahren, werden weitere Konstruktionen vorgestellt, die mittels elliptischen Kurven und bilinearen Abbildungen aufgebaut sind. Die nötigen mathematischen Grundlagen für diese Verfahren werden im Rahmen der Veranstaltung eingeführt. In Übungen werden die Methoden der beweisbaren

Sicherheit sowie die Funktionsweise von eingeführten Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.
- **Research Trends in Cryptography** - In diesem Seminar bekommen Studierende ein Einblick in aktuelle Forschungsfelder der Kryptographie. Die Schwerpunkte liegen bei neuen kryptographischen Konzepten, Methoden, Verfahren und Protokollen sowie bei deren Implementierung, Standardisierung und Anwendungen. Zu Beginn der Veranstaltung wird eine Auswahlliste von aktuellen Themen vorgestellt, die von Studierenden über die Dauer der Veranstaltung ausgearbeitet und am Ende vorgestellt werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikel (aus bekannten Tagungen) und Open-Source Quellen (z.B. Softwarebibliotheken, Standards) stützen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Katz, J. and Lindell, Y. Introduction to Modern Cryptography (2nd Edition), Chapman & Hall/CRC Cryptography and Network Security Series, 2014.

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen:

55481 VÜ Modern Cryptography: mündliches Fachgespräch von 20 Minuten,

55482 Seminar Research Trends in Cryptography: Erstellung und Abgabe einer schriftlichen Ausarbeitung (10 bis 20 Seiten) und eine Präsentation (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten vermitteln tiefes Verständnis von modernen kryptographischen Methoden und Verfahren. Die Veranstaltungen fördern analytisches Denken und entwickeln Fähigkeiten kryptographische Verfahren unter Verwendung von Security-by-Design Prinzipien zu entwerfen und zu analysieren sowie deren Einsatz in Anwendungen zu planen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet der Kryptographie und dient als gute Vorbereitung für weiterführende Lehrveranstaltungen rund um Kryptographie und ihren Anwendungen zum Schutz der Datensicherheit und Privatheit, etwa im Rahmen des Moduls „Privacy Enhancing Cryptography“.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird im WT angeboten. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Privacy Enhancing Cryptography	5563

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Manulis	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55631	VÜ	Private Data Processing	Pflicht	4
55632	VÜ	Private Authentication and Messaging	Pflicht	4
5563-V3	SE	Privacy Enhancing Cryptography in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende Kenntnisse in moderner Kryptographie sowie ein generelles Interesse am Einsatz von kryptographischen Verfahren und Protokollen zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern vorausgesetzt. Eine vorherige Teilnahme am Modul „Modern Cryptography“ ist wünschenswert, stellt jedoch keine formale Voraussetzung dar.

Qualifikationsziele

Die Studierenden kennen Designprinzipien und Funktionsweise von verschiedenen Verfahren und Protokollen zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern unter Verwendung von modernen kryptographischen Methoden. Sie sind in der Lage die kryptographische Lösungen kritisch zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um Privacy Enhancing Cryptography und entsprechenden Anwendungen.

Inhalt

- **Private Data Processing:** In dieser Vorlesung werden kryptographische Protokolle vorgestellt, mit deren Hilfe vertrauliche Daten durch eine oder mehrere Parteien verarbeitet werden können. Dabei geht es um Operationen auf numerischen und binären Daten sowie sichere Berechnungen von Funktionen zum Einsatz in diversen Anwendungsfällen, welche die Vertraulichkeit von verwendeten Eingabedaten während ihrer Verarbeitung erfordern. Es werden Szenarien kooperativer Datenverarbeitung unter zwei oder mehreren Teilnehmern sowie Operationen auf ausgelagerten (etwa in eine Cloud) Daten betrachtet. Themen der Vorlesung sind, u.a. secret sharing and threshold cryptography, Varianten von oblivious transfer, (fully) homomorphic encryption, secure two-party und multi-party computation, private function evaluation, private set intersection, private information

retrieval, secure data aggregation und searchable encryption. In Übungen wird die Funktionsweise und Sicherheit von Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.

- **Private Authentication and Messaging:** In dieser Vorlesung werden Privatsphäre schützende kryptographischen Verfahren und Protokolle zur sicheren Authentisierung und Nachrichtenaustausch vorgestellt. Im Fokus stehen solche Schutzziele wie Anonymität, Unverlinkbarkeit und Abstreitbarkeit, gekoppelt an die klassischen Sicherheitsziele einer Authentisierung bzw. Ende-zu-Ende-Verschlüsselung. Es werden Verfahren vorgestellt, die solche Schutzziele in zwei- sowie mehr-Parteien Anwendungen ermöglichen. Themen der Vorlesung sind, u.a., (multi-party) key exchange und secure messaging (inkl. Signal protocol, MLS), secret handshakes, anonymous communication (inkl. mix networks, onion routing), privacy-preserving signatures (inkl. ring und group signatures) sowie anonymous credentials.
- **Privacy Enhancing Cryptography in Practice:** In diesem praxisorientierten Seminar geht es um die Implementierung und praktische Verwendung von modernen kryptographischen Verfahren und Technologien zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern. In Bezug auf das ausgewählte Thema wird von den Studierenden eine weitgehend selbständig gefertigte prototypische Umsetzung eines Miniprojektes unter Verwendung von geeigneten open-source Softwarebibliotheken bzw. Technologien erwartet. Die Ergebnisse der Implementierungsarbeit sollen dann in einem Bericht beschrieben und während der Präsentation demonstriert werden. Mögliche Themen umfassen: homomorphic encryption, secure two- and multi-party computation, private information retrieval, searchable encryption, zero-knowledge proofs, distributed cryptography, attribute-based cryptography, secure messaging, privacy-preserving authentication, anonymous communication, usw.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio:

Zu 55631 und 55632: ein mündliches Fachgespräch von 30 Minuten über die Inhalte aus beiden Veranstaltungen,

In 55633: Erstellung und Abgabe einer Präsentation zur Demonstration von Ergebnissen des Miniprojektes (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 90 zu 10 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit um die wichtigen technologischen Aspekte der Privatheit und entsprechenden kryptographischen Methoden und Verfahren. Die Veranstaltungen vermitteln die

Fähigkeiten technische Verfahren zum Schutz der Daten und Privatheit zu entwerfen und ihr Einsatz in digitalen Anwendungen zu ermöglichen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Überschneidungsbereich des technologischen Privacy- und Datenschutzes und angewandter Kryptographie.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr in FT. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Angewandte Zahlentheorie	6034

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Andreas Nickel	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12111	VÜ	Algorithmische Zahlentheorie	Pflicht	5
12112	VÜ	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Pflicht	3
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Generelles Interesse an Mathematik und Theorie. Es wird empfohlen, das Modul "Zahlentheorie und Kryptographie" absolviert zu haben.Alternativ reichen bei entsprechender Einsatzbereitschaft Grundlagen zur Kryptographie und Kryptoanalyse aus, wie sie z.B. im Modul Kryptologie vermittelt werden.

Qualifikationsziele

Die Studierenden erlernen fortgeschrittene Konzepte und Algorithmen der algebraischen Zahlentheorie und werden mit einigen ihrer Anwendungen vertraut gemacht. Dabei handelt es sich um zahlentheoretische oder algebraische Methoden für den Entwurf von kryptographischen bzw. kryptoanalytischen Verfahren und solche, die in der Codierungstheorie eingesetzt werden.

Inhalt

Die Veranstaltung "Algorithmische Zahlentheorie" befasst sich mit grundlegenden Begriffen und Algorithmen der algebraischen Zahlentheorie. (Stichworte: Primelemente, Primalitätstests, Faktorisierung, elliptische Kurven, u.a.). Ein Großteil dieser abstrakten Konzepte ist fundamental für die moderne Kryptographie (Public Key) und die Codierungstheorie. Der Schwerpunkt dieser Vorlesung ist zwar die systematische Erarbeitung der theoretischen Grundlagen und grundlegenden Algorithmen, es wird aber auch immer wieder auf Anwendungen eingegangen. Ergänzt werden diese durch zahlentheoretische Konzepte, die eventuell in einer Post-Quantencomputer-Epoche relevant sein könnten.

Die Veranstaltung "Ausgewählte mathematische Methoden der Kryptographie und Codierungstheorie" befasst sich mit ausgewählten und fortgeschrittenen Themen aus der Kryptographie und/oder der Codierungstheorie. Hierhin gehören kryptographische Verfahren, die auf zahlentheoretischen Ergebnissen aufsetzen, und "gute" Codes, die

man mit Hilfe von algebraischen Kurven gefunden hat. Sowohl kryptographische als auch codierungstheoretische Inhalte sind vorgesehen; die Gewichtung zwischen diesen beiden Gebieten kann aber variieren.

Literatur

Zur VÜ Algorithmische Zahlentheorie:

- H. Cohen: A course in computational algebraic number theory, Graduate Texts in Mathematics 138, Springer
- O. Forster: Algorithmische Zahlentheorie, Springer
- J. Hoffstein, J. Pipher, J.H. Silverman: An Introduction to Mathematical Cryptography, Springer
- C. Karpfinger, H. Kiechle: Kryptologie. Algebraische Methoden und Algorithmen, Vieweg + Teubner

Zur VÜ Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie:

- W. Heise und P. Quattrocchi: Informations- und Codierungstheorie, Springer
- D. Jungnickel: Codierungstheorie, Spektrum Akad. Verlag
- N. Koblitz: Algebraic Aspects of Cryptography, Springer
- W. Lütkebohmert, Codierungstheorie, Springer-Vieweg

Leistungsnachweis

Mündliche Prüfung von 30 Minuten Dauer.

Verwendbarkeit

- Wahlpflichtmodul im Vertiefungsfeld Enterprise Security (ES) des Masterstudiengangs Cyber-Sicherheit.
- Wahlpflichtmodul im Vertiefungsfeld Cyber Network Capabilities (CNC) des Masterstudiengangs Cyber-Sicherheit.
- Wahlpflichtmodul im Vertiefungsfeld Security Intelligence (SI) des Masterstudiengangs Cyber-Sicherheit.

Dauer und Häufigkeit

Das Modul dauert 1 bis 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Herbsttrimester.

Modulname	Modulnummer
Middleware und mobile Cloud Computing	1398

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
13981	VL	Middleware und mobile Cloud Computing	Pflicht	3
13982	UE	Middleware und mobile Cloud Computing	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden Kenntnisse aus dem Bereich des Software Engineering, insbesondere der Objektorientierung (Modul Objektorientierte Programmierung). Wünschenswert sind Grundkenntnisse in der XML-Technologien sowie in einer der objektorientierten Programmiersprache, wie z. B. Java, Scala, C++.

Qualifikationsziele

Das *Modul Middleware und mobile Cloud Computing* zielt darauf ab, den Studierenden

vertiefend die Bedeutung der Integration als Kernaufgabe der Angewandten Informatik

näher zu bringen. Die Teilnehmer erhalten neben einem grundlegenden Verständnis für die Anforderungen an eine Middleware-basierte Integration theoretische und praktische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middleware-Konzepte und serviceorientierter Schnittstellen. In diesem Zusammenhang werden wissenschaftliche Methoden vermittelt, die die Teilnehmer in die Lage versetzen, in komplexen Anwendungssystemlandschaften eigenständig und systematisch einen höheren Integrationsgrad zu erreichen. Zudem werden grundlegende Aspekte von *Verteilten Systemen* wie Kommunikationsprotokolle, Austauschformate und Sicherheitsaspekte betrachtet. Die so vermittelten IT-technischen Kenntnisse befähigen die Teilnehmer darüber hinaus aus einer Cyber-Bedrohungsperspektive betrachtet, eine fundierte Analyse hinsichtlich möglicher Leistungsengpässe und Schwachstellen zu konzipieren sowie in der gegebenen IT-Landschaft zu implementieren. Ohne diese Kenntnisse und Fähigkeiten kann de-facto auf potenzielle Bedrohungsszenarien beim Betrieb komplexer IT-Systeme kaum geeignet begegnet werden. Die im Modul vermittelten Grundlagen versetzen die Teilnehmer in die Lage, geeignete Maßnahmen zur Cyber-Abwehr in Middleware-/ Cloud-Strukturen zu integrieren (Stichwort: *Security-as-a-Service*).

Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang

mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. Durch eigenständige Anwendung von Technologien wie *Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), .NET, Simple Object Access Protocol (SOAP) oder Representational State Transfer (REST)* erhalten die Teilnehmer Methoden-, Fach- und Umsetzungskompetenz im Umgang mit grundlegenden Middleware-Konzepten und deren Basistechnologien. In der Kombination aus theoretischer Behandlung und praktischer Vertiefung versetzt das Modul die Teilnehmer in die Lage, verteilte Anwendungen auf der Basis von Middleware zu entwerfen und systematisch in die Praxis umzusetzen.

Inhalt

Im heutigen Digitalzeitalter mit *Industrie 4.0, Digital Governance* und *Künstlicher Intelligenz* etc. agieren fast alle Systeme als vernetzte Fähigkeitsträger. Moderne Enterprise Anwendungen basieren auf Standard-Middleware-Architekturen, wo Funktionalität zunehmend über Cloud-basierte Dienste plattformübergreifend den Clients – insbesondere zunehmend mobilen Endgeräten – zur Verfügung gestellt wird. Das Modul bietet einen fundierten Einstieg in die aktuellen Middleware-Basistechnologien. Auf den Grundlagenkenntnissen der Objektorientierten Programmierung aufbauend werden entlang der Entwicklungslinie Schritt für Schritt aktuelle Middleware-Konzepte und -Technologien eingeführt. Das Modul etabliert dazu zunächst die Basisabstraktion und das Grundverständnis Middleware-basierter Systeme. Dabei werden grundlegende Fähigkeiten zur Beherrschung heterogener Anwendungslandschaften und deren Komplexitätsparameter vermittelt. Diese berücksichtigen die Dimensionen der *Kommunikation* und *Transaktion* sowie Zugriffsmöglichkeiten und Schutzaspekte in *Schichtarchitekturen*. Unabhängig von der jeweils eingesetzten Technologie nimmt das Abstraktionskonzept der *Schnittstellen-Basierung* eine zentrale Rolle beim Design verteilter Anwendungen und somit im gesamten Modul ein.

Im Folgenden wird tiefer auf die unterschiedlichen Integrationsparadigmen und -technologien mit ihren jeweiligen spezifischen Stärken und Schwächen (Fähigkeiten, Schwachstellen, Angriffspunkte usw.) eingegangen. Aktuelle Middleware-Dienste und Architekturkonzepte wie *Verteilte Objektmodelle*, *Komponentenmodelle* und *Service Oriented Middleware (SOA)* bilden den Schwerpunkt des zweiten Teils des Moduls. Hier werden jeweils zunächst die allgemeinen Prinzipien erläutert und dann anhand konkreter Beispiele Standard-Middleware-Technologien und deren zugrunde liegenden Konzepte und Prinzipien vertieft.

Der dritte Teil stellt das *Cloud-Konzept* in den Mittelpunkt und zeigt Schritt für Schritt an einfachen Beispielen die Entwicklung Cloud-basierter Dienste und deren Zugriff über mobile Clients (Apps). Zudem werden erste Einblicke in aktuelle Trends wie *Mirco-Service-Architekturen* oder *Containerisierung* gegeben.

Die begleitende Übung bietet die Gelegenheit, aktuelle Technologien anhand einfacher Beispiele kennen zu lernen und erste praktische Erfahrung im Umgang mit Middleware und mobilen, Cloud-basierten Anwendungen zu sammeln.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Literatur

1. Alexander Schill, Thomas Springer: Verteilte Systeme, Springer Vieweg, 2012
2. Chris Britton, Peter Bye: IT Architectures and Middleware: Strategies for Building Large, Integrated Systems; Addison-Wesley, 2004
3. Dieter Masak: Moderne Enterprise Architekturen, Springer, 2005
4. Binildas Christudas: Practical Microservices Architectural Patterns, Apress, 2019
5. Die Beauftragte der Bundesregierung für Informationstechnik: SAGA-Modul Technische Spezifikationen, Version 5.0.0, 2011

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informationssystemen und stellen somit eine Grundlage für Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/ Cyber Sicherheit dar.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Ausgewählte Kapitel des OR: Data-driven Optimization	2994

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Juniorprof. Dr. rer. nat. Maximilian Moll	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
29941	VÜ	Ausgewählte Kapitel des Data-driven Optimization	Pflicht	3
29942	VÜ	Quantum Machine Learning & Optimization	Wahlpflicht	3
29943	SE	Seminar: Ausgewählte Kapitel des OR	Wahlpflicht	3
29944	P	Praktikum: Ausgewählte Kapitel des OR	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in Methoden des Operations Research und des Data Minings oder der Statistik werden vorausgesetzt.

Qualifikationsziele

Studierende sollen in die Lage versetzt werden, sich selbstständig mit neuartigen Methoden der data-driven Optimization in Theorie und Praxis auseinander zu setzen. Hierzu sollen sie im Rahmen der Vorlesung, sowie vertiefend in Seminar und Praktikum, verschiedene Methoden analysieren und anwenden.

Hierbei soll nicht nur die Fähigkeit entwickelt werden Ansätze auf ihre theoretische Richtigkeit und praktische Anwendbarkeit zu beurteilen, sondern diese auf ein Problem hin anpassen zu können.

Schließlich soll das Identifizieren geeigneter Probleme und passender Lösungsansätze geschult werden.

Inhalt

Data-driven Optimization beschäftigt sich zukunftsweisend mit der Kombination von klassischen Optimierungsmethoden und daten-basierten Ansätzen. Im Gegensatz zu der klassischen Optimierung der letzten Jahrhunderte, die ausgehend von einem zu optimierenden Modell eine Lösung sucht, bietet das Data-driven Optimization die Möglichkeit, ohne eine exakte mathematische Abstrahierung des zugrunde liegenden Modells Optimierungsmethoden anzuwenden.

Das Modul bietet aufbauend auf dem vorhandenen Grundwissen einen vertiefenden Einblick in ausgewählte Themengebiete des data-driven Optimization. Neben der grundlegenden Problematik werden Themen aus dem Reinforcement Learning, Prescriptive Analytics und der konvexen Optimierung unter Unsicherheit behandelt.

Das Reinforcement Learning ist neben Supervised und Unsupervised Learning das dritte Teilgebiet des Machine Learnings und beschäftigt sich mit daten-basierten Ansätzen zu Problemen der klassischen Kontrolltheorie. Hierbei soll im Modul auch die Anwendung auf praxis-relevante Probleme herausgestellt werden, die über die bekannten Lösungen von Spielen, wie z.B. Go, hinausgehen.

Prescriptive Analytics stellt aufbauend auf Descriptive und Predictive Analytics die nützlichste und schwerste Stufe des Data Science dar. Hier müssen nicht nur datan-basierte Vorhersagen getroffen werden, sondern das zukünftige System auf eine gegebene Zielvorstellung hin optimiert werden. In der Vorlesung werden verschiedene grundsätzliche Herangehensweisen mit ihren Vor- und Nachteilen diskutiert, sowie die Abgrenzung zu Predictive Analytics konkretisiert.

Die konvexe Optimierung stellt ein zentrales Element des Operations Research und der modernen Entscheidungsunterstützung dar. In vielen Fällen sind jedoch die Parameter der Optimierungsmodelle nicht explizit bekannt, sondern müssen zunächst aus Daten abgeleitet werden. Die Vorlesung thematisiert, wie sich dies auf die zu wählenden Optimierungsverfahren auswirken muss.

Das Seminar greift aktuelle Publikationen zu den Themen der Vorlesung auf.

Im Praktikum setzen sich die Studierenden mit einer konkreten, praxis-nahen Problemstellung des data-driven Optimization auseinander.

In der Vorlesung Quantum Machine Learning and Optimization wird spezifisch auf die Verwendung von Quantum Computern für effizientere Algorithmen im Kontext der NISQ-Maschinen eingegangen.

Im Praktikum werden die Studierenden an die Lösung eines konkreten RL-Problems unter praxis-nahen Bedingungen herangeführt. Hierfür wird Ihnen ein entsprechendes Environment gestellt. Während jeder Student sich mit einem anderen konkreten Algorithmus aus der Vorlesung beschäftigt, werden sie durch verschiedenen Arbeitsschritte geführt. Abschließend werden die Performances der verschiedenen trainierten Algorithmen verglichen – der Vergleich untereinander dient dabei als Teil der Lernerfahrung, nicht aber der Bewertung.

Literatur

- Sutton, Richard S., and Andrew G. Barto. *Reinforcement learning: An introduction.* MIT press, 2018.
- Jacquier, Antoine, et al.*Quantum Machine Learning and Optimisation in Finance: On the Road to Quantum Advantage*. Packt Publishing Ltd, 2022

Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
• Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfelder Software- und Informationsmanagement, Geoinformatik sowie Modellierung, Operations Research, Simulation und Experimentation, außerdem im Anwendungsfach Mathematik und Angewandte Systemwissenschaften • Wahlpflichtmodul im Masterstudiengang WIN, Vertiefungsfeld Technologie-und Innovationsmanagement • Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Enterprise Security, Public Security sowie Security Intelligence
Dauer und Häufigkeit
Das Modul dauert 2 Trimester. Es beginnt immer im Frühjahrstrimester.
Sonstige Bemerkungen
Zum Absolvieren des Moduls sind neben der Pflichtveranstaltung "Ausgewählte Kapitel des Data-driven Optimization" zwei der drei Wahlpflichtveranstaltungen zu belegen.

Modulname	Modulnummer
Anwendungsgebiete der Data Science	3852

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38521	VÜ	Sentiment Analysis	Wahlpflicht	3
38522	VÜ	Social Media Mining	Wahlpflicht	3
38523	VÜ	Semantische Technologien	Wahlpflicht	3
38524	PRO	Modulprojekt Anwendungsgebiete der Data Science	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Kenntnisse in Programmierung und Software-Entwurf sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Die Studierenden lernen Herausforderungen und Methoden beim Text Mining kennen und lernen die besprochenen Techniken anzuwenden. Zudem lernen sie theoretische Ansätze auf konkrete, praxisrelevante Fragestellungen zu übertragen. Für exemplarische Aufgabenstellungen können die Studierenden bestehende methodische Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen. Sie können begründet argumentieren und eine von ihnen selbständig gefundene Lösung vertreten und reflexiv bewerten.

Inhalt

- In der Vorlesung „Sentiment Analysis“ soll die schon umfangreiche Forschungsliteratur zum Opinion Mining aufgearbeitet werden. Dabei reichen die Ansätze von der Text- bis zur Wortebene, die Aufgaben sind das Erkennen von Subjektivität vs. Objektivität, das Bestimmen der Perspektive von Autoren, das Extrahieren ihrer Meinung. Datenquellen können Review-Seiten aus dem Internet sein, Blog-Posts und -kommentare, Nachrichten auf Twitter, gesprochene Sprache, usw.
- In der Vorlesung „Social Media Mining“ wird exemplarisch die Entwicklung eines Systems besprochen, welches über soziale Netzwerke direkt oder indirekt an Unternehmen adressierte Meldungen, Nachrichten oder Kommentare erfasst, klassifiziert und auswertet. Hierbei werden Textmining- und Klassifikationsverfahren mit Fokus auf Kurztexten diskutiert und der begleitenden Übung praktisch vertieft.

- Die Vorlesung „Semantische Technologien“ gibt einen Einblick in Grundlagen und praktische Anwendungen wissensbasierter Softewarelösung. Sie gibt einen breiten Überblick über den Nutzen und die Möglichkeiten dieser Technologien. Semantische Technologien versetzen uns nicht nur in die Lage, Informationen zu speichern und wiederzufinden, sondern sie gemäß ihrer Bedeutung und Funktion entsprechend auszuwerten, zu verbinden, zu Neuem zu verknüpfen und so flexibel und zielgerichtet anzuwenden.
- Im Modulprojekt setzen sich Studierende unter Anleitung selbständig mit Texten und Aufgaben zum Modulthema auseinander und präsentieren ihre Ergebnisse geeignet in mündlicher und/oder schriftlicher Form. Zu Beginn des Modulprojekts werden die geplanten Einzelthemen angekündigt und festgelegt, in welcher Form die Ergebnisse zu präsentieren sind.

Literatur

- Allan Ramsay, Tariq Ahmad: Machine Learning for Emotion Analysis in Python, Packt Publishing, 2023.
- Matthew A. Russell, Mikhail Klassen: Mining the Social Web, O'Reilly Media, 2019.
- Archana Patel, Narayan C. Debnath: Data Science with Semantic Technologies, CRC Press, 2023.
- Marc Wintjen: Practical Data Analysis Using Jupyter Notebook, Packt Publishing, 2020.

Leistungsnachweis

Portfolio: Mit gleichen Anteilen zu jeder der Vorlesungen (mit Übung) und im Modulprojekt. Die Studierenden können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder eine Vorlesung mit Übungen und ein Modulprojekt einbringen. Die geforderten Einzelleistungen sind wie folgt:

- 38521: Schriftliche Klausur von 60 Minuten oder Fachgespräch von 30 Minuten. Die Art der Leistung wird zu Beginn des Moduls bekannt gegeben.
- 38522: Schriftliche Klausur von 60 Minuten oder Fachgespräch von 30 Minuten. Die Art der Leistung wird zu Beginn des Moduls bekannt gegeben.
- 38523: Schriftliche Klausur von 60 Minuten oder Fachgespräch von 30 Minuten. Die Art der Leistung wird zu Beginn des Moduls bekannt gegeben.
- 38524: Bearbeitung eines Projektes mit schriftlicher Ausarbeitung, Bearbeitungszeit: 8 Wochen, Umfang 20 Seiten.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science.

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester und beginnt jedes Jahr im HT.

Sonstige Bemerkungen

Die Vorlesungen und das Praktikum werden nicht alle jedes Jahr angeboten, aber in jedem Jahr mindestens so viele Lehrveranstaltungen, dass 6 ECTS-Leistungspunkte

erreichbar sind. Jeweils zu Beginn des Moduls wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Analyse unstrukturierter Daten	3853

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38531	VÜ	Analyse unstrukturierter Daten	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Programmierkenntnisse sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Die Studierenden lernen Herausforderungen und Methoden bei der Informationsbeschaffung und -extraktion kennen und lernen die besprochenen Analyse-Methoden anzuwenden. Sie lernen Verfahren der Analyse unstrukturierter Daten auf konkrete, praxisrelevante Fragestellungen (insb. im Bereich Wissensgewinnung) anzuwenden und können für exemplarische Aufgabenstellungen existierende Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen.

Inhalt

Dieses Modul gibt einen Einblick in die Herausforderungen und Verfahren, die bei der Analyse unstrukturierter Daten zum Einsatz kommen. Unstrukturierte Informationen sind in der Regel sehr textlastig, weshalb viele vorhersagende Analyse-Verfahren den Informationswert dieser Daten nicht nutzen können. Allerdings können textbasierte Medien (E-Mails, Webseiten-Inhalte, Fachartikel, Social Media Beiträge, etc.) u. a. dabei helfen, Trends zu erkennen, Wissen zu gewinnen und Fake News aufzudecken. Hierfür müssen Informationen identifiziert, extrahiert, aufbereitet und interpretiert werden. Die Herausforderung besteht darin, relevante Informationen zu erkennen, aus unstrukturierten Texten zu extrahieren und fehlende Informationen ggf. hinzufügen.

In der Veranstaltung werden auch Themen wie die Informationsgewinnung aus unterschiedlichen Quellen sowie Fragen der Qualitätssicherung bei der Datenspeicherung und des Datenmanagements in wissensbasierten Strukturen behandelt.

In der Übung werden theoretische und praktische Fragestellungen gleichermaßen adressiert. Der theoretische Teil dient zur Wiederholung der Vorlesungsinhalte. Im

praktischen Teil sind die Studierenden aufgefordert, ausgewählte Verfahren zur Analyse unstrukturierter Daten eigenständig zu implementieren. Für die Übungen sind Programmierkenntnisse erforderlich.

Literatur

- Soumen Chakrabarti: Mining the Web, Morgan Kaufmann, 2002.
- Henning Wachsmuth:Text Analysis Pipelines: Towards Ad-hoc Large-Scale Text Mining (Lecture Notes in Computer Science, Band 9383), Springer Verlag, 2015.
- Nikos Tsourakis: Machine Learning Techniques for Text, Packt Publishing, 2022.
- Anish Chapagain: Hands-On Web Scraping with Python, 2. Auflage, Packt Publishing, 2023.

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science mit Fokus auf die Analyse unstrukturierter Daten.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Post-Quantum Cryptography	3931

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
39311	VÜ	Introduction to Post-Quantum Cryptography	Pflicht	4
39312	VÜ	Selected Topics in Post-Quantum Cryptography	Pflicht	4
39313	SE	Post-Quantum Cryptography in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Grundkenntnisse in Mathematik (Diskrete Strukturen, Lineare Algebra, Wahrscheinlichkeitstheorie) und in Informatik (Algorithmenentwurf und -analyse) sowie in der Kryptographie (Basiskonzepte) vorausgesetzt. Notwendige (minimale) Grundlagen des Quantencomputings werden in den Lehrveranstaltungen eingeführt.

Qualifikationsziele

Die Studierenden kennen den Einfluss von Quantencomputern auf die Kryptographie (Shor, Grover) und deren Implikationen. Sie kennen quantenresistente mathematische Problemklassen, deren Sicherheit und Verwendung dieser zur Konstruktion kryptographischer Basismechnismen. Die Studierenden kennen Designprinzipien von aktuellen Post-Quanten Verfahren und deren Funktionsweise und haben einen Einblick in die aktuellen praktischen und theoretischen Herausforderungen der Post-Quanten Kryptographie. Sie sind in der Lage kryptographische Verfahren zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um die Post-Quanten Kryptographie und ihre Anwendungen.

Inhalt

Introduction to Post-Quantum Cryptography - In dieser Vorlesung werden die Gundlagen der Post-Quanten (oder quantensicheren) Kryptographie behandelt.
Es wird die Notwendigkeit der Neubetrachtung der Kryptographie aufgrund von Quantencomputern und relevanter Quantenalgorithmen (Shor, Grover) sowohl im Kontext symmetrischer als auch asymmetrischer Kryptographie diskutiert. Danach werden die Unterschiede zwischen klassischen Angreifern und Quantenangreifern sowie die Auswirkungen auf die beweisbare Sicherheit veranschaulicht. Der Hauptteil

der Vorlesung umfasst dann einen Überblick über relevante Klassen mathematischer Probleme die zur Konstruktion quantensicherer Kryptographie herangezogen werden. Dies umfasst hash-basierte Signaturen, multivariate Kryptographie, Kryptographie basierend auf fehlerkorrigierenden Codes, gitterbasierte Kryptographie sowie isogeniebasierte Kryptographie. In den Übungen werden die Kenntnisse aus der Vorlesung vertieft sowie konkrete Beispiele und Beweise betrachtet.

Selected Topics in Post-Quantum Cryptography - In dieser Vorlesung werden zuerst, aufbauend auf den in der ersten Vorlesung erarbeiteten Grundlagen, moderne Konstruktionsprinzipien aktueller beweisbar sicherer quantenresistenter kryprographischer Basismechanismen (asymmetrische Verschlüsselung bzw. KEMs und Signaturen) betrachtet. Dies umfasst sowohl generische Prinzipien wie auch spezifische Aspekte für ausgewählte Verfahren verschiedener Problemklassen. Danach werden ausgewählte und aktuell relevante Themen aus dem Bereich der Post-Quanten Kryptographie betrachtet: Dies umfasst sowohl praktische als auch theoretisch und stärker forschungsbezogene Aspekte. Beispielsweise die Standardisierung von und Migration zu Post-Quanten Kryptographie (z.B. Hybridisierung), die Integration von Post-Quanten Kryptographie (in Sicherheitsprotokolle oder aktuelle Anwendungen) wie auch die Konstruktion fortgeschrittener kryptographischer Verfahren basierend auf Post-Quanten Annahmen und damit in Verbindung stehende Herausforderungen. In den Übungen werden die Kenntnisse aus der Vorlsung vertieft sowie konkrete Beispiele und Beweise betrachtet.

Post-Quantum Cryptography in Practice - In diesem praxisorientierten Seminar geht es um den praktischen Einsatz von quantensicheren kryptographischen Verfahren.
In Bezug auf das ausgewählte Thema wird von den Studierenden eine weitgehend selbständig gefertigte prototypische Umsetzung eines Miniprojektes unter Verwendung von geeigneten open-source Softwarebibliotheken bzw. Technologien erwartet. Die Ergebnisse der Implementierungsarbeit sollen dann in einem Bericht beschrieben und während der Präsentation demonstriert werden.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen können zum Teil auch in englischer Sprache gehalten werden.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio:

Zu den Vorlesungen mit Übungen: ein mündliches Fachgespräch von 30 Minuten oder eine schriftliche Klausur von 60 Minuten über die Inhalte aus beiden Veranstaltungen; die Form des Leistungsnachweises wird zu Beginn des Moduls festgelegt.

Zum Seminar: Erstellung und Abgabe einer Präsentation zur Demonstration von Ergebnissen des Miniprojektes (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.
Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfelder Enterprise Security, Public Security, Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im Frühjahrstrimester.

Modulname	Modulnummer
Privacy Preserving Machine Learning	4213

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
42131	VL	Privacy Preserving Machine Learning	Pflicht	4
42132	SE	Selected topics in Privacy Preserving Machine Learning	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Grundkenntnisse in den Bereichen Machine Learning, Kryptologie, Datenschutz und Privacy. Gute Programmierkenntnisse (Python).

Qualifikationsziele
Vorlesung: Die Studierenden lernen und können die mathematische Definition von differential privacy verstehen und ihre wichtigsten Eigenschaften analysieren. Darüber hinaus werden Sie wichtige algorithmische Werkzeuge für die private Beantwortung einfacher numerischer und nicht-numerischer Abfragen kennenlernen, sowie ihre Garantien für den Schutz der Privatsphäre. Diese Mechanismen dienen als Bausteine zur Konstruktion privater Algorithmen für maschinelles Lernen. Wir werden uns insbesondere auf die private empirische Risikominimierung mit Techniken konzentrieren. Schließlich werden wir das dezentralisierte Modell der differentiellen Privatsphäre betrachten. Die Studierenden können am Ende verschiedene Ansätze vergleichen, ihre Vorteile und Nachteile besprechen, und entscheiden, welches der beste Ansatz zur Bewältigung der anstehenden Herausforderungen ist. Seminar: Die Studierenden können aktuelle differential privacy und federated learning Architekturen implementieren und evaluieren. Die Studierenden sind in der Lage, aktuelle Herausforderungen des datenschutzgerechten maschinellen Lernens zu verstehen, zu analysieren, zu evaluieren und zu diskutieren, um neue Lösungen zu finden. Darüber hinaus können sie fachliche Literatur und aktuelle Veröffentlichungen recherchieren, um Methoden zu finden, welche ihnen bei der Entwicklung neuer Lösungen helfen können. Die Studierenden können ihre Arbeit im Team präsentieren und Herausforderungen

diskutieren. Des Weiteren können die Studierenden Fragen zu den anderen Vorträgen formulieren und mit Ideen beitragen, um die Herausforderungen zusammen zu lösen.

Inhalt

Vorlesung:

- Einführung in differential privacy
- Der exponentielle Mechanismus & erweiterte Komposition
- Differentiell private empirische Risikominimierung
- Differentiell privater stochastischer Gradientenabstieg
- Federated learning

Seminar:

Die Studierenden wählen ein Projekt aus der Liste der angebotenen Projekte aus. Am Ende des Trimesters sollten die Studierenden eine Ausarbeitung und ggf. Code abliefern und ihre Arbeit in einer 20- bis 40-minütigen Präsentation (inkl. Q&A-Slot) vorstellen.

Literatur

- C. Dwork and A. Roth, The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, 2014
- K. Nissim et al., Differential Privacy: A Primer for a Non-technical Audience, Journal of Entertainment & Technology Law, 2018
- S. Vadhan, The Complexity of Differential Privacy, Tutorials on the Foundations of Cryptography, 2017
- P. Kairouz et al., Advances and Open Problems in Federated Learning, 2019

Leistungsnachweis

Portfolio: Zur Vorlesung ein 60-minütige schriftliche Klausur und zum Seminar eine Ausarbeitung (6 bis 10 Seiten), ggf. Code und eine 20- bis 40-minütige Präsentation (inkl Q&A-Slot). Die Bearbeitungsdauer für die Ausarbeitung und die Vorbereitung der Präsentation beträgt 4 bis 6 Wochen. Die Leistungen in der Klausur und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit und Kryptograhie, und vermitteln tiefes Verständnis von modernen Verfahren des Schutzes der Privatsphäre. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet des Schutzes der Privatsphäre durch biometrische Systeme.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Foundations of Distributed Systems and Blockchains	5118

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
51181	VÜ	Foundations of Distributed Systems and Blockchains	Pflicht	4
51182	SE	Research Topics in Security for Decentralized Systems	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Grundkenntnisse in Mathematik (Diskrete Strukturen, Lineare Algebra, Wahrscheinlichkeitstheorie) und in Informatik (Algorithmenentwurf und -analyse) vorausgesetzt. Basiswissen in der Kryptographie (Basiskonzepte) ist hilfreich, aber nicht notwendig (alle verwendeten Konzepte werden im Modul eingeführt).

Qualifikationsziele

Die Studierenden kennen grundlegende Konzepte in dezentralen Systemen (z.B. Fehlertoleranz und Konsensus) und lernen grundlegende kryptographische Mechanismen kennen, die zur Realisierung dieser Eigenschaften notwendig sind (z.B. Hashfunktionen, MACs und Signaturen). Diese Konzepte werden dann anhand von Blockchains und Kryptowährungen betrachtet und es werden weitere wichtige Konzepte im Kontext von Blockchains eingeführt (z.B. Proof-of-Work, Proof-of-Stake, Proof-of-Space). Die Studierenden lernen relevante kryptographische Mechanismen wie das Generieren von verteilten und verifizierbaren Zufallszahlen sowie das Feld der Threshold-Kryptographie und deren Anwendungen kennen. Darüber hinaus bekommen die Studierenden einen Einblick in Privatheits- und Skalierungsprobleme in Blockchains sowie in kryptographische Konzepte, mit denen diese Probleme gelöst werden können. Im Speziellen wird das Konzept des Verifiable Computing und so genannter Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) behandelt. Studierende sind in der Lage Herausforderungen in dezentralen Systemen (im Speziellen Blockchains) zu erkennen und zu analysieren sowie die Einsatzmöglichkeiten relevanter kryptographischer Mechanismen zur Lösung dieser Herausforderungen zu verstehen. Darüber hinaus kennen die Studierenden den aktuellen Stand der Forschung in diesem Feld.

Inhalt

Foundations of Distributed Systems and Blockchains - In dieser Vorlesung werden die Grundlagen von dezentralen Systemen sowie in diesem Kontext relevanter Kryptographie behandelt. Ein Schwerpunkt der Vorlesung liegt auf Blockchains und Kryptowährungen, insbesondere auf deren Grundlagen und Funktionsweise. Hier werden Mechanismen wie Proof-of-Work, Proof-of-Stake sowie Proof-of Space, Transaktionen sowie notwendige kryptographische Mechanismen (z.B. Merkle Trees) und deren Abstraktionen und Varianten behandelt. Es wird auch die Unveränderlichkeit von Blockchains kritisch hinterfragt und Konzepte zur „Aufweichung“ dieser Eigenschaft werden präsentiert. Als wichtiges kryptographisches Konzept wird die so genannte Threshold-Kryptographie eingeführt, die es ermöglicht kryptographische Funktionalität (z.B. das Erstellen einer Signatur) auf mehrere Parteien zu verteilen. Als verwandtes Thema wird auch die verteilte und verifizierbare Erzeugung von Zufallszahlen behandelt. Bei all diesen kryptographischen Konzepten wird immer der Bezug zu Anwendungen im Blockchain-Kontext veranschaulicht. Als ein weiteres wichtiges Konzept wird so genanntes Verifiable Computing und so genannte Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) behandelt. Diese Techniken ermöglichen das Lösen von Skalierbarkeits- und Privatheitsproblemen in Blockchains. In den Übungen werden die Kenntnisse aus der Vorlesung vertieft sowie konkrete Beispiele betrachtet.

Research Topics in Security for Decentralized Systems - In diesem Seminar bekommen Studierende einen Einblick in aktuelle Forschungsthemen an der Schnittstelle zwischen dezentralen Systemen und Sicherheit mit Fokus auf Einsatz von Kryptographie. Die Schwerpunkte liegen auf neuen kryptographischen Verfahren und Konzepten sowie deren Anwendungen in dezentralen Systemen und Blockchains im Speziellen. Zu Beginn des Seminars wird eine Themenauswahl vorgestellt, die von Studierenden über die Dauer des Seminars bearbeitet und am Ende präsentiert werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikel aus führenden wissenschaftlichen Konferenzen stützen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Vorlesung wird in deutscher Sprache gehalten, Teile der Übungen und des Seminars können auch in englischer Sprache gehalten werden.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen:

51181: Ein mündliches Fachgespräch von 20 Minuten oder eine schriftliche Klausur von 45 Minuten; die Form des Leistungsnachweises wird zu Beginn des Moduls festgelegt.

In 51182: Erstellung und Abgabe einer schriftlichen Ausarbeitung (10 bis 20 Seiten) und eine Präsentation (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfelder Enterprise Security, Public Security, Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und beginnt jedes Jahr in WT. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Mobile Security	5513

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gabi Dreo Rodosek	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11972	VÜ	Mobile Kommunikationssysteme	Pflicht	3
55131	VÜ	Sichere mobile Systeme	Wahlpflicht	3
55132	VÜ	Sensorik und Manipulationsdetektion	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für die Veranstaltungen im Modul werden grundlegende Kenntnisse in Rechnernetzen vorausgesetzt, wie sie z.B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten ein umfassendes Wissen der Funktionsweise mobiler Kommunikationsnetze. Sie können die wichtigsten Grundlagen drahtloser Kommunikationstechniken erläutern und die verschiedenen Verfahren und Systeme kategorisieren. Je nach erfolgter Auswahl innerhalb des Moduls haben sie vertiefte Kenntnisse in Bezug auf die Sicherheitsaspekte der Übertragungswege oder der Hardware-Komponenten. Sie sind in der Lage, die Wirksamkeit von Sicherheitsmaßnahmen einzuordnen und Sicherheitseigenschaften von mobilen Kommunikationssystemen zu bewerten. Sie erhalten eine erste Orientierung zum Vorgehen bei der Absicherung von mobilen Systemen durch Auswahl der Technologie und Konfiguration des Systems und den Einsatz spezieller Sicherheitsmechanismen.

Inhalt

Die **Pflichtveranstaltung** behandelt die wesentlichen Techniken zur Realisierung von mobiler (drahtloser) Kommunikation mit dem Schwerpunkt auf IT-Systemen. Dazu gehören die Funkübertragungstechniken, insbesondere die zellenbasierten Funksysteme, die Medienzugriffsverfahren, die die gemeinsame Nutzung des Funkraums koordinieren (Multiplexverfahren, Kollisionserkennung und -vermeidung), und die mobilen Varianten der Vermittlungsschicht (mobile IP, ad-hoc networking, Routingverfahren) und der Transportschicht (flow control, quality of service). Daneben werden die verschiedenen Arten der verwendeten mobilen Kommunikationssysteme vorgestellt: Drahtlose Telekommunikationssysteme (u.a. GSM, UMTS, LTE), Satellitensysteme, Rundfunksysteme (DAB, DVB) und drahtlose lokale Netze (u.a. WLAN, Bluetooth).

In der Wahlpflichtveranstaltung „**Sichere Mobile Systeme**“ werden zum einen verschiedene Kommunikationsstandards (u.a. WLAN, Bluetooth, und IEEE 802.15.4) vorgestellt, die im Bereich IoT ihren Einsatz finden, welche Einschränkungen sie haben und welche Sicherheitsaspekte sie erfüllen. Zum anderen werden konkrete Anwendungen wie elektronische Ausweise und mobiles Bezahlen näher betrachtet. Als Basisliteratur wird auf diverse Standarddokumente (u.a. vom BSI und IETF) verwiesen sowie auf das Buch von J. Schiller Mobilkommunikation, ISBN: 978-3827370600.

Ergänzend zu den Grundlagen werden in der Vorlesung **Sensorik und Manipulationsdetektion** Algorithmen, Protokolle und Paradigmen für den Einsatz von Sensornetzen sowie deren Absicherung vorgestellt. Dabei werden Konzepte wie etwa Lokalisierung, Zeitsynchronisation und datenzentrische Ansätze betrachtet sowie Lösungen für System-Software, Aggregation, Routing und Datenverteilung aus der Perspektive von Sensornetzen betrachtet. Ferner behandelt die Vorlesung Grundlagen, Systeme und Verfahren zur Detektion von Manipulationen. Dies beinhaltet die gesicherte Informationsübertragung in verteilten Systemen sowie die Bestätigung und Überprüfung von detektierten Ereignissen durch verschiedene Methoden.

Literatur

Literatur zur Lehrveranstaltung "Sichere mobile Systeme":

- J. Schiller: Mobilkommunikation, ISBN: 978-3827370600

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 20 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Public Security und Cyber Network Capabilities

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Staatliche IT-Sicherheit	5514

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Ulrike Lechner	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55141	VÜ	Schutz von kritischen Infrastrukturen	Pflicht	3
55144	SE	Internationale Sicherheitsarchitekturen und Krisenmanagement im Cyberraum	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Allgemeinwissen in Themen der IT-Sicherheit und zu IT-Sicherheitsmaßnahmen, so wie es in einem Bachelorstudiengang Informatik oder Wirtschaftsinformatik vermittelt wird.

Qualifikationsziele

- Studierende kennen Sicherheitsarchitekturen national und international mit wesentlichen Akteuren
- Studierende kennen gesetzliche Grundlagen, Normen und Standards der IT-Sicherheit Kritischer Infrastrukturen
- Studierende kennen IT-Sicherheitsmaßnahmen für Kritische Infrastrukturen, die Technik, Mensch und Organisation adressieren
- Studierende kennen Verfahren, IT-Sicherheitsmaßnahmen zu konzipieren und umzusetzen.

Inhalt

Die Veranstaltung „Schutz von Kritischen Infrastrukturen“ thematisiert gesetzliche Grundlagen der IT-Sicherheit Kritischer Infrastrukturen und die Umsetzung der gesetzlichen Forderungen in den verschiedenen Sektoren der Kritischen Infrastrukturen. Eine Fallstudienserie zu IT-Sicherheit Kritischer Infrastrukturen sowie konkrete Anwendungsbeispiele aus den Sektoren Kritischer Infrastrukturen stellen den Kern der Veranstaltung dar. Studierende lernen sowohl anhand von Fallbeispielen als auch anhand von Rahmenwerken wie den BSI IT-Grundschutz-Katalogen IT-Sicherheitsmaßnahmen kennen. Sie lernen Verfahren kennen, IT-Sicherheitsmaßnahmen für Kritische Infrastrukturen zu konzipieren, umzusetzen sowie zu evaluieren.

In der Veranstaltung „Internationale Sicherheitsarchitekturen und Krisenmanagement im Cyberraum“ stehen Cyber-Bedrohungen und Cyber-Angriffe, Modus Operandi der Täter und Cyber-Krisenmanagement für Unternehmen sowie staatlichen Konflikten

im Vordergrund. Dabei wird die bestehenden Cyber und IT-Sicherheitsarchitektur Deutschlands und Europas, die zugrunde liegenden Gesetzgebungen und zuständigen Behörden auf deutscher und europäischer Ebene sowie Strukturen, Prozesse, Rollen und Aufgaben eines Cyber-Krisenstabs beleuchtet. Anhand einer strategischen Cyber-Simulationsübung wird aufgezeigt, wie sich Cyberkrisen auswirken und wie diese effektiv bearbeitet werden können.

Am Ende des Seminars sind die Studierenden in der der Lage zu beurteilen, welche Arten von Cyber-Angriffen für welche übergeordneten Ziele angewandt werden, welche Tätergruppen es gibt und welche strategischen, organisatorischen und technischen Maßnahmen getroffen werden sollten, um die Unternehmenskrise nach einem erfolgreichen Cyber-Angriff zu vermeiden.

Literatur

- Ulrike Lechner, Sebastian Dännart, Andreas Rieb, Steffi Rudel. Case Kritis - Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen, Logos-Verlag. 2018.
- Michael Bartsch, Stefanie Frey. Cyberstrategien für Unternehmen und Behörden. Springer Vieweg, January 2017.
- Michael Bartsch, Stefanie Frey. Cybersecurity Best Practices. Springer Fachmedien Wiesbaden, July 2018.
- Thomas Rid. Cyber War Will Not Take Place. C. Hurst & Co Publishers Ltd, April 2013.

Leistungsnachweis

Portfolio mit Bearbeitung eines Praxisproblems in Gruppenarbeit zur Sicherheit Kritischer Infrastrukturen mit Ausarbeitung von 10 bis 20 Seiten und Präsentation von 15 bis 30 Minuten sowie Bearbeitung eines Praxisproblems in Gruppenarbeit zum Krisenmanagement mit Ausarbeitung von 10 bis 20 Seiten und Präsentation von 15 bis 30 Minuten. Die Bearbeitungszeit beträgt in beiden Fällen jeweils 8 bis 16 Wochen. In die Noten gehen die Bearbeitung eines Praxisproblems zur Sicherheit Kritischer Infrastrukturen und die Bearbeitung eines Praxisproblems zum Krisenmanagement jeweils zu 50% ein.

Verwendbarkeit

- Wahlpflichtmodul im Masterstudiengang WIN, Vertiefungsfeld Technologie- und Innovationsmanagement
- Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfeld Public Security

Dauer und Häufigkeit

Das Modul dauert 2 oder 3 Trimester, je nachdem, welche der beiden Lehrveranstaltungen zuerst besucht wird.

Modulname	Modulnummer
Modern Cryptography	5548

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Manulis	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55481	VÜ	Modern Cryptography	Pflicht	4
55482	SE	Seminar Research Trends in Cryptography	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende mathematischen Kenntnisse sowie ein generelles Interesse an moderner Kryptographie vorausgesetzt.

Qualifikationsziele

Die Studierenden kennen Designprinzipien und Funktionsweise von modernen kryptographischen Verfahren und Protokollen und beherrschen den Umgang mit entsprechender Sicherheitsmodellierung und -beweisführung. Sie sind in der Lage kryptographische Verfahren zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um Kryptographie und ihren Anwendungen.

Inhalt

- **Modern Cryptography** - In dieser Vorlesung werden moderne Methoden der Kryptographie sowie weiterführende kryptographische Verfahren und Protokolle detailliert vorgestellt und analysiert. Neben der allgemeinen Funktionsweise wird auf die Sicherheitsmodellierung und beweisbare Sicherheit eingegangen. Dazu werden, z.B., moderne Beweisführungsmethoden wie kryptographische Reduktionen eingeführt. Zu den Themen der Veranstaltung gehören unterschiedliche kryptographische Funktionalitäten, darunter Einwegfunktionen, Pseudozufallszahlengeneratoren, Hashfunktionen, Blockchiffren, message authentication codes, digitale Signaturen und Verschlüsselungsverfahren, sowie weiterführende Techniken wie Identifikationsverfahren und zero-knowledge Beweise. Neben den weit verbreiteten auf diskreten Logarithmen oder Integer Faktorisierung basierenden Verfahren, werden weitere Konstruktionen vorgestellt, die mittels elliptischen Kurven und bilinearen Abbildungen aufgebaut sind. Die nötigen mathematischen Grundlagen für diese Verfahren werden im Rahmen der Veranstaltung eingeführt. In Übungen werden die Methoden der beweisbaren

Sicherheit sowie die Funktionsweise von eingeführten Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.
- **Research Trends in Cryptography** - In diesem Seminar bekommen Studierende ein Einblick in aktuelle Forschungsfelder der Kryptographie. Die Schwerpunkte liegen bei neuen kryptographischen Konzepten, Methoden, Verfahren und Protokollen sowie bei deren Implementierung, Standardisierung und Anwendungen. Zu Beginn der Veranstaltung wird eine Auswahlliste von aktuellen Themen vorgestellt, die von Studierenden über die Dauer der Veranstaltung ausgearbeitet und am Ende vorgestellt werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikel (aus bekannten Tagungen) und Open-Source Quellen (z.B. Softwarebibliotheken, Standards) stützen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Katz, J. and Lindell, Y. Introduction to Modern Cryptography (2nd Edition), Chapman & Hall/CRC Cryptography and Network Security Series, 2014.

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen:

55481 VÜ Modern Cryptography: mündliches Fachgespräch von 20 Minuten,

55482 Seminar Research Trends in Cryptography: Erstellung und Abgabe einer schriftlichen Ausarbeitung (10 bis 20 Seiten) und eine Präsentation (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten vermitteln tiefes Verständnis von modernen kryptographischen Methoden und Verfahren. Die Veranstaltungen fördern analytisches Denken und entwickeln Fähigkeiten kryptographische Verfahren unter Verwendung von Security-by-Design Prinzipien zu entwerfen und zu analysieren sowie deren Einsatz in Anwendungen zu planen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet der Kryptographie und dient als gute Vorbereitung für weiterführende Lehrveranstaltungen rund um Kryptographie und ihren Anwendungen zum Schutz der Datensicherheit und Privatheit, etwa im Rahmen des Moduls „Privacy Enhancing Cryptography“.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird im WT angeboten. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Privacy Enhancing Cryptography	5563

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Manulis	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55631	VÜ	Private Data Processing	Pflicht	4
55632	VÜ	Private Authentication and Messaging	Pflicht	4
5563-V3	SE	Privacy Enhancing Cryptography in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende Kenntnisse in moderner Kryptographie sowie ein generelles Interesse am Einsatz von kryptographischen Verfahren und Protokollen zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern vorausgesetzt. Eine vorherige Teilnahme am Modul „Modern Cryptography“ ist wünschenswert, stellt jedoch keine formale Voraussetzung dar.

Qualifikationsziele

Die Studierenden kennen Designprinzipien und Funktionsweise von verschiedenen Verfahren und Protokollen zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern unter Verwendung von modernen kryptographischen Methoden. Sie sind in der Lage die kryptographische Lösungen kritisch zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um Privacy Enhancing Cryptography und entsprechenden Anwendungen.

Inhalt

- **Private Data Processing:** In dieser Vorlesung werden kryptographische Protokolle vorgestellt, mit deren Hilfe vertrauliche Daten durch eine oder mehrere Parteien verarbeitet werden können. Dabei geht es um Operationen auf numerischen und binären Daten sowie sichere Berechnungen von Funktionen zum Einsatz in diversen Anwendungsfällen, welche die Vertraulichkeit von verwendeten Eingabedaten während ihrer Verarbeitung erfordern. Es werden Szenarien kooperativer Datenverarbeitung unter zwei oder mehreren Teilnehmern sowie Operationen auf ausgelagerten (etwa in eine Cloud) Daten betrachtet. Themen der Vorlesung sind, u.a. secret sharing and threshold cryptography, Varianten von oblivious transfer, (fully) homomorphic encryption, secure two-party und multi-party computation, private function evaluation, private set intersection, private information

retrieval, secure data aggregation und searchable encryption. In Übungen wird die Funktionsweise und Sicherheit von Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.

- **Private Authentication and Messaging:** In dieser Vorlesung werden Privatsphäre schützende kryptographischen Verfahren und Protokolle zur sicheren Authentisierung und Nachrichtenaustausch vorgestellt. Im Fokus stehen solche Schutzziele wie Anonymität, Unverlinkbarkeit und Abstreitbarkeit, gekoppelt an die klassischen Sicherheitsziele einer Authentisierung bzw. Ende-zu-Ende-Verschlüsselung. Es werden Verfahren vorgestellt, die solche Schutzziele in zwei- sowie mehr-Parteien Anwendungen ermöglichen. Themen der Vorlesung sind, u.a., (multi-party) key exchange und secure messaging (inkl. Signal protocol, MLS), secret handshakes, anonymous communication (inkl. mix networks, onion routing), privacy-preserving signatures (inkl. ring und group signatures) sowie anonymous credentials.
- **Privacy Enhancing Cryptography in Practice:** In diesem praxisorientierten Seminar geht es um die Implementierung und praktische Verwendung von modernen kryptographischen Verfahren und Technologien zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern. In Bezug auf das ausgewählte Thema wird von den Studierenden eine weitgehend selbständig gefertigte prototypische Umsetzung eines Miniprojektes unter Verwendung von geeigneten open-source Softwarebibliotheken bzw. Technologien erwartet. Die Ergebnisse der Implementierungsarbeit sollen dann in einem Bericht beschrieben und während der Präsentation demonstriert werden. Mögliche Themen umfassen: homomorphic encryption, secure two- and multi-party computation, private information retrieval, searchable encryption, zero-knowledge proofs, distributed cryptography, attribute-based cryptography, secure messaging, privacy-preserving authentication, anonymous communication, usw.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio:

Zu 55631 und 55632: ein mündliches Fachgespräch von 30 Minuten über die Inhalte aus beiden Veranstaltungen,

In 55633: Erstellung und Abgabe einer Präsentation zur Demonstration von Ergebnissen des Miniprojektes (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 90 zu 10 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit um die wichtigen technologischen Aspekte der Privatheit und entsprechenden kryptographischen Methoden und Verfahren. Die Veranstaltungen vermitteln die

Fähigkeiten technische Verfahren zum Schutz der Daten und Privatheit zu entwerfen und ihr Einsatz in digitalen Anwendungen zu ermöglichen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Überschneidungsbereich des technologischen Privacy- und Datenschutzes und angewandter Kryptographie.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr in FT. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Analytische Modelle	1032

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Markus Siegle	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10321	VÜ	Quantitative Modelle	Pflicht	5
10322	VÜ	Verlässliche Systeme	Wahlpflicht	3
10323	VÜ	Zuverlässigkeitstheorie	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Wahrscheinlichkeitsrechnung auf Bachelor-Niveau wird vorausgesetzt. Voraussetzung ist ferner eine Vertrautheit mit Grundlagen der Architektur und des Entwurfs von Rechen- und Kommunikationssystemen.

Qualifikationsziele

Die Studierenden lernen, ein existierendes oder geplantes reales System auf ein Modell abzubilden und anhand des Modells Aussagen über die zu erwartende Leistungsfähigkeit und/oder Zuverlässigkeit zu machen. Sie werden in die Lage versetzt, die Zusammenhänge zwischen den diversen Parametern eines Systems und den zu erwartenden Leistungs- und Zuverlässigkeitskenngrößen zu verstehen. Die Studierenden sollten nach erfolgreicher Teilnahme an diesem Modul in der Lage sein, (Rechner-)Systeme performanter und verlässlicher zu entwerfen, bzw. existierende Systeme bezüglich Performance und Verlässlichkeit bewerten zu können.

Inhalt

Neben der Frage, ob ein Rechen- oder Kommunikationssystem seine funktionalen Anforderungen korrekt und vollständig erfüllt, spielt die Frage nach der Leistungsfähigkeit und Zuverlässigkeit des Systems eine zentrale Rolle. Modelle mit stochastischem Charakter sind ein wichtiges Hilfsmittel für die Leistungs- und Zuverlässigkeitsbewertung von Systemen.

In diesem Modul werden die Grundlagen solcher Modelle und ihrer quantitativen Analyse behandelt. Im Pflichtteil "Quantitative Modelle" werden einfache stochastische Prozesse, insbesondere Markov-Prozesse mit diskretem oder stetigem Zeitparameter eingeführt. Es werden wichtige Leistungs- und Zuverlässigkeitskenngrößen definiert und bestimmt. Wichtige Gesetzmäßigkeiten, wie das Gesetz von Little, werden erläutert. Es werden unterschiedliche Typen von Bediensystemen betrachtet, und schließlich verschiedene

Verfahren für die Analyse von Warteschlangennetzen und die numerische Analyse von Markovketten vorgestellt.

Die Wahlpflicht-Lehrveranstaltung "Verlässliche Systeme" fokussiert insbesondere auf Fehlertoleranz-Methoden und deren Bewertung zur Erhöhung der Systemzuverlässigkeit solcher Systeme. Neben zentralen Begrifflichkeiten werden Modellierungsmethoden wie Fehlerbäume, Zuverlässigkeitsblockdiagramme und Markov-Modelle für Systeme mit und ohne Reparaturen thematisiert.

In der alternativen Wahlpflicht-Lehrveranstaltung "Zuverlässigkeitstheorie" werden strukturelle Eigenschaften kohärenter Systeme betrachtet, d.h. die Funktionstüchtigkeit des Systems wird in Beziehung zur Funktionstüchtigkeit seiner Komponenten gesetzt. Die Studierenden lernen Methoden und Ansätze kennen, mit denen z.B. das Ausfall- und Überlebensverhalten von einzelnen Bauteilen oder Geräten (die als ein vernetztes System von Bauteilen aufgefasst werden können) modelliert und analysiert werden können.

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Angesichts der hohen Leistungs- und Zuverlässigkeitsanforderungen an informationsverarbeitende Systeme in den unterschiedlichsten Anwendungsbereichen (z.B. verteilte eingebettete Systeme, Prozesssteuerungen, sicherheitskritische Systeme, Workflow-Systeme oder paralleles wissenschaftliches Rechnen) bilden die erworbenen Kenntnisse einen wichtigen Bestandteil der Ausbildung von Informatikern.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Frühjahrstrimester.
Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Sonstige Bemerkungen

In diesem Modul ist neben der Pflichtveranstaltung (mit Übung) eine der beiden Wahlpflichtveranstaltungen (mit Übung) zu wählen.

Modulname	Modulnummer
Informations- und Codierungstheorie	1037

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Peter Hertling	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
1037	VÜ	Informations- und Codierungstheorie	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Es werden Grundkenntnisse in Analysis, linearer Algebra und Wahrscheinlichkeitstheorie vorausgesetzt.

Qualifikationsziele

Die Studierenden lernen einerseits grundlegende theoretische Begriffe zur Übertragung von Information durch einen Bitstrom kennen, sowie prinzipielle Grenzen der Informationsübertragung.

Andererseits lernen sie wichtige Codierungsmethoden kennen, die in der digitalen elektronischen Datenübertragung verwendet werden. Sie lernen zu beurteilen, welche Codierungsmethoden in welcher Situation vorzuziehen sind. Außerdem sollen sie selbst Algorithmen zur Codierung und Decodierung (auch Fehlerkorrektur) implementieren können.

Inhalt

Grundlegende Fragen der Informationsverarbeitung sind, wieviel Information man in einen Bitstrom hineincodieren kann und wieviel Information man durch das Senden eines Bitstroms in einer bestimmten Zeit von einem Ort zu einem anderen Ort übertragen kann, wenn der Bitstrom nur mit einer bestimmten Geschwindigkeit gesendet werden kann und die Sendung womöglich noch gestört wird. Diese Fragen werden in der Shannonschen Informationstheorie behandelt, die Inhalt dieser Veranstaltung ist. Dazu werden Grundbegriffe zu Codes eingeführt, der Begriff der Entropie, Nachrichtenquellen und Kanäle. Ziele sind der Quellencodierungssatz und der Kanalcodierungssatz von Shannon.

Anschließend werden in der Praxis wichtige Codierungsmethoden behandelt z.B. lineare Codes und Faltungscodes. Es werden Algorithmen und Ergebnisse zu derartigen Codierungsmethoden und zur Decodierung und Fehlerkorrektur einer übertragenen,

codierten, aber möglicherweise gestörten Nachricht behandelt werden. Am Ende soll noch eine kurze Einführung in die algorithmische Informationstheorie gegeben werden.

Literatur

- Thomas M. Cover, Joy A. Thomas: Elements of Information Theory, John Wiley & Sons, Inc., New York, 1991.
- Werner Heise, Pasquale Quattrocchi: Informations- und Codierungstheorie, Springer-Verlag, Berlin, 2. Auflage, 1989.
- Rudolf Mathar: Informationstheorie, B. G. Teubner, Stuttgart, 1996.
- Robert J. McEliece: The Theory of Information and Coding, Addison-Wesley Publishing Company, Reading, Massachusetts, 1977.
- Wolfgang Willems: Codierungstheorie und Kryptographie, Birkhäuser, Basel, 2008.

Leistungsnachweis

Mündliche Prüfung von 30 Minuten Dauer.

Verwendbarkeit

- Wahlpflichtmodul im Masterstudiengang Informatik, Vertiefungsfeld Theoretische Informatik
- Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfeld Security Intelligence (SI)
- Wahlpflichtmodul im Masterstudiengang Mathematical Engineering, Vertiefungsfeld IT-Sicherheit und Kommunikationssysteme (ITSK)
- Nützlich für alle Module, die mit Datenübertragung und elektronischen Kommunikationssystemen befasst sind.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Es findet üblicherweise im Wintertrimester statt, wird aber nicht in jedem Studienjahr angeboten. Die konkreten Angebotstermine können der Lehrveranstaltungsplanung der Fakultät für Informatik entnommen werden.

Modulname	Modulnummer
Middleware und mobile Cloud Computing	1398

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
13981	VL	Middleware und mobile Cloud Computing	Pflicht	3
13982	UE	Middleware und mobile Cloud Computing	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden Kenntnisse aus dem Bereich des Software Engineering, insbesondere der Objektorientierung (Modul Objektorientierte Programmierung). Wünschenswert sind Grundkenntnisse in der XML-Technologien sowie in einer der objektorientierten Programmiersprache, wie z. B. Java, Scala, C++.

Qualifikationsziele

Das *Modul Middleware und mobile Cloud Computing* zielt darauf ab, den Studierenden

vertiefend die Bedeutung der Integration als Kernaufgabe der Angewandten Informatik

näher zu bringen. Die Teilnehmer erhalten neben einem grundlegenden Verständnis für die Anforderungen an eine Middleware-basierte Integration theoretische und praktische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middleware-Konzepte und serviceorientierter Schnittstellen. In diesem Zusammenhang werden wissenschaftliche Methoden vermittelt, die die Teilnehmer in die Lage versetzen, in komplexen Anwendungssystemlandschaften eigenständig und systematisch einen höheren Integrationsgrad zu erreichen. Zudem werden grundlegende Aspekte von *Verteilten Systemen* wie Kommunikationsprotokolle, Austauschformate und Sicherheitsaspekte betrachtet. Die so vermittelten IT-technischen Kenntnisse befähigen die Teilnehmer darüber hinaus aus einer Cyber-Bedrohungsperspektive betrachtet, eine fundierte Analyse hinsichtlich möglicher Leistungsengpässe und Schwachstellen zu konzipieren sowie in der gegebenen IT-Landschaft zu implementieren. Ohne diese Kenntnisse und Fähigkeiten kann de-facto auf potenzielle Bedrohungsszenarien beim Betrieb komplexer IT-Systeme kaum geeignet begegnet werden. Die im Modul vermittelten Grundlagen versetzen die Teilnehmer in die Lage, geeignete Maßnahmen zur Cyber-Abwehr in Middleware-/ Cloud-Strukturen zu integrieren (Stichwort: *Security-as-a-Service*).

Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang

mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. Durch eigenständige Anwendung von Technologien wie *Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), .NET, Simple Object Access Protocol (SOAP) oder Representational State Transfer (REST)* erhalten die Teilnehmer Methoden-, Fach- und Umsetzungskompetenz im Umgang mit grundlegenden Middleware-Konzepten und deren Basistechnologien. In der Kombination aus theoretischer Behandlung und praktischer Vertiefung versetzt das Modul die Teilnehmer in die Lage, verteilte Anwendungen auf der Basis von Middleware zu entwerfen und systematisch in die Praxis umzusetzen.

Inhalt

Im heutigen Digitalzeitalter mit *Industrie 4.0, Digital Governance* und *Künstlicher Intelligenz* etc. agieren fast alle Systeme als vernetzte Fähigkeitsträger. Moderne Enterprise Anwendungen basieren auf Standard-Middleware-Architekturen, wo Funktionalität zunehmend über Cloud-basierte Dienste plattformübergreifend den Clients – insbesondere zunehmend mobilen Endgeräten – zur Verfügung gestellt wird. Das Modul bietet einen fundierten Einstieg in die aktuellen Middleware-Basistechnologien. Auf den Grundlagenkenntnissen der Objektorientierten Programmierung aufbauend werden entlang der Entwicklungslinie Schritt für Schritt aktuelle Middleware-Konzepte und -Technologien eingeführt. Das Modul etabliert dazu zunächst die Basisabstraktion und das Grundverständnis Middleware-basierter Systeme. Dabei werden grundlegende Fähigkeiten zur Beherrschung heterogener Anwendungslandschaften und deren Komplexitätsparameter vermittelt. Diese berücksichtigen die Dimensionen der *Kommunikation* und *Transaktion* sowie Zugriffsmöglichkeiten und Schutzaspekte in *Schichtarchitekturen*. Unabhängig von der jeweils eingesetzten Technologie nimmt das Abstraktionskonzept der *Schnittstellen-Basierung* eine zentrale Rolle beim Design verteilter Anwendungen und somit im gesamten Modul ein.

Im Folgenden wird tiefer auf die unterschiedlichen Integrationsparadigmen und -technologien mit ihren jeweiligen spezifischen Stärken und Schwächen (Fähigkeiten, Schwachstellen, Angriffspunkte usw.) eingegangen. Aktuelle Middleware-Dienste und Architekturkonzepte wie *Verteilte Objektmodelle*, *Komponentenmodelle* und *Service Oriented Middleware (SOA)* bilden den Schwerpunkt des zweiten Teils des Moduls. Hier werden jeweils zunächst die allgemeinen Prinzipien erläutert und dann anhand konkreter Beispiele Standard-Middleware-Technologien und deren zugrunde liegenden Konzepte und Prinzipien vertieft.

Der dritte Teil stellt das *Cloud-Konzept* in den Mittelpunkt und zeigt Schritt für Schritt an einfachen Beispielen die Entwicklung Cloud-basierter Dienste und deren Zugriff über mobile Clients (Apps). Zudem werden erste Einblicke in aktuelle Trends wie *Mirco-Service-Architekturen* oder *Containerisierung* gegeben.

Die begleitende Übung bietet die Gelegenheit, aktuelle Technologien anhand einfacher Beispiele kennen zu lernen und erste praktische Erfahrung im Umgang mit Middleware und mobilen, Cloud-basierten Anwendungen zu sammeln.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Literatur

1. Alexander Schill, Thomas Springer: Verteilte Systeme, Springer Vieweg, 2012
2. Chris Britton, Peter Bye: IT Architectures and Middleware: Strategies for Building Large, Integrated Systems; Addison-Wesley, 2004
3. Dieter Masak: Moderne Enterprise Architekturen, Springer, 2005
4. Binildas Christudas: Practical Microservices Architectural Patterns, Apress, 2019
5. Die Beauftragte der Bundesregierung für Informationstechnik: SAGA-Modul Technische Spezifikationen, Version 5.0.0, 2011

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informationssystemen und stellen somit eine Grundlage für Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/ Cyber Sicherheit dar.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Artificial Intelligence	2319

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Eirini Ntoutsi	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
23191	VÜ	Artificial Intelligence	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse in den Bereichen Algorithmen, Datenstrukturen, Statistik und Wahrscheinlichkeitsrechnung.

Qualifikationsziele

Der Kurs bietet eine Einführung in das Gebiet der Künstlichen Intelligenz und führt in die grundlegenden Ideen und Techniken ein, die dem Design von intelligenten Maschinen zugrunde liegen. Am Ende dieses Kurses werden Sie gelernt haben, wie man autonome (Software-)Agenten entwickelt, die in vollständig informierten, teilweise beobachtbaren und gegnerischen Umgebungen effizient Entscheidungen treffen. Zudem werden Sie erforschen, wie KI eingesetzt werden kann, um Entscheidungsprozesse zu optimieren, Bedrohungen zu erkennen und in dynamischen und unsicheren Umgebungen auf Sicherheitsvorfälle zu reagieren.

Inhalt

Künstliche Intelligenz hat fast jeden Aspekt unseres Lebens durchdrungen, von der Empfehlung von Inhalten und der Gesundheitsfürsorge bis hin zur vorausschauenden Polizeiarbeit und zum autonomen Fahren, und betrifft jeden, überall und jederzeit. Da die Nachfrage nach KI-Spezialisten steigt, wächst auch der Bedarf an Studierenden, die neue KI-Technologien entwickeln und anwenden können. Themen:

- Informed search
- Uninformed search
- Constraint Satisfaction Problems
- Adversarial search
- Markov Decision Processes
- Reinforcement Learning
- Local search and Optimization
- Concrete Cybersecurity Applications

Literatur
• Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach • Richard Sutton and Andrew Barto, Reinforcement Learning: An Introduction Zusätzlich erhalten die Studierenden ausgewählte aktuelle Fachartikel, die sich auf die neuesten Fortschritte in der KI und deren Anwendungen in der Cybersicherheit konzentrieren.
Leistungsnachweis
Schriftliche Prüfung von 80 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit in der Vertiefung Security Intelligence (SI)
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und wird im Wintertrimester (WT) angeboten.

Modulname	Modulnummer
Responsible Artificial Intelligence	2320

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Eirini Ntoutsi	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
23201	VÜ	Responsible Artificial Intelligence	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Gute Kenntnisse in maschinellem Lernen, Algorithmen, Statistik und Wahrscheinlichkeitsrechnung.

Qualifikationsziele

Der Bereich der verantwortungsvollen KI ist in letzter Zeit in dem Versuch entstanden, den Menschen in den Mittelpunkt von KI-basierten Systemen zu stellen, indem Aspekte wie Fairness, Erklärbarkeit, Zuverlässigkeit und Privatsphäre von KI-Systemen berücksichtigt werden. In diesem Kurs werden verschiedene Aspekte der verantwortungsvollen KI behandelt, wobei der Schwerpunkt auf fairnessbewusstem maschinellem Lernen und erklärbarer KI (XAI) liegt.

Am Ende des Kurses werden Sie gelernt haben, wie man Verantwortungsaspekte wie Fairness und XAI in den Entwurf und die Anwendung von KI einbeziehen kann.

Inhalt

Die diskriminierenden Effekte der KI-basierten Entscheidungsfindung auf bestimmte Bevölkerungsgruppen wurden bereits in einer Reihe von Fällen beobachtet, was zu einer zunehmenden Besorgnis der Öffentlichkeit über die Auswirkungen der KI auf unser Leben geführt hat; außerdem nimmt die Komplexität der KI-Modelle zu, was es schwierig macht zu verstehen, wie Entscheidungen getroffen werden und ob die Modelle sinnvolle Muster aus den Daten lernen. Themen:

- Responsibility aspects
- Fairness-aware learning
- Explainable AI
- Responsibility aspects in AI/ML pipelines

Literatur

- Virginia Dignum, Responsible Artificial Intelligence - How to Develop and Use AI in a Responsible Way, Springer, 2019

- Solon Barocas, Moritz Hardt, Arvind Narayanan, FAIRNESS AND MACHINE LEARNING Limitations and Opportunities, online, 2022
- Christopher Molnar, Interpretable Machine Learning - A Guide for Making Black Box Models Explainable, 2022

Leistungsnachweis
Schriftliche Prüfung von 80 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit in der Vertiefung Security Intelligence (SI)
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und wird jeweils im Herbsttrimester (HT) angeboten.

Modulname	Modulnummer
Machine Learning	2534

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Eirini Ntoutsi	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
23211	VÜ	Machine Learning	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse in den Bereichen Algorithmen, Datenstrukturen, Statistik und Wahrscheinlichkeitsrechnung. Gute Programmierkenntnisse (Python).

Qualifikationsziele

Der Kurs bietet einen Überblick über Methoden und Algorithmen des maschinellen Lernens für zwei zentrale Lernaufgaben, nämlich überwachtes und unüberwachtes Lernen. Im ersten Teil des Kurses werden für jede Aufgabe die wichtigsten Algorithmen und Techniken behandelt, einschließlich Experimentier- und Bewertungsaspekten.
Im zweiten Teil des Kurses werden wir uns auf spezifische Lernherausforderungen konzentrieren, darunter Populationsungleichgewicht und Datenknappheit. Am Ende des Kurses werden Sie gelernt haben, wie man maschinelle Lernmodelle für verschiedene Probleme erstellt, wie man ihre Leistung richtig bewertet und wie man spezifische Lernherausforderungen bewältigt.

Inhalt

Da (große) Datenmengen immer mehr zunehmen, steigt auch die Nachfrage nach einer automatisierten Analyse dieser Art von Daten weiter an. Mit der steigenden Nachfrage nach Data Scientists wächst auch der Bedarf an Studenten und Studentinnen, die ML-Technologien in verschiedenen Bereichen von Cybersicherheit bis hin zu Medizin und Ingenieurwesen entwickeln und anwenden können. Themen:

- Supervised learning
- Unsupervised learning
- Outlier detection
- Machine Learning with imbalanced data
- Machine learning under data scarcity

Literatur

- Shai Ben-David and Shai Shalev-Shwartz, Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press, 2014
- Mitchell T. M., Machine Learning, McGraw-Hill, 1997

• Wagner Meira and Mohammed Zaki, Data Mining and Machine Learning: Fundamental Concepts and Algorithms, Cambridge University Press, 2020
Leistungsnachweis
Schriftliche Prüfung von 80 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit in der Vertiefung Security Intelligence (SI)
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und wird jeweils im Frühjahrstrimester (FT) angeboten.

Modulname	Modulnummer
Machine Learning (erweitert)	2535

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Eirini Ntoutsi	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
23211	VÜ	Machine Learning	Pflicht	6
23212	P	Praktikum Machine Learning	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundkenntnisse in den Bereichen Algorithmen, Datenstrukturen, Statistik und Wahrscheinlichkeitsrechnung. Gute Programmierkenntnisse (Python).

Qualifikationsziele

Vorlesung **Machine Learning:** Der Kurs bietet einen Überblick über Methoden und Algorithmen des maschinellen Lernens für zwei zentrale Lernaufgaben, nämlich überwachtes und unüberwachtes Lernen. Im ersten Teil des Kurses werden für jede Aufgabe die wichtigsten Algorithmen und Techniken behandelt, einschließlich Experimentier- und Bewertungsaspekten. Im zweiten Teil des Kurses werden wir uns auf spezifische Lernherausforderungen konzentrieren, darunter Populationsungleichgewicht und Datenknappheit. Am Ende des Kurses werden Sie gelernt haben, wie man maschinelle Lernmodelle für verschiedene Probleme erstellt, wie man ihre Leistung richtig bewertet und wie man spezifische Lernherausforderungen bewältigt.

Praktikum **Machine Learning**: Ziel ist es, im Rahmen eines trimesterlangen Teamprojekts praktische Erfahrungen mit Methoden und Algorithmen der Künstlichen Intelligenz/des Maschinellen Lernens zu gewinnen.

Inhalt

Da (große) Datenmengen immer mehr zunehmen, steigt auch die Nachfrage nach einer automatisierten Analyse dieser Art von Daten weiter an. Mit der steigenden Nachfrage nach Data Scientists wächst auch der Bedarf an Studenten und Studentinnen, die ML-Technologien in verschiedenen Bereichen von Cybersicherheit bis hin zu Medizin und Ingenieurwesen entwickeln und anwenden können.

Vorlesung **Machine Learning:**

- Supervised learning
- Unsupervised learning

- Outlier detection
- Machine Learning with imbalanced data
- Machine learning under data scarcity

Praktikum **Machine Learning:** Die Studenten und Studentinnen wählen ein Projekt aus der Liste der angebotenen Projekte aus. Die Projekte lassen sich in zwei Kategorien einteilen: i) Akademische Projekte, die in der Regel auf veröffentlichten Arbeiten beruhen. Ziel ist es, die Ergebnisse der Autoren mit einigen Erweiterungen und Anwendungen auf neue Datensätze zu reproduzieren. ii) Anwendungsspezifische Projekte, die sich auf die Analyse interessanter Datensätze aus verschiedenen Anwendungsbereichen beziehen.

Am Ende des Trimesters sollten die Studierenden und Studentinnen guten Code (Python-Notebook) und einen kurzen Report (max. 5 Seiten) abliefern und ihre Arbeit - in einer 20-minütigen Präsentation und einem 10-minütigen Q&A-Slot - während eines Blockpraktikums am Ende des Trimesters vorstellen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden in englischer Sprache gehalten.

Literatur

- Shai Ben-David and Shai Shalev-Shwartz, Understanding Machine Learning: From Theory to Algorithms, Cambridge University Press, 2014
- Mitchell T. M., Machine Learning, McGraw-Hill, 1997
- Wagner Meira and Mohammed Zaki, Data Mining and Machine Learning: Fundamental Concepts and Algorithms, Cambridge University Press, 2020

Leistungsnachweis

Portfolio. Es sind die folgenden Leistungen zu erbringen: Zur Vorlesung mit Übung entweder eine Klausur (80 min) oder ein Fachgespräch (30 min); die Art der Leistung wird zu Beginn des Moduls bekanntgegeben. Im Praktikum muss im Rahmen eine Projektes Code (Python-Notebook) erstellt und ein Bericht (5 Seiten) geschrieben werden, und die Arbeit muss am Ende präsentiert werden (20 Minuten Präsentation und 10 Minuten Fragerunde); Bearbeitungsdauer: 10 bis 12 Wochen. Die Leistungen in der Klausur/ mündlichen Prüfung und im Praktikum gehen im Verhältnis 70 zu 30 in die Note ein.

Verwendbarkeit

Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit in der Vertiefung Security Intelligence (SI)

Dauer und Häufigkeit

Das Modul dauert 2 Trimester und beginnt im Frühjahrstrimester (FT) und wird im Herbsttrimester (HT) abgeschlossen.

Modulname	Modulnummer
Artificial Intelligence (erweitert)	2536

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Eirini Ntoutsi	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
23191	VÜ	Artificial Intelligence	Pflicht	6
23192	SE	Seminar Selected topics in Artificial Intelligence	Pflicht	2
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Grundkenntnisse in den Bereichen Algorithmen, Datenstrukturen, Statistik und Wahrscheinlichkeitsrechnung.

Qualifikationsziele

Vorlesung **Artificial Intelligence**: Der Kurs ist eine Einführung in das Gebiet der Künstlichen Intelligenz und führt in die grundlegenden Ideen und Techniken ein, die dem Design von intelligenten Maschinen zugrunde liegen. Am Ende dieses Kurses werden Sie gelernt haben, wie man autonome (Software-)Agenten entwickelt, die in vollständig informierten, teilweise beobachtbaren und gegnerischen Umgebungen effizient Entscheidungen treffen. Zudem werden Sie erforschen, wie KI eingesetzt werden kann, um Entscheidungsprozesse zu optimieren, Bedrohungen zu erkennen und in dynamischen und unsicheren Umgebungen auf Sicherheitsvorfälle zu reagieren.

Seminar **Selected topics in Artificial Intelligence**: Die Seminare zielen auf die eigenständige Erforschung eines wissenschaftlichen Themas auf der Grundlage einiger Veröffentlichungen und einer qualitativ hochwertigen Präsentation des Themas sowohl in schriftlicher (Report) als auch in mündlicher Form (Vortrag und Frage- und Antwortrunde). Dieses Seminar beschäftigt sich mit der Diskussion ausgewählter Themen der Künstlichen Intelligenz und des Maschinellen Lernens. Jedes Trimester steht ein anderes Thema im Mittelpunkt, z.B. spezifische Lernaufgaben und -methoden, Lernen für verschiedene Datentypen, Lernen unter spezifischen Datenherausforderungen, etc.

Inhalt

Künstliche Intelligenz hat fast jeden Aspekt unseres Lebens durchdrungen, von der Empfehlung von Inhalten und der Gesundheitsfürsorge bis hin zur vorausschauenden Polizeiarbeit und zum autonomen Fahren, und betrifft jeden, überall und jederzeit. Da

die Nachfrage nach KI-Spezialisten steigt, wächst auch der Bedarf an Studierenden, die neue KI-Technologien entwickeln und anwenden können.

Vorlesung **Artificial Intelligence:**
- Informed search
- Uninformed search
- Constraint Satisfaction Problems
- Adversarial search
- Markov Decision Processes
- Reinforcement Learning
- Local search and Optimization
- Concrete Cybersecurity Applications

Seminar **Selected topics in Artificial Intelligence:** Die Studentinnen und Studenten wählen ein Thema aus der Liste der vorgegebenen Themen. Für jedes Thema erhalten die Studentinnen und Studenten 3-5 Forschungspapiere. Ausgehend von den Seed Papers sollen die Studentinnen und Studentendie einschlägige Literatur untersuchen und ihre Ergebnisse, einschließlich einer vergleichenden Bewertung der verschiedenen Ansätze und offenen Herausforderungen, in einem 5-seitigen Report zusammenfassen. Darüber hinaus sollen die Studentinnen und Studenten ihren Kommilitoninnen und Kommilitonen konstruktives Feedback zu ihren Reports und Präsentationen geben (Peer Review). Schließlich sollen die Studentinnen und Studenten ihre Arbeit - in einer 20-minütigen Präsentation und einer 10-minütigen Fragerunde - während eines Blockseminars am Ende des Trimesters vorstellen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden in englischer Sprache gehalten.

Literatur

- Stuart Russell and Peter Norvig, Artificial Intelligence: A Modern Approach
- Richard Sutton and Andrew Barto, Reinforcement Learning: An Introduction

Zusätzlich erhalten die Studierenden ausgewählte aktuelle Fachartikel, die sich auf die neuesten Fortschritte in der KI und deren Anwendungen in der Cybersicherheit konzentrieren.

Leistungsnachweis

Portfolio. Es sind die folgenden Leistungen zu erbringen: Zur Vorlesung mit Übung ist entweder eine Klausur (80 min) oder ein Fachgespräch (30 min) zu absolvieren; die Art der Leistung wird zu Beginn des Moduls bekanntgegeben. Im Seminar sollen die Studierenden einschlägige Literatur untersuchen, ihre Ergebnisse in einem Bericht (5 Seiten) zusammenfassen, auch die Ergebnisse der anderen Studierenden diskutieren und am Ende Ihre Arbeit präsentieren (20 Minuten Präsentation und 10 Minuten Fragerunde); Bearbeitungsdauer: 10 bis 12 Wochen. Die Leistungen in der Klausur/ mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.

Verwendbarkeit

Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit in der Vertiefung Security Intelligence (SI)

Dauer und Häufigkeit
Das Modul dauert 1 Trimester und wird im Wintertrimester (WT) angeboten.

Modulname	Modulnummer
Responsible Artificial Intelligence (erweitert)	2537

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Eirini Ntoutsi	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
23201	VÜ	Responsible Artificial Intelligence	Pflicht	6
23202	SE	Responsible Artificial Intelligence	Pflicht	2
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Gute Kenntnisse in maschinellem Lernen, Algorithmen, Statistik und Wahrscheinlichkeitsrechnung.

Qualifikationsziele

Vorlesung **Responsible Artificial Intelligence:** Der Bereich der verantwortungsvollen KI ist in letzter Zeit in dem Versuch entstanden, den Menschen in den Mittelpunkt von KI-basierten Systemen zu stellen, indem Aspekte wie Fairness, Erklärbarkeit, Zuverlässigkeit und Privatsphäre von KI-Systemen berücksichtigt werden. In diesem Kurs werden verschiedene Aspekte der verantwortungsvollen KI behandelt, wobei der Schwerpunkt auf fairnessbewusstem maschinellem Lernen und erklärbarer KI (XAI) liegt.

Am Ende des Kurses werden Sie gelernt haben, wie man Verantwortungsaspekte wie Fairness und XAI in den Entwurf und die Anwendung von KI einbeziehen kann.

Seminar **Responsible Artificial Intelligence**: Die Seminare zielen auf die unabhängige Erforschung eines wissenschaftlichen Themas auf der Grundlage einiger Veröffentlichungen und einer qualitativ hochwertigen Präsentation des Themas sowohl in schriftlicher (Bericht) als auch in mündlicher Form (Präsentation und Frage- und Antwortsitzungen). Dieses Seminar widmet sich der Diskussion ausgewählter Themen der verantwortungsvollen Künstlichen Intelligenz. Jedes Trimester steht ein anderes Thema im Mittelpunkt, z.B. Multi-Diskriminierung, post-hoc Erklärbarkeit, kontrafaktische Erklärungen, Erklärbarkeit für bestimmte Datentypen, etc.

Inhalt

Die diskriminierenden Effekte der KI-basierten Entscheidungsfindung auf bestimmte Bevölkerungsgruppen wurden bereits in einer Reihe von Fällen beobachtet, was zu einer zunehmenden Besorgnis der Öffentlichkeit über die Auswirkungen der KI auf unser Leben geführt hat; außerdem nimmt die Komplexität der KI-Modelle zu, was es schwierig

macht zu verstehen, wie Entscheidungen getroffen werden und ob die Modelle sinnvolle Muster aus den Daten lernen.

Vorlesung **Responsible Artificial Intelligence**:
- Responsibility aspects
- Fairness-aware learning
- Explainable AI
- Responsibility aspects in AI/ML pipelines

Seminar **Responsible Artificial Intelligence**: Die Studentinnen und Studenten wählen ein Thema aus der Liste der vorgegebenen Themen. Für jedes Thema erhalten die Studentinnen und Studenten 3-5 Forschungspapiere. Ausgehend von den Seed Papers sollen die Studentinnen und Studentendie einschlägige Literatur untersuchen und ihre Ergebnisse, einschließlich einer vergleichenden Bewertung der verschiedenen Ansätze und offenen Herausforderungen, in einem 5-seitigen Report zusammenfassen. Darüber hinaus sollen die Studentinnen und Studenten ihren Kommilitoninnen und Kommilitonen konstruktives Feedback zu ihren Reports und Präsentationen geben (Peer Review). Schließlich sollen die Studentinnen und Studenten ihre Arbeit - in einer 20-minütigen Präsentation und einer 10-minütigen Fragerunde - während eines Blockseminars am Ende des Trimesters vorstellen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden in englischer Sprache gehalten.

Literatur

- Virginia Dignum, Responsible Artificial Intelligence - How to Develop and Use AI in a Responsible Way, Springer, 2019
- Solon Barocas, Moritz Hardt, Arvind Narayanan, FAIRNESS AND MACHINE LEARNING Limitations and Opportunities, online, 2022
- Christopher Molnar, Interpretable Machine Learning - A Guide for Making Black Box Models Explainable, 2022

Für das Seminar: Je nach dem Thema des Seminars kann jedes Trimester zusätzliches Lesematerial bereitgestellt werden.

Leistungsnachweis

Portfolio. Es sind die folgenden Leistungen zu erbringen: Zur Vorlesung mit Übung ist entweder eine Klausur (80 min) oder ein Fachgespräch (30 min) zu absolvieren; die Art der Leistung wird zu Beginn des Moduls bekanntgegeben. Im Seminar sollen die Studierenden einschlägige Literatur untersuchen, Ihre Ergebnisse in einem Bericht (5 Seiten) zusammenfassen, auch die Ergebnisse der anderen Studierenden diskutieren und am Ende Ihre Arbeit präsentieren (20 Minuten Präsentation und 10 Minuten Fragerunde); Bearbeitungsdauer: 10 bis 12 Wochen. Die Leistungen in der Klausur/ mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.

Verwendbarkeit

Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit in der Vertiefung Security Intelligence (SI)

Dauer und Häufigkeit
Das Modul dauert 1 Trimester und wird jeweils im Herbsttrimester (HT) angeboten.

Modulname	Modulnummer
Ausgewählte Kapitel des OR: Data-driven Optimization	2994

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Juniorprof. Dr. rer. nat. Maximilian Moll	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
29941	VÜ	Ausgewählte Kapitel des Data-driven Optimization	Pflicht	3
29942	VÜ	Quantum Machine Learning & Optimization	Wahlpflicht	3
29943	SE	Seminar: Ausgewählte Kapitel des OR	Wahlpflicht	3
29944	P	Praktikum: Ausgewählte Kapitel des OR	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in Methoden des Operations Research und des Data Minings oder der Statistik werden vorausgesetzt.

Qualifikationsziele

Studierende sollen in die Lage versetzt werden, sich selbstständig mit neuartigen Methoden der data-driven Optimization in Theorie und Praxis auseinander zu setzen. Hierzu sollen sie im Rahmen der Vorlesung, sowie vertiefend in Seminar und Praktikum, verschiedene Methoden analysieren und anwenden.

Hierbei soll nicht nur die Fähigkeit entwickelt werden Ansätze auf ihre theoretische Richtigkeit und praktische Anwendbarkeit zu beurteilen, sondern diese auf ein Problem hin anpassen zu können.

Schließlich soll das Identifizieren geeigneter Probleme und passender Lösungsansätze geschult werden.

Inhalt

Data-driven Optimization beschäftigt sich zukunftsweisend mit der Kombination von klassischen Optimierungsmethoden und daten-basierten Ansätzen. Im Gegensatz zu der klassischen Optimierung der letzten Jahrhunderte, die ausgehend von einem zu optimierenden Modell eine Lösung sucht, bietet das Data-driven Optimization die Möglichkeit, ohne eine exakte mathematische Abstrahierung des zugrunde liegenden Modells Optimierungsmethoden anzuwenden.

Das Modul bietet aufbauend auf dem vorhandenen Grundwissen einen vertiefenden Einblick in ausgewählte Themengebiete des data-driven Optimization. Neben der grundlegenden Problematik werden Themen aus dem Reinforcement Learning, Prescriptive Analytics und der konvexen Optimierung unter Unsicherheit behandelt.

Das Reinforcement Learning ist neben Supervised und Unsupervised Learning das dritte Teilgebiet des Machine Learnings und beschäftigt sich mit daten-basierten Ansätzen zu Problemen der klassischen Kontrolltheorie. Hierbei soll im Modul auch die Anwendung auf praxis-relevante Probleme herausgestellt werden, die über die bekannten Lösungen von Spielen, wie z.B. Go, hinausgehen.

Prescriptive Analytics stellt aufbauend auf Descriptive und Predictive Analytics die nützlichste und schwerste Stufe des Data Science dar. Hier müssen nicht nur datan-basierte Vorhersagen getroffen werden, sondern das zukünftige System auf eine gegebene Zielvorstellung hin optimiert werden. In der Vorlesung werden verschiedene grundsätzliche Herangehensweisen mit ihren Vor- und Nachteilen diskutiert, sowie die Abgrenzung zu Predictive Analytics konkretisiert.

Die konvexe Optimierung stellt ein zentrales Element des Operations Research und der modernen Entscheidungsunterstützung dar. In vielen Fällen sind jedoch die Parameter der Optimierungsmodelle nicht explizit bekannt, sondern müssen zunächst aus Daten abgeleitet werden. Die Vorlesung thematisiert, wie sich dies auf die zu wählenden Optimierungsverfahren auswirken muss.

Das Seminar greift aktuelle Publikationen zu den Themen der Vorlesung auf.

Im Praktikum setzen sich die Studierenden mit einer konkreten, praxis-nahen Problemstellung des data-driven Optimization auseinander.

In der Vorlesung Quantum Machine Learning and Optimization wird spezifisch auf die Verwendung von Quantum Computern für effizientere Algorithmen im Kontext der NISQ-Maschinen eingegangen.

Im Praktikum werden die Studierenden an die Lösung eines konkreten RL-Problems unter praxis-nahen Bedingungen herangeführt. Hierfür wird Ihnen ein entsprechendes Environment gestellt. Während jeder Student sich mit einem anderen konkreten Algorithmus aus der Vorlesung beschäftigt, werden sie durch verschiedenen Arbeitsschritte geführt. Abschließend werden die Performances der verschiedenen trainierten Algorithmen verglichen – der Vergleich untereinander dient dabei als Teil der Lernerfahrung, nicht aber der Bewertung.

Literatur

- Sutton, Richard S., and Andrew G. Barto. *Reinforcement learning: An introduction.* MIT press, 2018.
- Jacquier, Antoine, et al.*Quantum Machine Learning and Optimisation in Finance: On the Road to Quantum Advantage*. Packt Publishing Ltd, 2022

Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
• Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfelder Software- und Informationsmanagement, Geoinformatik sowie Modellierung, Operations Research, Simulation und Experimentation, außerdem im Anwendungsfach Mathematik und Angewandte Systemwissenschaften • Wahlpflichtmodul im Masterstudiengang WIN, Vertiefungsfeld Technologie-und Innovationsmanagement • Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Enterprise Security, Public Security sowie Security Intelligence
Dauer und Häufigkeit
Das Modul dauert 2 Trimester. Es beginnt immer im Frühjahrstrimester.
Sonstige Bemerkungen
Zum Absolvieren des Moduls sind neben der Pflichtveranstaltung "Ausgewählte Kapitel des Data-driven Optimization" zwei der drei Wahlpflichtveranstaltungen zu belegen.

Modulname	Modulnummer
Einführung in die Quanteninformationsverarbeitung	3010

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Dr. Dipl.-Phys. Sabine Tornow	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
30101	VÜ	Einführung in die Quanteninformationsverarbeitung	Pflicht	3
30102	P	Praktikum Quantenschlüsselaustausch	Wahlpflicht	3
30103	SE	Seminar Quantentechnologien	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in linearer Algebra. Vorkenntnisse in Quantenmechanik und Kryptographie sind hilfreich, aber nicht erforderlich.

Qualifikationsziele

Studierende verstehen Konzepte der Quanteninformationsverarbeitung (Quantenkommunikation, Quantenkryptographie, Quantenkodierungstheorie, Quantenalgorithmen und Quantenfehlerkorrektur) und können weitere Entwicklungen zu Quantenkryptographie, Algorithmen, Fehlerkorrektur und Quantenkommunikation einordnen und bewerten. Studierende können Experimente, z.B. zur Quantenkommunikation und Fehlerkorrekur implementieren und auf einem Quantencomputer testen und die praktische Realisierung des Quantenschlüsselaustausches experimentell umsetzen (siehe Praktikum).

Am Ende des Kurses sind die Studierenden in der Lage, den grundlegenden mathematischen Formalismus (z.B. Zustände, Kanäle) und die Schlüsselkonzepte zu erklären. Sie sind in der Lage, diese Konzepte und Methoden anzupassen und anzuwenden, um Probleme der Quanteninformationsverarbeitung zu lösen.

Inhalt

Vorlesung: Quanteninformation ist eine Synthese von Informatik, Quantentheorie und Informationstheorie. Quantensysteme werden zur Speicherung von Information und die Gesetze der Quantenmechanik zur Verarbeitung von Information verwendet. Die in diesen Systemen vorhandene Information kann nicht mit den Gesetzen der klassischen Informationstheorie beschrieben werden. Diese wird zur Quanteninformationstheorie erweitert. Die Quanteninformation ermöglicht eine fundamental neue Art der Informationsverarbeitung wie die Quantenteleportation, Quantenkryptographie und

Quanten-Algorithmen. Es werden folgende Themengebiete behandelt: Grundlagen der Quantentheorie, Quantenverschränkung, Quanten-Shannon-Theorie, effiziente Quantenalgorithmen, Quantenkryptographie, Quantenkanäle, Quantenfehlerkorrektur, Quantennetzwerke und Quantenkommunikation.

Praktikum:

- Durchführung eines QKD-Modellversuchs, der das BB84-Protokoll mit polarisiertem Licht in der Praxis umsetzt
- Detailliertes Wissen über die Schritte, die für ein QKD-Protokoll erforderlich sind
- Experimentelle Durchführung des Protokolls in Teams bestehend aus zwei Personen, die die Rolle von Sender und Empfänger übernehmen
- Versenden einer mit Quantenschlüsseln verschlüsselten Nachricht
- Verfassen eines Versuchsprotokolls

Seminar: Aktuelle Themen in den Bereichen der Quantentechnologie:

Quantensensorik, Quantum Memory, Quantum Repeater, Quantum Computing, Quantenkommunikation, Post-Quantum Kryprographie, Quantenmetrologie, Quantenbildgebung, usw.

Literatur

- Riccardo Manenti and Mario Motta: Quantum Information Science, Oxford University Press
- Thomas Vidick and Stephanie Wehner: Introduction to Quantum Cryptography, Cambridge University Press
- Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

- als Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit (MCYB)
- in Modul 5506 Kryptologie im Studiengang MCYB
- in Modul 3491 Algorithmen und Komplexität im Studiengang MINF
- in Modul 3820 Quantencomputer in Theorie und Praxis im Studiengang MCYB
- in Modul 1037 Informations- und Codierungstheorie im Studiengang MCYB
- in Modul 1289 Nachrichtentheorie und Übertragungssicherheit im Studiengang MCYB
- in Modul 5548 Modern Cryptography im Studiengang im Studiengang MCYB
- in Modul 2994 Ausgewählte Kapitel des OR: Data-driven Optimization MINF

Dauer und Häufigkeit

Das Modul wird jedes Jahr ab dem WT angeboten und dauert zwei Trimester. Die Vorlesung wird im WT angeboten, das Praktikum oder das Seminar im FT.

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	3396

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
33961	VÜ	Data Mining und IT-basierte Entscheidungsunterstützung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Grundkenntnisse zu mathematischen Methoden des Operations Research und der Statistik wie sie z.B. im Bachelor Informatik bzw. Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Insbesondere ist es das Ziel, IT-basierte Entscheidungsunterstützung unter der speziellen Cyberperspektive zu betrachten: Wie können Angriffe schneller erkannt, wie kann man sich optimal dagegen schützen und wie können Entscheidungsunterstützungssysteme gegenüber Cyberangriffen optimiert werden. Das Modul gibt einen Überblick über aktuelle Modelle und Verfahren sowie relevante Bedrohungsszenarien.

Inhalt

Die Studierenden sollen in dieser Veranstaltung mit den IT-basierten und entscheidungstheoretischen Grundlagen im Bereich der modernen Datenanalyse vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von geeigneten Analyseverfahren zur Erforschung von komplexen datenbasierten Zusammenhängen ("Exploratory Analysis").

Data Mining bedeutet dabei das Extrahieren von impliziten, noch unbekannten Informationen aus Rohdaten. Dazu sollten IT-Systeme in die Lage versetzt werden, Datenbanken und Datenansammlungen (z.B. im Bereich der Geoinformatik) automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert. Insbesondere das heutige maschinelle Lernen und das Verfahren des "Datafarming" stellen dafür die Werkzeuge und Techniken zur Verfügung, die in den Bereich des modernen Wissensmanagements (bis zur Begriffsanalyse) und "Datamining" hineinführen.

Literatur

- Decision Support Systems Developing Web-Enabled Decision Support Systems, Abhijit A. Pol and Ravindra K. Ahuja. Dynamic Ideas 2007.
- Exploratory Data Analysis Making Sense of Data: A Practical Guide to Exploratory Data Analysis and Data Mining, Glenn J. Myatt. John Wiley, 2006.
- Spatial Data Analysis Spatial Data Analysis - Theory and Practice, Robert Haining, Cambridge University Press 2003.
- Data Mining Data Mining: Practical Machine Learning Tools and Techniques (Second Edition) Ian H. Witten, Eibe Frank. Morgan Kaufmann 2005.
- Data Mining: A Knowledge Discovery, K. Cios, W. Pedrycz, R. Swiniarski Springer, 2007.
- Data Mining Introductery and Advanced Topics, Margaret Dunham, Prentice Hall, 2003.
- Advances in Knowledge Discovery and Data Mining, U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, editors , MIT Press, 1996.
- Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber. Morgan Kaufmann, 2006.
- Principles of Data Mining, David J. Hand, Heikki Mannila and Padhraic Smyth. MIT Press, 2000. Daniel T. Larose,
- Discovering Knowledge in Data: An Introduction to Data Mining, John Wiley 2004. Robert Nisbet, John Elder, IV and Gary Miner.
- Handbook of Statistical Analysis and Data Mining Applications. Elsevier 2009.
- Statistical Learning - Machine Learning Trevor Hastie, Robert Tibshirani, Jerome Friedman,
- The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Verlag, 2001. Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, Wiley-IEEE Press, 2002.

Weiterführende Literatur:

- Zeitreihenanalyse Time Series Analysis. Hamilton 1994.
- Reinforcement Lernen und Spieltheorie Reinforcement Learning: An Introduction. Sutton and Barto: MIT Press 1998.
- Fun and Games: A Text on Game Theory. Binmore, Linster, Houghton Mifflin 2000.
- Statistik Bayesian Data Analysis. Gelman, Carlin, Stern, Rubin: Chapman 1995. Introduction to Mathematical Statistics. Hogg, Craig: Prentice Hall 2004.
- Principles of Statistics. Bulmer: Dover 1979.
- Probability, Random Variables and Stochastic Proc., Papoulis, McGraw, Hill 2002.

Leistungsnachweis

Portfolio auf der Basis der folgenden vier Teilleistungen, je mit 25% gewichtet, für deren Bearbeitung die Studierenden einen Bearbeitungszeitraum von je 2 Wochen haben:

1. Analysebericht "Pre-Processing" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)
2. Analysebericht "Clustering" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)
3. Analysebericht "Classification" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)

4. Analysebericht "Outlier Detection" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)

Verwendbarkeit
Die Vorlesung kann durch weiterführende Veranstaltungen im Bereich der Datenanalyse fortgeführt werden, z.B. im Bereich der modernen Begriffsanalyse, des Algorithmic Engineering, im Rahmen von Spezialvorlesungen der Numerik und Statistik sowie der Geoinformatik. Ebenfalls bestehen enge Bezüge zu wissenschaftlichen Forschungsgebieten im Bereich der Künstlichen Intelligenz.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Anwendungsgebiete der Data Science	3852

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38521	VÜ	Sentiment Analysis	Wahlpflicht	3
38522	VÜ	Social Media Mining	Wahlpflicht	3
38523	VÜ	Semantische Technologien	Wahlpflicht	3
38524	PRO	Modulprojekt Anwendungsgebiete der Data Science	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Kenntnisse in Programmierung und Software-Entwurf sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Die Studierenden lernen Herausforderungen und Methoden beim Text Mining kennen und lernen die besprochenen Techniken anzuwenden. Zudem lernen sie theoretische Ansätze auf konkrete, praxisrelevante Fragestellungen zu übertragen. Für exemplarische Aufgabenstellungen können die Studierenden bestehende methodische Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen. Sie können begründet argumentieren und eine von ihnen selbständig gefundene Lösung vertreten und reflexiv bewerten.

Inhalt

- In der Vorlesung „Sentiment Analysis“ soll die schon umfangreiche Forschungsliteratur zum Opinion Mining aufgearbeitet werden. Dabei reichen die Ansätze von der Text- bis zur Wortebene, die Aufgaben sind das Erkennen von Subjektivität vs. Objektivität, das Bestimmen der Perspektive von Autoren, das Extrahieren ihrer Meinung. Datenquellen können Review-Seiten aus dem Internet sein, Blog-Posts und -kommentare, Nachrichten auf Twitter, gesprochene Sprache, usw.
- In der Vorlesung „Social Media Mining“ wird exemplarisch die Entwicklung eines Systems besprochen, welches über soziale Netzwerke direkt oder indirekt an Unternehmen adressierte Meldungen, Nachrichten oder Kommentare erfasst, klassifiziert und auswertet. Hierbei werden Textmining- und Klassifikationsverfahren mit Fokus auf Kurztexten diskutiert und der begleitenden Übung praktisch vertieft.

- Die Vorlesung „Semantische Technologien“ gibt einen Einblick in Grundlagen und praktische Anwendungen wissensbasierter Softewarelösung. Sie gibt einen breiten Überblick über den Nutzen und die Möglichkeiten dieser Technologien. Semantische Technologien versetzen uns nicht nur in die Lage, Informationen zu speichern und wiederzufinden, sondern sie gemäß ihrer Bedeutung und Funktion entsprechend auszuwerten, zu verbinden, zu Neuem zu verknüpfen und so flexibel und zielgerichtet anzuwenden.
- Im Modulprojekt setzen sich Studierende unter Anleitung selbständig mit Texten und Aufgaben zum Modulthema auseinander und präsentieren ihre Ergebnisse geeignet in mündlicher und/oder schriftlicher Form. Zu Beginn des Modulprojekts werden die geplanten Einzelthemen angekündigt und festgelegt, in welcher Form die Ergebnisse zu präsentieren sind.

Literatur

- Allan Ramsay, Tariq Ahmad: Machine Learning for Emotion Analysis in Python, Packt Publishing, 2023.
- Matthew A. Russell, Mikhail Klassen: Mining the Social Web, O'Reilly Media, 2019.
- Archana Patel, Narayan C. Debnath: Data Science with Semantic Technologies, CRC Press, 2023.
- Marc Wintjen: Practical Data Analysis Using Jupyter Notebook, Packt Publishing, 2020.

Leistungsnachweis

Portfolio: Mit gleichen Anteilen zu jeder der Vorlesungen (mit Übung) und im Modulprojekt. Die Studierenden können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder eine Vorlesung mit Übungen und ein Modulprojekt einbringen. Die geforderten Einzelleistungen sind wie folgt:

- 38521: Schriftliche Klausur von 60 Minuten oder Fachgespräch von 30 Minuten. Die Art der Leistung wird zu Beginn des Moduls bekannt gegeben.
- 38522: Schriftliche Klausur von 60 Minuten oder Fachgespräch von 30 Minuten. Die Art der Leistung wird zu Beginn des Moduls bekannt gegeben.
- 38523: Schriftliche Klausur von 60 Minuten oder Fachgespräch von 30 Minuten. Die Art der Leistung wird zu Beginn des Moduls bekannt gegeben.
- 38524: Bearbeitung eines Projektes mit schriftlicher Ausarbeitung, Bearbeitungszeit: 8 Wochen, Umfang 20 Seiten.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science.

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester und beginnt jedes Jahr im HT.

Sonstige Bemerkungen

Die Vorlesungen und das Praktikum werden nicht alle jedes Jahr angeboten, aber in jedem Jahr mindestens so viele Lehrveranstaltungen, dass 6 ECTS-Leistungspunkte

erreichbar sind. Jeweils zu Beginn des Moduls wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Analyse unstrukturierter Daten	3853

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38531	VÜ	Analyse unstrukturierter Daten	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Die Studierenden sollen grundlegende Programmierkenntnisse sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele
Die Studierenden lernen Herausforderungen und Methoden bei der Informationsbeschaffung und -extraktion kennen und lernen die besprochenen Analyse-Methoden anzuwenden. Sie lernen Verfahren der Analyse unstrukturierter Daten auf konkrete, praxisrelevante Fragestellungen (insb. im Bereich Wissensgewinnung) anzuwenden und können für exemplarische Aufgabenstellungen existierende Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen.

Inhalt
Dieses Modul gibt einen Einblick in die Herausforderungen und Verfahren, die bei der Analyse unstrukturierter Daten zum Einsatz kommen. Unstrukturierte Informationen sind in der Regel sehr textlastig, weshalb viele vorhersagende Analyse-Verfahren den Informationswert dieser Daten nicht nutzen können. Allerdings können textbasierte Medien (E-Mails, Webseiten-Inhalte, Fachartikel, Social Media Beiträge, etc.) u. a. dabei helfen, Trends zu erkennen, Wissen zu gewinnen und Fake News aufzudecken. Hierfür müssen Informationen identifiziert, extrahiert, aufbereitet und interpretiert werden. Die Herausforderung besteht darin, relevante Informationen zu erkennen, aus unstrukturierten Texten zu extrahieren und fehlende Informationen ggf. hinzufügen. In der Veranstaltung werden auch Themen wie die Informationsgewinnung aus unterschiedlichen Quellen sowie Fragen der Qualitätssicherung bei der Datenspeicherung und des Datenmanagements in wissensbasierten Strukturen behandelt. In der Übung werden theoretische und praktische Fragestellungen gleichermaßen adressiert. Der theoretische Teil dient zur Wiederholung der Vorlesungsinhalte. Im

praktischen Teil sind die Studierenden aufgefordert, ausgewählte Verfahren zur Analyse unstrukturierter Daten eigenständig zu implementieren. Für die Übungen sind Programmierkenntnisse erforderlich.

Literatur

- Soumen Chakrabarti: Mining the Web, Morgan Kaufmann, 2002.
- Henning Wachsmuth:Text Analysis Pipelines: Towards Ad-hoc Large-Scale Text Mining (Lecture Notes in Computer Science, Band 9383), Springer Verlag, 2015.
- Nikos Tsourakis: Machine Learning Techniques for Text, Packt Publishing, 2022.
- Anish Chapagain: Hands-On Web Scraping with Python, 2. Auflage, Packt Publishing, 2023.

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science mit Fokus auf die Analyse unstrukturierter Daten.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Deep Learning for IT-Security	4212

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
42121	VL	Deep Learning	Pflicht	4
42122	SE	Selected Topics in Deep Learning for IT-Security	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse in den Bereichen Machine Learning, Algorithmen. Gute Programmierkenntnisse (Python).

Qualifikationsziele

Vorlesung:

Die Studierenden verstehen die Grundprinzipien von Deep Learning Methoden, welche heutzutage weit verbreitet in der Künstlichen Intelligenz sind, insbesondere für Muster Erkennung oder Biometrie. Sie werden nicht nur mit linearen Netzen arbeiten, sondern auch mit Convolutional Neural Networks (CNN) für Bildverarbeitung und Long Short-Term Memory (LSTM) Networks fu#r die Verarbeitung von Sequenzen. Die Studierenden können verschiedene Ansätze vergleichen, ihre Vorteile und Nachteile besprechen, und entscheiden, welches der beste Ansatz zur Bewältigung der anstehenden Herausforderungen ist. Seminar:

Die Studierenden können aktuelle deep learning Architekturen implementieren und evaluieren. Die Studierenden sind in der Lage, aktuelle Herausforderungen des deep learnings und ihrer Anwendungen in der IT-Sicherheit zu verstehen, zu analysieren, zu evaluieren und zu diskutieren, um neue Lösungen zu finden. Darüber hinaus können sie fachliche Literatur und aktuelle Veröffentlichungen recherchieren, um Methoden zu finden, welche ihnen bei der Entwicklung neuer Lösungen helfen können. Die Studierenden können ihre Arbeit im Team präsentieren und Herausforderungen diskutieren. Des Weiteren können die Studierenden Fragen zu den anderen Vorträgen formulieren und mit Ideen beitragen, um die Herausforderungen zusammen zu lösen.

Inhalt

Vorlesung:

- Grundlagen der deep learning
- Convolutional Neural Networks
- Long Short-Term Memory (LSTM) Networks
- Generative Adversarial Networks (GAN) und Autoencoders (AE)
- Biometrische Erkennung und deep learning
- Angriffserkennug in der Biometrie: Presentation Attack Detection (PAD) und deep learning

Seminar:

Die Studierenden wählen ein Projekt aus der Liste der angebotenen Projekte aus.
Die Projekte werden Anwendungen der gelernten Algorithmen in der Cybersicherheit bearbeiten. Am Ende des Trimesters sollten die Studierenden eine Ausarbeitung und ggf. Code abliefern und ihre Arbeit in einer 20- bis 40-minütigen Präsentation (inkl. Q&A-Slot) vorstellen.

Literatur

- I. Goodfellow, Y. Bengio, A. Courville: Deep Learning (Adaptive Computation and Machine Learning series), The MIT Press; Illustrated Edition (18. November 2016), ISBN: 978-0262035613
- F. Chollet: Deep Learning with Python, Manning Publications, 2017, ISBN: 978-1617294433
- B. Bhanu, A. Kumar: Deep Learning for Biometrics, Springer, 2017, ISBN: 978-3319616568
- Forschungsartikel in peer-reviewed Konferenzen oder Journalen

Leistungsnachweis

Portfolio: zur Vorlesung ein 60-minütige schriftliche Klausur und zum Seminar eine Ausarbeitung (6 bis 10 Seiten), ggf. Code und eine 20- bis 40-minütige Präsentation (inkl Q&A-Slot). Die Bearbeitungsdauer für die Ausarbeitung und die Vorbereitung der Präsentation beträgt 4 bis 6 Wochen. Die Leistungen in der Klausur und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten vermitteln tiefes Verständnis von modernen Verfahren des deep learnings. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet der Biometrischen Erkennung.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im FT.

Modulname	Modulnummer
Angewandte Zahlentheorie	6034

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Andreas Nickel	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12111	VÜ	Algorithmische Zahlentheorie	Pflicht	5
12112	VÜ	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Pflicht	3
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Generelles Interesse an Mathematik und Theorie. Es wird empfohlen, das Modul "Zahlentheorie und Kryptographie" absolviert zu haben.Alternativ reichen bei entsprechender Einsatzbereitschaft Grundlagen zur Kryptographie und Kryptoanalyse aus, wie sie z.B. im Modul Kryptologie vermittelt werden.

Qualifikationsziele

Die Studierenden erlernen fortgeschrittene Konzepte und Algorithmen der algebraischen Zahlentheorie und werden mit einigen ihrer Anwendungen vertraut gemacht. Dabei handelt es sich um zahlentheoretische oder algebraische Methoden für den Entwurf von kryptographischen bzw. kryptoanalytischen Verfahren und solche, die in der Codierungstheorie eingesetzt werden.

Inhalt

Die Veranstaltung "Algorithmische Zahlentheorie" befasst sich mit grundlegenden Begriffen und Algorithmen der algebraischen Zahlentheorie. (Stichworte: Primelemente, Primalitätstests, Faktorisierung, elliptische Kurven, u.a.). Ein Großteil dieser abstrakten Konzepte ist fundamental für die moderne Kryptographie (Public Key) und die Codierungstheorie. Der Schwerpunkt dieser Vorlesung ist zwar die systematische Erarbeitung der theoretischen Grundlagen und grundlegenden Algorithmen, es wird aber auch immer wieder auf Anwendungen eingegangen. Ergänzt werden diese durch zahlentheoretische Konzepte, die eventuell in einer Post-Quantencomputer-Epoche relevant sein könnten.

Die Veranstaltung "Ausgewählte mathematische Methoden der Kryptographie und Codierungstheorie" befasst sich mit ausgewählten und fortgeschrittenen Themen aus der Kryptographie und/oder der Codierungstheorie. Hierhin gehören kryptographische Verfahren, die auf zahlentheoretischen Ergebnissen aufsetzen, und "gute" Codes, die

man mit Hilfe von algebraischen Kurven gefunden hat. Sowohl kryptographische als auch codierungstheoretische Inhalte sind vorgesehen; die Gewichtung zwischen diesen beiden Gebieten kann aber variieren.

Literatur

Zur VÜ Algorithmische Zahlentheorie:

- H. Cohen: A course in computational algebraic number theory, Graduate Texts in Mathematics 138, Springer
- O. Forster: Algorithmische Zahlentheorie, Springer
- J. Hoffstein, J. Pipher, J.H. Silverman: An Introduction to Mathematical Cryptography, Springer
- C. Karpfinger, H. Kiechle: Kryptologie. Algebraische Methoden und Algorithmen, Vieweg + Teubner

Zur VÜ Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie:

- W. Heise und P. Quattrocchi: Informations- und Codierungstheorie, Springer
- D. Jungnickel: Codierungstheorie, Spektrum Akad. Verlag
- N. Koblitz: Algebraic Aspects of Cryptography, Springer
- W. Lütkebohmert, Codierungstheorie, Springer-Vieweg

Leistungsnachweis

Mündliche Prüfung von 30 Minuten Dauer.

Verwendbarkeit

- Wahlpflichtmodul im Vertiefungsfeld Enterprise Security (ES) des Masterstudiengangs Cyber-Sicherheit.
- Wahlpflichtmodul im Vertiefungsfeld Cyber Network Capabilities (CNC) des Masterstudiengangs Cyber-Sicherheit.
- Wahlpflichtmodul im Vertiefungsfeld Security Intelligence (SI) des Masterstudiengangs Cyber-Sicherheit.

Dauer und Häufigkeit

Das Modul dauert 1 bis 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Herbsttrimester.

Modulname	Modulnummer
Signalverarbeitung	6050

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Knopp	-	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	60	90	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
60501	VÜ	Signalverarbeitung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Voraussetzungen laut Prüfungsordnung
keine
Empfohlene Voraussetzungen
Kenntnisse der Signal- und Systemtheorie, der Wahrscheinlichkeitsrechnung und stochastischer Prozesse und der höheren Mathematik.
Qualifikationsziele
Die Studierenden verstehen die mit dem Übergang vom kontinuierlichen Signal zum zeit- und wertdiskreten Signal einhergehenden Veränderungen von Signaleigenschaften. Sie wenden diese Signaleigenschaften eigenständig auf praktische Probleme an. Hierzu verfügen sie über einen sicheren Umgang mit Schlüsseltechniken der digitalen Signalverarbeitung im Zeit- und Frequenzbereich. Die Studierenden differenzieren ferner die Prinzipien der statistischen Signalklassifikation.
Inhalt
Die Studierenden werden in dieser Lehrveranstaltung spezifisch mit digitalen Signalen deterministischer und stochastischer Natur (Zufallssignalen) vertraut gemacht. Sie setzen sich im ersten Schritt mit der Darstellung von zeitkontinuierlichen und zeitdiskreten Signalen im Zeit- und Frequenzbereich als Fourier-Reihe, Fourier-Transformation, Laplace-Transformation, Z-Transformation und zeitdiskrete Fourier-Transformation (DTFT) auseinander. Dazu verdeutlichen sich die Studierenden erneut das Verfahren der Signalabtastung und dessen Effekte. Als wichtigstes Ergebnis dieses Abschnitts zu den Signaltransformationen erlernen die Studierenden das Werkzeug der diskreten Fourier-Transformation (DFT) und grenzen dieses zu anderen Verfahren ab. Dabei machen sie sich mit allen Effekten der DFT vertraut, insbesondere der Zusammenhänge von Zeit- und Frequenzauflösung, Aliasing und Leakage-Effekt. Spezifische Größen für Zufallssignale und Zufallsvariablen sowie allgemeine stochastische Prozesse, insbesondere die Autokorrelation, Kreuzkorrelation und das Leistungsdichtespektrum, vervollständigen das Bild basierend auf den Wiener'schen Theorien. Darauf aufbauend wird die Spektralschätzung und Spektralanalyse eingeführt. So erwerben die

Studierenden fundierte Kenntnis über die Spektralanalyse und Spektralschätzung von deterministischen Signalen und Zufallssignalen, wobei traditionelle, nicht-parametrische sowie parametrische Spektralschätzverfahren vermittelt werden. Zur Abrundung erlernen die Studierenden die Grundlagen der Parameterschätzung mithilfe von Statistiken höherer Ordnung (Higher-Order Statistics, HOS) und bestimmen die Schätzgüte anhand der wesentlichen Parameter Erwartungstreue und Schätzvarianz. Mithilfe der Cramer-Rao-Bound erlernen sie ferner, die Schätzgüte absolut sowie im Vergleich mit anderen Schätzverfahren zu beurteilen.

Literatur

- Kammeyer KD, Kroschel K: Digitale Signalverarbeitung. Springer Vieweg, 2022
- Oppenheim A, Schafer R: Discrete-Time Signal Processing: Pearson New International Edition. Pearson Education Limited, 2013

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer (sP-60).

Verwendbarkeit

- Pflichtmodul im Studiengang EIT M.Sc. für die Studienrichtung SKE
- Pflichtmodul im Studiengang ME M.Sc. für die Wahlpflichtgruppe ITSK
- Wahlpflichtmodul im Studiengang CYB M.Sc. für das Vertiefungsfeld SI
- Wahlpflichtmodul im Studiengang INF M.Sc. für das Anwendungsfach Elektrotechnik
- Wahlpflichtmodul MINT

Dauer und Häufigkeit

1 Trimester, in jedem WT

Modulname	Modulnummer
Kanalcodierung	6053

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Knopp	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	60	90	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
60531	VÜ	Kanalcodierung	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Voraussetzungen laut Prüfungsordnung
keine
Empfohlene Voraussetzungen
Kenntnisse der höheren Mathematik, der Signal- und Systemtheorie, wie sie in der Vorlesung „Signale und Kommunikationssysteme“ (BA Modul „Signale und Systeme“) erlernt werden sowie Kenntnisse von Kommunikationssystemgrundlagen, wie sie in der Vorlesung „Kommunikationstechnik“ (BA Modul „Kommunikationstechnik“) erlernt werden.
Qualifikationsziele
Die Studierenden erlernen in dieser Lehrveranstaltung die Grundlagen der Informationstheorie und darauf aufbauend die wichtigsten Methoden und Verfahren der Vorwärtsfehlerkorrektur und Kanalcodierung. Sie vertiefen dabei ihre Kenntnisse von spezifischen Codierungsverfahren und der Decodierung. Ferner erlernen Sie Werkzeuge und Kenngrößen zur analytischen Untersuchung von Codierungsverfahren und deren vergleichender Bewertung.
Inhalt
Die Studierenden erlernen die Grundlagen der Informationstheorie als Voraussetzung für den Entwurf von Vorwärtsfehlerkorrekturverfahren. Sie erhalten abschließend ein fundiertes Verständnis des Kanalcodierungstheorems, der Kanalkapazität verschiedener Übertragungskanäle und des Prinzips der Kanalcodierung. Die Studierenden werden mit Methoden zur Abschätzung der Leistungsfähigkeit von Codes vertraut gemacht; sie berechnen eigenständig Distanzeigenschaften wie die Hamming-Distanz. Sie erlernen das Prinzip der Maximum-Likelihood (ML) und Maximum-A-Posteriori (MAP) Decodierung, der Soft-in soft-out Decodierung und reflektieren diese am Beispiel der wichtigsten Codeklassen. Hierzu gehören lineare Blockcodes, Low-Density Parity Check Codes, Faltungscodes und Polarcodes. In Bezug auf die Blockcodes setzen sie sich analytisch und simulativ mit der Fehlerwahrscheinlichkeit auseinander. Die Studierenden vergleichen Low Density Parity Check (LDPC) Codes und erlernen deren Konstruktion und Bewertung anhand von Tanner Graphen. Für die Decodierung von

LDPC Codes konzentrieren sie sich auf Message Passing Decodierung. Faltungscodes verstehen die Studierenden anhand von Zustandsautomaten; die Decodierung von Faltungscodes führen sie mit Trellis-Graphen und dem Viterbi-Decodierverfahren aus. Schließlich erlernen die Studierenden den Nutzen der Codeverkettung und deren iterativer Decodierung, einschließlich der Grundlagen der Turbo-Codes. Zur Decodierung von Turbo-Codes konzentrieren sich die Studierenden auf die MAP Decodierung mit dem BCJR Algorithmus.

Literatur

- Bossert, M.: Channel Coding for Telecommunications. Wiley.
- Friedrichs, B.: Kanalcodierung. Springer
- Lin, S., Costello, D.: Error Control Coding. Prentice Hall.
- Johnson, S.: Iterative Error Correction. Cambridge.

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer (sP-60)

Verwendbarkeit

- Wahlpflichtmodul im Studiengang EIT M.Sc. für die Vertiefungsrichtung SKE
- Wahlpflichtmodul im Studiengang ME M.Sc. für die Wahlpflichtgruppe ITSK
- Wahlpflichtmodul im Studiengang CYB M.Sc. für das Vertiefungsfeld SI
- EIT MSc. Wahlpflichtmodul MINT

Dauer und Häufigkeit

1 Trimester, in jedem HT

Modulname	Modulnummer
Erweiterte Digitale Forensik	1162

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11621	VL	Erweiterte Digitale Forensik (Vorlesung)	Pflicht	3
11622	UE	Erweiterte Digitale Forensik (Übung)	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Voraussetzungen laut Prüfungsordnung
Das Modul 5505 muss bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.
Empfohlene Voraussetzungen
Das Modul 1551 soll bestanden sein.
Qualifikationsziele
Die Studierenden erwerben fortgeschrittene Kenntnisse und Fähigkeiten zur Durchführung einer IT-forensischen Untersuchung. Dazu gehören weitergehende Themen wie Hashfunktionen und Approximate Matching zur Erkennung bzw. Wiedererkennung von Artefakten, fortgeschrittene Dateisystemanalyse am Beispiel ext4, Linux-Analyse und fortgeschrittene Hauptspeicheranalyse.
Inhalt
Die Studierenden lernen fortgeschrittene Betriebssystemforensik am Beispiel von Linux kennen und arbeiten insbesondere mit Linux-Artefakten. Weiterführende Betrachtungen zur Sicherung und Analyse des Hauptspeichers werden mittels des Linux-Betriebssystems und des Frameworks Volatility behandelt. Weiterhin wird der Einsatz von kryptographischen sowie ähnlichkeitserhaltenden Hashfunktionen zur automatisierten (Wieder-)erkennung von Datenstrukturen betrachtet. Im Kontext der Dateisystemforensik wird ein aktuelles Dateisystem analysiert, beispielsweise ext4 wegen seiner Bedeutung für Android. Weiterhin wird ein aktuelles Themengiebt (z.B. Mobilfunkforensik, Netzwerkforensik, Automotive Forensik) bearbeitet.
Literatur
• Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018.

- Breitinger, Frank, et al. Approximate matching: definition and terminology. US Department of Commerce, National Institute of Standards and Technology, 2014.
- Baier, Harald. "Towards automated preprocessing of bulk data in digital forensic investigations using hash functions." it-Information Technology 57.6 (2015): 347-356.
- Kornblum, Jesse. "Identifying almost identical files using context triggered piecewise hashing." Digital investigation 3 (2006): 91-97.
- Baier, Harald, and Frank Breitinger. "Security aspects of piecewise hashing in computer forensics." 2011 Sixth International Conference on IT Security Incident Management and IT Forensics. IEEE, 2011.
- Carrier, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.
- Linux Ext4 Kernel Wiki. https://ext4.wiki.kernel.org/index.php/Main_Page
- Casey, Eoghan, Cameron H. Malin, and James M. Aquilina. Malware forensics: investigating and analyzing malicious code. Syngress, 2008.

Leistungsnachweis

Portfolio: Es sind die Lösungen aller 7 Übungsblätter schriftlich auf 5 Seiten zum Übungstermin via Ilias im pdf-Format abzugeben. Die Bearbeitungszeit beträgt je 1 Woche. Im Prüfungszeitraum des Wintertrimesters findet ein individuelles Fachgespräch der Dauer 30 Minuten statt. Die Modulnote ist zu 100% das Ergebnis des Fachgesprächs

Verwendbarkeit

Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.

Dauer und Häufigkeit

Das Modul dauert ein Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Vernetzte Operationsführung und Digitale Streitkräfte	1169

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11691	VL	Vernetzte Operationsführung und Digitale Streitkräfte	Pflicht	3
11692	UE	Vernetzte Operationsführung und Digitale Streitkräfte	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Wünschenswert aber nicht notwendig sind Kenntnisse im Bereich Unternehmensstrukturen und Middleware-Technologien, wie sie in Modulen für "Projektmanagement", "Enterprise Architecture und IT Service Management" und „Middleware und mobile Cloud Computing“ vermittelt werden.

Qualifikationsziele

Die Digitalisierung auf der Basis aktueller Informations- und Kommunikations-technologien dominiert zunehmend alle wirtschaftlichen, gesellschaftlichen und privaten Bereiche. Sie wird auch im sicherheitsrelevanten Kontext von (Cyber-) Verteidigung zunehmend zum Schlüsselfaktor und zentralen Gestaltungselement für alle involvierten Player. Klassisches Militär muss sich in hohem Tempo auf allen Ebenen den digitalen Herausforderungen stellen und wird so im Verbund mit Partnern und Verbündeten immer mehr zur „Digitalen Streitkraft“. Zukünftige Führungskräfte gilt es entsprechend auf diese Herausforderungen vorzubereiten.

Das Modul vermittelt die entsprechenden Grundlagen und Fähigkeiten zur Planung, Durchführung, Überwachung und Auswertung von Vernetzten Operationen (Stichwort Network Centric Warfare) auf der Basis der heute zur Verfügung stehenden Methoden, Werkzeuge und digitalen Technologien. Zunächst wird die zugrunde liegende Begriffswelt eingeführt und darauf aufbauend ein kritisches Gesamtverständnis der domänen-spezifischen Anforderungen einerseits sowie vertiefte Kenntnisse über Aufbau und Funktion der eingesetzten Applikationen und Standardsysteme andererseits vermittelt. Neben entsprechenden Anwendungsgrundlagen und wissenschaftlichen Ansätzen, werden Methoden zur eigenständigen Konzeption und Gestaltung angepasster IT-Lösungen unter Nutzung von Interoperabilitätsstandards und Sicherheitskonzepten für die Zusammenarbeit im multinationalen Umfeld vermittelt. Die Teilnehmer werden

so in die Lage versetzt, in einer späteren Verwendung strukturiert, eigenständig und methodisch fundiert gemeinsam mit anderen „Stakeholdern“ verantwortlich an der ständigen Weiterentwicklung der Digitalen Transformation von Streitkräften mitzuwirken.

Inhalt

Im gegenwärtigen Digital-Zeitalter wird unsere VUCA-Welt (Volatility, Uncertainty, Complexity, Ambiguity) vorwiegend durch Informationstechnologie geprägt. Mit der Globalisierung von Informationsflüssen in nahezu Lichtgeschwindigkeit nehmen Informationen die zentrale Bedeutung als „Rohstoff und Ware“ in den digitalen Wertschöpfungsketten des 21. Jahrhunderts ein. Für eine moderne Digitale Armee bilden Daten und Informationen die essenzielle Grundlage für Planung, Ausrichtung, Architektur, Operationsdurchführung sowie die permanente Weiterentwicklung gemäß der sich ständig ändernden Anforderungen. Hierfür müssen Entscheidern relevante Informationen zur richtigen Zeit am erforderlichen Ort in angemessener Qualität und Quantität zur Verfügung gestellt werden. Im Rahmen der gesamten, partnerübergreifenden Wertschöpfungskette sind relevante Daten und Informationen entsprechend interoperational, digital, schneller, besser etc. innerhalb der jeweiligen Verteidigungsallianz zur Verfügung zu stellen. Der Informationsverarbeitungsprozess umfasst dabei im Wesentlichen die Planung mittels formalisierter Modelle, die Umsetzung in geeignete IT-Systeme und Applikationen sowie deren fortlaufende Integration sowohl auf technischer als auch organisatorischer Ebene und zwar gemeinsam und abgestimmt mit den Schlüsselparametern Zielbezug, Fähigkeitsorientierung sowie Schutzbedarfen.

Die Wissenschaft und die „Defence Community“ stellen hierfür entsprechende Werkzeuge, Methoden und Standards zur Verfügung, um sowohl national als auch international im Kontext des NATO-Bündnisses für die sog. *Multi-Domain Operations (MDO)* die Voraussetzungen für eine Vernetzte Operationsführung zu schaffen. Entscheidungsgrundlage und zentrales verbindendes Element bildet hierbei das *Gemeinsame Rollenorientiertes Einsatzlagebild* (GREL) mit multi-dimensionalen Betrachtungsebenen, welches es zu generieren und ständig anzupassen gilt. Neben der klassischen *Red- and Blue-Perspektive* gilt es, immer weitere Dimensionen und Ebenen wie beispielsweise *Cyber Threat*, *Space* oder *Environmental* einzubinden.

Ohne eine systematische und ganzheitliche Entwicklungsstrategie für die Streitkräfte lässt sich die ständig zunehmende Komplexität dieser Systeme und Prozesse nicht mehr beherrschen. Der stetige Zuwachs an spezifischen Fähigkeiten und spezialisierten Diensten stellt ein „Moving Target“ dar. Die Problematik besteht zudem in der Erreichung von Anwendungs- und Datenkompatibilität unter den verschiedenen Systemen und Sicherheitsleveln sowie in der korrekten Interpretation der Semantik von Informationen unter strikter Einhaltung von Datenschutz und Vertraulichkeit. Das Modul bereitet die zukünftigen Führungskräfte auf diese Herausforderungen vor und vermittelt die entsprechenden Grundlagen, Methoden und Anwendungskenntnisse.

Zunächst erfolgt eine grundlegende Einführung in die Begriffswelt, die komplexen Anforderungen und den zu erfüllenden Anspruch einer NetOpFü im trägernahen Kontext. Dies beinhaltet die mit der digitalen Transformation verbundenen Anwendungssysteme sowie die im Zusammenhang stehenden Wissens- und Informationsstrukturen.

Anschließend erfolgt eine vertiefte Auseinandersetzung mit den aktuellen und im Rahmen der NATO-Streitkräfte unterstützenden Systemen und Integrationskonzepten des sog. *Federated Mission Networking (FMN*). Dies umfasst die zentralen Aspekte der Kompatibilität hinsichtlich integraler Interoperabilität und Sicherheit mit dem Ziel einer gemeinsamen multinationalen, streitkräfteübergreifenden Fähigkeitsweiterentwicklung.

Einblicke in den aktuellen Stand von Wissenschaft, Forschung und Technik werden an konkreten Beispielen vermittelt: *C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance)* und *Network Centric Warfare (NCW)*. An Fallbeispielen wird die Anwendung des zentralen Konzeptes *des Effects-based Approach to Operations (EBAO)* diskutiert. Weiterhin wird anhand ausgewählter Studien der zentrale Ansatz *des Concept Development & Experimentation (CD&E)* vorgestellt, der für die Gestaltung, Validierung und Einführung von IT-gestützten Verfahren und Methoden eine zentrale Bedeutung hat. Die dabei notwendigen administrativen und logistischen Prozesse zur Unterstützung der Führungsaufgaben runden die digitale Weiterentwicklungsstrategie ab.

Darüber hinaus vermittelt das Modul wichtige Grundlagen und Konzepte des *Knowledge Management* zur wissensbasierten Entscheidungsunterstützung in komplexen, vernetzten Operationen. Mittels der architekturbasierten Gestaltung auf der Basis von entsprechenden Rahmenwerken (*NATO Architecture Framework NAF*) wird *Enterprise Architecture* als systematischer Ansatz zur fähigkeitszentrierten Weiterentwicklung von Digitalen Streitkräften vorgestellt und vertieft. Dabei wird auch der gesamtplanerische Zusammenhang zur NATO und dem FMN aufgegriffen unter Berücksichtigung von Multi-Layer-Defence und -Security-Ansätzen.

In der begleitenden Übung haben die Teilnehmer Gelegenheit, einzelne Aspekte anhand von Standards, Best Practices und Beispielen aus Forschung und Praxis eigenständig zu vertiefen und so erste Anwendungserfahrungen zu sammeln. Abgerundet wird das Modul durch den Einbezug externer Experten, die Einblicke in ihre unmittelbaren praxisnahen Erfahrungen mit Lösungsansätzen im Kontext der Vernetzten Operationsführung geben.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Literatur

1. Sebastian Schäfer: Vernetzte Operationsführung – Eine Einführung, Luftwaffenamt, 2005
2. David S. Alberts, John J. Garstka, Frederick P. Stein: Network Centric Warfare, CCRP Publication Series, 2000
3. Michael-Günther Lux: Effects-Based Approach to Operations (EBAO), Luftwaffenamt, 2007
4. Dr. Lee Whitt: SmartCOP – the fusion of collaborative workspaces and the Common Operational Picture, International Command and Control Research and Technology Symposium, 2005
5. Edward A. Smith: Effects Based Operations (EBO) – Applying Network Centric Warfare in Peace, Crisis and War, Washington, 2002
6. Edward A. Smith: Complexity, Networking and Effects-Based Approaches to Operations, Washington, 2006

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Das Wahlpflichtmodul ist die Grundlage für weiterführende und vertiefende Veranstaltungen sowie wissenschaftliche Arbeiten im Kontext der Vernetzten Operationsführung. Es stellt Basiswissen für die Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/Cyber Sicherheit dar. Es stellt zudem eine gute Ergänzung mit den Wahlpflichtmodulen für "Projektmanagement" sowie "Enterprise Architecture und IT Service Management", die einen eher querschnittlichen, aber ebenso zentralen Blickwinkel etablieren.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im HT.

Modulname	Modulnummer
Digitale Forensik	1551

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15511	VL	Digitale Forensik (VL)	Pflicht	3
15512	UE	Digitale Forensik (UE)	Pflicht	3
15513	SE	Seminar zur IT-forensischen Gutachtenerstellung	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Voraussetzungen laut Prüfungsordnung

Das Modul 5505 muss bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.

Qualifikationsziele

Die Studierenden kennen die allgemeine IT-forensische Vorgehensweise und können diese bei der Durchführung IT-forensischer Analysen anwenden sowie in einem Gutachten dokumentieren. Sie kennen wichtige Spurenquellen im Betriebssystem Windows und können diese auswerten. Die Studierenden kennen Datenformate von verbreiteten Anwendungen und können diese analysieren. Sie wissen Sicherungs- und Analyseverfahren des Hauptspeichers und können diese anwenden. Wesentliche Anti-Forensik-Ansätze sind den Studierenden bekannt, und sie können diese bewerten. Weiterhin können die Studierenden Speichertechnologien erklären und digitale Spuren eingebetteter Systeme IT-forensisch sichern und auswerten.

Inhalt

Die Studierenden lernen die Betriebssystemforensik am Beispiel von Windows kennen und arbeiten insbesondere mit der Windows-Registry sowie Windows-Artefakten. Im Kontext der Anwendungsforensik wird das SQLite Datenbankformat behandelt und für Anwendungen wie Firefox, Thunderbird, Skype analysiert. Die Sicherung und Analyse des Hauptspeichers wird mittels des Windows-Betriebssystems und des Frameworks Volatility behandelt. Auf dem Gebiet der Anti-Forensik lernen die Studierenden die gängigen Kategorien von antiforensischen Maßnahmen kennen und bewerten. Flashbasierte Speichertechnologien sowie der direkte Zugriff auf einen Datenträger und die zugehörige Auswertung sind low-level Fertigkeiten, die die Studierenden einsetzen.

An Hand der Erstellung eines Gutachtens für ein Fallbeispiel werden im Rahmen des Seminars die gelernten Inhalte umfassend angewendet.

Literatur

- Carvey, Harlan. Windows registry forensics: Advanced digital forensic analysis of the windows registry. Elsevier, 2011.
- Carrier, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.
- Casey, Eoghan, Cameron H. Malin, and James M. Aquilina. Malware forensics: investigating and analyzing malicious code. Syngress, 2008.
- Hummert, Christian, and Dirk Pawlaszczyk, eds. Mobile Forensics-The File Format Handbook: Common File Formats and File Systems Used in Mobile Devices. Springer Nature, 2022.
- Solomon, David A., Mark E. Russinovich, and Alex Ionescu. Windows internals. Microsoft Press, 2009.
- Russinovich, Mark E., David A. Solomon, and Alex Ionescu. Windows internals, part 2. Pearson Education, 2012.
- Sanderson, Paul, et al. SQLite Forensics. Independently published, 2018.

Leistungsnachweis

Portfolio: Es sind die Lösungen von 6 der 8 Übungsblätter schriftlich auf 5 Seiten zum Übungstermin via Ilias im pdf-Format abzugeben und im zugehörigen Übungstermin aktiv zu erläutern. Die Bearbeitungszeit beträgt je 1 Woche. Im Rahmen des Seminars ist eine 15-seitige Ausarbeitung als exemplarisches Gutachten zu einer vorgegebenen Zweifelsfrage anzufertigen, die Bearbeitungszeit für die Ausarbeitung beträgt 10 Wochen im Zeitraum Mitte Dezember bis Ende Februar des Folgejahres. Über alle drei Lehrveranstaltungen wird ein 30-minütiges individuelles Fachgespräch durchgeführt, dessen Ergebnis zu 100% die Modulnote ist.

Verwendbarkeit

Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Einführung in die Quanteninformationsverarbeitung	3010

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Dr. Dipl.-Phys. Sabine Tornow	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
30101	VÜ	Einführung in die Quanteninformationsverarbeitung	Pflicht	3
30102	P	Praktikum Quantenschlüsselaustausch	Wahlpflicht	3
30103	SE	Seminar Quantentechnologien	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in linearer Algebra. Vorkenntnisse in Quantenmechanik und Kryptographie sind hilfreich, aber nicht erforderlich.

Qualifikationsziele

Studierende verstehen Konzepte der Quanteninformationsverarbeitung (Quantenkommunikation, Quantenkryptographie, Quantenkodierungstheorie, Quantenalgorithmen und Quantenfehlerkorrektur) und können weitere Entwicklungen zu Quantenkryptographie, Algorithmen, Fehlerkorrektur und Quantenkommunikation einordnen und bewerten. Studierende können Experimente, z.B. zur Quantenkommunikation und Fehlerkorrekur implementieren und auf einem Quantencomputer testen und die praktische Realisierung des Quantenschlüsselaustausches experimentell umsetzen (siehe Praktikum).

Am Ende des Kurses sind die Studierenden in der Lage, den grundlegenden mathematischen Formalismus (z.B. Zustände, Kanäle) und die Schlüsselkonzepte zu erklären. Sie sind in der Lage, diese Konzepte und Methoden anzupassen und anzuwenden, um Probleme der Quanteninformationsverarbeitung zu lösen.

Inhalt

Vorlesung: Quanteninformation ist eine Synthese von Informatik, Quantentheorie und Informationstheorie. Quantensysteme werden zur Speicherung von Information und die Gesetze der Quantenmechanik zur Verarbeitung von Information verwendet. Die in diesen Systemen vorhandene Information kann nicht mit den Gesetzen der klassischen Informationstheorie beschrieben werden. Diese wird zur Quanteninformationstheorie erweitert. Die Quanteninformation ermöglicht eine fundamental neue Art der Informationsverarbeitung wie die Quantenteleportation, Quantenkryptographie und

Quanten-Algorithmen. Es werden folgende Themengebiete behandelt: Grundlagen der Quantentheorie, Quantenverschränkung, Quanten-Shannon-Theorie, effiziente Quantenalgorithmen, Quantenkryptographie, Quantenkanäle, Quantenfehlerkorrektur, Quantennetzwerke und Quantenkommunikation.

Praktikum:

- Durchführung eines QKD-Modellversuchs, der das BB84-Protokoll mit polarisiertem Licht in der Praxis umsetzt
- Detailliertes Wissen über die Schritte, die für ein QKD-Protokoll erforderlich sind
- Experimentelle Durchführung des Protokolls in Teams bestehend aus zwei Personen, die die Rolle von Sender und Empfänger übernehmen
- Versenden einer mit Quantenschlüsseln verschlüsselten Nachricht
- Verfassen eines Versuchsprotokolls

Seminar: Aktuelle Themen in den Bereichen der Quantentechnologie:

Quantensensorik, Quantum Memory, Quantum Repeater, Quantum Computing, Quantenkommunikation, Post-Quantum Kryprographie, Quantenmetrologie, Quantenbildgebung, usw.

Literatur

- Riccardo Manenti and Mario Motta: Quantum Information Science, Oxford University Press
- Thomas Vidick and Stephanie Wehner: Introduction to Quantum Cryptography, Cambridge University Press
- Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

- als Wahlpflichtmodul im Studiengang Master Cyber-Sicherheit (MCYB)
- in Modul 5506 Kryptologie im Studiengang MCYB
- in Modul 3491 Algorithmen und Komplexität im Studiengang MINF
- in Modul 3820 Quantencomputer in Theorie und Praxis im Studiengang MCYB
- in Modul 1037 Informations- und Codierungstheorie im Studiengang MCYB
- in Modul 1289 Nachrichtentheorie und Übertragungssicherheit im Studiengang MCYB
- in Modul 5548 Modern Cryptography im Studiengang im Studiengang MCYB
- in Modul 2994 Ausgewählte Kapitel des OR: Data-driven Optimization MINF

Dauer und Häufigkeit

Das Modul wird jedes Jahr ab dem WT angeboten und dauert zwei Trimester. Die Vorlesung wird im WT angeboten, das Praktikum oder das Seminar im FT.

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	3396

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
33961	VÜ	Data Mining und IT-basierte Entscheidungsunterstützung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Grundkenntnisse zu mathematischen Methoden des Operations Research und der Statistik wie sie z.B. im Bachelor Informatik bzw. Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Insbesondere ist es das Ziel, IT-basierte Entscheidungsunterstützung unter der speziellen Cyberperspektive zu betrachten: Wie können Angriffe schneller erkannt, wie kann man sich optimal dagegen schützen und wie können Entscheidungsunterstützungssysteme gegenüber Cyberangriffen optimiert werden. Das Modul gibt einen Überblick über aktuelle Modelle und Verfahren sowie relevante Bedrohungsszenarien.

Inhalt

Die Studierenden sollen in dieser Veranstaltung mit den IT-basierten und entscheidungstheoretischen Grundlagen im Bereich der modernen Datenanalyse vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von geeigneten Analyseverfahren zur Erforschung von komplexen datenbasierten Zusammenhängen ("Exploratory Analysis").

Data Mining bedeutet dabei das Extrahieren von impliziten, noch unbekannten Informationen aus Rohdaten. Dazu sollten IT-Systeme in die Lage versetzt werden, Datenbanken und Datenansammlungen (z.B. im Bereich der Geoinformatik) automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert. Insbesondere das heutige maschinelle Lernen und das Verfahren des "Datafarming" stellen dafür die Werkzeuge und Techniken zur Verfügung, die in den Bereich des modernen Wissensmanagements (bis zur Begriffsanalyse) und "Datamining" hineinführen.

Literatur

- Decision Support Systems Developing Web-Enabled Decision Support Systems, Abhijit A. Pol and Ravindra K. Ahuja. Dynamic Ideas 2007.
- Exploratory Data Analysis Making Sense of Data: A Practical Guide to Exploratory Data Analysis and Data Mining, Glenn J. Myatt. John Wiley, 2006.
- Spatial Data Analysis Spatial Data Analysis - Theory and Practice, Robert Haining, Cambridge University Press 2003.
- Data Mining Data Mining: Practical Machine Learning Tools and Techniques (Second Edition) Ian H. Witten, Eibe Frank. Morgan Kaufmann 2005.
- Data Mining: A Knowledge Discovery, K. Cios, W. Pedrycz, R. Swiniarski Springer, 2007.
- Data Mining Introductery and Advanced Topics, Margaret Dunham, Prentice Hall, 2003.
- Advances in Knowledge Discovery and Data Mining, U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, editors , MIT Press, 1996.
- Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber. Morgan Kaufmann, 2006.
- Principles of Data Mining, David J. Hand, Heikki Mannila and Padhraic Smyth. MIT Press, 2000. Daniel T. Larose,
- Discovering Knowledge in Data: An Introduction to Data Mining, John Wiley 2004. Robert Nisbet, John Elder, IV and Gary Miner.
- Handbook of Statistical Analysis and Data Mining Applications. Elsevier 2009.
- Statistical Learning - Machine Learning Trevor Hastie, Robert Tibshirani, Jerome Friedman,
- The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Verlag, 2001. Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, Wiley-IEEE Press, 2002.

Weiterführende Literatur:

- Zeitreihenanalyse Time Series Analysis. Hamilton 1994.
- Reinforcement Lernen und Spieltheorie Reinforcement Learning: An Introduction. Sutton and Barto: MIT Press 1998.
- Fun and Games: A Text on Game Theory. Binmore, Linster, Houghton Mifflin 2000.
- Statistik Bayesian Data Analysis. Gelman, Carlin, Stern, Rubin: Chapman 1995. Introduction to Mathematical Statistics. Hogg, Craig: Prentice Hall 2004.
- Principles of Statistics. Bulmer: Dover 1979.
- Probability, Random Variables and Stochastic Proc., Papoulis, McGraw, Hill 2002.

Leistungsnachweis

Portfolio auf der Basis der folgenden vier Teilleistungen, je mit 25% gewichtet, für deren Bearbeitung die Studierenden einen Bearbeitungszeitraum von je 2 Wochen haben:

1. Analysebericht "Pre-Processing" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)
2. Analysebericht "Clustering" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)
3. Analysebericht "Classification" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)

4. Analysebericht "Outlier Detection" (Text mit maximal 3600 Zeichen (inkl. Leerzeichen) plus Visualisierungen und Jupyter Notebook Anhang)

Verwendbarkeit

Die Vorlesung kann durch weiterführende Veranstaltungen im Bereich der Datenanalyse fortgeführt werden, z.B. im Bereich der modernen Begriffsanalyse, des Algorithmic Engineering, im Rahmen von Spezialvorlesungen der Numerik und Statistik sowie der Geoinformatik. Ebenfalls bestehen enge Bezüge zu wissenschaftlichen Forschungsgebieten im Bereich der Künstlichen Intelligenz.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Compilerbau	3647

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau studiert die systematische Konstruktion von Compilern in allen Phasen, mithin der lexikalischen, syntaktischen und semantischen Analyse mit gängigen Verfahren. Die Vorlesung startet mit einer kleinen Untermenge der C Programmiersprache und vergrößert diese Menge schrittweise wie folgt:

- Unterstützung mehrerer skalarer Datentypen, z.B. Bool'sche Variablen
- Unterstützung mehrerer zusammengesetzter Datentypen, z.B. Records
- Unterstützung von komplexeren lokalen Variablen
- Unterstützung von Funktionen

Innerhalb der wachsenden Programmiersprache werden verschiedene Konzepte erörtert:

- Typüberprüfung
- Feldgrenzenüberprüfung
- Direkte Erzeugung von Maschinencode
- Optimierungen (Register Allokation, Peephole Optimization, etc.)
- Virtuelle Maschinen, Konstruktion und Optimierung.

Literatur
• Engineering a Compiler, Cooper & Torczon. • Modern Compiler Implementation in ML, Andrew Appel. • Modern Compiler Design, Grune et al. • Principles of Program Analysis, Fleming et al. • Compiler Construction, Waite und Goos. • Übersetzerbau: Band 1: Virtuelle Maschinen; Wilhelm, Seidl. • Übersetzerbau: Band 2: Syntaktische und semantische Analyse; Wilhelm, Seidl, Hack. • Übersetzerbau: Band 3: Analyse und Transformation; Seidl, Wilhelm, Hack. • Structure and Interpretation of Computer Programs; Abelson und Sussman. • How to Design Programs, Matthias Felleisen, Robert Bruce Findler, Matthew Flatt, Shriram Krishnamurthi. • Schreibe Dein Programm!; Herbert Klaeren, Michael Sperber. • The Little Schemer, Friedman, Felleisen.
Leistungsnachweis
Schriftliche Prüfung von 120 Minuten Dauer.
Verwendbarkeit
• Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfeld Software- und Informationsmanagement • Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Enterprise Security und Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Compilerbau (erweitert)	3648

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
36481	P	Praktikum Compilerbau	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau studiert die systematische Konstruktion von Compilern in allen Phasen, mithin der lexikalischen, syntaktischen und semantischen Analyse mit gängigen Verfahren. Die Vorlesung startet mit einer kleinen Untermenge der C Programmiersprache und vergrößert diese Menge schrittweise wie folgt:

- Unterstützung mehrerer skalarer Datentypen, z.B. Bool'sche Variablen
- Unterstützung mehrerer zusammengesetzter Datentypen, z.B. Records
- Unterstützung von komplexeren lokalen Variablen
- Unterstützung von Funktionen

Innerhalb der wachsenden Programmiersprache werden verschiedene Konzepte erörtert:

- Typüberprüfung
- Feldgrenzenüberprüfung
- Direkte Erzeugung von Maschinencode
- Optimierungen (Register Allokation, Peephole Optimization, etc.)
- Virtuelle Maschinen, Konstruktion und Optimierung.

Das Praktikum Compilerbau vertieft die Kenntnisse des Compilerbaus in verschiedene Richtungen (siehe Leistungsnachweis). Im Praktikum gibt es einen spezifischen Fokus auf Sicherheit-basierte Themen, es besteht z.B. die Moeglichkeit Control-Flow Integrity oder Software Diversity im eigenen Compiler aus dem vorhergehenden Trimester (also WT oder FT) zu implementieren.

Literatur

- Engineering a Compiler, Cooper & Torczon.
- Modern Compiler Implementation in ML, Andrew Appel.
- Modern Compiler Design, Grune et al.
- Principles of Program Analysis, Fleming et al.
- Compiler Construction, Waite und Goos.
- Übersetzerbau: Band 1: Virtuelle Maschinen; Wilhelm, Seidl.
- Übersetzerbau: Band 2: Syntaktische und semantische Analyse; Wilhelm, Seidl, Hack.
- Übersetzerbau: Band 3: Analyse und Transformation; Seidl, Wilhelm, Hack.
- Structure and Interpretation of Computer Programs; Abelson und Sussman.
- How to Design Programs, Matthias Felleisen, Robert Bruce Findler, Matthew Flatt, Shriram Krishnamurthi.
- Schreibe Dein Programm!; Herbert Klaeren, Michael Sperber.
- The Little Schemer, Friedman, Felleisen.

Leistungsnachweis

Der Leistungsnachweis ist ein Portfolio und besteht aus einer praktischen Ausarbeitung eines komplexeren Teilgebiets des Compilerbaus in dem eigenen, in der Compilerbau Übung erstellten Compiler. Die Teilgebiete umfassen folgende Aufgaben:

- Design und Implementierung eines einfachen Python Frontends für den erstellten Beispielcompiler.
- Design und Implementierung komplexer Datentypen, Unterstützung für Klassen, Objekte und dynamische Bindung von Methodenaufrufen.
- Backend-Optimierungen: Design und Implementierung eines automatischen Befehlsauswahlverfahrens auf Grundlage von Bottom-Up Rewriting Systems (BURS).
- Backend: Unterstützung einer zusätzlichen Backend-Architektur, z.B. RISC-V oder ARM.
- Sprachbasierte Sicherheit: Implementierung verschiedener Compiler-gestützter Verteidigungstechniken

Es kann nur ein Thema gewählt werden, die Bearbeitungszeit umfasst 6 bis 12 Wochen. Die Bearbeitung wird durch eine Präsentation mit einer Dauer von 20 - 40 Minuten, durch die Abgabe des Quelltextes der erbrachten Lösung (Umfang: 1000 - 2000 Codezeilen) und durch ein Fachgespräch mit zugehörigen Verständnisfragen, ebenfalls im Umfang von 20 - 40 Minuten, abgeschlossen.

Die Note wird wie folgt berechnet:

- 1/3: Implementierung zu Compilerbau Uebung
- 1/3: Implementierung des Praktikums

• 1/3: Muendliche Pruefung zum Thema der Praktikumsimplementierung
Verwendbarkeit
• Wahlpflichtmodul im Masterstudiengang INF, Vertiefungsfeld Software- und Informationsmanagement • Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Enterprise Security und Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Cyber Network Capabilities Methoden	3822

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Hartmut König	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3822 -V1	VÜ	CNC Methoden	Pflicht	3
3822 -V2	P	Praktikum CNC Methoden	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Betriebssystemen und Rechnernetzen, wie sie z. B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden, sowie Kenntnisse zu den Grundlagen der IT-Sicherheit aus den Pflichtfächern des Studiengangs. Die Anwendung von CNC-Methoden erfordert darüber hinaus detaillierte Kenntnisse der rechtlichen Rahmenbedingungen ihres Einsatzes. Deshalb wird empfohlen, das Modul Rechtliche Grundlagen CNC vorher (falls angeboten), in Begleitung zu diesem Modul oder danach unbedingt zu belegen.

Qualifikationsziele

Die Studierenden lernen die wichtigsten CNC-Methoden, u.a. die Grundlagen für die Informationstechnische Überwachung (Quellen-TKÜ und Onlinedurchsuchung), die Funktionsweise von Schwachstellen und Exploits und den sicheren Umgang mit diesen, Maßnahmen nach §100i StPO, Messenger-Überwachung, Gewinnung von OSINT-Daten und die dafür eingesetzten Werkzeuge kennen. Sie können die Einsatzfelder der Methoden eingrenzen, lernen die notwendigen Voraussetzungen und Schritte ihres Einsatzes kennen. Darüber hinaus erwerben sie praktische Fähigkeiten im Umgang mit CNC-Systemen und Werkzeugen.

Inhalt

Die Vorlesung behandelt die wichtigsten CNC-Methoden, stellt die Randbedingungen ihres Einsatzes vor, und erläutert die dafür notwendige Infrastruktur. Sie verweist auch auf die rechtlichen Rahmenbedingungen, die ausführlich im Modul *Rechtliche Grundlagen CNC* behandelt werden. Sie stellt die verschiedenen Phasen der Durchführung von CNC-Maßnahmen vor (Aufklärung, Einbringung, Datengewinnung, Rückstandsfreies Löschen) und erläutert wichtige Arbeitstechniken, z. B. Aufklärung auf dem Gerät, unentdecktes Bewegen im Netz, u.a.

Im Praktikum CNC-Methoden lernen die Studierenden, die in der Vorlesung vermittelten Techniken praktisch anzuwenden. Sie werden in die Nutzung verschiedener CNC-Systeme und Werkzeuge eingeführt, um komplexere Probleme aus der Praxis eigenständig bzw. in kleinen Teams zu lösen.
Leistungsnachweis
Schriftliche Prüfung von 90 Minuten Dauer.
Verwendbarkeit
Das Beherrschen von CNC-Methoden und -Werkzeugen und der sichere und verantwortungsvolle Umgang mit diesen ist essentielle Voraussetzung für einen Einsatz in der der Telekommunikationsüberwachung sowie der Weiterentwicklung dieser Methoden.
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Rechtliche Grundlagen Cyber Network Capabilities	3823

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Hartmut König	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3823-V1	VL	Rechtliche Grundlagen CNC	Pflicht	4
3823-V2	UE	Rechtliche Grundlagen CNC (Übung)	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Keine.

Qualifikationsziele

Die Studierenden lernen die rechtlichen Grundlagen für die informationstechnische Überwachung (Quellen-TKÜ und Onlinedurchsuchung) durch Polizei und Nachrichtendienste in Deutschland kennen und werden befähigt, die rechtlichen Rahmenbedingungen bei der Anwendung von CNC-Methoden in der Praxis richtig einzuschätzen und im Sinne eines angemessenen, grundrechtskonformen Interessenausgleichs zu beurteilen.

Das Modul sollte vor bzw. nach oder in Begleitung des Moduls CNC-Methoden belegt werden.

Inhalt

Die Vorlesung vermittelt Grundkenntnisse zu

- den im Zusammenhang mit Quellen-TKÜ und Onlinedurchsuchung stehenden grundrechtlichen Anforderungen
- Artikel 10 Gesetz
- den §§ 100 ff. StPO
- sowie den einschlägigen weiteren Regelungen der Strafprozessordnung (StPO), des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG) und den rechtlichen Grundlagen zur Durchführung einer Telekommunikationsüberwachung aus dem BKA-Gesetz, dem Bundesverfassungsschutzgesetz, dem BND-Gesetz, dem BSI-Gesetz und dem Zollfahndungsgesetz (ZfDG) als Teil der Gesamtrechtsordnung zwecks eigenständiger Einordnung und Beurteilung entsprechender Sachverhalte
- unter Berücksichtigung einschlägiger Rechtsprechung.

Des Weiteren sollen die Studierenden die TKÜ-Verordnung und die Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜV) kennenlernen und Beispiele aus der Praxis an Hand dieser Vorschriften sicher bewerten können. Abschließend wird auf den Errichtungserlass der ZITiS eingegangen.

Literatur

- Kipker, Rechtshandbuch Cybersecurity. C.H.BECK. ISBN 978-3-406-79263-2, 2. Auflage. 2023.
- Kipker/Reusch/Ritter, Kommentar Recht der Informationssicherheit. C.H.BECK. ISBN 978-3-406-78339-5. 2023
- Graulich/Schenke/Ruthig, Sicherheitsrecht des Bundes. C.H.BECK. ISBN 978-3-406-71602-7. 2. Auflage. 2019

Leistungsnachweis

Hausarbeit. Umfang: 10 Seiten, Bearbeitungszeit 3-4 Wochen.

Verwendbarkeit

Für den sicheren und verantwortungsvollen Umgang und den Einsatz von CNC-Methoden und -Werkzeugen ist es unabdingbar, den rechtlichen Rahmen und die einschlägigen Rechtsvorschriften zu kennen und Sachverhalte in der informationstechnischen Überwachung klar beurteilen und einordnen zu können.

Dauer und Häufigkeit

Das Modul dauert ein Trimester.

Modulname	Modulnummer
Post-Quantum Cryptography	3931

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
39311	VÜ	Introduction to Post-Quantum Cryptography	Pflicht	4
39312	VÜ	Selected Topics in Post-Quantum Cryptography	Pflicht	4
39313	SE	Post-Quantum Cryptography in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Grundkenntnisse in Mathematik (Diskrete Strukturen, Lineare Algebra, Wahrscheinlichkeitstheorie) und in Informatik (Algorithmenentwurf und -analyse) sowie in der Kryptographie (Basiskonzepte) vorausgesetzt. Notwendige (minimale) Grundlagen des Quantencomputings werden in den Lehrveranstaltungen eingeführt.

Qualifikationsziele

Die Studierenden kennen den Einfluss von Quantencomputern auf die Kryptographie (Shor, Grover) und deren Implikationen. Sie kennen quantenresistente mathematische Problemklassen, deren Sicherheit und Verwendung dieser zur Konstruktion kryptographischer Basismechnismen. Die Studierenden kennen Designprinzipien von aktuellen Post-Quanten Verfahren und deren Funktionsweise und haben einen Einblick in die aktuellen praktischen und theoretischen Herausforderungen der Post-Quanten Kryptographie. Sie sind in der Lage kryptographische Verfahren zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um die Post-Quanten Kryptographie und ihre Anwendungen.

Inhalt

Introduction to Post-Quantum Cryptography - In dieser Vorlesung werden die Gundlagen der Post-Quanten (oder quantensicheren) Kryptographie behandelt.
Es wird die Notwendigkeit der Neubetrachtung der Kryptographie aufgrund von Quantencomputern und relevanter Quantenalgorithmen (Shor, Grover) sowohl im Kontext symmetrischer als auch asymmetrischer Kryptographie diskutiert. Danach werden die Unterschiede zwischen klassischen Angreifern und Quantenangreifern sowie die Auswirkungen auf die beweisbare Sicherheit veranschaulicht. Der Hauptteil

der Vorlesung umfasst dann einen Überblick über relevante Klassen mathematischer Probleme die zur Konstruktion quantensicherer Kryptographie herangezogen werden. Dies umfasst hash-basierte Signaturen, multivariate Kryptographie, Kryptographie basierend auf fehlerkorrigierenden Codes, gitterbasierte Kryptographie sowie isogeniebasierte Kryptographie. In den Übungen werden die Kenntnisse aus der Vorlesung vertieft sowie konkrete Beispiele und Beweise betrachtet.

Selected Topics in Post-Quantum Cryptography - In dieser Vorlesung werden zuerst, aufbauend auf den in der ersten Vorlesung erarbeiteten Grundlagen, moderne Konstruktionsprinzipien aktueller beweisbar sicherer quantenresistenter kryprographischer Basismechanismen (asymmetrische Verschlüsselung bzw. KEMs und Signaturen) betrachtet. Dies umfasst sowohl generische Prinzipien wie auch spezifische Aspekte für ausgewählte Verfahren verschiedener Problemklassen. Danach werden ausgewählte und aktuell relevante Themen aus dem Bereich der Post-Quanten Kryptographie betrachtet: Dies umfasst sowohl praktische als auch theoretisch und stärker forschungsbezogene Aspekte. Beispielsweise die Standardisierung von und Migration zu Post-Quanten Kryptographie (z.B. Hybridisierung), die Integration von Post-Quanten Kryptographie (in Sicherheitsprotokolle oder aktuelle Anwendungen) wie auch die Konstruktion fortgeschrittener kryptographischer Verfahren basierend auf Post-Quanten Annahmen und damit in Verbindung stehende Herausforderungen. In den Übungen werden die Kenntnisse aus der Vorlsung vertieft sowie konkrete Beispiele und Beweise betrachtet.

Post-Quantum Cryptography in Practice - In diesem praxisorientierten Seminar geht es um den praktischen Einsatz von quantensicheren kryptographischen Verfahren.
In Bezug auf das ausgewählte Thema wird von den Studierenden eine weitgehend selbständig gefertigte prototypische Umsetzung eines Miniprojektes unter Verwendung von geeigneten open-source Softwarebibliotheken bzw. Technologien erwartet. Die Ergebnisse der Implementierungsarbeit sollen dann in einem Bericht beschrieben und während der Präsentation demonstriert werden.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen können zum Teil auch in englischer Sprache gehalten werden.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio:

Zu den Vorlesungen mit Übungen: ein mündliches Fachgespräch von 30 Minuten oder eine schriftliche Klausur von 60 Minuten über die Inhalte aus beiden Veranstaltungen; die Form des Leistungsnachweises wird zu Beginn des Moduls festgelegt.

Zum Seminar: Erstellung und Abgabe einer Präsentation zur Demonstration von Ergebnissen des Miniprojektes (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.
Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfelder Enterprise Security, Public Security, Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im Frühjahrstrimester.

Modulname	Modulnummer
Foundations of Distributed Systems and Blockchains	5118

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Daniel Slamanig	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
51181	VÜ	Foundations of Distributed Systems and Blockchains	Pflicht	4
51182	SE	Research Topics in Security for Decentralized Systems	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Grundkenntnisse in Mathematik (Diskrete Strukturen, Lineare Algebra, Wahrscheinlichkeitstheorie) und in Informatik (Algorithmenentwurf und -analyse) vorausgesetzt. Basiswissen in der Kryptographie (Basiskonzepte) ist hilfreich, aber nicht notwendig (alle verwendeten Konzepte werden im Modul eingeführt).

Qualifikationsziele

Die Studierenden kennen grundlegende Konzepte in dezentralen Systemen (z.B. Fehlertoleranz und Konsensus) und lernen grundlegende kryptographische Mechanismen kennen, die zur Realisierung dieser Eigenschaften notwendig sind (z.B. Hashfunktionen, MACs und Signaturen). Diese Konzepte werden dann anhand von Blockchains und Kryptowährungen betrachtet und es werden weitere wichtige Konzepte im Kontext von Blockchains eingeführt (z.B. Proof-of-Work, Proof-of-Stake, Proof-of-Space). Die Studierenden lernen relevante kryptographische Mechanismen wie das Generieren von verteilten und verifizierbaren Zufallszahlen sowie das Feld der Threshold-Kryptographie und deren Anwendungen kennen. Darüber hinaus bekommen die Studierenden einen Einblick in Privatheits- und Skalierungsprobleme in Blockchains sowie in kryptographische Konzepte, mit denen diese Probleme gelöst werden können. Im Speziellen wird das Konzept des Verifiable Computing und so genannter Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) behandelt. Studierende sind in der Lage Herausforderungen in dezentralen Systemen (im Speziellen Blockchains) zu erkennen und zu analysieren sowie die Einsatzmöglichkeiten relevanter kryptographischer Mechanismen zur Lösung dieser Herausforderungen zu verstehen. Darüber hinaus kennen die Studierenden den aktuellen Stand der Forschung in diesem Feld.

Inhalt

Foundations of Distributed Systems and Blockchains - In dieser Vorlesung werden die Grundlagen von dezentralen Systemen sowie in diesem Kontext relevanter Kryptographie behandelt. Ein Schwerpunkt der Vorlesung liegt auf Blockchains und Kryptowährungen, insbesondere auf deren Grundlagen und Funktionsweise. Hier werden Mechanismen wie Proof-of-Work, Proof-of-Stake sowie Proof-of Space, Transaktionen sowie notwendige kryptographische Mechanismen (z.B. Merkle Trees) und deren Abstraktionen und Varianten behandelt. Es wird auch die Unveränderlichkeit von Blockchains kritisch hinterfragt und Konzepte zur „Aufweichung“ dieser Eigenschaft werden präsentiert. Als wichtiges kryptographisches Konzept wird die so genannte Threshold-Kryptographie eingeführt, die es ermöglicht kryptographische Funktionalität (z.B. das Erstellen einer Signatur) auf mehrere Parteien zu verteilen. Als verwandtes Thema wird auch die verteilte und verifizierbare Erzeugung von Zufallszahlen behandelt. Bei all diesen kryptographischen Konzepten wird immer der Bezug zu Anwendungen im Blockchain-Kontext veranschaulicht. Als ein weiteres wichtiges Konzept wird so genanntes Verifiable Computing und so genannte Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zk-SNARKs) behandelt. Diese Techniken ermöglichen das Lösen von Skalierbarkeits- und Privatheitsproblemen in Blockchains. In den Übungen werden die Kenntnisse aus der Vorlesung vertieft sowie konkrete Beispiele betrachtet.

Research Topics in Security for Decentralized Systems - In diesem Seminar bekommen Studierende einen Einblick in aktuelle Forschungsthemen an der Schnittstelle zwischen dezentralen Systemen und Sicherheit mit Fokus auf Einsatz von Kryptographie. Die Schwerpunkte liegen auf neuen kryptographischen Verfahren und Konzepten sowie deren Anwendungen in dezentralen Systemen und Blockchains im Speziellen. Zu Beginn des Seminars wird eine Themenauswahl vorgestellt, die von Studierenden über die Dauer des Seminars bearbeitet und am Ende präsentiert werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikel aus führenden wissenschaftlichen Konferenzen stützen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Vorlesung wird in deutscher Sprache gehalten, Teile der Übungen und des Seminars können auch in englischer Sprache gehalten werden.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen:

51181: Ein mündliches Fachgespräch von 20 Minuten oder eine schriftliche Klausur von 45 Minuten; die Form des Leistungsnachweises wird zu Beginn des Moduls festgelegt.

In 51182: Erstellung und Abgabe einer schriftlichen Ausarbeitung (10 bis 20 Seiten) und eine Präsentation (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 60 zu 40 in die Note ein.

Verwendbarkeit
Wahlpflichtmodul im Masterstudiengang Cyber-Sicherheit, Vertiefungsfelder Enterprise Security, Public Security, Cyber Network Capabilities
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und beginnt jedes Jahr in WT. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Mobile Security	5513

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gabi Dreo Rodosek	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11972	VÜ	Mobile Kommunikationssysteme	Pflicht	3
55131	VÜ	Sichere mobile Systeme	Wahlpflicht	3
55132	VÜ	Sensorik und Manipulationsdetektion	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für die Veranstaltungen im Modul werden grundlegende Kenntnisse in Rechnernetzen vorausgesetzt, wie sie z.B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten ein umfassendes Wissen der Funktionsweise mobiler Kommunikationsnetze. Sie können die wichtigsten Grundlagen drahtloser Kommunikationstechniken erläutern und die verschiedenen Verfahren und Systeme kategorisieren. Je nach erfolgter Auswahl innerhalb des Moduls haben sie vertiefte Kenntnisse in Bezug auf die Sicherheitsaspekte der Übertragungswege oder der Hardware-Komponenten. Sie sind in der Lage, die Wirksamkeit von Sicherheitsmaßnahmen einzuordnen und Sicherheitseigenschaften von mobilen Kommunikationssystemen zu bewerten. Sie erhalten eine erste Orientierung zum Vorgehen bei der Absicherung von mobilen Systemen durch Auswahl der Technologie und Konfiguration des Systems und den Einsatz spezieller Sicherheitsmechanismen.

Inhalt

Die **Pflichtveranstaltung** behandelt die wesentlichen Techniken zur Realisierung von mobiler (drahtloser) Kommunikation mit dem Schwerpunkt auf IT-Systemen. Dazu gehören die Funkübertragungstechniken, insbesondere die zellenbasierten Funksysteme, die Medienzugriffsverfahren, die die gemeinsame Nutzung des Funkraums koordinieren (Multiplexverfahren, Kollisionserkennung und -vermeidung), und die mobilen Varianten der Vermittlungsschicht (mobile IP, ad-hoc networking, Routingverfahren) und der Transportschicht (flow control, quality of service). Daneben werden die verschiedenen Arten der verwendeten mobilen Kommunikationssysteme vorgestellt: Drahtlose Telekommunikationssysteme (u.a. GSM, UMTS, LTE), Satellitensysteme, Rundfunksysteme (DAB, DVB) und drahtlose lokale Netze (u.a. WLAN, Bluetooth).

In der Wahlpflichtveranstaltung „**Sichere Mobile Systeme**“ werden zum einen verschiedene Kommunikationsstandards (u.a. WLAN, Bluetooth, und IEEE 802.15.4) vorgestellt, die im Bereich IoT ihren Einsatz finden, welche Einschränkungen sie haben und welche Sicherheitsaspekte sie erfüllen. Zum anderen werden konkrete Anwendungen wie elektronische Ausweise und mobiles Bezahlen näher betrachtet. Als Basisliteratur wird auf diverse Standarddokumente (u.a. vom BSI und IETF) verwiesen sowie auf das Buch von J. Schiller Mobilkommunikation, ISBN: 978-3827370600.

Ergänzend zu den Grundlagen werden in der Vorlesung **Sensorik und Manipulationsdetektion** Algorithmen, Protokolle und Paradigmen für den Einsatz von Sensornetzen sowie deren Absicherung vorgestellt. Dabei werden Konzepte wie etwa Lokalisierung, Zeitsynchronisation und datenzentrische Ansätze betrachtet sowie Lösungen für System-Software, Aggregation, Routing und Datenverteilung aus der Perspektive von Sensornetzen betrachtet. Ferner behandelt die Vorlesung Grundlagen, Systeme und Verfahren zur Detektion von Manipulationen. Dies beinhaltet die gesicherte Informationsübertragung in verteilten Systemen sowie die Bestätigung und Überprüfung von detektierten Ereignissen durch verschiedene Methoden.

Literatur

Literatur zur Lehrveranstaltung "Sichere mobile Systeme":

- J. Schiller: Mobilkommunikation, ISBN: 978-3827370600

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 20 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Wahlpflichtmodul im Masterstudiengang CYB, Vertiefungsfelder Public Security und Cyber Network Capabilities

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Offensive Sicherheitsüberprüfungen	5523

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55091	VÜ	Penetration Testing	Pflicht	6
55093	P	Penetration Testing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Gute Kenntnisse in den Bereichen Netzsicherheit und Systemsicherheit, wie in den gleichnamigen beiden Modulen vermittelt.

Qualifikationsziele

Die Studierenden können organisationsinterne Überprüfungen der IT-Sicherheitseigenschaften von Systemen, Diensten und Netzen planen und durchführen. Sie beherrschen Testmethoden auf Netz-, Anwendungs- und Systemebene und haben ausgewählte aktuelle Werkzeuge für diesen Zweck kennengelernt. Sie kennen die Aufgabenbereiche und Randbedingungen von Red Teams und Pentesting-Dienstleistern.

Inhalt

Die Vorlesung Penetration Testing führt in die Aufgabengebiete von Pentesting- bzw. Red-Teams ein. Für verschiedene Anwendungsgebiete wie das Sicherheitstesten einzelner Systeme, komplexerer IT-Dienste und ganzer Rechnernetze und IT-Infrastrukturen werden die Vor- und Nachteile verschiedener Testvarianten wie Whitebox- und Blackbox-Tests analysiert. Unter Orientierung an bewährten Good-Practice-Dokumentationen wie OWASP und OSSTMM werden praxisrelevante Angriffsvarianten von der Reconnaissance-Phase bis zum Einbringen von Exploit-Payloads behandelt. Ebenso werden die strukturierte Erstellung von Pentesting-Berichten und deren Auswertung durch die auftraggebende Organisation betrachtet.

Das Praktikum Penetration Testing stellt auf Basis einer Praktikumsinfrastruktur (abgeschottete Laborumgebung) Aufgaben, in denen die Studierenden als fiktiver Auftragnehmer eines technischen Penetrationstests fungieren. Mithilfe ausgewählter bereitgestellter Softwarewerkzeuge müssen die für Pentests ausgewählten Systeme, Dienste und Subnetze erkundet und auf verschiedenste Verwundbarkeiten untersucht werden, ohne den Betrieb der übrigen Infrastruktur zu beeinträchtigen. Für einige Überprüfungen müssen eigene Werkzeuge bzw. Skripte/Payloads konzipiert und

implementiert werden. Über die gewählte Vorgehensweise, die einzelnen Schritte der Durchführung und die zu priorisierenden Ergebnisse ist eine Ausarbeitung zu erstellen, die vom Stil her an Pentest-Berichte angelehnt ist.

Literatur

- M. Kofler et al.: Hacking & Security. Rheinwerk Verlag, 2022
- P. Calderon: Nmap Network Exploration and Security Auditing Cookbook. Packt Publishing Ltd, 2021
- P. Kim and J.Faircloth: The Hacker Playbook 3. Secure Planet LLC, 2015
- V. K. Velu: Mastering Kali Linux for advanced penetration testing. Packt Publishing Ltd, 2017

Leistungsnachweis

Portfolio. Der Leistungsnachweis besteht aus zwei Teilen: (1) schriftliche Klausur von 60 Minuten Dauer; (2) praktischer Leistungsnachweis in Form eines Penetrationstests (Pentests), einschließlich der Anfertigung eines schriftlichen Berichts. Für den Pentest wird eine Labor-Umgebung bereitgestellt, die ein mittelständisches Unternehmen simuliert. Der Zugang zum Labor erfolgt per VPN, was die Durchführung des Pentests ortsunabhängig ermöglicht. Die Bearbeitung erfolgt nach Ausgabe der Aufgabenstellung und muss innerhalb von 10 Wochen abgeschlossen sein. Der Pentest-Bericht muss einen Manager-Teil und einen Admin-Teil enthalten und zwischen 30 und 60 Seiten umfassen.

Die Leistungen in der schriftlichen Klausur und im Praktikum gehen im Verhältnis 50 zu 50 in die Note ein.

Verwendbarkeit

- Wahlpflicht für das Vertiefungsfeld Cyber Network Capabilities (CNC) im Studiengang MCYB
- Wahlpflicht für das Vertiefungsfeld Enterprise Security (ES) im Studiengang MCYB
- Wahlpflicht im Studiengang MME, Wahlpflichtgruppe ITSK
- Wahlpflicht im Studiengang MCAE

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Modern Cryptography	5548

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Manulis	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55481	VÜ	Modern Cryptography	Pflicht	4
55482	SE	Seminar Research Trends in Cryptography	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende mathematischen Kenntnisse sowie ein generelles Interesse an moderner Kryptographie vorausgesetzt.

Qualifikationsziele

Die Studierenden kennen Designprinzipien und Funktionsweise von modernen kryptographischen Verfahren und Protokollen und beherrschen den Umgang mit entsprechender Sicherheitsmodellierung und -beweisführung. Sie sind in der Lage kryptographische Verfahren zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um Kryptographie und ihren Anwendungen.

Inhalt

- **Modern Cryptography** - In dieser Vorlesung werden moderne Methoden der Kryptographie sowie weiterführende kryptographische Verfahren und Protokolle detailliert vorgestellt und analysiert. Neben der allgemeinen Funktionsweise wird auf die Sicherheitsmodellierung und beweisbare Sicherheit eingegangen. Dazu werden, z.B., moderne Beweisführungsmethoden wie kryptographische Reduktionen eingeführt. Zu den Themen der Veranstaltung gehören unterschiedliche kryptographische Funktionalitäten, darunter Einwegfunktionen, Pseudozufallszahlengeneratoren, Hashfunktionen, Blockchiffren, message authentication codes, digitale Signaturen und Verschlüsselungsverfahren, sowie weiterführende Techniken wie Identifikationsverfahren und zero-knowledge Beweise. Neben den weit verbreiteten auf diskreten Logarithmen oder Integer Faktorisierung basierenden Verfahren, werden weitere Konstruktionen vorgestellt, die mittels elliptischen Kurven und bilinearen Abbildungen aufgebaut sind. Die nötigen mathematischen Grundlagen für diese Verfahren werden im Rahmen der Veranstaltung eingeführt. In Übungen werden die Methoden der beweisbaren

Sicherheit sowie die Funktionsweise von eingeführten Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.
- **Research Trends in Cryptography** - In diesem Seminar bekommen Studierende ein Einblick in aktuelle Forschungsfelder der Kryptographie. Die Schwerpunkte liegen bei neuen kryptographischen Konzepten, Methoden, Verfahren und Protokollen sowie bei deren Implementierung, Standardisierung und Anwendungen. Zu Beginn der Veranstaltung wird eine Auswahlliste von aktuellen Themen vorgestellt, die von Studierenden über die Dauer der Veranstaltung ausgearbeitet und am Ende vorgestellt werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikel (aus bekannten Tagungen) und Open-Source Quellen (z.B. Softwarebibliotheken, Standards) stützen.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Katz, J. and Lindell, Y. Introduction to Modern Cryptography (2nd Edition), Chapman & Hall/CRC Cryptography and Network Security Series, 2014.

Leistungsnachweis

Portfolio auf der Basis der folgenden Leistungen:

55481 VÜ Modern Cryptography: mündliches Fachgespräch von 20 Minuten,

55482 Seminar Research Trends in Cryptography: Erstellung und Abgabe einer schriftlichen Ausarbeitung (10 bis 20 Seiten) und eine Präsentation (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen.

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 80 zu 20 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten vermitteln tiefes Verständnis von modernen kryptographischen Methoden und Verfahren. Die Veranstaltungen fördern analytisches Denken und entwickeln Fähigkeiten kryptographische Verfahren unter Verwendung von Security-by-Design Prinzipien zu entwerfen und zu analysieren sowie deren Einsatz in Anwendungen zu planen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf dem Gebiet der Kryptographie und dient als gute Vorbereitung für weiterführende Lehrveranstaltungen rund um Kryptographie und ihren Anwendungen zum Schutz der Datensicherheit und Privatheit, etwa im Rahmen des Moduls „Privacy Enhancing Cryptography“.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird im WT angeboten. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Privacy Enhancing Cryptography	5563

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Manulis	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55631	VÜ	Private Data Processing	Pflicht	4
55632	VÜ	Private Authentication and Messaging	Pflicht	4
5563-V3	SE	Privacy Enhancing Cryptography in Practice	Pflicht	1
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende Kenntnisse in moderner Kryptographie sowie ein generelles Interesse am Einsatz von kryptographischen Verfahren und Protokollen zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern vorausgesetzt. Eine vorherige Teilnahme am Modul „Modern Cryptography“ ist wünschenswert, stellt jedoch keine formale Voraussetzung dar.

Qualifikationsziele

Die Studierenden kennen Designprinzipien und Funktionsweise von verschiedenen Verfahren und Protokollen zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern unter Verwendung von modernen kryptographischen Methoden. Sie sind in der Lage die kryptographische Lösungen kritisch zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um Privacy Enhancing Cryptography und entsprechenden Anwendungen.

Inhalt

- **Private Data Processing:** In dieser Vorlesung werden kryptographische Protokolle vorgestellt, mit deren Hilfe vertrauliche Daten durch eine oder mehrere Parteien verarbeitet werden können. Dabei geht es um Operationen auf numerischen und binären Daten sowie sichere Berechnungen von Funktionen zum Einsatz in diversen Anwendungsfällen, welche die Vertraulichkeit von verwendeten Eingabedaten während ihrer Verarbeitung erfordern. Es werden Szenarien kooperativer Datenverarbeitung unter zwei oder mehreren Teilnehmern sowie Operationen auf ausgelagerten (etwa in eine Cloud) Daten betrachtet. Themen der Vorlesung sind, u.a. secret sharing and threshold cryptography, Varianten von oblivious transfer, (fully) homomorphic encryption, secure two-party und multi-party computation, private function evaluation, private set intersection, private information

retrieval, secure data aggregation und searchable encryption. In Übungen wird die Funktionsweise und Sicherheit von Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.

- **Private Authentication and Messaging:** In dieser Vorlesung werden Privatsphäre schützende kryptographischen Verfahren und Protokolle zur sicheren Authentisierung und Nachrichtenaustausch vorgestellt. Im Fokus stehen solche Schutzziele wie Anonymität, Unverlinkbarkeit und Abstreitbarkeit, gekoppelt an die klassischen Sicherheitsziele einer Authentisierung bzw. Ende-zu-Ende-Verschlüsselung. Es werden Verfahren vorgestellt, die solche Schutzziele in zwei- sowie mehr-Parteien Anwendungen ermöglichen. Themen der Vorlesung sind, u.a., (multi-party) key exchange und secure messaging (inkl. Signal protocol, MLS), secret handshakes, anonymous communication (inkl. mix networks, onion routing), privacy-preserving signatures (inkl. ring und group signatures) sowie anonymous credentials.
- **Privacy Enhancing Cryptography in Practice:** In diesem praxisorientierten Seminar geht es um die Implementierung und praktische Verwendung von modernen kryptographischen Verfahren und Technologien zum Schutz der Vertraulichkeit von Daten und Privatheit von Benutzern. In Bezug auf das ausgewählte Thema wird von den Studierenden eine weitgehend selbständig gefertigte prototypische Umsetzung eines Miniprojektes unter Verwendung von geeigneten open-source Softwarebibliotheken bzw. Technologien erwartet. Die Ergebnisse der Implementierungsarbeit sollen dann in einem Bericht beschrieben und während der Präsentation demonstriert werden. Mögliche Themen umfassen: homomorphic encryption, secure two- and multi-party computation, private information retrieval, searchable encryption, zero-knowledge proofs, distributed cryptography, attribute-based cryptography, secure messaging, privacy-preserving authentication, anonymous communication, usw.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Relevante Quellen werden im Rahmen der Veranstaltungen angegeben.

Leistungsnachweis

Portfolio:

Zu 55631 und 55632: ein mündliches Fachgespräch von 30 Minuten über die Inhalte aus beiden Veranstaltungen,

In 55633: Erstellung und Abgabe einer Präsentation zur Demonstration von Ergebnissen des Miniprojektes (10 bis 20 Minuten). Bearbeitungsdauer: 8 Wochen

Die Leistungen in der Klausur/mündlichen Prüfung und im Seminar gehen im Verhältnis 90 zu 10 in die Note ein.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit um die wichtigen technologischen Aspekte der Privatheit und entsprechenden kryptographischen Methoden und Verfahren. Die Veranstaltungen vermitteln die

Fähigkeiten technische Verfahren zum Schutz der Daten und Privatheit zu entwerfen und ihr Einsatz in digitalen Anwendungen zu ermöglichen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Überschneidungsbereich des technologischen Privacy- und Datenschutzes und angewandter Kryptographie.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr in FT. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Angewandte Zahlentheorie	6034

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Andreas Nickel	Wahlpflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12111	VÜ	Algorithmische Zahlentheorie	Pflicht	5
12112	VÜ	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Pflicht	3
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Generelles Interesse an Mathematik und Theorie. Es wird empfohlen, das Modul "Zahlentheorie und Kryptographie" absolviert zu haben.Alternativ reichen bei entsprechender Einsatzbereitschaft Grundlagen zur Kryptographie und Kryptoanalyse aus, wie sie z.B. im Modul Kryptologie vermittelt werden.

Qualifikationsziele

Die Studierenden erlernen fortgeschrittene Konzepte und Algorithmen der algebraischen Zahlentheorie und werden mit einigen ihrer Anwendungen vertraut gemacht. Dabei handelt es sich um zahlentheoretische oder algebraische Methoden für den Entwurf von kryptographischen bzw. kryptoanalytischen Verfahren und solche, die in der Codierungstheorie eingesetzt werden.

Inhalt

Die Veranstaltung "Algorithmische Zahlentheorie" befasst sich mit grundlegenden Begriffen und Algorithmen der algebraischen Zahlentheorie. (Stichworte: Primelemente, Primalitätstests, Faktorisierung, elliptische Kurven, u.a.). Ein Großteil dieser abstrakten Konzepte ist fundamental für die moderne Kryptographie (Public Key) und die Codierungstheorie. Der Schwerpunkt dieser Vorlesung ist zwar die systematische Erarbeitung der theoretischen Grundlagen und grundlegenden Algorithmen, es wird aber auch immer wieder auf Anwendungen eingegangen. Ergänzt werden diese durch zahlentheoretische Konzepte, die eventuell in einer Post-Quantencomputer-Epoche relevant sein könnten.

Die Veranstaltung "Ausgewählte mathematische Methoden der Kryptographie und Codierungstheorie" befasst sich mit ausgewählten und fortgeschrittenen Themen aus der Kryptographie und/oder der Codierungstheorie. Hierhin gehören kryptographische Verfahren, die auf zahlentheoretischen Ergebnissen aufsetzen, und "gute" Codes, die

man mit Hilfe von algebraischen Kurven gefunden hat. Sowohl kryptographische als auch codierungstheoretische Inhalte sind vorgesehen; die Gewichtung zwischen diesen beiden Gebieten kann aber variieren.

Literatur

Zur VÜ Algorithmische Zahlentheorie:

- H. Cohen: A course in computational algebraic number theory, Graduate Texts in Mathematics 138, Springer
- O. Forster: Algorithmische Zahlentheorie, Springer
- J. Hoffstein, J. Pipher, J.H. Silverman: An Introduction to Mathematical Cryptography, Springer
- C. Karpfinger, H. Kiechle: Kryptologie. Algebraische Methoden und Algorithmen, Vieweg + Teubner

Zur VÜ Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie:

- W. Heise und P. Quattrocchi: Informations- und Codierungstheorie, Springer
- D. Jungnickel: Codierungstheorie, Spektrum Akad. Verlag
- N. Koblitz: Algebraic Aspects of Cryptography, Springer
- W. Lütkebohmert, Codierungstheorie, Springer-Vieweg

Leistungsnachweis

Mündliche Prüfung von 30 Minuten Dauer.

Verwendbarkeit

- Wahlpflichtmodul im Vertiefungsfeld Enterprise Security (ES) des Masterstudiengangs Cyber-Sicherheit.
- Wahlpflichtmodul im Vertiefungsfeld Cyber Network Capabilities (CNC) des Masterstudiengangs Cyber-Sicherheit.
- Wahlpflichtmodul im Vertiefungsfeld Security Intelligence (SI) des Masterstudiengangs Cyber-Sicherheit.

Dauer und Häufigkeit

Das Modul dauert 1 bis 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Herbsttrimester.

Modulname	Modulnummer
Seminarmodul CYB	5501

Konto	Seminar - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Pflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	24	126	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55011	SE	Seminarmodul MCYB	Pflicht	2
Summe (Pflicht und Wahlpflicht)				2

Empfohlene Voraussetzungen

Keine formalen Voraussetzungen, aber je nach Themengebiet sind Kenntnisse aus Modulen bestimmter Fächer wesentliche Grundlage. Wenn ein Vertiefungsfeld gewählt wird, dann ist es empfehlenswert, das Seminar zu einem Thema dieses Vertiefungsfeldes zu belegen.

Qualifikationsziele

Die Studierenden haben Kenntnisse zu vertieften und speziellen fachlichen Themen des jeweiligen Themengebiets. Zusätzlich erwerben sie folgende Schlüsselqualifikationen:

- Die Fähigkeit, anspruchsvolle englische Originalliteratur zu lesen und zu verstehen.
- Die Fähigkeit, vor einem Fachpublikum einen Vortrag zu einem nichttrivialen wissenschaftlichen Thema zu entwerfen (also auch didaktisch richtig zu gestalten) und ihn unter Einsatz üblicher Medien abzuhalten.
- Die Fähigkeit, zu Diskussionen über wissenschaftlichen Themen beizutragen.
- Die Fähigkeit, Texte von ca. 15-30 Seiten zu verfassen, i.d.R. zur Erklärung wissenschaftlicher Inhalte.

Inhalt

Seminare behandeln wechselnde fachliche Themen, die auf Lehrstoffen aus dem Master-Studium aufbauen. Die Themen können schon vorhandene fachliche Interessen und Schwerpunkte vertiefen. Die Seminare werden in Kleingruppen durchgeführt. Die angebotenen Seminare werden vor Beginn des Moduls hochschulöffentlich bekannt gegeben. In der Regel arbeitet jeder Teilnehmer einen Vortrag zu vorgegebener Literatur aus und präsentiert ihn in der Gruppe, die anschließend Fragen dazu stellt. Außerdem wird die Teilnahme an den Diskussionen zu allen Vorträgen erwartet.

Das Seminarmodul stärkt die Fähigkeit der Studierenden zur wissenschaftlichen Recherche und zur Präsentation wissenschaftlicher Erkenntnisse. Es versetzt die Studierenden verstärkt in die Lage, sich Erkenntnis und Wissen selbstständig aktiv zu

erarbeiten und zu reflektieren, statt diese überwiegend rezeptiv aufzunehmen. Durch die exemplarische Vertiefung der im Studium behandelten Inhalte werden Studierende an die Forschung herangeführt, die für eine universitäre Ausbildung unverzichtbar ist.

Literatur

Die zu verwendenden Literaturquellen hängen vom Thema ab und werden in jedem Seminar angegeben.

Leistungsnachweis

Referat (30 bis 60 Minuten) mit schriftlicher Ausarbeitung oder Seminararbeit mit Vortrag (20 bis 40 Minuten). Die Bearbeitungszeit beträgt jeweils insgesamt 100 bis 140 Stunden. Es sind im Einzelnen folgende Leistungen zu erbringen:

- Erstellen einer schriftlichen Ausarbeitung
- Abhalten einer Präsentation

Die Note ergibt sich i.w. aus der Qualität der Präsentation und der schriftlichen Ausarbeitung. Der Umfang der schriftlichen Ausarbeitung beträgt 15 bis 30 Seiten.
Bei einem Referat liegt der Schwerpunkt auf der mündlichen Präsentation, bei einer Seminararbeit auf der schriftlichen Ausarbeitung. Ob der Leistungsnachweis des Seminars ein Referat oder eine Seminararbeit ist, wird am Anfang jedes Seminars von der verantwortlichen Dozentin bzw. dem verantwortlichen Dozenten bekannt gegeben.

Verwendbarkeit

- Seminarmodul (Pflicht) im Studiengang MCYB

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Seminare werden in jedem Trimester angeboten. Es wird empfohlen, das Seminar im 2., 3. oder 4. Fachtrimester zu belegen.

Sonstige Bemerkungen

Aus den jeweils angebotenen Seminaren zu unterschiedlichen Themen ist eines auszuwählen.

Zum Arbeitsaufwand: Der Hauptaufwand liegt in der Aufarbeitung eines Themas und der einmaligen Ausarbeitung des eigenen Vortrags. Dabei entfallen von den 126 Stunden Workload jeweils etwa 2/3 auf das Durcharbeiten der Literatur, und 1/3 auf das Erstellen der Vortragsfolien und Ausarbeitung.

Modulname	Modulnummer
Masterarbeit CYB	5500

Konto	Masterarbeit - CYB 2025

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Marta Gomez-Barrero	Pflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
900	0	900	30

Empfohlene Voraussetzungen
Vorausgesetzt werden die allgemeinen Kenntnisse aus dem Master-Studium.

Qualifikationsziele
Die Studierenden können eine anspruchsvolle Aufgabe selbständig analysieren und mit wissenschaftlichen Methoden bearbeiten. Sie haben Erfahrung in der Entwicklung von Lösungsstrategien und in der Dokumentation ihres Vorgehens. Sie haben in einem speziellen Forschungsgebiet der Cyber-Sicherheit vertiefende praktische Erfahrung gesammelt.

Inhalt
In der Master-Arbeit soll eine Aufgabe aus einem begrenzten Problemkreis unter Anleitung selbständig mit bekannten Methoden wissenschaftlich bearbeitet werden. In der Arbeit sind die erzielten Ergebnisse systematisch zu entwickeln und zu erläutern. Sie wird in der Regel individuell und eigenständig durch die Studierenden bearbeitet, kann aber je nach Thema auch in Gruppen von bis zu drei Studierenden bearbeitet werden.

Literatur
Die zu verwendende Literatur hängt vom Thema der Masterarbeit ab und wird bei der Vergabe des Themas der Masterarbeit angegeben.

Leistungsnachweis
Es ist eine schriftliche Ausarbeitung zu erstellen und diese ist im Rahmen eines Kolloquiums zu präsentieren. Die Präsentation findet als Vortrag von ca. 20-30 Minuten Dauer mit daran anschließenden Fragen statt. Die Präsentation wird benotet und geht mit 1/15 (entspricht 2 Leistungspunkten) in die Modulnote ein.

Verwendbarkeit
Die Anfertigung der Master-Arbeit bereitet auf eigenständige systematisch durchgeführte Arbeitsvorgänge in der beruflichen Tätigkeit oder der wissenschaftlichen Forschung vor.

Dauer und Häufigkeit
Das Modul dauert 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester. Als Startzeitpunkt ist das Wintertrimester im 2. Studienjahr vorgesehen.

Modulname	Modulnummer
studium plus 3, Seminar und Training	9903

Konto	Studium+ Master

Modulverantwortliche/r	Modultyp	Empf. Trimester
Zentralinstitut studium plus	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	72	78	5

Qualifikationsziele

***studium plus*-Seminare:** Die Studierenden erwerben profunde **Allgemeinbildung und Schlüsselqualifikationen** für künftige Führungskräfte, um das Studium als starke, mündige Persönlichkeiten zu verlassen. Die *studium plus*-Seminare bereiten die Studierenden dadurch auf ihre Berufs- und Lebenswelt vor und ergänzen die im Studium erworbenen Fachkenntnisse. Die Allgemeinbildung und die Befähigung zu ganzheitlichem Denken erweitern die Perspektive des Fachstudiums. Dadurch lernen die Studierenden, das im Fachstudium erworbene Wissen in komplexe Zusammenhänge einzuordnen und ausgewählte Themen in Relation zu anderen Wissenschaften zu setzen.

Die exemplarische Auseinandersetzung mit gesellschaftsrelevanten Fragestellungen befähigt die Studierenden zu eigenständiger Urteilsbildung und kompetenter Positionierung in aktuellen Diskussionen, schult ihre personalen, sozialen und methodischen Kompetenzen und erweitert ihre Führungsqualitäten z.B. durch die Einführung in Konfliktlösungsstrategien und interkulturellen Dialog. Damit verfügen die Studierenden über zentrale Schlüsselkompetenzen für ihr späteres Berufsleben innerhalb wie außerhalb der Bundeswehr. Durch die Vermittlung von Wissen werden die mündige Teilhabe an sozialen, kulturellen und politischen Prozessen der modernen Gesellschaft und daraus entspringendes verantwortliches Handeln gefördert. Damit steht die Persönlichkeitsbildung der Studierenden in ihren intellektuellen, ethischen und pragmatisch-sozialen Dimensionen im Fokus.

***studium plus*-Trainings**: Die Studierenden erwerben **personale, soziale und methodische Kompetenze**n, um als Führungskräfte auch unter komplexen und teils widersprüchlichen Anforderungen handlungsfähig zu bleiben bzw. um ihre Handlungskompetenz wiederzuerlangen. Damit ergänzt das Trainingsangebot die im Rahmen des Studiums erworbenen Fachkenntnisse insofern, als diese fachlichen Kenntnisse von den Studierenden in einen berufspraktischen Kontext eingebettet werden können und Möglichkeiten zur Reflexion des eigenen Handelns angeboten werden.

Inhalt

Die ***studium plus* -Seminare** bieten Lerninhalte, die Allgemeinbildung und Schlüsselqualifikationen vermitteln und die Partizipationsfähigkeit steigern. Sämtliche Inhalte sind auf den Erwerb personaler, sozialer oder methodischer Kompetenzen ausgerichtet. Sie bilden die Persönlichkeit und erhöhen die Beschäftigungsfähigkeit. Bei der Vermittlung von **Allgemeinbildung** werden die Studierenden beispielsweise

mit den Grundlagen fachfremder Wissenschaften vertraut gemacht, sie lernen Denkweisen und "Kulturen" anderer wissenschaftlicher Disziplinen und Wissensgebiete kennen. Bei der Vermittlung von **Orientierungswissen** im Sinne der Erkenntnis politischer Zusammenhänge, historischer Hintergründe und ethischer Fragestellungen steigern die Studierenden ihr Reflexionsniveau, indem sie sich exemplarisch mit gesellschaftsrelevanten Themen auseinandersetzen. Bei der Vermittlung von Partizipationswissen steht der Erwerb von Schlüsselkompetenzen im Vordergrund.
Die Seminare finden wöchentlich an einem - mit der jeweiligen Fakultät vereinbarten - Wochentag in den sog. Blockzeiten oder auch am Wochenende statt, wobei den Studierenden die Wahl frei steht.

Die *studium plus*- Trainings entsprechen den Trainings für Führungskräfte in modernen Unternehmen und bieten **berufsrelevante** und an den Themen der aktuellen Führungskräfteentwicklung von Organisationen und Unternehmen orientierte **Lerninhalte und Komptenzen**. Sie finden überwiegend am Wochenende statt. Einen detaillierten und aktualisierten Überblick bietet das jeweils gültige Trainingsangebot von studium plus.

Leistungsnachweis

***studium plus*-Seminare**: in **Seminaren** werden **Notenscheine** erworben. Die Leistungsnachweise, durch die der Notenschein erworben werden kann, legt der/ die Dozent/in in Absprache mit dem Zentralinstitut studium plus vor Beginn des Einschreibeverfahrens für das Seminar fest. Hierbei sind folgende Formen möglich: Seminararbeit, Portfolio (bestehend aus mehreren kleinen Teilleistungen: Referat, Hausarbeit, Gruppenarbeit, Mitarbeit in der Lehrveranstaltung etc.). Bei einem Portfolio erhält der Studierende verbindliche Angaben darüber, mit welchem prozentualen Anteil die jeweiligen Teilleistungen gewichtet werden. Der bzw. die Modulverantwortliche gibt zu Beginn der jeweiligen Veranstaltung bekannt, welcher Leistungsnachweis aus den genannten Alternativen verlangt wird, wie lange die konkrete Bearbeitungszeit beträgt und welchen Umfang die zu erbringende Leistung hat. Der Erwerb des Scheins ist an die regelmäßige Anwesenheit und aktive Mitarbeit im Seminar gekoppelt. Bei der während des Einschreibeverfahrens stattfindenden Auswahl der Seminare durch die Studierenden erhalten diese verbindliche Informationen über die Modalitäten des Scheinerwerbs für jedes angebotene Seminar.

***studium plus*-Trainings**: in Trainings werden Teilnahmescheine erworben. Die erfolgreiche Teilnahme setzt aktive, engagierte Mitarbeit im Training sowie respektvollen Umgang miteinander voraus. Die Trainings sind unbenotet, die Zuerkennung der ECTS-Leistungspunkte setzt jedoch die aktive, engagierte Teilnahme an der gesamten Trainingszeit voraus.

Verwendbarkeit

Das Modul ist für sämtliche Masterstudiengänge gleichermaßen geeignet.

Dauer und Häufigkeit

Das Modul dauert 2 mal 1 Trimester.Das Modul findet statt im ersten Studienjahr jeweils im Frühjahrstrimester und im Herbsttrimester. Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Übersicht des Studiengangs: Konten und Module

Legende:

FT	= Fachtrimester des Moduls
PrFT	= frühestes Trimester, in dem die Modulprüfung erstmals abgelegt werden kann
Nr	= Konto- bzw. Modulnummer
Name	= Konto- bzw. Modulname
M-Verantw.	= Modulverantwortliche/r
ECTS	= Anzahl der Credit-Points

FT	PrFT	Nr	Name	M-Verantw.	ECTS
		7	**Pflichtmodule - CYB 2025**		**44**
2	2	5502	Netzsicherheit	G. Dreo Rodosek	6
1	2	5503	Hardwaresicherheit	K. Buchenrieder	6
1	1	5504	Datenschutz und Privacy	A. Wacker	6
2	2	5505	Systemsicherheit	G. Teege	6
1	1	5506	Kryptologie	D. Slamanig	6
2	2	5507	Anwendungssicherheit	W. Hommel	6
2	3	5508	Security- und IT- Management	U. Lechner	8
		8 -11	**Überkonto Wahlpflicht - CYB 2025**		**36**
6	6	1651	Grundlagen der Informationssicherheit	W. Hommel	6
		8	**Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2025**		**30**
4	4	1162	Erweiterte Digitale Forensik	H. Baier	6
3	3	1169	Vernetzte Operationsführung und Digitale Streitkräfte	A. Karcher	6
1	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
4	4	1446	Identitätsmanagement	D. Pöhn	6
1	1	1507	Enterprise Architecture und IT Service Management	A. Karcher	6
3	4	1551	Digitale Forensik	H. Baier	9
4	4	3010	Einführung in die Quanteninformationsverarbeitung	S. Tornow	6
1	1	3396	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
3	5	3584	Language-based Security	S. Brunthaler	6
1	2	3647	Compilerbau	S. Brunthaler	6
1	2	3648	Compilerbau (erweitert)	S. Brunthaler	9
3	4	3931	Post-Quantum Cryptography	D. Slamanig	9
2	2	4211	Biometric Recognition	M. Gomez-Barrero	6
2	2	4212	Deep Learning for IT-Security	M. Gomez-Barrero	6
3		4213	Privacy Preserving Machine Learning	M. Gomez-Barrero	6
1	1	5118	Foundations of Distributed Systems and Blockchains	D. Slamanig	6
3	3	5523	Offensive Sicherheitsüberprüfungen	A. Wacker	9
1	1	5548	Modern Cryptography	M. Manulis	6
	3	5563	Privacy Enhancing Cryptography	M. Manulis	9
	5	6034	Angewandte Zahlentheorie	A. Nickel	9
		9	**Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2025**		**30**
1	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
3	3	2994	Ausgewählte Kapitel des OR: Data-driven Optimization	M. Moll	9
	4	3852	Anwendungsgebiete der Data Science	M. Geierhos	6
3	3	3853	Analyse unstrukturierter Daten	M. Geierhos	6

3	4	3931	Post-Quantum Cryptography	D. Slamanig	9
3		4213	Privacy Preserving Machine Learning	M. Gomez-Barrero	6
1	1	5118	Foundations of Distributed Systems and Blockchains	D. Slamanig	6
2	4	5513	Mobile Security	G. Dreo Rodosek	6
3	3	5514	Staatliche IT-Sicherheit	U. Lechner	6
1	1	5548	Modern Cryptography	M. Manulis	6
	3	5563	Privacy Enhancing Cryptography	M. Manulis	9
		10	**Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2025**		**30**
	3	1032	Analytische Modelle	M. Siegle	9
1	1	1037	Informations- und Codierungstheorie	P. Hertling	6
1	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
1	1	2319	Artificial Intelligence	E. Ntoutsi	6
3	3	2320	Responsible Artificial Intelligence	E. Ntoutsi	6
2	2	2534	Machine Learning	E. Ntoutsi	6
2	3	2535	Machine Learning (erweitert)	E. Ntoutsi	9
1	1	2536	Artificial Intelligence (erweitert)	E. Ntoutsi	9
3	3	2537	Responsible Artificial Intelligence (erweitert)	E. Ntoutsi	9
3	3	2994	Ausgewählte Kapitel des OR: Data-driven Optimization	M. Moll	9
4	4	3010	Einführung in die Quanteninformationsverarbeitung	S. Tornow	6
1	1	3396	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
	4	3852	Anwendungsgebiete der Data Science	M. Geierhos	6
3	3	3853	Analyse unstrukturierter Daten	M. Geierhos	6
2	2	4212	Deep Learning for IT-Security	M. Gomez-Barrero	6
	5	6034	Angewandte Zahlentheorie	A. Nickel	9
1	1	6050	Signalverarbeitung	A. Knopp	5
3	3	6053	Kanalcodierung	A. Knopp	5
		11	**Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2025**		**30**
4	4	1162	Erweiterte Digitale Forensik	H. Baier	6
3	3	1169	Vernetzte Operationsführung und Digitale Streitkräfte	A. Karcher	6
3	4	1551	Digitale Forensik	H. Baier	9
4	4	3010	Einführung in die Quanteninformationsverarbeitung	S. Tornow	6
1	1	3396	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
1	2	3647	Compilerbau	S. Brunthaler	6
1	2	3648	Compilerbau (erweitert)	S. Brunthaler	9
3	3	3822	Cyber Network Capabilities Methoden	H. König	6
3	2	3823	Rechtliche Grundlagen Cyber Network Capabilities	H. König	6
3	4	3931	Post-Quantum Cryptography	D. Slamanig	9
1	1	5118	Foundations of Distributed Systems and Blockchains	D. Slamanig	6
2	4	5513	Mobile Security	G. Dreo Rodosek	6
3	3	5523	Offensive Sicherheitsüberprüfungen	A. Wacker	9
1	1	5548	Modern Cryptography	M. Manulis	6
	3	5563	Privacy Enhancing Cryptography	M. Manulis	9
	5	6034	Angewandte Zahlentheorie	A. Nickel	9
		12	**Seminar - CYB 2025**		**5**
3		5501	Seminarmodul CYB	M. Gomez-Barrero	5

		13	**Masterarbeit - CYB 2025**		**30**
4	5	5500	Masterarbeit CYB	M. Gomez-Barrero	30
		99MA (neu)	**Verpflichtendes Begleitstudium plus**		**5**
		9903	studium plus 3, Seminar und Training	Z. studium plus	5

Übersicht des Studiengangs: Lehrveranstaltungen

Legende:

FT	= Fachtrimester der Veranstaltung
Nr	= Veranstaltungsnummer
Name	= Veranstaltungsname
Art	= Veranstaltungsart
P/Wp	= Pflicht / Wahlpflicht
TWS	= Trimesterwochenstunden

FT	Nr	Name	Art	P/Wp	TWS
	23192	Seminar Selected topics in Artificial Intelligence	Seminar	Pf	2
	30102	Praktikum Quantenschlüsselaustausch	Praktikum	WPf	3
	30103	Seminar Quantentechnologien	Seminar	WPf	3
	35842	Seminar Language-based Security	Seminar	Pf	2
	38524	Modulprojekt Anwendungsgebiete der Data Science	Projekt	WPf	3
	42112	Selected Topics in Biometric Recognition	Seminar	Pf	2
	42122	Selected Topics in Deep Learning for IT-Securit	Seminar	Pf	2
	42131	Privacy Preserving Machine Learning	Vorlesung	Pf	4
	42132	Selected topics in Privacy Preserving Machine Learning	Seminar	Pf	2
	55011	Seminarmodul MCYB	Seminar	Pf	2
	55132	Sensorik und Manipulationsdetektion	Vorlesung/Übung	WPf	3
	55482	Seminar Research Trends in Cryptography	Seminar	Pf	2
	5563-V3	Privacy Enhancing Cryptography in Practice	Seminar	Pf	1
1	10101	Ausgewählte Kapitel der IT-Sicherheit	Vorlesung/Übung	Pf	3
1	10102	Netzsicherheit	Vorlesung/Übung	Pf	3
1	1037	Informations- und Codierungstheorie	Vorlesung/Übung	WPf	5
1	11432	Sicherheit in der Informationstechnik	Vorlesung/Übung	Pf	3
1	13981	Middleware und mobile Cloud Computing	Vorlesung	Pf	3
1	13982	Middleware und mobile Cloud Computing	Übung	Pf	2
1	15071	Enterprise Architecture und IT Service Management	Vorlesung	Pf	3
1	15072	Enterprise Architecture und IT Service Management	Übung	Pf	2
1	23191	Artificial Intelligence	Vorlesung/Übung	Pf	6
1	25381	Eingebettete Systeme	Vorlesung	Pf	2
1	25382	Eingebettete Systeme	Übung	Pf	1
1	33961	Data Mining und IT-basierte Entscheidungsunterstützung	Vorlesung/Übung	Pf	5
1	36481	Praktikum Compilerbau	Praktikum	Pf	3
1	51181	Foundations of Distributed Systems and Blockchains	Vorlesung/Übung	Pf	4
1	51182	Research Topics in Security for Decentralized Systems	Seminar	Pf	2
1	55041	Datenschutz	Vorlesung/Übung	Pf	3
1	55042	Privacy Enhancing Technologies	Vorlesung/Übung	Pf	3
1	55061	Einführung in die Kryptographie	Vorlesung/Übung	Pf	3
1	55062	Kryptoanalyse	Vorlesung/Übung	Pf	3
1	55481	Modern Cryptography	Vorlesung/Übung	Pf	4
1	60501	Signalverarbeitung	Vorlesung/Übung	Pf	5
2	10103	Praktikum Netzsicherheit	Praktikum	Pf	3
2	10104	IT-Forensik	Vorlesung/Übung	Pf	3

2	10106	Sicherheitsmanagement	Vorlesung/Übung	Pf	3
2	10107	Sichere vernetzte Anwendungen	Vorlesung/Übung	Pf	3
2	10321	Quantitative Modelle	Vorlesung/Übung	Pf	5
2	23211	Machine Learning	Vorlesung/Übung	Pf	6
2	29942	Quantum Machine Learning & Optimization	Vorlesung/Übung	WPf	3
2	36471	Compilerbau	Vorlesung	Pf	2
2	36472	Compilerbau	Übung	Pf	4
2	3823-V1	Rechtliche Grundlagen CNC	Vorlesung	Pf	4
2	3823-V2	Rechtliche Grundlagen CNC (Übung)	Übung	Pf	2
2	42111	Biometric Recognition	Vorlesung	Pf	4
2	42121	Deep Learning	Vorlesung	Pf	4
2	55031	Embedded Systems Security	Vorlesung/Übung	Pf	3
2	55051	Betriebssystemsicherheit	Vorlesung/Übung	Pf	3
2	55071	Language-based Security	Vorlesung	Pf	3
2	55131	Sichere mobile Systeme	Vorlesung/Übung	WPf	3
2	55144	Internationale Sicherheitsarchitekturen und Krisenmanagement im Cyberraum	Seminar	Pf	3
2	55631	Private Data Processing	Vorlesung/Übung	Pf	4
3	10322	Verlässliche Systeme	Vorlesung/Übung	WPf	3
3	10323	Zuverlässigkeitstheorie	Vorlesung/Übung	WPf	3
3	10471	IT-Governance	Vorlesung/Übung	Pf	4
3	11691	Vernetzte Operationsführung und Digitale Streitkräfte	Vorlesung	Pf	3
3	11692	Vernetzte Operationsführung und Digitale Streitkräfte	Übung	Pf	2
3	11972	Mobile Kommunikationssysteme	Vorlesung/Übung	Pf	3
3	12111	Algorithmische Zahlentheorie	Vorlesung/Übung	Pf	5
3	15511	Digitale Forensik (VL)	Vorlesung	Pf	3
3	15512	Digitale Forensik (UE)	Übung	Pf	3
3	23201	Responsible Artificial Intelligence	Vorlesung/Übung	Pf	6
3	23202	Responsible Artificial Intelligence	Seminar	Pf	2
3	23212	Praktikum Machine Learning	Praktikum	Pf	3
3	29941	Ausgewählte Kapitel des Data-driven Optimization	Vorlesung/Übung	Pf	3
3	29943	Seminar: Ausgewählte Kapitel des OR	Seminar	WPf	3
3	29944	Praktikum: Ausgewählte Kapitel des OR	Praktikum	WPf	3
3	35841	Praktikum Language-based Security	Praktikum	Pf	4
3	3822 -V1	CNC Methoden	Vorlesung/Übung	Pf	3
3	3822 -V2	Praktikum CNC Methoden	Praktikum	Pf	3
3	38521	Sentiment Analysis	Vorlesung/Übung	WPf	3
3	38531	Analyse unstrukturierter Daten	Vorlesung/Übung	Pf	6
3	39311	Introduction to Post-Quantum Cryptography	Vorlesung/Übung	Pf	4
3	55091	Penetration Testing	Vorlesung/Übung	Pf	6
3	55093	Penetration Testing	Praktikum	Pf	3
3	55141	Schutz von kritischen Infrastrukturen	Vorlesung/Übung	Pf	3
3	55632	Private Authentication and Messaging	Vorlesung/Übung	Pf	4
3	60531	Kanalcodierung	Vorlesung/Übung	WPf	5
4	11621	Erweiterte Digitale Forensik (Vorlesung)	Vorlesung	Pf	3
4	11622	Erweiterte Digitale Forensik (Übung)	Übung	Pf	3

4	12112	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Vorlesung/Übung	Pf	3
4	14461	Identitätsmanagement	Vorlesung/Übung	Pf	3
4	14462	Seminar Identitätsmanagement	Seminar	Pf	3
4	15513	Seminar zur IT-forensischen Gutachtenerstellung	Seminar	Pf	3
4	30101	Einführung in die Quanteninformationsverarbeitung	Vorlesung/Übung	Pf	3
4	38522	Social Media Mining	Vorlesung/Übung	WPf	3
4	38523	Semantische Technologien	Vorlesung/Übung	WPf	3
4	39312	Selected Topics in Post-Quantum Cryptography	Vorlesung/Übung	Pf	4
4	39313	Post-Quantum Cryptography in Practice	Seminar	Pf	1