New Challenges for IT-Security Research in ICT

Udo Helmbrecht, Rainer Plaga
Federal Office for Information Security (BSI)
Bonn, Germany

Paper for the 40th Session
World Federation of Scientists International Seminars on Planetary Emergencies
August 19-24, 2008, Erice, Italy

Abstract

Threats in information and communication technology (ICT) have substantially increased over the last years. The dependence on modern communication technology in professional and private environments results in an increase of IT risks. Trojan horses and DoS attacks with bot-nets are the most challenging attacks we have today. But we are also faced with new attack possibilities: data encrypted today with classical cryptographic methods and stored for long periods may be attacked with the help of quantum computers. There may be new mathematical possibilities to crack classical cryptography. New technological possibilities to eavesdrop using stray radiation may come up. The quality of attacks increases. Over the period of time technological possibilities of single individuals will tomorrow vastly exceed the one of governments today. Thus we need a cutting edge ICT-security research to be prepared for the upcoming threats. This paper gives an overview of current technological trends and proposes to create a new culture for the cooperation of the security community and academic community.

Introduction

The security of a system can be described as its ability to support the confidentiality and integrity of its data and the availability of the system itself. This security has been attacked by several kinds of malware nearly since the beginning of information technology. The first reports on PC viruses were published 20 years ago. At that time malware was transferred from one computer to another by floppy-disks. As the IT systems of public administrations, the industry and private users are completely networked in our days malware can spread around the world within seconds to attack unprotected PCs. A number of new malware types is registered every day. "Zero day exploits" take advantage of lack in IT-security immediately after they are published. The percentage of Spam messages in overall E-mail communication is increasing at an alarming rate, and the growing number of phishing attacks also reduces the confidence in the security of the Internet. Since the first occurrence of PC-viruses the number of attacks as well as the motivation of the attackers has changed substantially. The first individual computer hackers who were spurred by "sporting" ambition have been almost completely replaced by professional criminals. The attacks are also becoming more selective and cunning. Criminal "business models" such as identity theft and blackmail are facilitated due to the increasing shift of everyday activities such as shopping or banking via the Internet. Virtual identities enable criminals to remain almost totally anonymous and in this scenario systems of private users are very popular targets. But also complete companies and public administrations are targets of attacks and it is not easy to localize the origin of the attack. Every PC-user can be estimated as an (un)certainty factor in an everyday environment, because victims of malware can become unwilling offenders if their computers are compromised in a bot-net. Also employees can cause considerable damage to companies as a result of thoughtless behavior.

Threats - Today and Tomorrow

The Report on the IT security situation in Germany [1] shows the dramatic increase of attacks by Trojan horses and the increasing quality of attacks by organized crime:

Trojan horses

Trojan horses are programs which are active on computers without the knowledge of the owners and secretly execute disruptive functions. Modern Trojan horses offer the attackers a wide range of communication and control options as well as a large number of functions which can be combined as required. They can completely control the computers of other users, spy on data, record keyboard inputs and screen outputs or sabotage IT systems. They also have highly developed camouflage functions, and download updates from the Internet to the infected computers.

Trojan horses are, for example, used for the organization of bot-nets and phishing attacks, and their use for selective espionage is steadily increasing.
As a result, the threats for agencies and companies which depend on the confidentiality of their data have changed dramatically. The potential damage caused by espionage is complex and serious. Threats to national security, economic losses, disclosure of negotiation positions or compromising of individuals or institutions can be the consequence. For selective attacks contemporary malware can be modified to suit the individual environment of the victim's PC-system so that malware cannot be detected by virus protection programs. Communication with the attacker takes place over the Internet and uses standard protocols which are required for Internet and E-mail usage. For this reason firewalls do not offer any protection in these cases.

DoS Attacks

A Denial-of-Service attack (DoS attack) is a term used to refer to an attack on the availability of an IT system or service with the aim, for example, of preventing users from accessing an online shop. Therefore attackers exploit vulnerabilities in operating systems or applications to make a system or a service inoperable. Much more frequently systems are saturated with useless data packages to paralyze them. In order to increase the volume of data and make the attacks even more effective, an increasing number of distributed Denial-of-Service attacks (DDoS attacks) has been observed in recent years. For this purpose attackers first obtain execution rights on several unprotected computers of other users and install DDoS software. The computers which are taken over by the attackers then participate in coordinated attacks in this manner without the knowledge of the computer owners. A reason for this tremendous increase in this type of attack is assumed to be the distribution of bot-nets. DDoS attacks are still a serious threat for regular operation of Internet servers. They cannot be prevented, but it is possible to at least make them difficult by using the measures available to this purpose.

Bot-nets

A bot (short for robot) describes a program which works by remote control. In the context of malware, a bot is a program which enables an attacker to remotely control infected computers. The term bot-net refers to a number of infected PCs which are linked by remote control and which are abused for certain actions. Bot-nets are, for example, used to run DDoS attacks or for sending Spam. Attackers mainly target vulnerabilities in networks to infect a PC with a bot. Bot programs are now more frequently smuggled onto the computers of users by means of E-mail attachments or manipulated websites. The central control element of a bot-net is the Command-and-Control server (C&C server). Computer systems infected with a bot establish a connection to this server autonomously and receive their orders from the server. The number of smaller and therefore more maneuverable bot-nets has increased. The advantage for the operator is that the bot-nets are more difficult to detect due to the higher flexibility and can more easily avoid being destroyed. The threat constituted by bot-nets is persistently high. As in other fields of IT manipulation, the perpetrators are increasingly spurred by criminal intent. Their “business models” include click fraud, password espionage by means of key loggers and password sniffers, DDoS attacks on competitors or blackmail.

Technological Trends

Another challenge is pervasive computing [2] or the so-called “Internet of things”: distributed networked computing power everywhere for everyone. The ICT-components are becoming smaller and smaller. They will be integrated in products we use in our everyday life and transform these products into smart objects which are connected with each other and can communicate via radio frequencies. These smart objects will not be part of a fixed environment or application but will spontaneously cooperate in ad-hoc networks. On the one hand the embedded ICT components are becoming more and more ubiquitous, on the other hand ambient computing components will become more or less invisible for humans. Most of the components will have numerous interfaces to communicate with their environment, but there will not be a visual interface anymore. They will receive information about users and their environment from sensors and adjust their behavior according to that data. A new class of security attacks will be seen: attacks against the network infrastructure to manipulate sensor nodes, routing information or the data communication or even cloning of sensors. Therefore we need new security mechanisms.

Another technological trend are sensor networks: a flexible mobile detection of persons and objects. Power consumption is critical for this technology. We need novel sensor combinations and new security mechanisms with very low power consumption.

The miniaturization of RFID (Radio-frequency identification) chips is still going on. Siemens and Infineon announced an RFID tag with an area of 0.8 mm^2. RFID tags usually send out their serial number in plain text. Attackers can clone tags at will, they can track and monitor them. The most critical threats are those concerning authenticity and privacy. We need improved security mechanism for asymmetric cryptography based on elliptic curves. The tag uses a true random number generator based on Galois Ring Oscillators.

For identity management BSI and NXP presented a mobile cryptographic smartcard reader of two password based protocols for secure connection establishment between contactless smartcard and terminal. This allows forward secrecy of the session keys and security against off-line dictionary attacks.

The most challenging technology is quantum computing. In 1982 Richard Feynman had the idea to simulate quantum mechanical systems by - what we call today - quantum computers. In classical computing based on the von Neumann Architecture we store data as bits representing 0 or 1. In quantum computing we have so-called Qubits, representing physical states, i.e. the spins of an electron or a polarised-photon. A quantum computer makes direct use of distinctively quantum mechanical phenomena, such as superpostion and entanglement, to perform quantum mechanical operations on the data. Finally, upon termination of the algorithm, the result needs to be read off. In the case of a classical computer, we read out the data. Quantumly, we measure the final state, which is equivalent to collapsing the quantum state down to a classical distribution.

For quantum computers an algorithm that calculates the secret key from the publicly available information in asymmetric cryptographic codes within a time that grows only slowly (polynomial) with the key size has been proposed by Peter Shor [4]. By this algorithm for the factorization of prime numbers the encryption of RSA would be possible. A quantum computer of about 200 QuBits is sufficient to break all asymmetric cryptographic algorithms known today. No key size for which the classiacal algorithm withstands attacks by quantum computers for a sufficiently long “foreseeable future” can then be proposed. Therefore the currently used asymmetric cryptosystems and especially PKI (Public Key Infrastructure) systems are threatened by quantum computers. This threat exists even today, before quantum computers are available, because attackers can store chiffrates today and decrypt them in many years later. Because many data sets, e.g. medical records, must remain confidential for decades, already today the quantum computer constitutes a tangible risk for the security of information.

Today we act mostly reactive: for new security vulnerabilities we update or patch systems, for new viruses we update the virus scanner, if we detect new Trojan horses we install new patches again. This shows that we need a new security paradigm to increased prevention by sustainable ICT-security research. We see three sustainable measures:

- Long term security:
  quantum cryptography, fading channels
- Classical cryptography:
  research into cryptanalysis algorithms on adiabatic quantum computers
- Perimeter security:
  wireless sensor nets for mobile perimeter security, systematic research of “side channels”

BSI IT-Security Research

We are faced with new attack possibilities, for example, that data encrypted with classical cryptographic methods today and stored for long periods may be attacked with the help of quantum computers in the future. There may be new mathematical possibilities to crack classical cryptography. New technological possibilities to eavesdrop using stray radiation may come up. The quality of attacks increases. Over the period of time technological possibilities of single individuals twill tomorrow vastly exceed the one of governments today.

The BSI concentrates on four main topics: Internet early warning systems, trusted computing, biometrics for identity cards and quantum information.

Internet Early Warning Systems

Against the Internet threats described above we need new prevention strategies for the protection against new attacks. Therefore BSI invests in research on early warning via new sensor data collection and analysis. The goal is to extend the BSI IT Early Warning System by implementation and evaluation of new types of sensors and components. This includes investigation of technical, organizational and legal implications.

Trusted Computing

The BSI is liaison member of the Trusted Computing Group [5] and Germany supports the trusted computing initiative. Key requirements by the German Federal Government are the availability of the specifications, open standards, interoperability and certified products [6]. For national classified material an information-processing-systems we need special high secure infrastructure, the so-called Secure Inter-Network Architecture SINA [7].

Therefore we do research on self-protecting IT systems and highly secure embedded processor platforms.

Biometrics for identity management

In 2005 the Federal Government of Germany issued the new electronic passport (ePass) with biometric elements to increase the security features and the binding between person and document by introducing a facial image in the ePass. In 2007 the biometric data of the fingerprints were also included. The next step is to improve the controlling infrastructure. Therefore the BSI invests in live finger detection. For secure electronic business over the Internet a secure authentication is needed. The German government announced an electronic national identity card for 2010 and the BSI invests in innovative security token platforms.

Identity management in Internet business has many aspects. The provider wants to know who the customer is, the customer wants to be sure that the Internet portal is not faked. With localization technologies like GPS one can offer specific new methods for identification and localization.

Research is being done to improve fake detection of biometrics, e.g. to prove aliveness. The above mentioned trends will allow us to build a security architecture for micro sensor networks to realize for example a flexible border surveillance network by using temperature sensors. Those applications have to be based on a reference model for secure sensor networks.

Quantum Information

We concentrate our research activities on quantum computer resistant cryptographic mechanisms and security technologies, the selection and investigation of quantum computer resistant cryptographic algorithms, including security implementations and prototypical applications, and the practical realization of those algorithms. The following applications are particularly relevant: encryption, electronic signatures, authentication, data integrity. In particular we will deal with the implementation of the selected algorithms on different platforms, functionality aspects, security aspects, resistance against side-channel attacks, and fault attacks.

Culture of Cyber Security in research

In the academic research community there is a natural tendency only to concentrate on fundamental research problems. But in cryptography and security the attacker looks for the weakest point in the system. Therefore the security professional has to be on the lookout not for the most interesting case but the worst case. Moreover she has to strive for completeness in her analysis, a requirement that is very rare in pure research. There are no pernicious consequences from overlooking some interesting special possibility that occurs in some fundamental theory. Overlooking just one special attack possibility might render a security system brittle. Another “cultural difference” concerns the need to make all claims explicitly comprehensible in a security analysis. It is convenient and effective to rely on a large body of knowledge that is “commonly known”. However, experience teaches that a very small fraction of the “common wisdoms” always turn out to erroneous. This fact is of course known to the research community. There is a common saying that a theory that agrees with all experiments must be wrong because some of the experiments will always turn out to contain errors.

Invariably – e.g. by trial and error – the attackers will sooner or later exploit these gaps. The only and imperfect way to mitigate this risk is to require an explicit statement with source for each claim in an analysis. Theories in fundamental research are very useful even if they are thought to work only in certain parameter ranges. In a sense one might claim that most – but not all – fundamental theories are of this type. On the contrary a security model cannot tolerate such parameter ranges because the attacker will tend to concentrate to exploit gaps that arise in these ranges.

Another important principle that needs to stressed in security is the “system idea”. In security the sum of the parts is often less secure than the parts itself**.** One major reason for this is flaws in the implementation of a composed system. In many cases cryptographic systems were broken, not because of the weakness of the algorithm but because of bad implementations on computers. An example are passwords of Unix based systems. They are hashed and the password cannot be recovered from the hash. But the hashes have been stored readable for everyone, which makes the system vulnerable for dictionary attacks by anybody using the system A classical weakness in the design of the system which can be solved by making the hashes readable by the administrator and the system itself only.

The following table summarizes some different approaches and the experience shows, that attacking security problems with a purely academic-research approach results in systems that are easy to break.

	Security Community	Research Community	Risks
1.	The attacker will tend to exploit the simplest vulnerability, the worst case ...	... not the academically most interesting/challenging	system is easy to break
2.	Completeness must be achieved ...	... special cases suffice most of the time.	system can be broken in various ways
3.	All ideas/terms/facts must be explicitly, rigorously stated ...	... facts “known in the community” can be assumed.	results in design errors due to misunderstandings
4.	The security model must be reliable for all parameters possible in practice ...	... models that break down for certain parameters can be very valuable.	system model that fails to describe an attack and thus breaks down.

Thus we need a “culture of research in security” covering and uniting various disciplines. Clearly the security community dearly needs the input of the research community to develop novel security mechanism. Which security-related problems might be most useful in such an endeavor? As a classification, we propose to distinguish between practical i.e. applied problems, pseudopractical problems and fundamental problems as described above:

Practical problems

are useful to identify and eliminate weak points of systems. Proposal: build a physical system that withstands real attackers. To tackle such problems is clearly useful in practice but it might also lead to interesting fundamental ideas. Interesting science is often done as a response to a practical challenge. The ivory tower is not necessarily the most productive work place.

Pseudopractical problems

are practical problems that cannot be solved within the “foreseeable” future, say within five to ten years. This, for example could be the quest to build a physical system that is “provably secure” or to build a large scale quantum computer. The usefulness of pseudoapplied problems is questionable because it is difficult to find common criteria to decide which strategies are best to reach a goal that can be reached only very far in the future.

Fundamental questions

are typically questions regarding the “axioms” of a research field. A fundamental problem of quantum mechanics is the border between quantum effects and classical physics, when quantum systems interact with their environment. Decoherence, the loss of superposition and the collapse of the wave function, is a fundamental problem for our understanding of nature but also a potential practical obstacle for constructing quantum computers. Therefore new and improved experiments are needed to observe superposition effects on macroscopic or “large scale” objects.

The quantum information field is currently strongly driven by the above “pseudoapplied problems”. For the discussion of large quantum computers this can hardly be replaced by practical problems. We propose to introduce fundamental questions as a stronger driver, by this we mean as one proposal to build a system that tests validity of superposition principle on as “large” scales as possible.

There is a need for further research on the question, what is “large”. One should introduce an abstract model to concisely define “large”, which might include mass and size in non-trivial ways.

Such tests could have two results: either an explicit collapse of the wave function which would mean an increased security of classical cryptography (“and perhaps a trip to Stockholm”) or continued large scale quantum coherence, which would give confidence in concrete step toward practical quantum computers.

Another possibility of this type would be experiments that search for nonlinearities in the temporal evolution of quantum states, induced e.g. by purely classical gravitational interactions [8]. Again a positive result would lead to a deep new insight into new laws of Nature and a negative results would strengthen our trust into the security of quantum cryptography.

Summary

The increasing use of the Internet, the successful implementations of business models on one side and organized crime in the Internet on the other side together with new technological trends cause a new approach to ICT-security research. This is because our approaches to secure Internet communication depends on authentication, decryption, digital signatures, electronic identities which all depend on cryptographic algorithms. So we must be sure that today's data is secure in 20, 30 and more years. Thus we have to improve the classical cryptographic algorithms, i.e. elliptic curves, and face the challenges of new technologies like quantum computers. The authors propose to introduce a new culture in academic research to work not only on specific problems, but more to look for a holistic approach from fundamental questions (what is “large” for quantum computers) to practical questions in daily implementations, because attackers are mostly looking for the weakest point in the targeted system.

References

[1] "Report on the IT security situation in Germany", BSI, Bonn/Germany, March 2007 (http://www.bsi.bund.de/english/publications/).

[2] "Pervasive Computing", BSI Study, 2006 (http://www.bsi.bund.de/literat/studien/percenta).

[3] Quantum Computation and Quantum Information, Michael A. Nielsen, Isaac L. Chuang, Cambridge University Press, 2002

[5] Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, P. Shor, SIAM J. Sci. Statist. Comput. 26 (1997) 1484.

[5] Trusted Computing Group, Beaverton, USA (https://www.trustedcomputinggroup.org).

[6] "Key requirements on Trusted Computing", BMWI (http://www.bmwi.de/English/Navigation/Technology-policy/The-information-society/secure-it-platforms,did=241614.html).

[7] "SINA / Secure Inter-Network Architecture", (http://www.bsi.de/fachthem/sina).

[8] "A fundamental threat to quantum cryptography: gravitational attacks", R. Plaga, Eur. Phys. J. D 38, 409-413 (2006).