The next step in IT security after Snowden

Norbert Pohlmann

Institute for Internet Security - if(is),
Westphalian University of Applied Sciences Gelsenkirchen
Neidenburger Str. 43, 45877 Gelsenkirchen, Germany

Abstract

The Internet with its many innovative opportunities became a continuously growing relevance in our modern society. Through advanced software solutions and complex correlations between protocols, services and infrastructures, vulnerabilities of Internet technologies are becoming more diverse and much larger than ever before. Attacks on high values within IT systems and their availability are executed more distributed, sophisticated and professional. There is also a noticeable industrialization of cybercrime, resulting in a professionalized sustainability, which is not to be underestimated and which has never existed before. Some particularly striking security problems, arising from the critical assessment of the current IT security situation, could be solved by appropriated paradigm shifts.

Keywords: IT security problems, vulnerabilities, proactive IT security, object IT security

1 Evaluation of the IT security situation

Over the period of time our IT security problems have become bigger and bigger not smaller. The problems have become even greater with the NSA affair. So the risk-level is constantly rising. But, what are the biggest IT security problems we have to handle at the moment?

Figure 1: Evaluation of the IT security risks

First IT security problem: "Too many software vulnerabilities"
Software represents an evolving portion of added value in all sectors. It is used in PCs, Notebooks, Smartphones, large datacenters, but also increasingly in cars, industrial plants, critical infrastructures, houses, and similar application areas. A major security problem is the amount of software vulnerabilities. The software quality of operating systems and applications is for today's threat landscape no longer sufficient. Currently, the error density averages 0.3, referring to the number of bugs per 1.000 lines of code in high quality software. Since common operating systems consist of about 10 million lines of code, there are about 3.000 errors to find. Parts of them represent potential targets for attacks. The software companies do a lot to decrease the number of vulnerabilities in their software. Nevertheless, criminal organizations are still able to exploit this smaller number of vulnerabilities very professional. And this situation will not change in the near future. The opportunity to use these vulnerabilities in software is too easy.

Second IT security problem: "Insufficient anti malware protection"
Malware is the generic term for "Malicious software" such as viruses, worms, and Trojan horses. Attackers, like criminal organizations, spies, and terrorists, exploit software vulnerabilities to install malware on IT devices. Injection of malware on IT devices almost happens unnoticed, through e-mail attachments or so called "drive-by" downloads on insecure websites. The Institute for Internet Security currently assumes that every twentieth IT device in Germany is infected by unwanted malware, controlled by botnets. Therefore attackers are able to retrieve information via key-loggers and Trojans, to distribute Spam and execute DDoS attacks, even to encrypt data and demand ransom for decryption [1] [2] [3]. Critical observations show that today's detection rate of anti-malware products is only between 75% and 95%. The detection rate of direct attacks on IT systems is only averaging 27%.

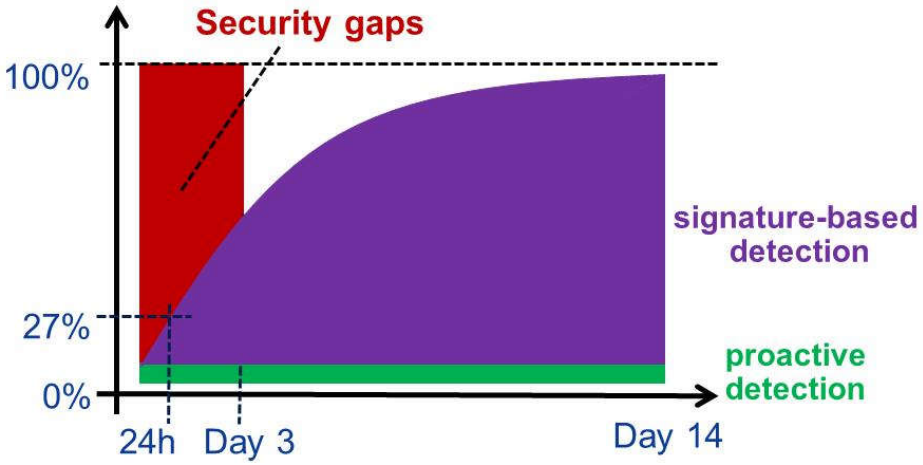

Figure 1: Insufficient anti-malware protection

This is because of the fact that the most important detection mechanisms are still signature based today. And that means we need time to identify new malware and distribute new signature. And in this time the attackers have a very good opportunity to use the security gap to install new and targeted malware. The portion of proactive malware detection is increasing but not high or successful enough [4]. So the result is: we have insufficient anti-malware protection!

Advanced persistent threat (APT) is the concept, which has established itself for intelligent malware like Stuxnet and Flame international. It is usually considered as a targeted attack with complex technologies and tactics, as well as background information on victim's IT systems and its surroundings. In this case, the attacker puts great effort in successfully accessing a victim's IT system and staying undetected over a long period of time. The purpose of APT is to spy out as

many information as possible or to cause damage. Currently, there are no suitable defense technologies against this kind of sophisticated attacks with intelligent malware.

Third IT security problem: "No international solutions for identification and authentication"
In 2014, we still use passwords for authentication in the Internet. The resulting problems are well known: the usage of bad passwords, or a single well-considered password, which is used for multiple applications. Via e-mail or HTTP, passwords are transmitted as plain text throughout the Internet. Each year, high damage results from using password as an insecure authentication technology.

Fourth IT security problem: "Insecure Web sites on the Internet"
The most frequently form of distributing malware is through insecure company websites on the Internet. Typically with the help of Drive-by downloads. The mal-code is for example executed in hidden iframes on the website and can go undetected even by an experienced user. We know from own measurements at the Institute for Internet Security that 2.5 % of the German measured websites are infected with malware. In the US we measure only 1.01 percent and in Japan 0.51 percent [5]. A major problem regarding websites, results from companies and government agencies, focusing only on user guides, color schemes and performance, but not on IT security. This is like a logistics company using trucks without brakes in road traffic.

Fifth IT security problem: "New threats through the use of mobile devices"
The advantages of mobile devices, such as Smartphones and tablets are impressive. Through various communication interfaces like WLAN, UMTS and LTE, the Internet with its services is always and everywhere available. The touchscreen makes the devices easy and quick to use. They are multi-functional: mobile phone, computer, navigation system, music player and access to the company network - all in one device. With "local based service", useful and innovative services are added. But with mobile devices, new vectors of attack occur, which are causing more risks. Changing and insecure environments, like airports, train stations and cafés, increase the probability of accidental loss and targeted theft. The potential of creating motion profiles and the ease of public inspection are not to be underestimated. We have to face the challenge “mass instead of class”. Users download too many Apps and accept the access to every data the App wants. But, there are apps, for example a “voice recorder apps” that is implemented and offers for free to spy on our smartphones [6]. The Business model: "Paying with personal information" instead of money is a problem.

Sixth IT security problem: "Insufficient Internet literacy of its users"
Internet users need to know the dangers of the Internet, otherwise they harm themselves and others, for example through infections of malware. Based on a BITKOM survey in 2012, 30% of all Internet users have no personal firewall and 28% no anti-malware solution on their devices. This leads to none adequately protection of the IT devices of the Internet user.

Seventh IT security problem: “Manipulated IT and IT security technologies”
The NSA inserting backdoors, sabotaging standards and technology and is making therefore our business and Internet life insecure! For example “bad random generators” make the operation of encryption useless. Not only the NSA can use the vulnerability to have access to our values also criminal organizations and business spies can do that. And that is a really bad situation for all of us!

Other IT security challenges we have at the moment are: Too high risks in e-mail communication, Cloud Computing, Smart everything opens new attack vectors, and so on.

2 Changes in the general condition

The Internet itself goes beyond all borders and cultures. There are different opinions about, what is right and what is wrong. Examples: We have different legal frameworks in data protection in Europe and the US, but also diverse culture backgrounds in the field of privacy. Another example of different opinions is: Protection of intellectual property - China and the rest of the world see this point different and that makes life challenging in the global village. The US believe that spying "friends" is part of the global protection of terrorism.

The uncertainties of different legal systems must be taken into account. But still there are too many countries, where no criminal prosecution is possible. Additionally, we currently are experiencing a radical development and alteration within in the IT and the Internet, through social networks like Facebook, Twitter, even through cloud computing and critical infrastructures. Changes of frameworks result in additional and currently known challenges. In Germany we change from nuclear power to alternative electrical power supply. That means we build up intelligent smart grid systems which are connected to the Internet. But that means all the Internet attacks we know also apply for our electrical power supply. Every time in the past when the electrical power supply didn´t work we had dead people. So this is a real cyber war issue!

Basically insecure, manipulated and poorly implemented IT technology, combined with an insufficient Internet literacy of its users, indicates the need for a paradigm shift with regards to the ability of using Internet technologies and services with less risk in future.

3 Paradigm shift

So what does the evaluation of the IT security situation mean? The IT security problems are known, but the todays IT security approaches can´t handle the challenge. We have to change some paradigms we have in IT and IT security to reach an adequate level of risk. The following proposals will describe some paradigm shifts which can help us to come out of this bad IT security situation.

Paradigm shift - much more encryption for a sustainable protection of our data
An important paradigm shift is that we need much more encryption to protect us appropriated. IPSec is for the encrypted communication between companies or parts of companies. In the Institute for Internet Security we measure that every 125th IP packed in the internet is IPSec encrypted [7]. Since Snowden the growth rate of IPSec is 60 %.

SSL/TLS is for example for the encrypted communication between the browser and the web servers. Here we measure that every 7th IP packed in the internet is SSL/TLS encrypted. Since Snowden the growth rate of SSL is 90 %. The reason for that is that the companies started to offer SSL/TLS as default.

But we also need to catch up with e-mail encryption, disc-, file encryption, and so on. But it is very important that we take into account some needed requirements. One important requirement is trustworthy encryption technology that means no backdoors, strong random numbers, correct implementation, and so on. But we also need trustworthy IT security infrastructure. That means for example all PKI stuff and root certificates have to come from Germany.

Paradigm shift - responsibility versus indifference
Currently, the major technology producer and service providers like Google, Apple, Facebook and Microsoft determine, what we as users need. But for their solutions they don't take responsibility. What we need, however urgently, is a producer responsibility such as in the automotive industry! If

we buy a car today, the producer takes full responsibility. Although the automobile manufacturers are working together with several hundred suppliers, there is only one contact person for us to approach. On a regular basis the manufacturers check all functionalities of their cars and if they detect a failure, big recalls are started, aiming to resolve failures, before actual problems occur. This has created a great confidence in the manufacturers. But who is taking over responsibility for IT systems? In the end there will be no one. If the IT vendors would start to take over responsibility, today's IT security problems would be considerably lower. As a result, software and hardware would be better aligned and errors would be found and fixed more easily.

Another "responsibility" aspect is validation and certification. Validation and certification is an establish business. The idea is independent and qualified organizations prove or improve the quality of IT or IT security products and solution. As a result we have more secure trustworthy products which are testified by trusted third parties. This way is necessary because the user can't do it himself.

Paradigm shift - proactive versus reactive security solutions

With today's reactive IT security systems, such as anti-malware and intrusion detection systems, we are tracking IT attacks. This means that when IT security systems detect an attack by a corresponding attack signature or anomaly, it tries to protect the system as quickly as possible to reduce damage. One analogy of reactive IT security is the „Airbag approach": If it happens, it should hurt less.

The growing diversity and complexity of our IT devices and infrastructures lead to the need of considerably more reliable, robust and effective IT security concepts. We must distance our self from the exclusively use of reactive, toward modern and proactive IT security systems, which can prevent the execution of intelligent malware, one of the biggest problems at present [8].

Proactive IT security systems operate for example with a security kernel with separation and isolation technology combined with intelligent cryptographic security mechanisms. Proactive IT security systems provide a secure and trustworthy base in your own and in the computers from others. One analogy of proactive IT security is the „ESP strategy": Avoid skidding, before it happens.

Trusted Platform

We need a Trusted Platform for modern and intelligent IT security solutions in our distributed virtual world. For that we need appropriated IT security architecture, IT security principles and – mechanisms which help us to build up a trusted IT system.

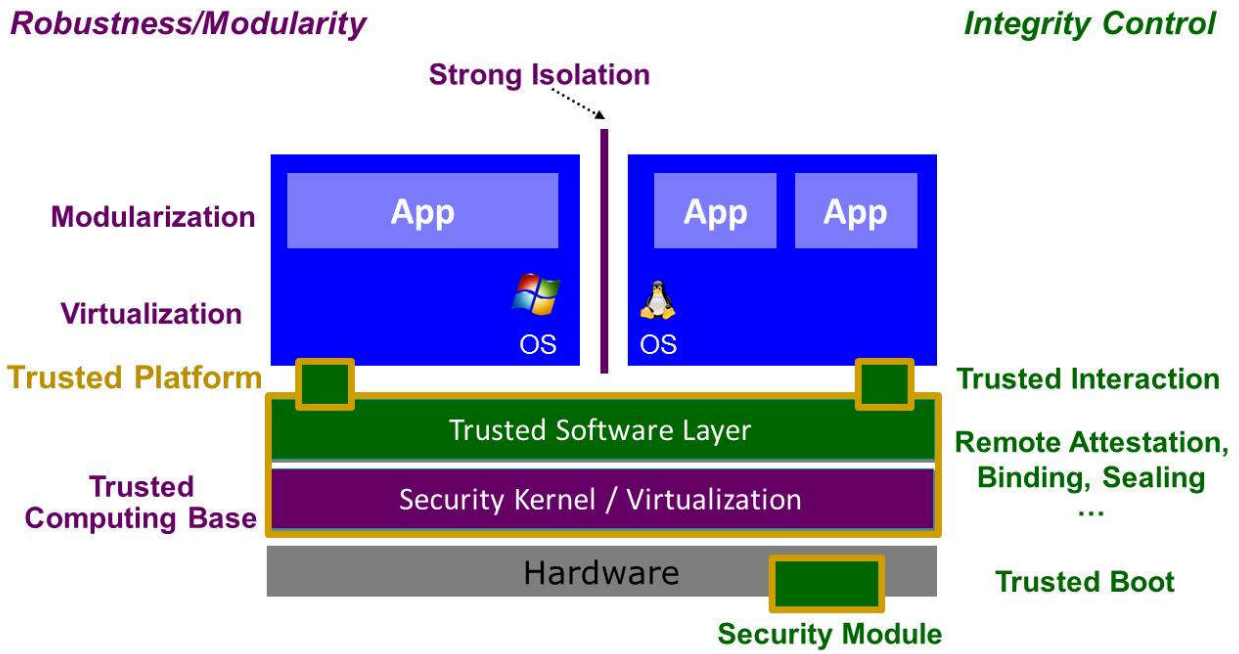

Figure 2: Trusted Platform architecture, principles and mechanisms

In this appropriated IT security architecture we have the given hardware of our IT system. By definition, the "trusted computing base" is the critical part of an IT system. The idea is, if a vulnerability is present in the "trusted computing base", then the whole IT system will be affected. If a vulnerability exists outside the trusted computing base (TCB), the potential for harm will be limited based on a security policy. For this reason, a trusted computing base (TCB) has to be very carefully designed and implemented. A trusted computing base (TCB) based for example on a security (micro) kernel with virtualization technology has approximately 100,000 line of code. This number of line of codes can be very good semi-formal verified and therefore offers a significantly better protection than normal operating systems. With the help of “virtualization” we can use the advantage of robustness, which we use for a long time for server systems. The IT system can very easily go back to a stable state and start from there again. The security aspect of “strong isolation” ensures that the virtual machines running separately and cannot influence each other. This is a very important feature. The security aspect of “modularization” gives us the ability to run applications that go together in one virtual machine and positioning applications, which should be separated into different virtual machines. Here we have an interesting design freedom, which helps us to achieve a high level of security. We can run several applications with different security needs in different virtual machines. So, modularization together with strong isolation is a very helpful security feature [9]. With the security aspect “Integrity Control”, the integrity and therefore the trusted state of an IT system can be checked. The Trusted Software Layer provides trusted security services which help us to make IT systems more trustworthy.

The “Security Module” is for example a TPM with intelligent cryptographic functions on the level of smart card security. It was always a dream of IT security specialists to have a security module on an IT system available! What are the major benefits? First: The security modules offer very high security with a low investment, because a TPM cost approximately 1 euro. Second: The security modules are already available on the vast majority of IT systems! One reason is that the hardware needs the TPM to be Microsoft ready. Therefore the widespread introduction of trusted platform using TPM is quite easy! Third: The security modules are already integrated in a PKI infrastructure. That makes the handling of the security management with TPM simple.

“Trusted Boot” ensures that the IT system is only active in a defined trusted state. That means we can identify changes in software and so we are able to identify malware. “Remote Attestation” gives us the opportunity to measure the trustworthiness of others IT systems before an interaction to the others IT system with this IT system will be started. “Binding” and “Sealing” are additional trusted computing functions which help us to build up a modern intelligent IT security system. The terms “Trusted Interaction” cover the security function in the Trusted Security Service that provides trustworthy entering, storage, transmission and display of data. All security aspects together represent the trusted base or the trusted platform.

Paradigm shift - object versus perimeter security
The idea of defense model perimeter security is to protect a set of computer systems and networks with the help of Firewalls, VPNs, Intrusion detection and so on. The perimeter security approach has the assumption that the computers and the networks are fixed installed. But in our modern world uses we work much more flexible and distributed with the help of mobile devices. Today for example nearly everybody has the opportunity to use a smartphone as a hotspot to go via a mobile provider in the internet without passing the central firewall system of his organization. So we have to realize that perimeter security can’t protect us like in the past! What we really need is object Security with information flow control. The Idea is domain object-oriented security, in which the objects are provided with rights. The rights define who can use the object with which action in which IT environment. These give us a general approach to handle the security very flexible. Object lifecycle protection combined with distributed policy enforcement even on foreign systems will protect our assets. Important to realize is that we need a trustworthy base for intelligent object security. Objects should be securely exchanged between all trustworthy IT systems in the world. But here we need a common security infrastructure and we have to find out who should be responsible for this needed security infrastructure.

Paradigm shift - collaboration versus isolation
Basically insecure and poorly implemented technology, as well as the insufficient Internet literacy of its users, causes damages through attacks. A company, which became victim of an attack, usually tries to solve the problem alone and isolated. The details of successful executed attacks, the attackers procedures, the extent of damage and the effectiveness of countermeasures, therefore, remain unused for the society. Through a well-structured and trustworthy cooperation between companies and authorities, an overall increased IT security could be achieved. Consequentially, the current security situation would be better assessable, critical vulnerabilities could be identified in collaboration, resistance could be increased, the defense costs reduced and the access to qualified security professionals could be optimized. And therefore we also need a business model for the defenders collaboration. A business model with less money for security mechanisms, and as a result a common lower risk-level for the companies and governments those are willing to collaborate.

4 Summary and outlook

If we want to strategically utilize the positive possibilities of modern IT and the Internet, we will quickly need to adopt new pathways and a change of paradigm in IT and IT security, with the result of a better IT security and trustworthiness. The proposed paradigm shifts will be expensive, and it requires coordination between producer and the user companies. A modern society should recognize the needs and quickly implement these steps to be adequately protected.

References

[1] C. Rossow, C. Dietrich, C. Kreibich, C. Grier, V. Paxson, N. Pohlmann, H. Bos, M. van Steen: "Prudent Practices for Designing Malware Experiments: Status Quo and Outlook". 33rd IEEE Symposium on Security and Privacy, S&P 2012, San Francisco, CA, USA 2012

[2] C. Dietrich; N. Pohlmann; C. Rossow: „Exploiting Visual Appearance to Cluster and Detect Rogue Software". In ACM Symposium On Applied Computing (SAC), 2013

[3] C. Rossow; C. Dietrich; H. Bos, L. Cavallaro; M. van Steen; F. Freiling; N. Pohlmann: "Network Traffic Analysis of Malicious Software". In Proceedings of the Workshop on Building Analysis Datasets and Gathering Experience Returns for Security - BADGERS 2011, Salzburg, Austria, April 2011.

[4] T. Bottesch; M. Ollig: Maschinelle Erkennung von Malware auf Basis statischer und verhaltensbasierter Merkmale. Master Thesis at the Institute for Internet Security at the Westphalian University of Applied Sciences Gelsenkirchen, Germany, 2010

[5] S. Feld; N. Pohlmann; M. Sparenberg; B. Wichmann: „Analyzing G-20´Key Autonomous Systems and their Intermeshing using AS-Analyzer". In Proceedings of the ISSE 2012 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2012 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag, Wiesbaden 2012

[6] O. Achten, N. Pohlmann: "Sichere Apps – Vision oder Realität? ", DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Springer Fachmedien, Wiesbaden, 03/2012

[7] N. Pohlmann, I. Siromaschenko, M. Sparenberg: „Das „Schengen-Routing" zu Ende gedacht - Direktvermittlung", iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 02/2014

[8] M. Linnemann, N. Pohlmann: „Turaya - Die offene Trusted Computing Sicherheitsplattform", in "Open Source Jahrbuch 2007", Hrsg.: B. Lutterbeck, M. Bärwolff, R. Gehring, Lehmanns Media, Berlin, 2007

[9] D. Bothe, C. Fein, N. Pohlmann, E. Reich, A. Speier: „Draft of a Dynamic Malware Detection on Trustworthy Endpoints". In Proceedings of the ISSE 2013 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2013 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Springer Vieweg Verlag, Wiesbaden 2013