SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World* [†]

Deliverable D4.1: First Report on Threats on the Future Internet and Research Roadmap

Abstract: This deliverable presents an overview of current and emerging threats identified by the three working groups at the end of the first year of the project. In addition, this deliverable contains the first research roadmap in the area of System Security.

Contractual Date of Delivery	August 2011
Actual Date of Delivery	September 2011
Deliverable Dissemination Level	Public
Editor	Davide Balzarotti

The *SysSec* consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
Institut Eurécom	Principal Contractor	France
IICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

[†]The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257007.

Contents

Acknowledgments

A number of researchers and external experts contributed to the definition of the future threats and to the research roadmap presented in this document. We would like to thank all the members of the Industrial Advisory Board, the 56 external members of the three working group mailing lists, and all the participants of the February Face-to-Face working group meeting. Their positive discussion and invaluable feedback was very important to help us define the content of this deliverable.

In particular, we would like to thank the following people (presented in alphabetic order) for their important contribution to this document:

Leif Axelsson *(VTEC)*
Gunnar Björkman *(ABB Germany)*
Julio Canto *(Hispasec)*
Marc Dacier *(Symantec)*
George Danezis *(Microsoft)*
Herve Debar *(Telecom SudParis)*
Jean-Pierre FAYE *(Thales)*
Ted Herman *(University of Iowa)*
Thorsten Holz *(Rurh University, Bochum)*
Jaap-Henk Hoepman *(TNO and Radboud University, Nijmegen)*
John Ioannidis *(Google)*
Engin Kirda *(Northeastern University)*
Chirstopher Kruegel *(University of California, Santa Barbara)*
Rita Lenander *(E.ON Nordic)*
Angelos Stavrou *(George Mason University)*
Wolfgang Trexler *(Bank Austria)*
Giovanni Vigna *(University of California, Santa Barbara)*

Part I

Threats

1 Introduction

In this first part of the deliverable we present a summary of the main threats identified by the three *SysSec* Working Groups during the first year of the project. We decided to preserve the division of threats by area instead of presenting a single, unified list. Therefore, the following three chapters reflect the topic associated to each Working Group, respectively focusing on *Malware and Fraud*, *Smart Environment*, and *Cyberattacks*. Each chapter include a mix of current and emerging threats, with a focus on the short- and mid-term future. In addition, we also decided to avoid any rating or risk assessment, postponing the decision of which area is more important and which area requires more attention from the research community to the roadmap presented in the second part of this document.

The threat selection process was based on four different types of contributions. A first draft of the threats list was initially prepared by each Working Group, based on the personal experience of its members in the area under study. This preliminary version was later extended to take into account the feedback provided by WorkPackage 5, WorkPackage 6, and WorkPackage 7. The objective of these three WorkPackages during the first year of the project was, among other things, related to the analysis of the state of the art, and the study of trends in the topic of scientific publications. Obviously, by carefully reviewing the related work, the WorkPackages' members were able to get a better understanding of how different threats evolved in the past, and how new ones can emerge in the future in relation to new technologies.

After these two initial steps, performed internally by the members of the consortium, we decided to extend the discussion to other international experts. Therefore, a number of external experts were selected by each Working Group to participate to the first face-to-face meeting held in Amsterdam in February 2011. At the meeting, whose outcome is summarized in the Appendix, each Working Group first presented its findings and its pre-

liminary list of possible threats. The list was then discussed during a plenary brainstorming session, that included all the participants and the invited experts. This step was extremely important because it allowed the Working Groups to receive critics and feedbacks from people with different opinions and quite different backgrounds.

Finally, the results of the meeting were summarized and discussed in the project's mailing lists with an even broader community of international experts, including people from both academia and industry.

The final results, with additional details about the sources of information adopted by each Working Group to prepare its list of threats, are presented in the next chapters.

2

Current and Emerging Threats in Malware and Fraud

Contents

The threats presented in this chapter are the results of brainstorming and discussion within the *SysSec* Project, within the *SysSec* Working Groups at the first *SysSec* Working Group meeting in Amsterdam in February 2011, and in the Malware and Fraud Working Group's mailing list. This list represents our initial point of view on the classes of threats that we think will become increasingly relevant over the next years.

2.1 Background

Malware and Fraud are two extensive areas when viewed without restriction. In fact, in a broader sense, almost any threat and the intention behind it can be reduced to the malware or fraud areas. Therefore, this chapter discusses different types of malware and their difference concerning the platform for which they are implemented.

Recently, one of the major change in this area was caused by the vast amount of devices with a reasonable processing power that are capable of connecting to the Internet. Ten years ago, only PCs were an attractive target for malware writers, simply because they were the only devices capable of running the malicious code itself. Recently, however, Smart phones, Laptops, or even storage devices like NAS systems are running traditional operating systems and are becoming the target of miscreants.

Additionally, with Internet access being omnipresent, previously isolated facilities are becoming interconnected and publicly available, opening new opportunities to ill-intended adversaries. In the rest of this chapter we discuss some of these targets and the threats related to them.

2.2 Threats

2.2.1 Malicious Hardware

Malicious hardware that incorporates backdoors, kill-switches or other malicious functionality is not a new concept. However, recent research [16] has demonstrated that flexible and powerful malicious functionality can be easily implemented with a small amount of additional circuitry. Furthermore, recent events such as the Aurora [13] attacks on Google, as well as Stuxnet [9], have demonstrated the impact of advanced, targeted attacks performed by sophisticated actors with significant resources at their disposal. The combination of these two factors means that the real-world use of malicious hardware may become much more widespread in the near future. Since detecting hardware backdoors is a challenging, open research problem, it is even possible that these attacks are already in the wild today.

Malicious functionality can be added when a component is designed, but it could also potentially be added at the fabrication stage. This is of

course extremely problematic since silicon fans are concentrated in a few countries, which are therefore in the position to deploy malicious hardware for intelligence, industrial espionage or sabotage all over the world. We can distinguish two classes of attacks based on malicious hardware:

- Targeted attacks: inject malicious functionality into a specific component that will be used at a specific target organization.
- Blanket attacks: inject flexible malicious functionality into all components produced at a facility. Later, exploit it opportunistically.

2.2.2 Attacks Against the Cloud

As cloud computing models increase in popularity, they raise a number of new security concerns, and new threats emerge as a consequence of technical and organizational changes. For the purpose of this discussion, we consider a rather wide definition of cloud computing that includes Sofware-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [3]. We can summarize threats against the cloud into three broad categories:

- Attacks against virtualization: These are attacks against the virtualization technology that underlies cloud-computing. Weaknesses in this technology may allow attacks against the hypervisor or against co-hosted virtual machines, ranging from leakage of coarse-grained load information to full compromise.
- API-level attacks against cloud services: In addition to general-purpose computing clouds such as Amazon AWS, we are also seeing the explosive growth of specialized clouds that provide services such as file hosting, device synchronization and music streaming. Each of these services typically exposes its own complex API, that may suffer from vulnerabilities that lead it to compromise user's privacy or worse.
- Old attacks with new implications: When a cloud-computing provider suffers any kind of compromise to its infrastrcuture, this has additional implications compared to when the same compromise occurs within an ordinary company's network infrastructure. This has been recently demonstrated by the compromise of Sony's PSN network. In this case, the compromise caused a month-long downtime of the PSN service that is used by millions of users, and led to the theft of users' personal information (including credit card details) on a massive scale. If a general-purpose cloud computing platform were compromised, the consequences could be even more severe, and the ramifications uncertain. For individual customers it might be difficult to even find out if

their virtual machines had been compromised, making it very difficult to select remediation actions.

2.2.3 Advanced Malware

Advanced malware already exists today. Many of the advanced capabilities that we will list in this section have already been demonstrated either as proof-of-concept (by security researchers) or by real malware that is in the wild today. Nonetheless, malware will continue to evolve to circumvent defenses against it and to improve its effectiveness alongside the social and technological evolution of the Internet.

- Advanced botnets with stealthy and robust C&C: a reliable and secure Command and Control infrastructure that is robust against take-down attempts is a crucial component of a successful botnet. Likewise, making C&C communication stealthy and hard to detect can help keep the botnet out of the limelight so that less effort is spent against it by security practitioners and law enforcement. We expect advanced architectures such as the hybrid client-server and peer-to-peer model used by Koobface [28] to be further refined and to gain in popularity over time.

- Exploit social networks and automated social engineering for propagation. In a sense, social propagation has been around since early email-based worms started spreading to an infected user's list of contacts. However, social networking or messaging platforms that support rich media and make large amounts of user information available significantly widen the design space for such attacks.

- Cross-platform malware that targets mobile devices as well as PCs. We also expect to see malware that "crosses the boundary" between platforms e.g. by propagating from a user's PC to his smartphone.

- Software marketplaces as new distribution channels for malware. Software marketplaces and "App stores" provide users with a central repository of software for their devices and, in the near future, for their PCs. Under this distribution model, software may be vetted to some extent by the platform operator before being made available to users. Nonetheless, app stores are no panacea against Trojan horses, because it is not possible in practice for the store to automatically verify that a piece of software is not malicious. Instead, app stores lead to a new threat model, where the malware authors have to "game the system", and maximize the lifetime of their applications in the marketplace (until they are discovered and banned) as well as their visibility to users

during this period. For this, malware could manipulate the reputation systems on which these marketplaces are based to try and reach a wide audience of potential Trojan victims.

- Virtualization-based malware (ring -1 malware).

- Resource hijacking: compromised accounts at hosting providers, network servers, email providers, social networks or other online services can be traded on the underground market and used to enable further large-scale attacks. It is extremely challenging to defend against this threat because such attacks would use the valid credentials of valid users to perform malicious activity.

- Online currencies: malware may make use of emerging online currencies (web money, in-game currencies, bitcoin, etc.). This could include directly stealing a victim's online money, money laundering, and more sophisticated attacks that interfere with the markets for online goods.

2.2.4 Mobile Malware

Large-scale epidemics of mobile malware have been predicted over the past years. While a variety of malicious software for mobile devices has indeed been observed in the wild, large-scale outbreaks have yet to materialize. However, advanced mobile devices that are essentially general purpose computers have greatly increased in number, and have converged upon a few successful platforms that have a number of attractive characteristics for online criminals:

- Large population of mobile devices (including smart phones as well as tablets).

- Complex software (e.g.: including full-featured web browsers) and slow patch cycle (firmware updates). This means that vulnerabilities are likely and that the window of opportunity for exploiting them can be significant.

- Third-party applications: with the success of third-party applications, Trojan horses can be a successful malware distribution model, even in the absence of vulnerabilities (especially if combined with social engineering).

- Valuable targets: smart phones carry with them large amounts of private and potentially valuable information, as well as offer immediate opportunities for monetization (by calling toll numbers or purchasing products using a user's account).

- Two-factor authentication: an SMS sent to a mobile number has become the most widely-deployed approach for two-factor authentication to online services, and is already deployed by Google, Facebook, Twitter as well as a large number of European banks. This approach of course fails once an attacker is able to compromise a user's computer *and* his cell-phone (or when a single device is used for both roles), making the cell-phone an even more valuable target for attackers.
- The advent of mobile payment systems in the near future, where a cell phone becomes a virtual wallet for payments based on near-field communication, will make cell-phones an even more profitable attack target.

2.2.5 Information Risks

The vast amounts of electronic data that are currently being collected, together with the increasing availability of algorithms and computing resources to mine this data, create a huge amount of opportunities for this information to be leveraged for benign as well as malicious purposes.

- Government open data: Large amounts of data are being made available in digital form by public institutions, as part of an unprecedented push towards transparency in government and data-driven policy-making. This can have huge social and economic benefits, but it also poses some risks. New data correlation opportunities may lead to unforeseen consequences. Datasets released in anonymous form, for instance, may be de-anonymized by correlating them with additional datasets. Furthermore, this information could potentially be leveraged for targeted attacks or phishing.
- Tracking: Service providers are collecting large amounts of information on their users, particularly if they operate in jurisdictions where there are few restrictions on their use of this data. This includes location information obtained through GPS hardware, as well as from cellular telephony infrastructure, and even by looking up the addresses of wireless access points in databases that have been collected by efforts such as Google Street View. Furthermore, users are providing increasing amounts of information about themselves to social networking services, without always being aware of the privacy implications. The combination of these factors leads to serious threats to user privacy. Furthermore, all of this information on a user might be obtained by miscreants through legal or illegal means: by simply crawling the internet for public information, by buying it from those who collect it, with or without user consent, or by stealing it as a consequence of a compromise at a service provider or of a user's account. Once it falls in

the wrong hands, this information can also be leveraged for advanced social engineering and phishing attacks.

2.2.6 Targeted Attacks

A large part of the underground economy of internet crime revolves around attacks that ultimately aim to steal money from a user's credit card or bank account. More targeted attack, however, may be aimed at specific, high-value individuals, or even at stealing from a company's accounts. Furthermore, directly stealing money is not the only goal of targeted attacks. Attackers have infiltrated corporate networks, stealing data for political or economic reasons (industrial espionage) or to disrupt an organization's operations. Recent events, such as the "Aurora" [13] attacks against Google and other US companies, and the Stuxnet [9] worm that targeted Iran's uranium enrichment infrastructure, have highlighted the importance of understanding and defending against targeted attacks. These attacks are hard to detect and defend against for a number of reasons. Of course, more sophisticated attacks that use custom malicious code and infrastructure and rely on 0-day exploits are harder to defend against. However, targeted attacks are also intrinsically more difficult to study, because the techniques we use to collect data on malicious activity (such as honeypots, spamtraps, etc.) do not capture such attacks, making it hard for researchers to obtain a realistic understanding of these attacks as they are deployed in the wild. The threat of targeted attacks is very varied and can cover a number of aspects:

- Private or government-sponsored attacks.
- Attacks against SCADA industrial control systems, that can bridge the boundary between the digital and the physical worlds.
- Insider threats. When the adversary is a well-funded organization, the risk of an insider becoming a willing or unwilling accomplice becomes concrete.
- Risks of interconnection of networks with different security levels: High security networks may be compromised because of their interconnections with less critical networks.
- Inside-outside border blurring. The old-fashioned security model where there are clear boundaries between outside and inside the network is now largely obsolete, making developing new security models a necessity. As soon as employees connect a laptop or mobile device to a network, network administrators can no longer assume that threats only come from outside (because the mobile device may have been compromised while outside the network).

3

Current and Emerging Threats in Smart Environments

Contents

The *Smart Environment* expert group met in Amsterdam, February 2011, to identify and discuss new threats related to the area in question. As a seed to the discussion, we used the threats identified in the EU/FP7 project FORWARD, as well as a draft of a deliverable on low-capability devices. Even though the main ideas in the text below are from the Amsterdam meeting, we have also incorporated ideas from meetings with other experts, for example representatives from the EU/FP7 project VIKING. It should be noted that many of the FORWARD threats still hold, and for that reason this chapter should be seen as an incremental update of the results presented in the FORWARD whitebook based on current trends.

3.1 Background

In the *Smart Environment* expert group, we are concerned with low-capability devices. However, there is a continuous range of such devices and what they are capable of. For that reason, a threat and the corresponding mitigating security mechanism may look very different depending on the type of device and the environment it is located within. For example, for some RFID tags we have a clear understanding of many of their vulnerabilities even though we do not have solutions for the problems. Minor fraudulent data in a single smart meter are not a major concern for an electricity company but rather within the acceptable margin of loss. In this environment, attacks against aggregate information are more severe.

Public key cryptography can be used by some devices, but not by others. It is expected that some devices will increase their capabilities in the future, but, as pointed out by the experts, certain parameters will not change much over the next couple of years. For example, power management is of paramount importance for sensor networks. In a couple of years, it is expected that new nodes will run on better hardware, using less power. This will probably lead to more bits used for encryption, but power management will still have a major influence on every piece of code running on the node.

As sensor networks are integrated more and more often into applications that monitor restricted areas and play a critical role in maintaining security and/or safety of facilities they will probably attract the interest of active attackers that have an interest in making the sensor network report erroneous information. Sensor networks have become part of the infrastructure that controls traffic between borders of neighboring countries.

Mirroring the background of the experts, the discussion focused especially on low-capability devices, such as sensor networks, and environments such as electricity networks with smart meters and SCADA systems, as well as vehicular networks. The latter being environments which traditionally have been physically and logically isolated but now are more widely in-

terconnected. Also the implications of *Stuxnet* (see previous chapter) was discussed.

For systems in the smart environment, many traditional security mechanisms do not work, either because the underlying assumptions are not valid (no patching possible) or because of more practical reasons (proprietary protocols). Many of the problems identified in the FORWARD project are still very much valid, but there are also new trends that will possibly lead to new types of attacks as outlined below.

3.2 Security challenges in SCADA systems and the smart grid

The expert group discussed the unique challenges to systems in the Smart Environment group. The discussion focused on issues in the smart grid and SCADA systems.

One of the underlying conflicting assumptions between the IT and the electricity world is the updating frequency of both software and hardware. For the former, we expect software to be updated frequently (compare Microsoft's patch Tuesday) and hardware is replaced every couple of years. For the latter, the hardware has a working life of 15–20 years. The systems are seldom patched and they are often in an isolated area. Given that the life cycles are so different, the question is how to design software that can work well in these environments.

The cultures between the people working with IT contra the people working with, for example, electricity networks are also different. For the former, security permeates many design decisions. For the latter, they see themselves as "engineers" and they do not consider themselves to work with IT systems. Sometimes there is the idea that as long as encryption is used, enough security is in place. However, the smart meters, for example, have a regular web interface and it is expected that the built in server may have similar vulnerabilities as to a regular web server. When one company wanted to buy millions of smart meters with good security primitives, most vendors did not have suitable products and even fewer could supply such a large order. Some systems still use unencrypted communication, others are shipped with a world-wide global password that cannot be changed. Even though there are several vendors, most systems seem to run an old version of Microsoft Windows, mirroring the development for regular operating systems (*monoculture*).

Another major problem is the use of *proprietary protocols*. TCP/IP is used to a certain point, but then proprietary protocols are dominating. Even though there are standards, there are proprietary extensions created by the large vendors of SCADA systems. This in turn means that regular security tools cannot easily be run on such networks but need to be specifically

adapted to the new protocols. Currently, not many companies offer security testing for SCADA systems.

An experience of running anti-virus products on a SCADA systems was also discussed. It was reported that there were many false alarms, because certain behavior deemed malicious by the tool was actually a legitimate program. Many times, these systems are time critical and need to be running 24h/7 and they cannot crash. Unfortunately, a regular penetration test within this environment will most likely crash RTUs, sometimes requiring a *manual* reboot.

Even though possible security cannot increase the cost of a unit by much due to the large deployment, many units that have already been deployed lack even basic security primitives. A key challenge is to increase the security, without redesigning the whole system and investing in new hardware. Minor issues are not a problem, but attacks or fraudulent behavior should not be allowed to propagate through the system or attack central points, such as the SCADA system for power generation or the back office in the headquarters. There is also a discussion on who owns the data in such networks (the electricity company or the consumer of electricity) and there are many privacy issues related to smart meters, as they can be queried on an individual basis.

Among the challenges, there may also be opportunities. It was discussed that the profile of some of these devices would probably be more regular than an ordinary computer, thus making it easier to deploy anomaly-based or specification-based detection. It was also discussed how certain *super-units* could be interspersed into the system to collect samples. These units would have more capabilities than the regular units and be able to detect and possibly mitigate attacks. Across Europe, test beds are also built by industry so that researchers can investigate the system properties. It is believed that some attacks seen for regular computers will also be seen within this environment, so experience from regular networks is important.

3.3 Threats

3.3.1 Accessibility

One major problem for smart environments may be the accessibility of the devices themselves, be it either physically or logically. A device can, for example, be *physically unprotected* as in the case of a traditional sensor network where the nodes are in exposed or accessible areas, meaning that there is no true insider / outsider; it is easy to throw in a new node. It is important to avoid architectures with single point of failure properties. This implies that the network as a whole, most likely on the more powerful nodes, must be able to compensate for failures, attacks and compromised nodes. In

the case of cell towers, there is more physical protection but such systems are still sensitive. On the other end of the spectrum is the relatively well protected server farm.

A device may also be logically accessible. Many systems in the smart environment, such as SCADA systems or other industrial process control systems, used to be isolated and thus built with certain underlying security assumptions. For example, consider a vehicle. Vehicles have been isolated, but this will begin to change in the next three to five years. Since vehicles are safety critical systems, securing the connected car becomes a major challenge. The internal network of a car today consists of 50 to 100 computers communicating over an internal network, a size similar to an ordinary office. Vehicles will also use multiple interfaces for communication, they will use different protocols and third party applications will soon be offered. The complexity of this problem warrants attention to security.

Researchers have already shown that it is possible to attack vehicles, for example via the multimedia system in the car. This problem will become even more serious when vehicles begin to communicate with the outside world.

Many applications, such as remote diagnostics and software download will be offered by the car vendors, and the demand for third party applications is also coming up. The need for a solid framework for security work is therefore crucial. We especially see the need to

- create a framework for securing the internal network in vehicles,
- create a framework for communication (v2v, v2i) including Internet communications, and
- define generic security models for different types of communicating applications.

3.3.2 System Complexity

Many systems in the smart environment consist of small, not-so-capable but numerous devices. There is thus a problem of scale. Humans cannot easily control thousands of computers and much less so embedded sensors with radios and processors. For that reason, detection and monitoring of these devices have to be further automated so that the output is filtered and reduced. One challenge is that some of these devices are very cheap, and security cannot cost much per device in a large deployment. As the number of such devices that comprise an environment increases the probability of faults or accidental events also increases. There is no user interface to many of the devices and no central control or management point.

3.3.3 Maintainability

One major challenge is maintainability of the system. For different reasons, smart environment systems are costly to update. In the case of the smart grid, the hardware investments made now are supposed to last at least 20 years. Updating the sensors for a toll road is also very expensive.

Even software upgrades can be costly if they have to be done manually on the device. For that reason, several systems offer wireless reprogramming to allow updates (as is the case for some smart meters). Even though such a system is flexible, the updating feature can be turned into an attack. Even simple commands can be turned into methods to disable a node, such as a change of radio frequency for communication or a request to reboot.

3.3.4 More capable devices

As mentioned in the introduction, the capabilities of the devices will most likely increase in the near term with more cores, using less battery. Even though it means that better security primitives can be used, there may also be an associated risk with this development. Today most nodes use carefully hand-written code. With increased functionality, a higher level programming will become possible, offering a simplified java, python or maybe even a limited virtual machine. As seen with regular computers, such a development may open up new vulnerabilities and should be carefully studied.

3.3.5 Network Layer Protocols and Services

Security is not something that can be added to an insecure system to be able to withstand attacks. Security needs to be part of most protocols and algorithms in the system. Otherwise the attacker can chose to attack the unsecured parts. Therefore, it is important to have secure algorithms for all the basic services that are needed in sensor networks. Such services include: i) Routing Protocols, ii) Aggregation, iii) Localization, iv) Clock Synchronization, v) Clustering, and vi) Key Management.

3.3.6 Ubiquitous Readers

We have already mentioned that the capabilities of the devices will increase in the future. The processor technologies will improve, as well as the power, so that the devices will be more powerful using less power. But also the radio chips will be improved, providing more frequencies and more protocols to a lesser price, many times capable of combining several frequencies and protocols. Readers to a wide range of systems will thus become widely available.

One recent development is the NFC (Near Field Communication) reader and emitter on cell phones. With the phone, it is possible to read many

things and maybe also to falsify information and create what would appear to be false RFID tags. Attacks that before required specialized equipment may soon be more prevalent and it is a development to carefully monitor.

3.3.7 Attacks against the non-ICT component

For many systems found in the smart environment, the ICT component is just one part of the whole system. A sensor network is usually deployed to measure physical properties such as temperature, air quality, or vibrations. A smart meter measures voltage and power usage. It is probable that we will see more attacks that either target the non-ICT component or target both systems simultaneously. For example, false sensor data can be created with a laser, directed radiation or chemical sprays. By changing the sensor data, you may get the response you want from the system. In electricity networks, the voltage can be changed in one node, affecting the logic of others and, if done right, this may then propagate to a larger scale.

4 Current and Emerging Threats in Cyberattacks

Contents

The threats presented in this chapter are the results of brainstorming and discussion within the *SysSec* Project, within the *SysSec* Working Groups at the first *SysSec* Working Group meeting in Amsterdam in February 2011, as well as discussions with members of the Cyberattacks working group and other experts in the area of Cybersecurity. The threats discussed in the remainder of this section will have increasing impact in terms of security in computing systems and networks in the following years.

4.1 Background

The focus of the Cyberattacks working group is to improve our understanding in new and emerging types of cyberattacks, such as attacks on and by mobile phones and other such highly-connected smart appliances, web attacks, attacks on home and office automation devices, cross-domain attacks, attacks on individual citizens as well as infrastructure, etc. It is also the goal of the working group to advance the State-of-the-Art in the area of detection and mitigation of such cyberattacks.

4.2 Threats

4.2.1 Web Services and Applications

The key value of the web, and the network in general, is the services developed, deployed and provided to end users. These services unfortunately provide fertile ground for attackers to thrive, as inevitably, new services are bound to have security flaws. The reason for this is twofold. Firstly, typically new software tends to be more vulnerable as all its quirks and bugs may have not manifested during the testing phase. Secondly, there is tremendous pressure and urgency in companies to push out new and appealing services for end users, this leads to higher chances of security flaws creeping into the software, as features take precedence over security.

This of course will have direct consequences on end user security as we have come to depend on these online services in our daily lives. For example, by compromising a news service, miscreants may spread misinformation which can have direct financial and social impact. By taking down government web services relating to tax or other internal revenue, one will cause major impact on a country's economy. By infecting an online storage service, individuals or organizations may lose important data stored online.

Also, the inverse types of attacks are possible. That is, miscreants can use infected or otherwise compromised online services to attack all types of end appliances. This has been traditionally possible against personal computers, but as users start using their phones, tablets or other smart devices

to synchronize their data with online sources, or download applications for personal use, we expect these types of attacks to increase.

4.2.2 Privacy

Data "living" on the Internet are an invaluable source of information about every conceivable topic. However, in recent years, data put on the Internet have evolved from purely encyclopedic information about a variety of topics, and simple user pages, to much more personal information. This trend has been facilitated by the growth of social networking sites. A social network is a social structure that is made up of nodes that represent individuals or organizations. These nodes may be tied to each other by properties such as friendship and general interests. As these online communities, such as Facebook, MySpace, Orkut, Twitter, LinkedIn, and others, have been adopted by Internet users, miscreants have started abusing them for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc.

The reason such attacks are possible, is due to the nature of information users upload to social networking sites. Users typically give their e-mail address, where they went to school, what they studied, jobs they held, places they lived, their relationship status, family information, their friends, hobbies, places they have visited, likes and dislikes, etc. There is really no limit to the amount and detail of personal information users will upload. From the attacker's perspective this is fertile ground for learning about their victims. The e-mail addresses can be used for spamming, friend information can be used for targeted attacks, and data about other habits can be used for blackmailing.

The attacker can also correlate information from multiple social networking sites, along with other sites, such as blogs and online forums, to really learn things about their potential victims. The more information they hold, the more likely it becomes that they can somehow exploit their target.

4.2.3 Critical Infrastructures

The border between what we traditionally considered critical infrastructures and the public Internet is quickly disappearing. Change is taking place in both directions. That is, on one hand, critical infrastructures are becoming more connected to the public network, on the other, ICT infrastructures are becoming ever more necessary to our daily lives.

For example, one can think of the telephony network as a traditional critical infrastructure, used by billions to communicate. However, what we are witnessing is an ongoing migration towards VoIP services, effectively eliminating the line between the telephony network and the data network.

Recent work has shown how one can exploit VoIP services to attack emergency service land lines [15].

The same applies for other technologies as well. For example we can consider the case of data centers, and cloud computing infrastructures in general. Such environments host numerous services used by thousands of business and millions of users. This makes them ideal targets for attackers. Taking down a cloud provider, or penetrating their infrastructure and stealing or modifying data, can lead to serious disruptions, and possibly millions of Euros of damages. Currently we are not trained to view or consider these online services as critical infrastructure, in the same sense as we view the electric power grid as critical infrastructure. We believe this must change, and the sooner this happens the better we can prepare for possible future attacks.

4.2.4 Smart, Mobile and Ubiquitous Appliances

We are currently witnessing the penetration of smart and mobile devices in every facet of our society. Past scenarios about devices and sensors, static and mobile, being deployed universally, are quickly becoming reality. These devices have varying characteristics but their underlying common features are: ever-increasing computational capabilities and continuous connectivity, be it Ethernet, WiFi, GSM, 3G, Bluetooth, radio, or even infrared.

These devices take many forms, that may rarely remind us of the traditional personal computers we are so used to, but in reality they are very much vulnerable to similar types of attack vectors, customized to each specific device. For example, medical appliances such as pacemakers, have been shown to be vulnerable to attacks [10]. Such vulnerabilities may lead to direct loss of life.

Attacks however, do not need to be directly threatening to human life to be serious in nature. Smartphones are a case in point. Nowadays, our phones hold a treasure of sensitive information; phone numbers of our family, friends and colleagues, personal photos, financial data, passwords, virtual cash, location information, etc. In some respect, our phones may be a more valuable target to attackers than our personal computers or servers.

Malware taking over our phones, we believe, is a very real threat. One possible source is malicious applications that the user installs without realizing its true intentions. As users are willing to download and run programs from online sources on their smartphones, they become trained to accept without thinking pretty much any request the application may make. For example, access to the network, to storage, or even debug mode of the phone. This leaves users vulnerable to software that may provide some surface functionality, e.g. a game, and stealthily steal information in the background.

Exploiting such devices is often easy due to a number of factors, not all applicable in all cases: limited computational power to run full fledged security software like antivirus, firewalls, or intrusion detection systems, dependency on battery power, so even if security software exists it may not be practical to run, lacking security design, ease-of-use trumping security requirements, easy physical access by attackers, etc.

4.2.5 Insiders

One of the often overlooked factors in cyberattacks is the malicious insider [7]. Opportunists, disgruntled employees or even malicious plants from competitors and adversaries, all pose tremendous challenges for ICT security. Typically, organizations follow the model of forming a strong perimeter to repel attacks coming from the outside [27]. This is expected, as traditionally insiders are considered trusted by the mere attribute of already being on the inside. Unfortunately this is not always the case. Employees change position and move from one department to the other, new ones are hired, some leave and never get their privileges revoked.

Insider attacks are more dangerous than attacks from outsiders, as insiders probably have easier and more direct access to the assets they aim to compromise. Additionally, they may already know of the countermeasures put in place, or have other intelligence that will help them in their goals. Furthermore, security mechanisms are typically tailored to counter outsiders. These are placed at choke-points along the perimeter of an organization. Once inside, very little defenses are in place. To make matters worse, insiders also have a lower chance of getting caught, since as we said, defenses are along the perimeter, but also because we are trained to look to the outside for malicious activities.

Once an insider goes rogue, they may sabotage the organization, for example by modifying or deleting data, locking out computing systems and networks, etc. In these cases, the malicious insider may be easier to detect and track. In other cases, where the malicious insider has more long-term goals, they may start stealing the organizations intellectual property. Such attacks are harder to detect, and even if detected, an organization may not be willing to admit such events.

Due to the above, it is imperative for organizations to form policies and implement controls that monitor, detect and prevent access to sensitive resources, irrespectively of who may be considered trusted or not.

4.2.6 Network Core Attacks

The core Internet infrastructure will continue to be under threat by miscreants. The reason for this is that it is a high-value target. But not only that, it is also an enabler of other, more complex, attacks. Obviously, these threats

and attacks are not new, but as new devices and services are deployed, there will be new opportunities for causing damage. For this reason, we expect to continue seeing attacks such as: attacks on routers, attacks on DNS, Denial of Service, etc.

An important thing to note is that as the Internet is quickly becoming a unifier for all sorts of communication services, attacks on the core network will inevitably have more impact. For example, people use the Internet as a replacement for the traditional telephony network. This is not solely done by individuals, entire telecommunication companies base their business model of selling telephony services that run over the Internet, transparently to their customers. Any disruption on the core Internet infrastructure will certainly cause them great financial loss. It is also interesting to note that other infrastructure, for example wireless telephony networks are becoming part of the core Internet infrastructures. The reason for this is that people rely on their mobile phones to get access to the Internet. So, detecting and mitigation new attacks targeting the cellular network will become critical as this merging of networks evolves.

Part II

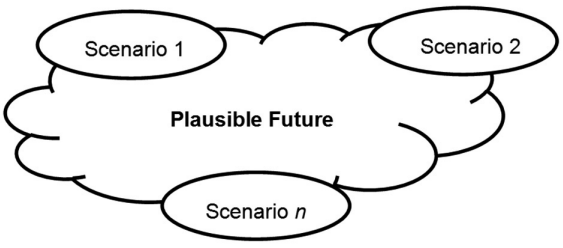
Scenarios and Research Roadmap

5 Introduction

In the second part of this document we try to distill the list of threats presented so far into two comprehensive attack scenarios. Each scenario is represented by a short story that describes a hypothetical, but realistic, situation. The goal is to group together threats in different areas and explain how an attacker can exploit a sequence of vulnerabilities to perpetuate his malicious plan.

The choice of the two scenarios is based on their likelihood and on the trends we observed in previous security incidents. Therefore, what we present here is not something that could happen in a remote future, but instead something that could potentially be observed in the wild either nowadays or in a near to mid-term future.

The scenario itself is presented as a synthetic description of an event, or a series of events, and actions for a certain time period in the future. Here it should be noted that the method adopted to generate the scenarios is a well-known practice adopted by the movie industry and theatre for entertainment purposes. Generally, the practical implementation of the scenario method in the planning process gives a possibility for building a "plausible future" by using experts' opinion and/or statistical data trends [24].



What is important to note are the different creative techniques and the methods to extract and synthesize the experts' knowledge. In particular, these techniques mainly consist of brainstorming sessions and application of the Delphi method [11]. However, round table discussions,

role games, system analysis, and achieved results validation [24, 25] are also common techniques to develop scenarios.

The approach which is adopted here is a simplified version of the *plausible future* building that is applied in two steps: (i) brainstorming and (ii) round table discussion combined with Delphi method for practical fast threats and context definition and selection. It is important to note that this methodological framework is one of the well-known best practices that are currently utilized for future planning in the security area for very complex problems, like the *comprehensive approach operationalization*, by both the EU and NATO [8, 24].

Based on the results of our analysis, the last chapter of this part proposes a number of research directions that need to be further investigated in the near future. This list should serve as a *roadmap* to try to prevent or mitigate the threats depicted in this document. As such, it targets the research topics addressed by the *SysSec* project in Workpackages 5, 6, and 7, but it also presents a broader picture that can be used by other researchers in the field and by the entire stakeholder community of the *SysSec* project.

6

First Scenario: the bank job

Contents

6.1 In a nutshell

A paranoid user John chooses a bank that sends confirmation codes about John's Internet banking transactions to his mobile phone—an out of band signalling channel. The scheme seems secure, but still the attackers manage to plunder John's bank account.

6.2 The story

John worried about security. He used long, impossible to guess passwords on all his machines. All his data was encrypted, and he made sure his firewall and virus scanners were up-to-date. Even so, he only visited well-known webpages operated by bona-fide organizations, and stayed away from the Internet's seedier sites. After all, he did not want to lie awake fretting about whether his computer had been compromised. He had attended too many SysSec meetings. He was slightly paranoid.

That is also how he had picked his bank. A rock solid bank with a rock solid reputation. Not that it was old-fashioned. On the contrary, it offered a wealth of choices for Internet banking. It was just that it made sure that all transactions were secure. In fact, the bank was almost as paranoid as he was—it did not even trust John's own machine.

The security was solid: all data communication was encrypted with a strong encryption scheme. But it did not stop there. Besides all the usual Internet banking protection schemes, this bank also dealt with the unlikely event that his computer was compromised. Every time he performed a transaction, the bank would send a message to his mobile phone with a summary of the transaction and a code to confirm the transaction. SMS security. Whatever attackers did with his PC, they could not see what was on the smart phone's screen.

And it was no inconvenience, really. John had his smartphone with him at all times. He used it as a portable photo book, a calendar, a browser, and so on. Not that he would trust it completely. He knew full well that he could lose the phone and he really did not want to lose the data. No, John was savvy enough to synch his phone every night. Making sure all data was backed up. He took security seriously.

So the interaction was safe and convenient also. John trusted the bank and used the service happily for a long time. He only stopped after his account had been emptied by a sophisticated Cyber attack.

6.3 Explanation

The security scheme with an out-of-band signalling channel is fairly powerful, but there is no security guarantee. In this case, the seemingly reasonable

assumption that attackers cannot 'see' the phone's display was wrong. The assumption that staying away from websites with bad reputation will keep you safe is also wrong.

What happened? The key thing is that the attackers compromised both John's phone *and* his computer. While this sounds hard, there are many ways to do it. We discuss three.

Infect the phone via the computer After visiting a legitimate website, the browser on John's PC was infected by a drive by download. Legitimate websites are not always secure websites. Often they provide a forum or message board where users can post comments and questions and interact with each other. If the website does not properly sanitize the 'comments', attackers can embed anything they want in these fields, including malicious scripts that subsequently load content to exploit the browser—a drive-by-download.

The drive-by-download was not enough. The attackers were after John's savings. To obtain access to his account, they needed access to his phone. However, this was easier than it sounds. Traditionally, phones functioned well as out of band signalling channels. Nowadays, however, they do not do quite so well: smart phones typically synchronize regularly with a user's computer(s).

Using privilege escalation, the attackers compromised the interaction between the phone and John's machine. From there on, it was straightforward to compromise the phone to obtain access to the software that displayed the transaction and the code. For instance, Android phones allow full access to a phone by means of a debugging interface that permits attackers to install or modify software. If needed, they could even 'root' the phone. Apple's iPhones have similar functionality.

This is not science fiction either. The Zeus banking Trojan, which targets Windows-based computers, is already used to target victims' mobile phones too[1]. The new variant of Zeus SymbOS/Zitmo may be used to intercept confirmation text messages that the bank sends to John's phone during his online banking activities, allowing criminals to thwart the bank's two-factor SMS authentication and approve transactions without the victim knowing it. The scheme used by Zeus is a bit more messy than that of the scenario described above, but still effective: the compromised browser simply prompts users for their phone numbers and phone model. It then uses that information to send a text message to the victim that contains a link to a version of the malware written for that mobile platform. It is more messy because of the additional steps and the need for user involvement, but otherwise the scheme is comparable.

[1] http://news.cnet.com/8301-27080_3-20017762-245.html

Infect the computer via the phone The attacker can achieve the same effect by starting from the phone. Again, John is the victim of a drive-by-download that compromises his phone. This may well be easier, since the phone runs code that is as vulnerable as that on the PC, but without virus scanners and other security checks. The malware on the phone should now find ways to compromise the PC.

Fortunately (for the attacker), the phone interacts with very complex software stacks on the PC. For instance, when John's phone synchronizes with the computer, his contacts and calendar entries are transferred between the phone and a program like Outlook. Similar things hold for the pictures on John's phone. The software stacks are complex and vulnerable—witness the many exploits against programs like Outlook in the past. A buffer overflow or similar exploit against these programs provides the attackers with a foot hold on the PC. From there, they can escalate privileges to take over the browser.

Infect the computer *or* the phone via the cloud Finally, attackers can use the cloud to compromise either the phone, or the computer, or both. Users frequently interact between their phones and computers using cloud services. Services like Dropbox[2], for instance, are available for both types of devices. But an even simpler example may be the well-known email attachment.

A compromised phone could modify an email attachment or drop box file to cause a compromise on the computer. Alternatively, the computer could compromise the phone. Either way, the attacker achieves the goal of compromising both devices involved in the transaction.

6.4 Final remarks

Using either of the three methods, the attackers control all parts needed to steal John's money. The concrete threat we have to deal with is that a single attack may well infect more than one device, if doing so is worthwhile (in financial terms, or otherwise).

Incidentally, the scenario also demonstrates an unfortunate side-effect of security measures: people may start trusting them blindly. John trusted the bank. Due to the solid security measures, he was not worried about Internet banking and may not have kept an eye on all transactions. Otherwise he may have spotted the rogue behavior earlier, before he actually realized that his bank account was emptied.

[2] https://www.dropbox.com/android

7

Second Scenario: The peccadillo

Contents

In this scenario, we describe how organized crime possibly could take over a number of smart meters in several countries. In the scenario we assume that the meters have vulnerabilities but that these cannot be exploited remotely. The criminal group in question does not have the resources to infect the meters themselves, so they trick the owners of houses and apartments to install the malware for them by using a Trojan that promises to reduce the energy bill for the consumer.

7.1 The Story

Abigail is an average user of computers and internet technologies. She has a laptop and an iPhone, making it convenient for her to browse the web and check for emails. Even though not a security expert, she is well aware of the common well-communicated threats that come with computers, such as viruses, worms, diverse email offers for fraudulent services and the like. Accordingly, she tries to protect personal data and important credentials for her accounts to the best of her knowledge. As a result, she is pretty safe from phishing attacks, Nigerian scams and even most browser-based infections. In her understanding, internet connectivity is the culprit when it comes to those threats. Therefore, she takes at least some precautions when dealing with connected devices like her laptop or her smartphone.

Abigail is currently living in an apartment, where each household uses smart metering to provide additional information including power consumption, average usage, and peak information to the end user. In her extensive browsing sessions she stumbled upon the following interesting forum-entry.

```
----On 4th July, Maximilian wrote:-------------------------
Yeah, i know, and the prices for electricity here are just
insane....
-------------------------------------------------------------

Uh, yeah but that can be helped. On http://hidemypower.to they
offer firmware mods for almost every smart meter currently in
use. You just toss it on an SD card, plug it in, reset the
device and that's it. It modifies the counter or something, so
only 85% of your actually used electricity is reported to the
device. Worked great for me, and i can buy stuff with the
spare money *g*. The best thing is: The company will never
know, cause they have no way to monitor if the meter has a
jailbreak installed or not.
```

And that got Abigail thinking. It sounded quite reasonable and the installation procedure sounded fairly straight-forward. Besides, the term ”jail-

break" had a nice ring to her. She didn't want her smart meter to be restricted. As she had managed to jailbreak her iPhone, she could certainly give it a shot with the smart meter. From a morality perspective she was not even particularly troubled. In the end, everyone is doing it, right? And there should not be any direct consequences as her smart meter was not connected to her Internet. After some consideration, she decided to go through with it.

The installation procedure was fairly simple and it could easily be done with the memory card of her digital camera. After flashing a short *ENJOY* on the display of the smart meter, everything went back to normal and Abigail even wondered if there was actually a difference compared to the state before. But her next energy bill proved that it actually worked. Little did she suspect that the newly installed firmware gave full control of the smart meter to a criminal network, including the power of cutting her electricity at will.

About twelve months after her installation procedure, something strange happened. Her fridge and her heat-pump, both connected directly to the smart meter to save energy, turned off at exactly the same time. While not very suspicious, this was the first time the devices seemed to act in the same manner. Curiously, a complete power outage followed only seconds after the incident. It lasted for more than an hour and as far as Abigail could tell, the whole block was affected. Finally, the power came back on and when she zapped through the news, she heard reports of a well-coordinated cyberattack which was apparently responsible for the power outage. Well, stranger things have happened lately, but she really thought the government should do something about it.

7.2 Explanation

What actually happens in the scenario is a characteristic case of backdoor functionality integrated in a piece of useful software. The firmware Abigail flashes to her smart meter does not only modify the reported ticks from the internal D/A Converter responsible for measuring the consumed power, but it also creates a backdoor through which the smart meter can be remotely controlled. Just like a bot-infected machine in a normal environment, the backdoor has no noticeable effect on the usual behavior of the infected device.

Abigail's assumption that the smart meter is not connected to a network is only partially correct. While the device is not connected to her personal network, the company monitoring their devices certainly needs the means to remotely access their devices. Smart meters today often consist of the traditional metering module, but also a processing unit and a communication unit to collect and then communicate the customer's usage to the utility

company. How this uplink is implemented is not described in the scenario and in reality it strongly depends on the device itself which protocol or technology is used. Possibilities range from full-blown ethernet connections over power line communication (PLC) to wireless technologies like 3G and GPRS.

As with any complex device, there are often vulnerabilities that can be exploited by an attacker. For example, Davis gave a presentation at Blackhat 2009 [6], where he discussed the insufficient hardware in the meters to ensure adequate protection. In his example, he showed how a smart meter could be hacked and then how, by using self-replicating code, a larger portion of the network could be compromised. In this scenario, we are more restrictive and only assume a meter can be exploited if one has physical access to it. In Figure 7.1 we show a modern smart meter that also includes a slot for a memory card. In the scenario, inserting a specially-prepared SD card into the smart meter, triggers and exploits a vulnerability in the file system code.

To lure users to install the malicious code, the criminal group copied a common technique used for traditional malware by hiding the malware in a beneficial cloak. They used people's greed to trick them into installing the malware, unfortunately a plausible scenario knowing the human mind.

In reality, the attack depends on three main factors to be possible:

1. **The smart meter coverage of the concerned country**. Even throughout the European Union there are large differences in smart-meter coverage. Austria, for instance, uses good old polyphase meters while Sweden and Italy provide almost completed smart-meter coverage even for private households. Still, plans are such that most EU countries target complete smart meter coverage by the end of 2020.

2. **The capabilities of the metering device.** Most smart meter vendors are under the pressure to provide a huge variety of connectivity possibilities to make sure every demand of the utility company can be met. In the end, getting the assignment to supply each and every nationwide household with such devices is a multi-million Euro commission. Figure 7.1, for instance, shows a smart meter which was opened for testing purposes. Besides USB, ethernet and serial ports, it also comes with an SD card slot (marked red) to provide all possible interfaces in case they are requested. Using them for malicious purpose is just a question of finding the right vulnerability. There exists work to secure the meter, such as controling the installed firmware [20], but the meters are relatively cost-sensitive and often no mechanism apart from simple passwords and cryptographic communication channels are used.

3. **The user's dedication.** Fraudulently modifying electricity meters to report smaller consumed amounts has always been of interest to some

Table 7.1: The layout of a modern smart meter.

customers. Actually, there are even instruction videos how this can be done with a traditional meter using magnets.[1] The only difference with smart meters is that it needs the right piece of software for the modification instead of the right magnet. McLaughlin et al. [22] further describe the means how energy theft could happen.

Complicating the attack is also the fact that many smart meters are built to be tamper proof, and some even send alarms to the utility company if the container is breached. These alarms, however, are often ignored in practice as it is costly to send out an operator to check the meter manually. As soon as the new firmware is installed on the meter, the alarms can also be reset.

With a large number of meters compromised, the final element of the scenario can then be executed. With the malware in place and the connectivity of the meters, the malware author has a botnet of decent size at hand. Having control of the smart meter means having control of the *on/off*-switch of the meter itself [1], and in the future maybe even the control of individual appliances in the home. If the meter controls appliances, the utility company can change their users' background energy usage as needed, thus flattening possible power peaks that would otherwise have a negative impact on the network. As a compensation, the utility company can grant lower prices for their customer. A win-win situation one would think.

But not if a botmaster controls a large portion of these devices. The grid is relatively fragile, in the sense that some minor disturbance can cascade and cause major interruptions [29], where the Northeast Blackout in the U.S. in 2003 is an example [14]. In this scenario, the bot master decided to switch off all controlled devices at the same time. As a result, the supplying power grid experienced a surge, which in turn was handled by shutting

[1] http://www.metacafe.com/watch/4659119/electric_meter_hack_how_to_cut_your_electricity_bill_in_half/

down the effected clusters, forcing the neighboring clusters to handle the additional load and resulting in a cascading failure.

Most likely, the botmaster needs to control quite a number of smart meters to have a significant effect but he can also infiltrate higher-level devices, starting from the concentrator which manages multiple such smart meters up to the management PCs responsible for actually administrating the power grid. Liu et al [21] discuss how false measurements can influence state estimation algorithms used in the core of the grid to possibly lead to large blackouts. Even though values from the smart meters are mostly used for billing purposes today, there are discussions about extending their use which may influence also the energy production systems. The consequences of the loss of power have been documented elsewhere [17, 18].

All through the scenario, our victim Abigail is not even aware of her contribution even though she was partially responsible for it.

7.3 Final remarks

In this scenario, a criminal group takes control over a number of smart meters in several countries by tricking users to install a Trojan on their devices. The group creates an advanced malware, disguised as software that could decrease the electricity bill, that will take control over the smart meter.

Smart environments are gaining popularity from day to day. It is just a matter of time until ordinary households are part of a well-connected grid that ensures transparent and hopefully secure supply of essentials such as electricity, gas or water. History has shown that when a technological system is handed to millions of users, it is only a matter of time before it gets compromised. This assumption was true for gaming consoles (Wii, XBox, PS3) or smartphones (iPhone, iPad) and it will also hold true for smart meters where even more can be gained. Securing these devices completely will never be possible, but we should at least invest some effort to raise the bar high enough to make them less attractive targets.

8

Research Roadmap

Contents

8.1 Introduction

One of the main activities of the SysSec project consists of defining and updating a yearly *roadmap* of research areas that need to be addressed in order to mitigate the threats identified by each Working Group. The roadmap will serve the twofold objective of driving the research conducted by the SysSec's partners in WP5, WP6, and WP7 and of serving as a guideline for other researchers in the field of system security.

In the previous chapters of this deliverable, we presented a list of upcoming threads, grouped in the area of Malware and Fraud, Smart Environments, and Cyberattacks. However, as we pointed out in the two comprehensive scenarios presented in Chapters 6 and Chapter 7, many threats are interconnected to each other and are common between different research topics. The role of this chapter, and therefore of the research roadmap, is to analyze the current status of each threat and the research that needs to be done to mitigate it. Based on the result of our analysis, we can then group the threats together in a number of research areas according to their priority.

Roadmap Definition Process

The collaboration with external experts, both through the project's mailing list and the participation to the face-to-face meeting in Amsterdam, helped us to achieve a more general and precise view of which areas of system security need to be better investigated in the close future. One of the outcomes of the meeting (see the Appendix for more details) is the result of the brainstorming activity we conducted to identify the main "forces" that are responsible for changing the IT world, and that therefore can give us a possible direction toward which we need to focus our effort. The result of the brainstorming can be summarized by few, important keywords: *mobility*, *increasing lack of privacy*, *24/7 connectivity*, and *cloud computing*. The starting point for the meeting discussion was the *White Book* published at the end of the Forward Project [5]. The document contained a number of recommendations for future research based on the likelihood and severity of a number of identified upcoming threats. The main difference between the result of the white book and the content of this chapter is in the scope of the document.

The White Book was written to be a comprehensive overview of all possible upcoming threats, grouped in eight categories and ranked based on four different aspects: impact, likelihood, obliviousness, and R&D needs. The *SysSec* yearly roadmap aim instead at being a more focused document, in which we review the current state of the threats identified in the past to update the research workplan for the upcoming years.

In addition to the White Book, we refined our roadmap by taking into account the content of similar roadmaps and strategic documents recently published in Europe and in the United States (a more comprehensive overview of such previous work is presented in Chapter 9).

In the rest of this chapter we summarize the key themes we identified and we propose a roadmap developed around five "horizontal" areas: privacy, targeted attacks, mobility, emerging technologies, and usable security.

8.2 Privacy - Bring Back to the User the Control of His Data

More and more personal information about an increasing number of users will be stored online in the near future. Social networking sites are a very well known example of this trend, but, unfortunately, they are just the tip of the iceberg of a much larger phenomenon. File hosting services, cloud computing, back-up solutions, medical databases, and web emails are other examples of services that store personal information outside the direct control of the users.

Such a large amount of information requires to be carefully protected and regulated in order to preserve the citizens' privacy. However, what we noticed from a number of severe incidents recently reported in the news, is that privacy is *NOT* just about encryption. Cryptography is indeed a fundamental basic block for every system that aims at preserving the user's privacy. However, as many recent attacks have demonstrated, criminals are often able to compromise the privacy of millions of users without breaking any data or protocol encryption. Therefore, we believe that it is very important to invest in the system research aspects related to the users' privacy.

Recommendations and Research Directions:

> Researchers should investigate how to protect users against sophisticated attacks that aim at disclosing their personal information. For example, it is important to promptly detect functionalities that can be abused to correlate data available in public records and de-anonymize user accounts in many online services.

8.3 Targeted Attacks - The Needle in a Haystack

The recent Stuxnet incident has been an eyeopener regarding the possible impact of advanced, targeted attacks that can be performed by sophisti-

cated actors with significant resources at their disposal.[1] The attack clearly showed how our current defense tools, policies, and infrastructures failed in front of a threat that was designed to focus against a specific target instead of blindly targeting the entire community.

Malicious hardware, as discussed in Chapter 2, can also be used as a very subtle vector to perform extremely hard to detect attacks against critical infrastructure, large corporation, and government organizations. However, targeted attacks do not necessarily need to be extremely sophisticated and, in their simpler form, can pose a very serious threat also against normal users. Targeted spam, for example, is extremely effective in phishing users credentials. Also ad-hoc banking trojans could be developed in the near future to avoid detection by targeting only a restricted group of individuals.

In addition, we believe there is a serious risk that attackers will soon start developing automated techniques to customize attacks based on private user information and aggregated data collected from multiple online sources.

Recommendations and Research Directions:

> We believe it is very important for researcher to develop new techniques to collect and analyze data associated to targeted attacks. The lack of available datasets, in addition to the limitation of the traditional analysis and protection techniques, is one of the current weak point of the war against malware. In this area, the problem is often to find the needle of the targeted attack in the haystack of the traditional attacks perpetuated every day on the Internet.
>
> In addition, researchers should also focus on new defense approaches that takes into account alternative factors (such as monetization), and large scale prevention and mitigation (e.g., at the Internet Service Providers (ISP) level).

8.4 Security of New and Emerging Technologies

Analyzing and securing emerging technologies has always been a core objective in the area of system security. Unfortunately, it is often the case that new services and new devices are released before the research community had a chance of studying their security implications.

In the near future, we can identify four topics, in the area of new and emerging technologies, that need to be studied from a security point of view:

Cloud Computing - The Cloud is quickly changing the way companies run their business. Servers can be quickly launched and shut down via ap-

[1] http://en.wikipedia.org/wiki/Stuxnet

plication programming interfaces, offering the user a greater flexibility compared to traditional server rooms.

From a system security perspective, there are a number of aspects that are specific to cloud computing. For instance, the impact of "insider threats", the issues related to privacy and "data management", and the attacks against the "virtualization" infrastructure.

Online Social Networks - As these online communities, such as Facebook, MySpace, Orkut, Tweeter, LinkedIn, and others, have been adopted by millions of Internet users, miscreants have started abusing them for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc. Monitoring and securing social networks is therefore very important to protect the users from a large spectrum of attacks.

Smart Meters - This new class of devices is a clear example of a new technology that has been rapidly deployed without the required security protection mechanisms. Studying and fixing this devices should therefore be one of the goal of system security researchers.

SCADA Networks - Even though SCADA is not exactly a new technology, these devices were initially designed to be isolated and thus built with certain underlying security assumptions. Since now many industrial process control systems became reachable from the outside (even when, as shown by Stuxnet, the attacker has to cross an "airgap"), the security of these network has become an important priority.

Recommendations and Research Directions:

Security new and emerging technologies before it is too late is one of the main priority of the system security area. In this direction, it is important to sponsor activities and collaboration between academia and the industrial vendors to maximize the impact of the research and reduce the time required for the analysis and the experiments.

8.5 Mobility

We are currently witnessing the penetration of mobile devices in every facet of our society. This devices have varying characteristics but their underlying common features are: ever-increasing computational capabilities and continuous connectivity, be it Ethernet, WiFi, GSM, 3G, Bluetooth, radio, or even infrared.

Exploiting such devices is often easy due to a number of factors, not all applicable in all cases: limited computational power to run full fledged security software like antivirus, firewalls, or intrusion detection systems, dependency on battery power, so even if security software exists it may not be practical to run, lacking security design, ease-of-use trumping security requirements, easy physical access by attackers, etc.

Recommendations and Research Directions:

> We believe it is very important to focus our research toward the security of mobile phones. In particular, we need new tools and techniques that can be deployed to the current smartphone systems to detect and prevent attacks against the device and its applications.

8.6 Usable Security - Focusing on the Weakest Link

The importance of human factors was one of the main point that emerged from the brainstorming activity between the member of the consortium and the international experts.

On one side, the engineers that design new devices often do not consider themselves to work with IT systems and therefore do not care or do not know about computer security issues. On the other side, several end users would just give permissions and click on every link or button to reach their goal (often as simple as playing a game on their mobile phone).

This is a very important, and difficult to solve, problem. The impact of new defense techniques greatly depends on the assumption made on the final users and on their involvement in the security process.

Recommendations and Research Directions:

> We believe that a study of the usability of security countermeasures is very important and it will become even more critical in the future. If we want to progress in this direction, we need *interdisciplinary* efforts that bring together experts from different fields (engineering, system security, psychology, . . .).

8.7 Conclusions

In this chapter we presented a short roadmap for the research in the system security area. This document will serve as a guideline for the work of the three technical project's workpackages, as well as for other researchers in the fields. Our roadmap can be summarized in five topics:

1. System security aspects of privacy
2. Collection, detection, and prevention of targeted attacks
3. Security of emerging technologies, in particular the Cloud, online social networks, and the devices adopted in the critical infrastructures
4. Security of mobile devices
5. Usable security

It is important to remember that this roadmap does not intend to be a comprehensive document covering all aspects of system security. Instead, we wanted to present a focused overview of the most important aspects that need to be addressed in the future. We will then update this document every year, monitoring changes in the threat landscape and promptly reacting to new, emerging, attacks.

Part III

Related Work and Appendices

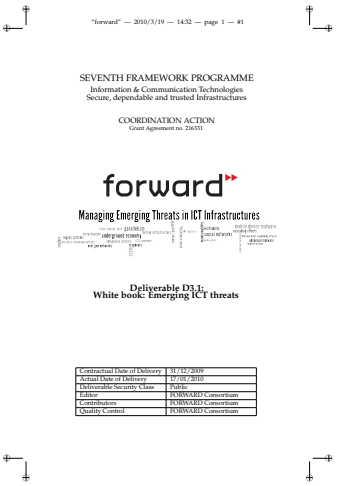
9 Related Work

Contents

In this chapter, we will review previous roadmaps (and similar strategic documents) in the area of Cyber Security. We will first focus on roadmaps which have been developed during the recent years in Europe and, then, we will focus on roadmaps which have been developed in the US.

9.1 Europe

9.1.1 The FORWARD Project


"forward" — 2010/3/19 — 14:32 — page 1 — #1

SEVENTH FRAMEWORK PROGRAMME
Information & Communication Technologies
Secure, dependable and trusted Infrastructures

COORDINATION ACTION
Grant Agreement no. 216331

forward

Managing Emerging Threats in ICT Infrastructures

Deliverable D3.1:
White book: Emerging ICT threats

Contractual Date of Delivery	31/12/2009
Actual Date of Delivery	07/01/2010
Deliverable Security Class	Public
Editor	FORWARD Consortium
Contributors	FORWARD Consortium
Quality Control	FORWARD Consortium

During 2008 and 2009, the FORWARD project, supported by the European Commission, established working groups (i) to discuss best practices, progress and priorities, (ii) set the research agendas to be pursued in Europe and (iii) identify possible new research areas and threats that need to be addressed[1]. The main result of the project, the FORWARD Whitebook, contained detailed and concrete scenarios of how adversaries can leverage the emerging threats identified by the FORWARD project working groups to carry out their malicious actions [5].

These scenarios illustrated future dangers and provided arguments to policy makers that are needed to support research in critical areas. The main research areas identified by FORWARD were grouped into several categories:

- *Networking*
- *Hardware and Virtualization*
- *Weak Devices*
- *Complexity*
- *Data Manipulation*
- *Attack Infrastructure*
- *Human Factors*
- *Insufficient Security Requirements*

- **Networking**. This area includes (i) attacks against the infrastructure of the Internet, such as against routers and routing algorithms, (ii) denial of service attacks where strategic links or essential backbone nodes are taken out of service, and (iii) wire-tapping attacks where the confidentiality or integrity of traffic is compromised, both on wired and wireless links. In addition to attacks against the Internet infrastructure, attacks may also be directed against end devices including (i) denial of service attacks against servers on the Internet, for example, by exploiting known vulnerabilities in applications or systems, (ii) distributed denial of service attacks, where the Internet infrastructure and the large number of unprotected nodes on the Internet are used to drown selected sites in traffic, and (iii) improper design or improper use of the services that the Internet offers, for example, the design

[1] http://www.ict-forward.eu/

of mission-critical systems that are accessible from the Internet and possibly in-turn also depend on its services.

- **Hardware and Virtualization**. This is probably the lowest level in the systems hierarchy where attackers may choose to operate. Although these attacks are usually difficult to deploy, they can remain stealthy for quite some time and thus be very effective. Such attacks may include (i) malicious hardware, and (ii) attacks within the cloud.

- **Weak Devices**. Capitalizing on their small size and power requirements, such devices have recently enjoyed widespread deployment in the form of lightweight sensors, and RFID. Their deployment in the wild, and their mostly wireless communication abilities make them vulnerable to a wide variety of attacks including (i) information snooping, (ii) inserting false or misleading information, (iii) jamming radio channels, (iv) making nodes run out of battery by never letting them sleep, (v) giving the impression of phantom nodes that do not exist, (vi) giving the impression of connectivity that does not exist, and (vii) making messages go through an attacking node that can selectively drop messages from the system. Mobile phones (and PDAs) also fall under this category of weak devices, and can also be a target for attacks including (i) mobile malware, (ii) eavesdropping, and (iii) DoS Attacks.

- **Complexity**. Over the past years we have been building increasingly complex systems which, by definition, are more prone to errors and attacks. Since these systems are difficult, if not impossible, to accurately model, they are challenging to test and may lead to several threats including: (i) unforeseen cascading effects, (ii) large-scale deployment of any attack, (iii) vulnerable system parts due to incomplete system maintenance, (iv) dormant functionality hidden in a program, and (v) race conditions and bugs due to multi-threaded/parallel nature of applications.

- **Data Manipulation**: more people, more data, more value. As more people use the Internet, and as more organizations collect and store data on-line, we are bound to see an increasing number of attacks against (or based on) these data. The attacks may target several dimensions including: (i) erosion of privacy due to ubiquitous sensors, (ii) false sensor data due to fabrication or falsification, (iii) data leaked from social networks, and (iv) data gathered from (or for) on-line games.

- **Attack Infrastructure**. To launch large-scale attacks, several adversaries develop and deploy distributed offensive platforms (such as botnets), which serve as underground economy support structures serv-

ing (and operating on) advanced malware designed to evade detection and resist capture.

- **Human Factors**. Humans are usually the weakest link the security of several systems. Either as insider threats, or as end users, they may be the key element in the success of a cyber attack. Humans interact with security in several aspects including (i) user interfaces, which clearly convey a security (or lack thereof) to the user, (ii) insiders, who may have the access mechanisms needed to compromise a system, (iii) social engineering using all forms of communication, such as email, VoIP phones, and Instant Messaging Systems, and (iv) targeted attacks to individuals or groups of people.
- **Insufficient Security Requirements**. Some systems, such as legacy systems (sometime deployed even before the deployment of the commercial Internet), may have security requirements which are not adequate for the current time and scale.

9.1.2 The Riseptis Report

RISEPTIS, a high-level advisory body in ICT research on security and trust, was formed by the `thinktrust` project[2] to provide visionary guidance on policy and research challenges in the field of security and trust in the Information Society [23]. It did so by formulating recommendations on: (i) Policy environment and (ii) Research Agenda. Their recommendations, also knows as "The RISEPTIS Report" identifies four major areas in their Research Agenda:

- *Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet*
- *Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability*
- *Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)*
- *Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management*

[2] http://www.think-trust.eu

9.1.3 The INCO-Trust Report

INCO-TRUST, a Coordination Action project, supported in part by the European Commission, targets international cooperation in the area of Trustworthy, Secure and Dependable ICT infrastructures. Its goals are (i) to promote collaboration and partnerships between researchers from the developed countries and (ii) to leverage and harmonize efforts on the respective sides related to the building and maintenance of large-scale trustworthy ICT systems and infrastructures and the services they deliver. INCO-Trust produced a final report where it suggested several recommendations for research collaborations including:

- *International alignment: preparation of policy frameworks to enable global collaboration and interoperability*
- *Variety: cooperation on topics related to security and diversity.*
- *Scalability: cooperation on topics related to security and complexity*
- *Reciprocity: cooperation on topics related to security and interoperability*
- *Secrecy: cooperation on the issues of digital sovereignty and dignity*
- *Negotiation: cooperation on the theme of security and trust*
- *Security expertise: cooperation on topics related to security and technological challenges of security*
- *Protection: cooperation on topics related to security and cyber-defense*

9.1.4 The EffectsPlus Project

The EFFECTSPLUS project has started a research roadmapping activity in the area of Trust and Security for the Future Internet [30]. By mobilizing a critical mass of researchers they have identified several research challenges in the area of Trust and Security including: *(i) Enabling Users To Better Understand And Control Security, (ii) Helping Businesses To Assess And Make Decisions About Risk, (iii) Designing Adequate Tools For Building Secure Systems, (iv) Developing And Deploying Suitable Security Metrics, (v) Assurance, (vi) Expressing And Enforcing Security Policies, (vii) Identity, (viii) Cloud Computing, (ix) Achieving Transparency, (x) Dealing With Privacy Issues, (xi) Building and Composing Services, (xii) Developing Models For Prediction / Anticipation, (xiii) Building Systems That Are Resilient, (xiv) Handling Socio-Economic Change, (xv) Improving Risk Assessment, (xvi) Handling Systems Issues, (xvii) Guaranteeing Availability, and (xviii) Coping With The Deluge Of Devices.*

After identifying the (research) challenges, the constituency went on to identify approaches and potential solutions to tackle the trust and security challenges for the Future Internet. These solutions include: *(i) Better Languages And Tools For Specifying Secure Software, (ii) Improved Assurance Methods, (iii) Privacy-Aware Software Development, (iv) Cooperation On Issues Of National Security, (v) Development Of Universally Acceptable Digital Identifiers, (vi) Development Of Rich And Expressive Security Models, (vii) Development Of Tools For Tracking Data, (viii) Enhancement Of Legislation To Accommodate Technological Developments, (ix) Education Of Citizens, (x) Research And Investment In Security Tools And Technology, and (xi) Consideration Of Novel, Radical Approaches.*

- *Languages and Tools*
- *Assurance methods*
- *Privacy*
- *National Security*
- *Digital Identifiers*
- *Security Models*
- *Data Tracking*
- *Legislation*
- *Education*
- *Tools and Technology*
- *Radical Approaches*

9.1.5 The Digital Agenda Communication

Recently, the European Commission published a communication to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on a "Digital Agenda for Europe" [4]. In this report, the Commission states that "*the overall aim of the Digital Agenda is to deliver sustainable economic and social benefits from a digital single market based on fast and ultra fast internet and interoperable applications*" and that "*Europeans will not embrace technology they do not trust - the digital age is neither 'big brother' nor 'cyber wild west'*". Although the report focuses more on policy issues and less on the research problems, it still gives an indication of important directions for the future. These directions include:

– *Cyberattacks*
– *NIS Policy*

- Present measures, including legislative initiatives, to combat cyber attacks against information systems by 2010, and related rules on jurisdiction in cyberspace at European and international levels by 2013
- Present in 2010 measures aiming at a reinforced and high level Network and Information Security Policy, including legislative initiatives such as a modernized European Network and Information Security Agency (ENISA), and measures allowing faster reactions in the event of cyber attacks, including a CERT for the EU institutions.

9.1.6 Future Internet Assembly Research Roadmap

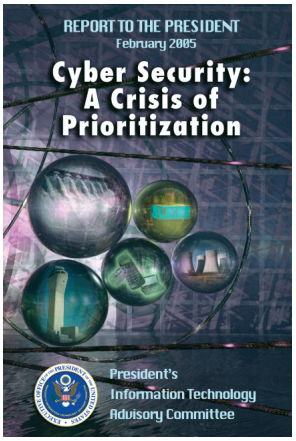
The Future Internet Assembly has recently created a roadmap which captures the ideas and contributions of the Future Internet community on the research priorities for the 8th Framework Program. The roadmap presents research which can be carried in the second half of the 2010 decade and which will have a lasting impact beyond 2020. The roadmap covers all aspects of the Future Internet, including Business Societal Challenges and Technology. Specifically, in the area of security, the roadmap presents the following priorities as outlined by the EffectsPlus Project:

- *Better Languages And Tools For Specifying and Developing Secure Software*
- *Improved Assurance Methods*
- *Privacy-Aware Software Development*
- *Cooperation On Issues Of National Security*
- *Development Of Universally Acceptable Digital Identifiers*
- *Development Of Rich And Expressive Security Models*
- *Development Of Tools For Tracking Data*
- *Enhancement Of Legislation To Accommodate Technological FIA Developments*
- *Education Of Citizens*
- *Research And Investment In Security Tools And Technology*
- *Consideration Of Novel, Radical Approaches*

9.2 The United States

9.2.1 A Crisis of Prioritization

One of the seminal works in this area has been the report titled "Cyber Security: A Crisis of Prioritization" [2, 19]. Ordered by the President of the United States and implemented by the President's Information Technology Advisory Committee, the report suggested that Information Technology Infrastructure is "Critical", treated software as a major vulnerability, suggested that current solutions (such as endless patching) are not adequate, urged for the development of fundamentally new security models and methods, and elevated Cyber Security to the level of *National Importance*. In this line, the report outlined several Cyber Security Research Priorities including:



- *Authentication*
- *Secure fund. Internet Protocols*
- *Software Assurance*
- *Holistic approach to System Security*
- *Monitoring and Detection*
- *Mitigation and Recovery*
- *Cyber Forensics*
- *Models and Testbeds*
- *Metrics, Benchmarks and Best Practices*

- *Usable and Reliable* **Authentication**. *Although there exist a lot of useful work on cryptographic protocols we need more research in usable and large-scale authentication which at the same time would decouple authentication from identification in order to address privacy issues.*
- **Secure fundamental Internet protocols** *including BGP (Border Gateway Protocol) and DNS (Domain Name Service).*
- **Secure software engineering and Software assurance**. *Research is needed to develop secure programming languages and code that remains secure even when executed in different environments.*
- *Provide a* **holistic approach to System Security**. *That is, the security of an integrated system is much more than just securing its individual components. For example, we need ways to build secure systems both from trusted and untrusted components.*
- *Facilitate continuous* **Monitoring and Detection** *of malicious activities and attacks, including Intrusion Detection, real-time data collection, anomaly detection and appropriate data presentation that will allow operators to better understand incidents in progress.*
- *Develop* **Mitigation and Recovery methodologies**, *to respond to unforeseen events and recover from any resultant damage. This area includes rapid automated discovery of outages and attacks, new architectures to enable rapid recovery, simplify systems to reduce human errors, and provide fault tolerance and graceful degradation*

- *Improve* **Cyber Forensics** *to more effectively catch criminals and deter criminal activities. To enable Law Enforcement Agencies to identify criminal activities in Cyber Space, we need sophisticated Cyber Forensics tools and mechanisms, such as traceback of network traffic to identify origins of attacks, efficient search of massive data stores to identify stolen information, and identifying attackers based on their behavior.*

- **Model new technologies and provide TestBeds** *to experiment with them. Such testbeds and methodologies should scale to millions of nodes, should scale to very large amounts of data and should be designed in such a way as to preserve the confidentiality of data.*

- *Some scientific disciplines have developed universally acknowledged metrics and benchmarks which enable researchers measure the effectiveness of their approaches and provably compare their contribution to the state of the art. In this spirit, we need to develop* **Security Metrics, Benchmarks and Best Practices** *for the Cyber Security field as well.*

9.2.2 Designing a Digital Future

More recently, the President's Council of Advisors on Science and Technology provided a new report on how Network and Information Technology (NIT) will play a fundamental role in the future of America and the World [12]. In addition to stating the importance of NIT, the report clearly underlines that advances in Network and Information Technologies accelerate the pace of discovery in nearly all other fields in science and engineering. Although, not specifically restricted to Cyber Security, the report identifies the following list of key R&D topics in trustworthy systems and Cyber Security.

– *Characterization*
– *Social Dimensions*
– *Foundations*
– *Policies*
– *Detect and Mitigate Attacks*
– *Survivable core*

- **Advance trustworthy system characterization**. *Clearly specify the desired properties of a system, which, in addition to nominal functionality, should include the ability of the system to operate in the face of failures and attacks.*
- **Understand and improve the social dimensions of trustworthy systems and Cyber Security.** *Systems designed for human users (i) should be able to take into account the possibility of human error and (ii) should be able to capitalize in the "wisdom of crowds" to detect and identify attacks.*
- **Create foundations for Cyber Security,** *including fundamental mechanisms for authentication, authorization, and trust management.*
- **Formulate the definition and application of security and privacy policies.**
- **Improve methods to detect and mitigate security attacks.** *Such methods should include mechanisms to operate while an attack is in progress and forensic capabilities to identify attack sources during and after the attack.*
- **Develop methods for the implementation of a "survivable core" of essential cyber-infrastructure.**

9.2.3 Network and Information Research and Development

In a more recent report regarding the President's budget for 2012, the Subcommittee on Networking and Information Technology Research and Development outlines the current R&D priority areas which range from fundamental investigation of scientific bases for hardware, software, and system security to applied research in security technologies and methods, approaches to cyber defense and attack mitigation, and infrastructure for realistic experiments and testing [26].

- **Inducing change**: *Coordinated cybersecurity R&D themes to direct efforts toward understanding the root causes of known threats with the goal of disrupting the status quo with radically different approaches to substantially increase the trustworthiness of national digital infrastructure; the initial themes focus on supporting informed trust decisions, enabling risk-aware safe operations in compromised environments, and increasing adversaries. costs and exposure*

- **Foundations**: *Cybersecurity as a multidisciplinary science; models, logics, algorithms, and theories for analyzing and reasoning about trust, reliability, security, privacy, and usability; assured and trustworthy systems; cyber security metrics; social and technical dimensions of a trustworthy computing future; risk modeling; secure software engineering and development; cryptography and quantum information science for secure computing and communications; science of security.*

- **Applied information infrastructure security**: *Secure virtual platforms; assured information sharing; security for mobile, wireless, and pervasive computing; development of a secure and safe "identity ecosystem", including frameworks, standards, models, and technologies; security automation; secure protocols; vulnerability detection and mitigation; cloud computing; health IT; smart grid*

- **Mission assurance**: *Activities and processes that ensure an organization's ability to accomplish its mission in an all-hazard cyber environment; cyber conflict defense Infrastructure for R&D: Testbeds, cyber test*

ranges, tools, platforms, repositories to support cyber security experimentation and analysis.

9.2.4 NITRD CSIA IWG

Recently, Federal Networking and Information Technology Research and Development (NITRD) Program[3] and its Cyber Security Information Assurance (CSIA) Interagency Working Group (IWG), have identified three initial Research and Development themes in the area of Cyber Security: (i) Moving Target, (ii) Tailored Trustworthy Spaces, and (iii) Cyber Economic Incentives.

9.2.4.1 Moving Target

Attackers are currently capitalizing on their asymmetric position. They have all the time in the world to study a target, understand its vulnerabilities and develop offenses which will hit the target effectively. This approach suggests that we should develop and deploy mechanisms which will continually shift the target for the attackers and breaking their asymmetric advantage. To realize this goal research is required to address the following:

- *Develop abstractions and methods that will enable scientific reasoning regarding Moving Target mechanisms and their effectiveness,*
- *Characterize the vulnerability space and understand the effect of system randomization on the ability to exploit those vulnerabilities,*
- *Understand the effect of randomization of individual components on the behavior of complex systems, with respect to both their resiliency and their ability to evade threats,*
- *Develop a control mechanism that can abstract the complexity of Moving Target systems and enable sound, resilient system management,*
- *Enable the adaptation of Moving Target mechanisms as the understanding of system behavior matures and our threat evolves.*

9.2.4.2 Tailored Trustworthy Spaces

In this area research is needed to develop the following points.

[3] www.nitrd.gov

- *Trust negotiation tools and data trust models to support negotiation of policy.*
- *Type-safe languages and application verification, tools for establishment of identity or authentication as specified by the policy.*
- *Data protection tools, access control management, monitoring and compliance verification mechanisms to allow for informed trust of the entire transaction path.*
- *Resource and cost analysis tools.*
- *Hardware mechanisms that support secure. bootload and continuous monitoring of critical software.*
- *Least privilege separation kernels to ensure separation and platform trust in untrustworthy environments.*
- *Application and operating systems elements that can provide strong assurance that the program semantics cannot be altered during execution.*
- *Support for application aware anonymity to allow for anonymous web access; and platform security mechanisms and trust-in-platform establishment.*

9.2.4.3 Cyber Economic Incentives

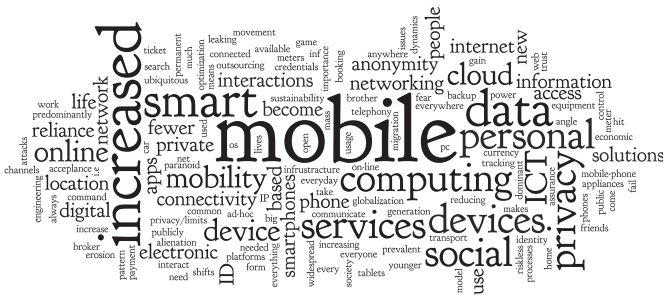
In this area research is needed to develop the following points

- *Explore models of cybersecurity investment and markets*
- *Develop data models, ontologies, and automatic means of anonymizing or sanitizing data*
- *Define meaningful cybersecurity metrics and actuarial tables*
- *Improve the economic viability of assured software development methods; provide methods to support personal data ownership*
- *Provide knowledge in support of laws, regulations and international agreements*

A

Working Group Brainstorming

A.1 Changes



February 23rd 2011 found all the working groups of SysSec in Amsterdam in VU brainstorming on emerging threats and vulnerabilities. To kick start the discussion, all members were asked to state the major changes they see in ICT and which changes will influence Cyber Security and Privacy. In this section we list all their responses. We provide the responses without any editing (apart from a few spelling errors). We kept the original style of writing (even for those cases where a $>$ was used to mean "implies"). We see that predicted upcoming changes relate to mobility, (lots of) data, (loss of) privacy and smart environments.

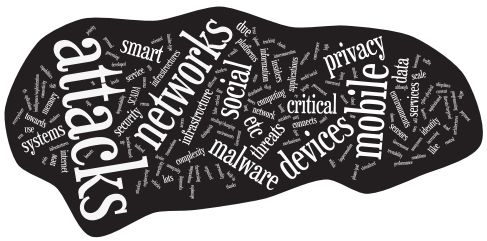
- erosion of (online) privacy
- knowledge/information is the new currency ; economic power shifts
- 24/7 connectivity (everyone with everything)
- more private information available publicly
- privacy
- mobility
- electronic identity will be prevalent

- on-line interactions will be the dominant way of social interactions
- younger generation much more open with their lives - no more privacy
- mass migration of services to the internet (i.e. broker services, ticket booking)
- more “tracking” technologies
- mobile phone location, common pattern with friends
- smart meter $>$ appliances I use
- public cameras $>$ what I do
- car $>$ location
- permanent fear for leaking personal data
- gadgets
- the privacy/limits of personal data will be more discussed
- social engineering based attacks will hit more people as data on net increases
- reducing the personal anonymity
- alienation
- access to all information and network devices will be predominantly mobile
- fewer and fewer backup solutions to take over when digital electronic solutions fail (so: increasing reliance on ICT everywhere)
- personal inf only in digital form
- riskless society
- environmental changes IT
- increased ad-hoc device to device connectivity
- ubiquitous computing (smartphones, tablets,..)
- everyday life dynamics will be increased
- less anonymity
- people will become more paranoid. trust and assurance issues will gain more importance

- privacy will become more important
- ICT (IP?) based command and control channels to every angle device we own
- credentials: new game we needed, but we dont know where they will come from (telephony, banking, transport, ID, ...)
- use of your private pc and mobile-phone at work
- smart grid and smart meters makes you communicate with your “home” equipment from anywhere
- pervasive computing acceptance
- smart infrastructure
- sustainability
- increased mobility
- technological big brother
- “always connected” to internet $>$ mobile phone will have access to “my” life
- social networking as a means for search
- mobility and mobile infrastructure
- cloud computing and data outsourcing
- widespread usage of smartphones increase of smart devices
- globalization ; need or desire to interact online
- more online services
- web ID
- social network
- mobile apps
- cloud computing
- mobile devices
- mobile phones used for payment
- few mobile OS platforms

- movement of data and apps to a cloud model
- increased availability of networking on mobile devices
- increased optimization of services and processes through increased reliance on ICT

A.2 Threats



The second question we asked the Working Group members was to identify the major Cyber Security threats they perceive for the next few years. In this section we record their responses as we received them. We did not edit them in any way (apart from minor spelling error corrections). Thus, the style, syntax and grammar may vary from one response to another. From a quick glance it seems that several of them are concerned about mobility, privacy, malware, and critical systems. Interestingly enough, several of them have touched upon the social dimension of security and privacy mostly as it manifests itself in social networks.

- attacks on critical infrastructures
- ubiquitous sensors
- there is a shift from "hiding data" towards "sharing data" within governments. This brings the problem of "interconnection of networks" with different security levels.
- Government A connects to Government D, military nets connects with each other etc. This will bring a new "intelligence/sophistication" level to all attacks we know. Attacks to authorization mechanisms may be top priority.
- threats due to scale
- attacks on distributed systems and clouds
- attacks on high performance computation systems such as grids
- scale and complexity (lots of devices, applications, connectivity, services, users)

- privacy and tracking (social networks, information leads, gadgets and networks)
- (trustability) lack of trust
- insiders in networks
- threats due to complexity
- increased availability of unsecured services for attackers
- threats due to privacy issues
- stealing/changing user identity in the network
- smart mobile devices, anonymous access to internet
- insider-type attacks
- upcoming malware for mobile platforms (this time really, thanks to convergence towards 3 platforms: windows, android, iphone)
- attacks on cyber-physical systems governing critical infrastructures, vehicles, etc.
- increasing attacks on virtualized environments targeting the cloud computing infrastructure as a service model"
- targeted attacks
- wireless networks vulnerabilities
- smart environments like homes, cars, traffic control etc. protection
- connectivity in between e-mails, skype social networks and false anonymity and personality
- network service attacks
- critical infrastructure attacks
- the borders that distinguish insiders from outsiders are becoming less clear
- social networks
- critical infrastructure IT security
- race conditions (will hurt dependability)
- critical infrastructures and SCADA will see more attacks now that stuxnet has shown the way

- ultra mobile devices
- IPv6
- malware for new architectures (arm, gpu)
- return oriented programming
- malware (for SCADA)
- memory corruption is dead - long live to memory corruption
- all current threats tailored to the mobile world/social networks”
- organized (cyber) crime
- mobile payment systems
- botnets
- privacy
- data everywhere, computing power everywhere
- malware for mobile devices
- sophisticated phishing attacks (through social networks, mobile devices, apps)
- malware for mobile devices
- government developed malware
- threats/targeted attacks against critical infrastructures
- espionage and ransom (threatening by losing their data) against citizens
- attacks against mobile smart phone/pad devices and applications
- attacks against the privacy and personal information in social networks
- attacks that stem from the use of the mobile device capabilities (location-based services) as sensors
- loss of privacy
- lots of “built-in” security in applications and OS etc.
- more use of cyberattacks against “greenpeace”, etc.

- social engineering and human error
- attacks in smart environments (smart devices like cars, stores, a/c, ...)
- attacks to privacy (social networks, etc.)
- identity theft (impersonation, transactions over the internet)"

A.3 Likelihood of an attack

In this section we quantify how the adoption/deployment of a technology might increase the likelihood of an attack. For example, has the evolution of social networks changed the likelihood of an attack against the privacy of a user? To show this likelihood, we construct a 2-D matrix. The rows of the matrix are the new technologies (such as social networks an mobile phones) while the columns of the matrix represent the assets we are trying to protect Each cell represents (with color) how likely is a particular technology to increase the probability of an attack to the particular asset.

Assets / Threat-Enabler	**Personal** Assets				**Societal** Assets		**Professional** Assets
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.
Anonymous Internet Access	Medium	Medium	Low	Low	Medium	Low	Medium
Ubiquitous networks	High	High	High	High	Low	Low	Low
Human Factors	High	High	High	High	High	High	High
Insider attacks	High	High	High	High	High	High	High
Botnets	High	High	High	High	High	High	High
Program Bugs	High	High	High	High	High	High	High
Scale and Complexity	High	High	High	High	High	High	High
Mobile Devices	High	High	High	High	Medium	Low	High
24/7 connectivity	High	High	High	High	Low	Low	High
more private info available	High	High	Medium	High	Low	Low	Low
smart meters	High	High	Medium	High	High	Low	Low
Tracking	High	High	Medium	High	Low	Low	High
Smart Environments	High	High	Medium	High	Medium	Low	High
Unsecured Devices	High	High	High	High	Low	Low	High
Social networks	High	High	Medium	Medium	Low	Low	Low
Cyber-physical connectivity for Infrastructures, cars etc.	High	Low	Medium	High	High	Low	High
Organized Cyber Crime	High	High	High	High	High	Low	High
Mobile Malware	High	High	High	High	Medium	Low	High
SCADA Malware	Low	Low	Low	Low	High	Low	Medium
	Privacy (Human Rights)	Digital Identity	Financial Assets	Health Safety	Critical Infrastructures	GRIDS Clouds	Data Sales etc.

Table A.1: This table shows how Cyber Security threats and enablers facilitate attacks towards personal, professional and societal Assets. The rows of the table are the threats (such as Mobile Malware) or the enablers (such as Social Networks) which can be abused by aggressors to compromise personal, professional and societal assets. Each cell of the table corresponds to how likely is a given threat-enabler to influence the respective asset. (darker is higher)

Bibliography

[1] R. Anderson and S. Fuloria. Who controls the off switch? In *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, pages 96–101. IEEE.

[2] M.R. Benioff and E.D. Lazowska, editors. *Cyber Security: A Crisis of Prioritization*. National Coordination Office for Information Technology Research and Development, February 2005.

[3] Yanpei Chen, Vern Paxson, and Randy H. Katz. What?s new about cloud computing security? Technical Report UCB/EECS-2010-5, EECS Department, University of California, Berkeley, Jan 2010.

[4] European Commission. A digital agenda for europe, May 2010. COM(2010) 245.

[5] The Forward Consortium. White book: Emerging ict threats, January 2010. http://www.ict-forward.eu/media/publications/forward-whitebook.pdf.

[6] Mike Davis. Smartgrid device security: Adventures in a new medium, July 2009. http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf.

[7] Theodosis Dimitrakos, Fabio Martinelli, Peter Y. A. Ryan, and Steve A. Schneider, editors. *Formal Aspects in Security and Trust, Fourth International Workshop, FAST 2006, Hamilton, Ontario, Canada, August 26-27, 2006, Revised Selected Papers*, volume 4691 of *Lecture Notes in Computer Science*. Springer, 2007.

[8] EU FP7 Project SEC 2010 - 2012. Foresight security scenarios: Mapping research to a comprehensive approach to exogenous eu roles. Internet. www.focusproject.eu, 2010.

[9] N. Falliere, L.O. Murchu, and E. Chien. W32. stuxnet dossier. *Symantec Security Response*.

[10] Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. Security and privacy for implantable medical devices. *IEEE Pervasive Computing*, 7:30–39, 2008.

[11] Harold Linstone and Murray Turoff (Eds.). The delphi method: Techniques and applications. Internet. http://www.is.njit.edu/pubs/delphibook/, 2002.

[12] John P. Holdren, Eric Lander, and Harold Varmus, editors. *Designing a Digital Future: Federally Funded Research and Development in Networking and Information Technology*. Office of Science and Technology Policy, December 2010.

[13] Google Inc. A new approach to china. "http://googleblog.blogspot.com/2010/01/new-approach-to-china.html", jan 2010.

[14] New York independent system operator. Report on the august 14 blackout. "http://www.hks.harvard.edu/hepg/Papers/NYISO.blackout.report.8.Jan.04.pdf", jan 2004.

[15] Alexandros Kapravelos, Iasonas Polakis, Elias Athanasopoulos, Sotiris Ioannidis, and Evangelos P. Markatos. D(e—i)aling with VoIP: Robust Prevention of DIAL Attacks. In *ESORICS*, pages 663–678, 2010.

[16] Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou. Designing and implementing malicious hardware. In *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats*, pages 5:1–5:8, Berkeley, CA, USA, 2008. USENIX Association.

[17] Krisberedskapsmyndigheten. Omvärldsexempel 2005. Published by Krisberedskapsmyndigheten, Sweden, 2005. KBM:s dnr:0280/2005.

[18] Krisberedskapsmyndigheten. En sammanfattning av rapporten: faller en – faller då alla? ISBN: 978-91-85797-24-0. Published by Krisberedskapsmyndigheten, Sweden, 2007. KBM:s dnr:0021/2007.

[19] Susan Landau, Martin R. Stytz, Carl E. Landwehr, and Fred B. Schneider. Overview of Cyber Security: A Crisis of Prioritization. *IEEE Security and Privacy*, 03(3):9–11, 2005.

[20] Michael LeMay and Carl Gunter. Cumulative attestation kernels for embedded systems. In Michael Backes and Peng Ning, editors, *Computer Security ESORICS 2009*, volume 5789 of *Lecture Notes in Computer Science*, pages 655–670. Springer Berlin / Heidelberg, 2009.

[21] Yao Liu, Peng Ning, and Michael K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, pages 21–32, New York, NY, USA, 2009. ACM.

[22] Stephen McLaughlin, Dmitry Podkuiko, and Patrick McDaniel. Energy theft in the advanced metering infrastructure. In Erich Rome and Robin Bloomfield, editors, *Critical Information Infrastructures Security*, volume 6027 of *Lecture Notes in Computer Science*, pages 176–187. Springer Berlin / Heidelberg, 2010.

[23] George Metakides. Trust in the information society, January 2010. http://www.think-trust.eu/downloads/public-documents/riseptis-report/download.html.

[24] Zlatogor Minchev and Velizar Shalamanov. Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach. In *RTO-MP-SAS-081, Symposium on "Analytical Support to Defence Transformation, Boyana, Bulgaria, April 26-28, 22-1 22-16*, 2010.

[25] Minh-Tuan Nguye and Madeleine Dun. Some methods for scenario analysis in defence strategic planning, australian dod, joint operations division defence science and technology organisation, dsto-tr-2242, 2009.

[26] Subcommittee on Networking, Information Technology Research, and Development. The networking and information technology research and development program: Supplement to the presidents budget for fiscal year 2012, February 2011. http://www.nitrd.gov/pubs/2012supplement/FY12NITRDSupplement.pdf.

[27] Salvatore Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclair, Sean Smith, and Shlomo Hershkop, editors. *Insider Attack and Cyber Security: Beyond the Hacker (Advances in Information Security)*. Springer, 2008.

[28] D.M. Thomas, K. an Nicol. The koobface botnet and the rise of social malware. In *5th International Conference On Malicious and Unwanted Software (Malware)*, 2010.

[29] U.S. Department of Homeland Security, Science and Technology Directorate. National power grid simulation capability: Needs and issues. Internet. http://www.anl.gov/ese/pdfs/PowerGridBrochure.pdf, December 9–10, 2008. National Power Grid Simulator Workshop, Argonne, Illinois.

[30] Nick Wainwright and Nick Papanikolaou. Trust and security research roadmap, an analysis of discussions at effectsplus clustering and roadmapping events, 2011. http://www.effectsplus.eu/files/2011/04/Trust-and-Security-Research-Roadmap-Draft-1.pdf.