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 D4.4: Final Report on Threats on the Future Internet: A Research Outlook

**Abstract:** This deliverable presents the final update on the emerging threats identified by the three working groups at the end of the project. The deliverable also contains the updated version of the research roadmap in the area of System Security.

| | |
|---|---|
| Contractual Date of Delivery | August 2014 |
| Actual Date of Delivery | September 2014 |
| Deliverable Dissemination Level | Public |
| Editor | Davide Balzarotti |
| Contributors | All *SysSec* partners |
| Quality Assurance | Christian Platzer, Ali Rezaki |

The *SysSec* consortium consists of:

| | | |
|---|---|---|
| FORTH-ICS | Coordinator | Greece |
| Politecnico Di Milano | Principal Contractor | Italy |
| VU University 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.

## Document Revisions & Quality Assurance

### Internal Reviewers

1. Christian Platzer (Technical University of Vienna)
2. Ali Rezaki (TUBITAK-BILGEM)

### Revisions

| Ver. | Date | By | Overview |
|---|---|---|---|
| 1.6 | 26/3/2014 | *Editor* | Addressed final comments and added one more paragraph to Chapter 4 |
| 1.7 | 25/3/2014 | *Editor* | Fixed document template |
| 1.5 | 23/3/2014 | #1 | Modified text in 4.5 to better reflect the discussion with the experts |
| 1.4 | 20/3/2014 | #2 | Removed redundant text in Chapter 3 |
| 1.3 | 19/3/2014 | #1 | Small fixes committed to Chapters 1-4 |
| 1.2 | 17/3/2014 | #2 | Many sentences improved in all three chapters |
| 1.1 | 3/9/2014 | *Editor* | Typos fixed in all chapters. |
| 1.0 | 30/8/2014 | *Editor and WG Leaders* | First complete draft. |
| 0.1 | 4/8/2014 | *Editor* | First skeleton of the Deliverable. |

# Contents

# Acknowledgments

A number of researchers and external experts contributed to the discussion that helped 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:

| | |
|---|---|
| Simin Nadjm Tehrani | *Linkoping University* |
| Lorenzo Cavallaro | *Royal Holloway University* |
| Vassilis Prevelekis | *Technical University Braunschweig* |
| Judith Rossebo | *ABB* |
| Angelos Stavrou | *George Mason University* |
| Wolfgang Trexler | *Bank of Austria* |

# 1 Executive Summary

The deliverable is divided in three chapters. In the first, we discuss the changes we observed in the system security area after we published the Red Book, in August 2013. Several relevant events happened in our community in the past year. This chapter also presents the opinions we collected about those events from a number of international experts, during a meeting held in Brussels in May 2014.

In the second chapter, we present an overview of the emerging threats identified by the three working groups during the first three years of the project. These threats reflect the opinions collected from all the experts during the entire project. Each working group (respectively *Malware and Fraud*, *Smart Environments*, and *Cyberattacks*) discuss the threats and research directions they proposed in the past, emphasizing which assumptions held true and which did not.

Finally, the last chapter of this deliverable presents an update of the research roadmap, adding two more research directions to what we already proposed in the third year of the project. We believe that this final document will serve as a supplement of the Red Book, shaping the research in system security for years after the end of the SysSec project.

# 2 One Year After the Red Book

## 2.1 The Red Book

In August 2013, the SysSec consortium and its constituency published the *Red Book: the SysSec Roadmap for Systems Security Research*. The book is a summary of the research conducted during the first three years of the project, presented in an organized form to target several different communities – including security researchers, policy makers, and journalists. In particular, experienced and young researchers can find an in-depth description of several interesting research topics, enriched with a survey of the related work on the area and a list of challenges and open problems that could be solved within the context of a Ph.D. thesis. Policy Makers can benefit from the executive summary that presents an high-level overview of the book content, and from the list of Grand Challenge Research Problems in the area of Systems Security. These challenges require a long-term, collaborative effort and they constitute excellent directions for future funding in the system security area. Finally, journalists were targeted by enriching the book with several examples describing the impact of each threat and the worst case scenarios to be expected in each topic. We believe that this is very important to help journalists who want to accurately reports fact, without under- or over-estimating the impact of emerging security threats.

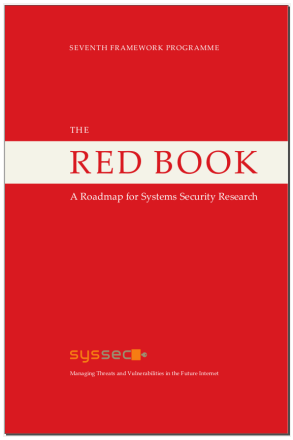
The content of the book is organized around eleven security topics, spanning most of the areas of system security:

- Anonymity
- Software Vulnerabilities
- Social Networks
- Critical Infrastructure Security

- Authentication and Authorization
- Security of Mobile Devices
- Security of Legacy Systems
- Usable Security
- Botnets
- Malware
- Social Engineering and Phishing

Each chapter clearly describes the problem from a technical perspective, and its potential impact to the society by describing who is going to be affected by it. Each chapter then goes into details to present what the SysSec consortium expects to happen in the near future in the presented area, and what is the worst thing that could happen if we do not promptly react and improve its security. Finally, each chapter focuses on the scientific angle of the problem, summarizing the related work and enumerating a number of concrete problems for which existing solutions still do not provide a satisfactory level of protection.

### 2.1.1 The Impact of the Red Book




One year after its publication, it may still be too early to measure the impact of the Red Book. However, the figures show a widespread and increasing interest in the document, confirming the importance of our roadmap to shape and inspire other people's research activities.

So far, over 150 printed copies of the book have been shipped to different members of the system security community, academic researchers, industry experts, policy makers, and members of the European Commission. The number is still growing, as more and more people are contacting us to request a copy of the book.

In addition to the printed copies, the electronic version of the book was downloaded almost 3000 times from over 2000 unique /24 networks. We believe that this is clear evidence for the impact of the Red Book, both within and beyond our community.

## 2.2 One Year Later

In June 2013, while the Red Book was in the proofreading phase, an NSA contractor named Edward Snowden escaped from the United States to Hong Kong and started disclosing to the media a large number of classified NSA documents. The purpose of these documents was to unveil the existence of a secret, massive surveillance program designed to infiltrate, collect, store, and analyze a large amount of telephony and Internet traffic.

These documents, released little by little over the course of the past year, have deeply shaken the world of system security and privacy. Therefore, we decided to organize a discussion around this topic with a number of invited experts, during the working group meeting that took place in Brussels in May 2014. The brainstorming session had three main objectives: first, to discuss whether (and to which extent) the experts were surprised by these recent events; second, to identify what can be the impact of the NSA scandal on our research agenda; and finally to understand if what we presented in the Red Book was still relevant today, after these new events took place.

The result of the discussion can be summarized around two major points:

**The technical side** – The main outcome of our experts meeting is that nothing of what has happened in the past year was particularly surprising from a technical point of view. In other words, all the surveillance mechanisms, the wiretapping devices, the firmware backdoors, the large scale correlation systems, and everything else that was part of the disclosed NSA arsenal was mainly shocking because of its scale and pervasiveness. However, the technology was already known. At the same time, it was interesting to see how the NSA had been actively using techniques to backdoor hardware devices for many years, even though the research community turned its attention to this problem only in the past few years.

Since the effort of the SysSec consortium is focused on the forecast, detection, and mitigation of **technical** threats, the NSA scandal has only a limited effect on our previous work and predictions. In other words, everything we said in the Red Book is still valid, and actually even more relevant in the light of recent events.

**The economical and social side** – If the technical sophistication was not what surprised our community, the other aspects of the NSA scandal certainly did. On one side, we may have largely underestimated the scale and the amount of effort and money involved in this kind of surveillance activity. If it was reasonable to believe that nation states have such programs in place for national security, the extent of these activities were still quite surprising. Along the same line, some of our

experts were also surprised to discover that the United States was one of the main actor in the new world of state-sponsored spyware.

Another important aspect is that these recent events may have a direct impact on our understanding of the common "adversary". In other words, every security research needs to carefully explain what is the threat model, the ability and resources of the adversary against which we need to protect our systems. The geographical and economical scale of the events we witnessed in the past year may permanently shift the attack model towards something more complex and powerful compared to what we were using in the past. This is an ongoing process that started with the Stuxnet incident, and that the NSA scandal contributed to accelerate.

In the next chapters we will elaborate on the impact of recent changes on our previous threat forecasts. In particular, Chapter 3 will present a separate discussion for each working group – summarizing the work that has been done so far and highlighting the mistakes and the main points that are still relevant for the future.

## 2.3 Forecasting the Future in System Security

The purpose of WorkPackage 4 is to forecast the future threats in the area of system security. The first step towards this goal was our initial roadmap (Deliverable D4.1), published in 2011. The document was then updated every year to extend and adjust our forecast by taking into account new events and developments in the area. As we already mentioned before, this effort culminated in 2013 with the publication of the Red Book.

Unfortunately, with this last deliverable, we will not have a chance to tune the roadmap in the next year. Therefore, we wondered if it was better to extend the reach of our forecast, so far limited to a window of a couple of years, further into the future. Again, this was something we discussed within our working groups and with the experts invited to our face-to-face meeting in Brussels.

The answer to this question was quite unanimous: The vast majority of our experts thought that the appropriate forecast time window is not more than **two years**. Few went up to five, while for some of the experts more than one year is already pure guesswork. This result reflects the initial choice adopted by the SysSec consortium. In fact, the system security area is moving very fast and researchers are often struggling to catch up with the frequent changes in the threat landscape. Moreover, unpredictable large scale events are not unusual, and they are often the spark that steers the research community towards rapidly emerging topics. For these reasons, we believe that long-term predictions are too imprecise to be used in our

roadmap. Trying to brainstorm about new threats that *may* appear five or ten years from now is like trying to get the weather forecast for a weekend still three months away. As an example, five years ago Android security did not even exist, and today is one of the most active topics of our area.

# 3 Working Groups: the Past and the Future

## 3.1 Introduction

The essential task of each Syssec Working Group is to collect expert input for various research areas, namely *Malware and Fraud*, *Smart Environment*, and *Cyberattacks*.

This input is supposed to fulfill two tasks. First, it provides the necessary background to estimate what we need to expect for the future. Second, it helps to judge if previous estimates were correct and if certain predictions held true. Especially with documents like the Red Book or the Second year Roadmap at hand, it is interesting to see which assumptions held true and which did not. Furthermore, the NSA scandal and other security-related developments of the last months are perfect gauges to measure the accuracy of our previous predictions. Did we anticipate them? Was the community surprised? These questions were answered in the last expert meeting, reminiscing previous discussions.

The following sections will summarize the past activity of each working group, in the light of the recent events.

## 3.2 Malware and Fraud

According to the SysSec description of work, the *Malware and Fraud* working group covers all aspects of malicious code and fraudulent activities on the Internet. In particular, as the name suggests, it focuses on the discussion of new malware infection and propagation techniques, and on the way cyber-criminals are able to profit from malicious code and stolen information. The rest of this section is therefore divided in two parts, respectively focusing on the development of these two aspects: Malware and Fraud.

### 3.2.1 Malware

Most predictions for future malware that have been given throughout the Syssec project were conservative. In other words, the malware landscape was viewed as a pretty static, unchanging construct. This assumption was based on the fact, that malicious software works quite well as it is currently most prevalent: On Windows x86 systems. It has been well-established that battling this kind of threat is a never-ending arms race that is ultimately bound to be more efficient for the attacker than for the defender. One reason is that on the defense-side, an open computing platform without a controlled ecosystem is targeted. There is no such thing as an app store for Windows 7 applications. On the other hand, the defender is either a researcher with limited capabilities, or an AV company with a certain time-to-market.

In the following subsection we briefly discuss the most important predictions from all three previous years and to what extend they held true.

#### 3.2.1.1 Previous assumptions

- **Mobile Malware:** With the emergence of full-fledged mobile operating systems like IOS, Android or Windows Mobile, concerns about malicious software targeting these devices arose as well. During the very first research roadmap (Deliverable 4.1), this threat was not tagged with the utmost priority. The assumption was, that these devices come with their own ecosystem and unlike Windows or Linux machines, can be closely supervised by the company behind it. This assumption is still accurate. While it is true that certain brands of viruses made the transition to the mobile world, like Zitmo (Zeus in the mobile) for example, the risk of being exposed is far lower than on PCs. The majority of infectors require a manual installation and/or circumvention of integrated security mechanisms like automatic market checks. In other cases, the malware even requires a rooted device.
  A detailed description of Research in this area is given in Deliverable 7.4 and 5.5.

- **Cross-platform Malware:** A different focus concerns the area of Cross-platform Malware. The basic assumption here was, that authors of malicious software are intrinsically bound by economic values and therefore also bound to OS distribution numbers. Writing a piece of software is work and depending on how well it pays off, it is either done or not. With Windows still as the most prevalent OS on the market, this picture has not changed much in recent years. However, a transition from using stand-alone applications to Browser-based solutions for everything an ordinary user needs has occurred. As a result, malware authors are presented with the opportunity to use browser exploits for their initial infections and later drop an executable or binary tailored for the underlying operating system. Research has proved that such an approach is feasible and that some exploits already work on multiple platforms (e.g. Windows and OSX). However, the expected rise in non-Windows malware has not occurred. In the experts' opinion, the reason is simply, that the current infrastructure works well as it does and that there is no need to change that. A few thousand additional infections on OSX does not justify the effort to create an additional binary. All experts agreed that until Windows loses its place as the most popular operating system, this picture will remain unchanged. And that will most probably not happen in the next two years.

- **Malicious Hardware:** A widely discussed topic both in the expert meetings and in previous deliverables is malicious hardware. Initially, the topic only included bogus circuits and hidden backdoors directly implemented into a chip. Later, the definition was broadened to hardware-enabled attacks like exploiting test modes or hardware bugs. Both areas have received the most attention from all threats we listed during the past three years. This attention came from two very different angles. First, hardware-based reverse engineering has gained importance in the research community. As an example, we mentioned the risk of leaving test facilities on an ASIC because they can later be used to circumvent the chip's protection mechanisms. In [27], this exact approach was used to access key material and firmware information of a protected chip. This proves that hardware can not be neglected when making security considerations. A highly motivated and dedicated attacker can exploit such a feature.
  The other, more worrying side concerns trust in the hardware supply chain. This is what started the discussion in the first place. It was proven years ago that well crafted hardware circuits can be designed such that they are next to impossible to discover, even when they are looked for. We knew they could be there and considering all the necessary stages when producing consumer electronics, it is more than plausible that malicious circuits could be introduced at some point.

What we did not anticipate was that these backdoors could also be introduced by the manufacturer itself because the company receives pressure from the government. From a technical perspective it does not matter where the circuitry was introduced. Therefore, we were mildly surprised when Edward Snowden revealed that the NSA supposedly introduced hardware backdoors in cisco routers before they were being shipped. This statement, however, raises the very important question of who to trust in the hardware supply chain and is further discussed in Section 3.2.1.3.

- **Information Risks:** Finally, the probably most interesting predictions were made in respect to user privacy and the risk of rich profiles on the internet. At project start, the main concern was that companies may utilize publicly available information to build rich profiles of people and use them for their own purpose. This threat was also discussed in the Red Book, where we depicted cases where the younger generation might grow up in an environment which is constantly under scrutiny. This environment was envisioned as something where secrets are unable to exist, simply because smart algorithms are so powerful that they can deduce facts from not directly related indices. This is where the line between the working groups became blurry. On one hand, this scenario is the classic form of a cyber attack (working group 7) on a person's privacy. On the other hand, there is software enabling it in the first place, which fits the category for working group 5. And in this particular case, the software even has a name: *XKeyscore*. This software, which was also revealed by Edward Snowden during the NSA espionage scandal in 2013, is capable of correlating various events and wiretapped connections to form a sophisticated profile of a specific target.
  Claiming that we foresaw this during the creation of the Red Book would be an overstatement. Furthermore, the experts were admittedly surprised when the scandal hit the news. However, the surprise was not because of the technology that was used or the level of sophistication of the XKeyscore software. The astonishing thing was the level of influence, a government can assert on productive systems and company infrastructure. With this key restriction fallen, the technological possibility to create even more sophisticated profiles than what we have already seen opens the door for worse scenarios than what we experienced so far.

#### 3.2.1.2 Research

Another benefit of having a group of experts is the opportunity to get different views on how research in this area evolved. Not only from University

personnel, but also from the industry, where the view on the topic is more pragmatic.

In the past four years, malware research was still one of the topmost priorities of the security community. And this is not expected to change soon, since malicious programs are still an enormous factor in computer security. There was, however, a noticeable shift from traditional, x86 systems to mobile malware. This shift is a pro-active one. In 2013, for example, mobile malware research was roughly equal to x86 systems. Still, the amount of available and active malware for mobile devices is far below the numbers for Windows-based programs. An overview of the most relevant publications in this direction is given Deliverable 5.5, the final report on Malware and Fraud.

The decision to conduct research in a certain area is finally also influenced by the acceptance received in the scientific community. Even though malware packers, botnets and sophisticated evasion techniques are still a big problem for AV vendors and users, these problems have been addressed before and partially even solved. From a researcher perspective it is thus more beneficial to tackle new problems and try to solve them instead of implementing an existing approach by creating and maintaining a finished product rather than a proof-of-concept prototype.

#### 3.2.1.3 Working group Meeting

On an annual basis, we invited three to four experts for each working group to join in a discussion. In our first year, we had separate meetings for each group but it turned out to be more productive to join experts in a single meeting and discuss a broader range of problems. One goal of these meetings was to discuss how well the previous roadmaps have been defined, as described above. The other objective was to exploit the experts' knowledge and discover trends in these key areas. For malware specifically, it comprised discussing interesting types of malware, new command infrastructure and evasion techniques or even completely new genotypes.

Over the past years, malware did not develop erratically. Instead, new developments and new forms of attacks were developed incrementally. When a certain kind of attack did not yield good enough results, a switch to some other technology took place. It is important to note here that two very distinct factors are necessary for a successful malware infection.

1. An infection strategy and
2. a malware binary.

The statement about constantly evolving binaries are mainly meant for the second point, the binary itself. To date, a well-crafted sample includes

sophisticated protection against reverse-engineering, a packing mechanism of some sort to thwart signature based detection and countermeasures against dynamic analysis. This picture has not changed much in recent years. A decent polymorphism strategy is still good enough to force reaction times of a day or more before the malware is flagged by AV companies. That timeframe is more than enough for a 0-day attack. Still, researchers try to devise new and bulletproof detection mechanisms, but the bottom line is that this is the arms race security researchers are talking about.

A far more staggering development took place where infection strategies are concerned. In 2011, E-mail attachments were still the main distribution channel for new malware. This picture changed since then. Nowadays, the main infection strategy is to exploit the Browser and drop a binary that way. There is, however, another possibility for an infection. By far, the best success rate is achieved by a willing target. By social engineering, for instance, a victim can be tricked into installing a certain piece of software. Or even better, if a benign piece of software is infected with a backdoor, chances are high, that it will be installed. One of the experts depicted a case, where the government forces an AV company to include custom code in their own virus scanner. After 2013, such a case is plausible.

This line of argumentation ultimately ends in the question who to trust. And that is not limited to software alone. The same can be done with hardware like described in the sections above. As a bottom line conclusion, the members agreed that there is no real countermeasure against government surveillance save to go without technology at all. And that is a step most citizens are unwilling to take.

### 3.2.2 Fraud

The original definition of fraud, according to the Oxford Dictionary is a

> "*wrongful or criminal deception intended to result in financial or personal gain.*"

While this definition may be accurate, it is simply too wide for criminal activity in Computer Systems. One may argue that cheating at a computer game may fall in this category. There is, however, a large difference between an aimbot for a third person shooter and credit card fraud. During our working group meetings, we agreed that financial gain is the foremost objective when conducting computer fraud.
This topic seems to be one of the most constant and slow-changing threats in the current computer landscape. It has been there from the beginning and is not expected to vanish soon. As with Information Security, fraudulent activities always comprise a social component. A user has to be tricked into disclosing information, carry out detrimental activities or enable the attacker to do it for him. Before the Internet age, there were phone scams

and credit card fraud as well, but on a much smaller scale. Unfortunately, researchers are restricted in their ability to create technical solutions for this problem. The main countermeasure when battling Internet fraud is user education. Since raising awareness is a time consuming task, the only other way is to devise fool-proof systems that are very hard to misuse. Some examples in the banking sector have shown that it is possible to do that. We explain how in the following sections.

Analogous to the Malware Section, we give an overview of hot topics from previous roadmaps, how they were perceived in their danger level and how the then-perceived future differs from the present.

#### 3.2.2.1 Previous assumptions

- **Phishing:** During the creation of the Red Book and in all of the experts meetings, phishing came up as one of the most dangerous enablers for internet fraud. We essentially grouped the various forms of phishing into the categories intelligence-gathering and malware infections. Other forms dealt with various forms of social engineering, which is discussed as a separate point here. The common prediction was, that phishing attacks will still be here in 3 years and most probably also at a later time. Interestingly, the number of phishing attacks on a global scale experienced a heavy decline during the first half of 2013 [14]. With only 58% the number of attacks on a single domain compared to the previous year, this decline is most probably owed to an equal decline in compromised shared virtual servers used for the attack. According to APWG [14], the chinese market is now the preferred place to conduct such attacks. In the western countries, domain registration for phishing sites nearly doubled. However, deciding which targets are most likely hit, is hard to estimate. In general, these attempts either try to get credential for the impersonated site or lure a user into clicking a link where the target site contains malware. Overall, the phishing landscape is quite stable on a global scale, with a noticeable shift towards western countries.

- **Social Engineering:** Closely related to phishing is of course the social engineering aspect. Whenever a phishing attempt is made, there is also a connected social component. It can be a statement about a pending credit, money that is lying around or even a call from an impersonated bank clerk demanding access to the netbanking account. This form of social engineering even got its own name - vishing (from voice phishing). Its effectiveness is unbroken. In times where direct contact is rare, a voice on the other side immediately raises trust and thus works perfectly as an enabler for banking fraud. In the working

groups, the participants could not see any possibility to mitigate this threat other than raising awareness and educate users as good as possible. The technology to counter social engineering is there, but as soon as an attack leaves the technological level, it is harder to come by.

- **Credit Card Fraud:** A very popular form of fraud still is credit card fraud. According to the latest report from the european central bank [7], it is gaining polularity again, even though the total sum of money is still below its all-time high from 2008. The major advantage when dealing with credit cards compared to bank accounts is that not all cases require a human to cash out the fraud money. Internet transactions (CNP for Card Not Present) can easily be done with total anonymity. Unless credit card transactions are only carried out with a mandatory pin, and thus a check by the card's chip, this picture is not expected to change in the future. Again, the technical solution to provide a more reliable payment solution exists, while the actual implementation is delayed or not possible at all.

#### 3.2.2.2 Research

Research in the field of fraud is very sparse to say the least. Not because the problems are unsolvable but because the solutions need to be adopted by the population to work. Legacy systems have always been the counter pole to security. On the other hand, CERTS (Computer emergency response teams) try to fight incidents by broadcasting threats as soon as possible. This also includes new or particularly well-crafted phishing attempts or waves of credit card frauds.
Still, these practical efforts are not backed by theoretical research. Instead, the community targets to devise new and effective methods to create intrinsically secure systems which are easy to use. From that angle, an enormous effort is done to disable fraud in the first place, before there is even a chance it happens.

#### 3.2.2.3 Working groups

An interesting insight was given on the most prevalent form of internet fraud: Netbanking. During the working group meetings we had several experts from or with strong ties to the banking sector. According to their reports, there is a practical shift in banking fraud. With the introduction of two-factor, two-channel authentication (e.g. password and TAN-SMS), some countries were able to reduce the amount of direct banking fraud (stealing netbanking credentials and creating unsolicited transactions) to a negligible amount. There are, however, still cases where accounts are stolen, together

with access to the second channel. To get the money out of the banking system, the attackers now hire money mules from developing countries or from the near eastern countries, promise them a fake job and instruct them to withdraw the stolen money physically. If they get caught, they don't even know who they are working for and therefore reduce the involved risk for the backer enormously. From a technological aspect there are reported cases where even two-factor authentication is thwarted by using social engineering skills. A trustful user can easily lose all money put aside in a single successful attack.
The participants saw these kinds of fraud as a logical evolution of "ordinary" frauds, as it always existed. As long as there is human judgment involved, there will be a possibility to conduct such an attack.

## 3.3 Smart Environments

The focus of the smart environment expert group is low-capability devices, ranging from simple sensor networks to more heterogeneous systems with more capable hardware. As there is a continuous range of such devices and what they are capable of, 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. In some environments, a single compromised unit might be unacceptable. In others, a few compromised units will not affect the system detrimentally as long as the aggregated data in the whole environment is almost correct. For yet other environments, the two cases are very similar. They consist of simple but many very homogeneous units, meaning that if a single one is compromised the attack can easily be repeated to control the whole network.

This Red Book is the pivotal result from WorkPackage 4, where the material is organized to target several groups in society, such as politicians, journalists, other researchers, as well as new PhD students that are looking for important topics in system security. The book presented a uniform view of the threat landscape (regardless of working group). With this final deliverable for WorkPackage 4, Final Report on Threats on the Future Internet: A Research Outlook, we return to the original expert groups to discuss the roadmaps produced with a research outlook with possible incremental changes to the threats described in the Red Book. The following section is based on meetings with experts, discussions on the mailing lists, as well as the final expert meeting that took place in Brussels in May 2014. We briefly discuss the most important predictions from all three previous years and to what extend they held true.

### 3.3.1 Previous assumptions

In the smart environment working group, we used three example systems to focus the discussions for the research roadmap and the result from the roadmap was then incorporated in the research directions taken the following year. In D6.1: Report on the State of the Art of Security in Sensor Networks we surveyed the state of the art of sensor networks. In D6.2: Intermediate Report on the Security of the Connected Car we investigated and documented the security of the connected car. In D6.3: Advanced Report on Smart Environments we concentrated on the smart grid and the transitions this particular environment are faced with in the coming years. Especially in the third deliverable, we also covered critical infrastructures (as part of the electricity grid).

In the first roadmaps, we listed the following problems and challenges for the development of smart environments: accessibility, system complexity, maintainability, more capable devices, ubiquitous readers, network layer protocols and attacks against the non-ICT component. We also identified the need for a scientific methodology and tools to analyze parts of the smart environment (data, protocols, firmware). With the Red Book, the threats found in our working group were merged with the ones from the other groups resulting in eleven significant threats that will need further investigation in the future.

Considering these predictions in hindsight it is interesting to see what the last four years have brought to the landscape of smart environments. The discussion below is divided into types of systems with a discussion of the attacks and trends we can see for each of these environments.

#### Industrial Control Systems: Highly sophisticated and targeted malware

Just before the SysSec project formally started, a bomb went through the security community with the discovery of Stuxnet in June 2010. Stuxnet was a highly targeted, very sophisticated malware probably created by a very knowledgeable group of experts with excellent resources. Details of the malware are now well-known and have been described elsewhere. Both Syssec experts and external experts have agreed that Stuxnet changed the security landscape. What is possible to do, what assumptions can / should we make in our threat model? Stuxnet also has political ramifications in that offensive techniques are now openly discussed.

Questions also arose if this was an anomaly – a single instance that would not be repeated – or if this would be a blueprint to create many malware variants that would flood the world.

Statistics from the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) from DHS in the US show that attacks are increasing to-

wards industrial control systems, with especially the energy sector being more targeted than other sectors [19].

Many of the systems found in this environment are legacy systems (a threat described in the Red Book) and one of the vectors of attack is through weak authentication (another threat in the Red Book) [20]. Furthermore, most of these incidents are not widely reported. Patching is not easy and the vulnerabilities might stay within the systems until the hardware is upgraded.

In the outlook for the malware and fraud working group described in Chapter 3.2.1.3, it is noticed that even if malware exists for other platforms, the prevalence of Windows make this the number one target for malware writers. It is simply not worth the effort to develop malware for other platforms when one can target Windows. A similar argument seems to hold for the smart environment. We do not see malware being developed by the casual attacker for systems controlling critical infrastructures. However, there are highly sophisticated targeted attacks against the environment which challenge our detection and response capabilities. Similarly compared to Stuxnet, the malware *Dragonfly* has been discovered during the summer of 2014. According to analysis by Symantec, Dragonfly is very technically sophisticated and seems to be the result of state-sponsored operation. The goal seems to be cyber espionage even though it could also sabotage systems [42].

#### The AMI and the Connected Car

Broadening the scope, we observe that also other smart environment systems are being attacked. In the first year of Syssec, we proposed a scenario where a user hacked her smart meter to reduce her electric bill by changing the firmware. A year later, a cyber intelligence bulletin from FBI obtained by Krebs-OnSecurity (April 2012) describes how smart meters have been hacked to reduce the energy consumption of the customer, resulting in a large financial loss for the energy company. A similar scandal happened in Malta in 2014, where smart meters were manipulated to save money for the customers. The latter attack targeted the measurement unit of the smart meter (attacking the non-ICT component, as described in our roadmaps) by placing magnets on the smart meter. This is not a new attack, but with the new smart meters remote readings are possible meaning that any local tampering will not be discovered by the utility unless they send a person to the premise in question. Thus, it is clear the attacker will take the easiest path to reach their goal. In reporting less energy consumption, one can either change the reporting firmware or change the sensors recording the usage in the first place.

Attacks against the connected car have been documented in the scientific literature, as we described in the D6.2: Intermediate Report on the Security of the Connected Car. Experts point out that writing exploits require a sig-

nificant effort, meaning that it is likely that only targeted attacks directed at certain individuals will be developed in the next few years [5] [34].

It should also be noted that vulnerabilities in the traffic system itself outside the connected car have recently been reported, in that sensors are placed to control traffic lights etc. [9]. If the security of such systems is very lax, even people without much technical skills can hack them and cause accidents [6]. It should be pointed out that often companies prefer not to release any information about existing vulnerabilities. Some car companies have even sued academic researchers to not release any findings about vulnerabilities in their products [49].

### Attacking new consumer IoT devices

The vulnerabilities of small office, home office equipment have been reported previously. However, during 2014 a wide-range attack against IoT (Internet of Things) devices was discovered. The aim seems to have been to have the devices send spam. The devices ranged from routers to televisions to even a refrigerator. As not many emails originated from any single IP, it was difficult to filter the spam based on IP addresses. It seems that the devices in this particular attack were compromised through the use of default passwords or misconfigurations [37].

Another attack, this time against the United States Chamber of Commerce, was about cybertheft and exfiltration of information and lasted for months until the FBI stepped in and informed them about the attack. They tried to clean up their network but they discovered later that the office printer and even a thermostat kept communicating with a malicious address [36].

If operating systems from, for example, cell phones are reused also for other devices it is likely that wide-range non-targeted attacks might also compromise other types of devices running the same system. Many of the consumer devices have very lax security and a user might never log in even to change the default factory password. For that reason, it is likely these types of compromises will increase as more devices are networked.

### Sensors and data collected in the smart environment and Privacy

One of the topics highlighted in the Red Book is privacy. More and more data is produced, collected and aggregated about individuals. Many of the smart environment systems collect sensitive data. Already in last year's deliverable, D6.3: Advanced Report on Smart Environments, we discussed privacy concerns in relation to the smart grid and AMI. However, the problem is prevalent in many other types of systems and sometimes not so easy to foresee.

Taking the connected car as an example, the idea is to collect more data from the environment to improve roads and maybe even weather predictions of storm fronts. If cars communicated when the windshield wiper is turned on or when there is a bump in the road, the information can be aggregated and used to send out a repair crew for a road. However, such clues would also pinpoint the actual location of the car and its driver if the data is misused [50].

A recent paper demonstrates a similar concern. Insurance companies want to know the speed of the driver, and might be willing to offer a lower premium if the speed is shared. However, only knowing the speed of the car makes it possible to map how and where the car has been driven [26].

Given the plethora of sensors deployed, it might also be difficult to model exactly what information may be collected by which sensor and how it is then used. As an example, consider a modern phone with a microphone, a camera, GPS, Internet connection and accelerometers. The use of the microphone is restricted by application permissions. However, similar readings may be achieved by using the accelerometers, sensors where the measurements are not at all as restricted [33]. Thus, even if an app has no permissions to use the microphone, it may still be able to surreptitiously record confidential conversations.

### 3.3.2 Research

Over the meetings with the experts, it has been highlighted that it is expected that the use of devices in smart environments will increase over the coming years. These kinds of devices will also be found in areas where their correct function is of utmost importance, such as in critical infrastructures. Clearly, immersing them into new environments where they can collect and transmit data will have clear consequences for privacy. For some systems we understand the threat model, but we do not know how to fix it (RFID tags), while for others we need further investigation to understand the risks.

Even though some devices will increase their capabilities in the near future, certain parameters of such sensors will not change significantly over the next couple of years unless a new disrupting technology is found. For example, even though new nodes will run on better hardware, using less power, power management will remain of paramount importance for sensor networks. The security solutions need to be adapted to the special requirements of the environment in question, meaning that power management will still have a major influence on every piece of code running on nodes.

Over the years of Syssec, it has become clear that systems in the smart environment space are often systems of systems. As an example from above, the smart grid is a very large system of systems. The home is becoming a complex system of systems, where (in the future) some devices might even

record very sensitive health records of the occupants. The same holds true for an airplane or a modern car.

To better illustrate the problem, we can have a look at the modern car. Some parts are governed by compliance and are seen as a very critical piece of the car. These systems are developed very carefully, many times using formal methods. However, the overall platform is cost-sensitive. Other systems (such as the media player) are not developed as carefully and might contain less stringent code. In that these two systems can interfere with each other today, attackers can leap from one system to the next [11].

One of the gaps described in the previous roadmaps was the lack of methodologies to study and understand proprietary environments. The research community has responded to this point and several efforts to analyze embedded systems and firmware have been recently published [52]. However, other problems are intrinsic to the systems themselves. Looking at the electrical grid in the US as an example, it has been projected that just destroying a few substation might cause cascading failures to a national level. Such attacks do not need to be cyber attacks, but also simple physical coordinated attacks can cause havoc. Thus, the attacker will always target the easiest attack vector [46] [45]. Making such systems resilient is a major undertaking.

## 3.4 Cyberattacks

### 3.4.1 Overview

Another area that received predictions throughout the SysSec project is the area of Cyberattacks. Many different kinds of cyberattack threats were presented in the past deliverables and in our first research roadmap that were results of brainstorming and discussion within the SysSec Project, within the SysSec Working Groups throughout the held meetings, as well as discussions with experts in the field. The main prediction in the area of Cybersecurity was that the threats discussed in the project would have increasing impact in terms of security in computing systems and networks in the following years.

In the following subsection we briefly discuss to what extend such a prediction holds true for the different kinds of cybersecurity threats identified throughout the project. The identified threats were new and emerging types of cyberattacks, such as attacks on and by mobile phones and other such highly-connected smart appliances, web attacks on home and office automation devices, cross-domain attacks, attacks on individual citizens as well as infrastructure, etc.

### 3.4.2 Previous assumptions

- **Web Services and Applications**

  As described in our first roadmap (Deliverable 4.1), services represent the core value in the web, and by extension in the network in general. Unfortunately, these services can be misused by attackers to fulfil their malicious intentions, as new services arising are bound to have security flaws. As argued during our first research roadmap, the source of this problem is twofold. First of all, new software typically tends to be more vulnerable as all its quirks and bugs may have not been eliminated during the testing phase. Second, there is a tremendous pressure and urgency in companies to push out new and appealing services for end users, which in turn leads to higher chances of security flaws creeping into the software, as features take precedence over security.

  Moreover, several consequences were identified on the end user security stemming from this reasons with both financial and social impact. The assumption there was that *users have come to depend on these online services in their daily lives*. Moreover, *as phones, tablets and other smart devices are used to access such services, this will lead to an increase of the aforementioned cyber attacks to web services and applications*. These assumptions are still accurate. There is an increase of the cyber attacks the last years. According to Kaspersky Lab's study titled "Financial cyber threats in 2013" [28], cyber-criminals are trying even harder to steal confidential data and money from bank accounts of the users by creating fake sites and web pages imitating financial organizations or internet resources. Moreover, in the same report Kaspersky mentions that an increasing number of banks offer electronic wallets, internet banking, phone banking and similar services, which as they state, has as a result an increase on online attacks, and they advise those banks to enhance their protection against financial cyber threats.

  A detailed description of research in this area is given in Deliverable 5.4 (Intermediate Report on Internet Fraud) and D7.4 (Advanced Report on Cyberattacks).

- **Social Networks & Privacy**

  Another topic that the Cyberattacks working group focused its attention on throughout the SysSec project was related with the impact that data collection, data aggregation and data usage could have on users privacy and hence on citizens privacy in general. As discussed in our first and second research roadmap (Deliverable 4.1 and 4.2 respectively) as well as in the Red Book, data put on the Internet have changed so that they are no longer purely encyclopedic in nature but

they are much more related with personal information. This trend has been facilitated by the growth of social networking sites. In recent years many of them have popped up such as `Facebook`, `MySpace`, `Orkut`, `Twitter`, `LinkedIn`, and others which were massively adopted rapidly by the public.

Unfortunately, the users of such online communities have become targeted by attackers for a variety of purposes, including stalking, identity theft, spamming, direct advertising, spreading of malware, etc. The reason of such incidents is the plethora of personal information that users reveal on such sites. Users do not hesitate to disclose information about their email address, their education, their family information, places they visited, their preferences etc. to such sites. Such vast amount of information can be valuable for attackers in order to launch their targeted attacks. Moreover, attackers can correlate information that users upload to other online sources like blogs and online forums in order to exploit their targets more easily.

In the Red Book it was stated that *"As such technology is continuously being integrated into our lives, it is to be expected that more information will be gathered and more people will be affected in the future"*. This assumption is still valid, as more and more attacks have been seen the recent years on such social networks [39, 48] and as many studies state that users do not give adequate attention to their privacy as the majority of them have the privacy settings disabled [31, 17]. As a result, computer security companies encourage social network users to protect themselves from social attacks through advises [32].

- **Critical Infrastructures**

  A different focus concerns the area of Critical Infrastructures (CI), which are systems or assets that are vital in modern society and economy. Examples of such systems are water supply, electricity, transportation, financial services, health care and telecommunication. A survey of the security risks that these systems pose, past incidents and the state-of-the-art solutions to such issues is included in the Red Book. The main and general assumption that was made for those systems was that *the threat and risks posed will continue to be of importance* as the set of what is considered critical infrastructure continues to grow. This assumption is still valid if we consider the recent threat on supervisory control and data acquisition (SCADA) systems which found more than 60,000 of them exposed online with vulnerabilities that could be exploited to take *full control of systems running energy as well as chemical and transportation systems* [16]. Moreover, recently Homeland Security announced that US-CERT processed approximately 190,000 cyber incidents involving Federal agencies, criti-

cal infrastructure and the Department of Homeland Security's industry partners, that is equivalent to 68% increase of critical infrastructure threats from 2011 to 2012 [30]. This lead the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework for the protection of critical infrastructure [43]. All these incidents, as well as recent studies showing that cyber threat is moving to critical infrastructure [18] proves that the aforementioned assumption is still accurate.

- **Smart, Mobile and Ubiquitous Appliances**

  As already discussed in 3.2.1.1, malicious software targeting mobile devices is a fact. Assumptions about mobile malware and smartphone devices have partially been discussed in 3.2.1.1. Another assumption that was made about mobile malware is that *one possible source is malicious applications that the users installs without realizing its true intentions*. That is, users are willing to download applications from online sources like appstores and they become trained to run them and *accept without thinking* pretty much any request the applications may make and the potential risks that may be associated with them. This assumption is still accurate as most of the mobile malware tries to exploit end-user ignorance in order to compromise the smart devices [8, 51].

  Another assumption was made about the other form of devices that have started to become capable to connect to the Internet (Internet of Things). The assumption there was that *such devices will be very much vulnerable to similar types of attack vectors as the traditional commodity systems, customized for each specific device*. Although, this kind of appliances are not yet part of our lives, some of them, like medical appliances such as pacemarkers and other devices like home security video cameras [22, 44, 13], have been shown to be vulnerable to attacks. These facts partially show that the aforementioned assumption is still valid. More such incidents are expected in the near future.

- **Network Core Attacks**

  The general assumption for the core Internet infrastructure was that it will continue to be under threat by miscreants. In the first SysSec research roadmap (Deliverable 4.1), there was stated that core Internet is also an enabler of other, more complex, attacks. Thus arose the following assumption: *we expect to continue seeing attacks such as: attacks on routers, attacks on DNS, Denial of Service, etc*. This assumption is still true as many incidents of such kind of attacks have been seen recently [40, 35] and we believe that it will continue to be valid for the foreseeable future.

In the second research roadmap (Deliverable 4.2), we discussed the role of how important the Internet is in communications, as the traditional telephony network is migrating onto the Internet and other services as well like television, videogaming etc.. The assumption there was that *such services are prime candidates for todays attackers, and a simple way of attacking such services is by taking down the underlying functionality inside the network core.* This assumption is still accurate as many such attacks have appeared recently [12, 38].

### 3.4.3 Research

Many aspects of our daily life including communication, economy, national security depend on a secure cyberspace. Cyberattacks have increased dramatically in recent years with negative consequences from personal information thievery, and damage to commercial interests to the even more serious ones like damage to the economy, national security, the environment or human welfare.

Cybersecurity research is one of the most important aspects of security. And this is not expected to change as attackers have started to focus against specific web services and applications and end devices such as smartphones and tablets. Furthermore, as the concept of Internet of Things is becoming a reality with more and more appliances to connect to the Internet, this will provide a fertile ground for future cyberattacks targeting an entirely different ecosystem.

During the meetings with the experts, it was decided to conduct research in the field of cyberattacks. An overview on the most relevant publications in this area can be found in Deliverable 7.4, the advanced report on Cyberattacks. Research in this field will continue to evolve. The dawn of the *Internet of Things* is expected to be paralleled by new forms of cyberattacks. The need to thwart these threats will result in a multitude of new research directions.

# 4 Future Roadmap

## 4.1 Introduction

In the Red Book we broadened the scope of our study, discussing and proposing open problems in most of the areas of system security. However, for this final document we decided to go back to a more concise roadmap (as proposed in "D4.2: Second Report on Threats on the Future Internet and Research Roadmap") that only emphasize a limited set of key research directions.

As we discussed in the previous chapter, all the topics we proposed in the past four years of the Syssec project are still relevant today. However, based on the opinions we collected from the external experts who collaborate with the three working groups, we decided to update the final roadmap with two changes. First, we decided that the security of embedded devices deserved its own category, focused in particular on the security of the Internet of Things. Second, we updated the list of key emerging technologies that need to be quickly secured, due to their relevance and the current amount of research in the field. In this case, the list was extended with the addition of the Medical sector.

The result is a roadmap composed of the following six areas:

- *System Security Aspects of Privacy*
  with a special focus on big data analysis and correlation.

- *Targeted Attacks*
  with a special focus on data collection and on preventing social engineering attacks.

- *Security of New and Emerging Technologies*
  with a special focus on Cloud Computing, Critical Infrastructures, Social Networks, and Medical Devices.

- *Mobile Security*
  with a special focus on containing the information leaks and on the use of hardware-assisted virtualization.
- *Usable Security*
  with a special focus on interdisciplinary efforts to improve authentication, and management of personal information.
- *Security of Embedded Devices*
  with a special focus on the Internet of Things.

Most of these topics have already been extensively described in the previous roadmaps and in the Red Book. In the rest of the chapter we focus on the changes we introduced during the fourth year of the project.

## 4.2 New Roadmap Direction: Security of Embedded Devices

Embedded systems are omnipresent in our everyday life. For example, they are the core of various Common-Off-The-Shelf (COTS) devices such as printers, mobile phones, home routers, and computer components and peripherals. They are also present in many devices that are less consumer oriented such as video surveillance systems, medical implants, car elements, SCADA and PLC devices, and basically anything we normally call *electronics*. The emerging phenomenon of the Internet-of-Things (IoT) will make them even more widespread and interconnected.

All these systems run special software, often called *firmware*, which is usually distributed by vendors as *firmware images* or *firmware updates*. Several definitions for *firmware* exist in the literature. The term was originally introduced to describe the CPU microcode that existed "somewhere" between the hardware and the software layers. However, the word quickly assumed a broader meaning, and the IEEE Std 610.12-1990 [1] extended the definition to cover the *"combination of a hardware device and computer instructions or computer data that reside as read-only software on the hardware device"*.

Nowadays, the term *firmware* is more generally used to describe the software that is embedded in a hardware device. Like traditional software, embedded devices' firmware may have bugs or misconfigurations that can result in vulnerabilities for the devices which run that particular code. Due to anecdotal evidence, embedded systems acquired a bad security reputation, generally based on case by case experiences of failures. For instance, a car model throttle control fails [24] or can be maliciously taken over [10, 29]; a home wireless router is found to have a backdoor [25, 4, 23], just to name a few recent examples.

Manual security analysis of firmware images yields accurate results, but it is extremely slow and does not scale well for a large and heterogeneous dataset of firmware images. As useful as such individual reports are for a particular device or firmware version, these alone do not allow to establish a general judgment on the overall state of the security of firmware images. Moreover, devices may also be branded under different names but may actually run either the same or similar firmware. Such devices will often be affected by exactly the same vulnerabilities, however, without a detailed knowledge of the internal relationships between those vendors, it is often impossible to identify such similarities. As a consequence, some devices will often be left affected by known vulnerabilities even if an updated firmware is available.

As a result, we believe that much research is needed in the area of embedded device security.

## 4.3 Special Focus on the Internet of Things

As already mentioned in the Red Book, one key factor that has changed in the Internet world nowadays is its *complexity*. In the past years there were only interconnected computers that constituted the whole Internet. Today, more and more devices like smart devices, smartphones and tablets are beginning to connect to the Internet. Moreover, we are moving into a new era with a tremendous variety of Internet-enabled devices. Such devices will vary from home appliances and security systems to public transport vehicles and conventional cars. This new world where any device will be able to connect to the Internet is called *Internet of things*. This Internet of things, as stated in the Red Book, is a future for communication and computing devices that has already begun.

This growth in devices' Internet connectivity is at an all-time high and is showing no tendency to slow down. According to Gartner [21], the Internet of things will grow to nearly 26 billion devices by 2020. Similarly, ABI Research estimates that by the end of the same year there will be more than 30 billion devices wirelessly connected to the Internet of things [41].

### 4.3.1 A new era of security issues

Apparently, this growth of Internet of things establishes new opportunities for technological development and advances. On the other hand, along with every new technological development come new kinds of cyber-security threats that target this development. These new kinds of threats are becoming very serious as the devices from the Internet of things, such as wearable devices or smart appliances etc., are starting to collect and aggregate personal information. Pieces of information such as the geolocation, the time

and recurrence can be used in order to draw conclusions that may affect the privacy of the user.

Users seem to be very aware of the security risks that threaten their computers and of mobile malware that targets their mobile devices. Unfortunately, a very small minority of users are aware of the threats that may target the diverse set of different devices in the Internet of things. For this reason, there is a need for well-established protection mechanisms designed in a user friendly fashion.

### 4.3.2 A series of unfortunate threats

Although the Internet of things is still in the early stages, many examples of threats have surfaced confirming the need for protection measures already mentioned. Below, there is a list with some threats recently discovered to target the "Internet of things".

- **Linux.Darlloz** [47]. Kaoru Hayashi recently found a new kind of worm that target hidden devices such as home routers, set-top boxes, and security cameras that run the Linux operating system.
- **Linux.Aidra** [3]. This malware targets small devices like cable and DSL modems that later adds to a botnet, and are available for attackers in order to perform denial-of-service (DDoS) attacks.
- **Vulnerable security cameras** [13]. Internet-connected home security video cameras with faulty software that leave them open to online viewing, and in some instances listening, by anyone with the cameras Internet address.

### 4.3.3 Recommendations and Research Directions

There is a need for protection mechanisms for the different devices that can participate in the Internet of things. Protection mechanisms that are already well-established and currently deployed in conventional computing systems and mobile devices, may be inappropriate for the devices of Internet of things. We recall some of the problems that these solutions may suffer from, which we have already mentioned in the Red Book, and should be carefully and well understood when designing protection mechanisms:

- **Simplicity**: Usable security must be simple. A normal user cannot be willing to deal with the task of creating a security policy for accessing the Internet, for example. Therefore, very complicated methods of securing a device are bound to be rejected by the masses.
- **Transparency:** Even security-aware users can not always deduce how a system works and where the possibilities for attacks arise. A good

example here is a registered e-mail address that is used somewhere else without notification to identify a user. There are threats for some users that cannot be anticipated without a deeper knowledge of the underlying system.

- **Restrictiveness:** Most security solutions impose restrictions on their users. Passwords must be entered and memorized, device locks must be removed before using a device, firewalls prohibit unconfined network usage, etc. Users who see their devices as tools to do a job, which simply have to work properly, will gladly sacrifice security for convenience if given the choice. Therefore, the choice of which options to give the end-user for circumventing or re-defining security-critical aspects has to be a well-considered one.

## 4.4 New Emerging Domain: E-health and implantable devices

In the past years, we discussed few new domains that we believed needed a special attention from the system security community. The list includes *Social Networks*, *SCADA* and *Smart Meters* infrastructures (or more in general, what now goes under the umbrella of Critical Infrastructures), and *Cloud Computing*. This year we decided to add the *medical domain*, both in terms of security of implantable and medical devices, and in terms of public information and electronic health systems.

The first point is related to the security of embedded devices, already presented in the previous section. Networked medical devices are more and more common, and their security and reliability is paramount for the physical safety of patients. If an attacker can remotely control or just take down one of these systems during operation, people may get injured or even die. And as it happened for some of the other domains we mentioned, also medical devices were designed by engineers trained in their domain and with no experience in computer security. Again it will be a race between researchers trying to secure these systems and attackers trying to gain some profit by exploiting them.

The second point in the medical domain is instead related to the privacy of medical records, and of other medical information collected from user devices. For instance, the collection of information of the nutrition habits of a user as drawn by the regular purchase of different food types, may divulge religion or ongoing health concerns [15]. This is one major security risk among the others that arises from the Internet of things world which should be carefully addressed. This is not a research direction per-se, as we witnessed similar problems with other technologies (such as social networks).

However, it is a new emerging domain that needs to be investigated, as medical information must remain private and under control of the users.

## 4.5 Technologies that will disappear in the next ten years

If predicting new technologies that will rise in the next decade may be a futile exercise, trying to forecast which technology will disappear may be an easier task. To test the experts who participated to our meeting in Brussels, we asked them to write their opinion on colorful post-it notes that were then used to drive the discussion and brainstorming session (similar to what we did during the second year to investigate the future of cybercrime).

The question was simple: "*Which technology do you think that will disappear in the next 10 years, and which are the consequences for security?*"

From the tens of answers we collected, three were repeated multiple times by different experts:

**Face-to-Face meetings** Video conference systems are already in use in many organizations, and they are rapidly improving in terms of quality and provided features. It is reasonable to believe that in the next 10 years we will observe a decline in face-to-face meetings, that will be replaced by sophisticated two- or three-dimensional video conferencing software.

At a first look, this may not seem too relevant for security. However, it is enough to look back at the recent widespread surveillance mechanisms adopted by several governments to understand the impact of this change. Both, telephone and Internet communication are routinely wiretapped, even when cryptographic tools are used (e.g., TOR networks). Live meetings are now the only way to communicate that is still out of reach of a nation-wide surveillance system. If these face-to-face meetings were to disappear, it is going to be difficult to enforce the privacy of our communication. Even worse, when virtual meetings will be the rule and not the exception, people meeting in person will be automatically flagged as suspicious and they will inevitably attract the attention.

Moreover, virtual meetings will open the door to new classes of sophisticated impersonation attacks, similar to what is now done by spoofing email addresses.

**Paper Money** Tech evangelist Sam Pitroda predicted that paper money will disappear by 2040 [2], replaced by online transactions. Our experts believe that in some countries this might actually happen sooner than that, even as soon as 10 years from now. Such a big change in the society will certainly have a number of consequences also in the world of system security. One immediately comes to mind: Electronic payments are traceable. Nowadays is still possible to pay cash for small purchases, and thus achieve a little anonymity. But privacy will be harder to enforce without paper money. Pre-paid cards are now anonymous, because they can be paid in cash. When this will not be possible anymore, anonymous and untraceable payment systems (such as Bitcoins) will gain popularity – and maybe even risk to become illegal.

**Hard Copies of Documents** This is an ongoing transformation, and paperless offices already exist all around the world. However, governments and institution still keep hard copies of important documents in their archives. When all the information and human knowledge will exist only in digital form, the possibility for attackers to forge and manipulate information will have an even more serious impact on our society. Identity stealing and impersonation attacks may reach a different level of sophistication, making it very hard to distinguish what is real and what has been falsified by an attacker.

## 4.6 Conclusion

This deliverable presented a critical summary of the threats and of the research topics discussed over the past four years in the three working groups: Malware and Fraud, Smart Environments, and Cyberattacks. It also presented an updated discussion of what has changed since the publication of the Red Book, exactly one year ago. Several important events have affected the system security landscape, starting from the NSA surveillance scandal. We discussed the impact of such changes with a number of international experts who collaborate with our working groups, and we concluded that while the scale and origin of the new threats was certainly unexpected, the technical details of these operations were instead not surprising. In fact, most of them had been largely anticipated by our previous roadmaps.

Based on this discussion, in this chapter we presented an updated version of the Research Roadmap in System Security. While all the topics we presented so far are still actual and important today, we decided to extend the roadmap with a new research direction (i.e., the security of embedded devices and of the Internet of Things) and with a new emerging area (i.e., the medical sector, including both the security of implantable devices and of public electronic-health systems).

Finally, we tried to look forward in the future - moving the horizon of our discussion to ten years from now. In this experiments we did not focus on the new technologies that will appear, since this is extremely difficult in our field, but on the ones that will likely disappear – and on their impact on the security and privacy of our society.

We believe that the study we conducted in the Syssec project on the future threats of our field, in particular in the form of the Red Book, will serve as useful reference for future research in our area.

# Bibliography


[1] IEEE Standard Glossary of Software Engineering Terminology. *IEEE Std 610.12-1990*, pages 1–84, 1990.

[2] Paper money will disappear in 30 years. Internet. http://ibnlive.in.com/news/paper-money-will-disappear-in-30-years-sam-pitroda/130784-11.html,, 2010.

[3] Lightaidra - embedded linux device botnet, 2013. http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices.

[4] Slashdot: Backdoor found in TP-Link routers, March 2013.

[5] Mark Anderson. Black Hat 2014: Hacking the Smart Car. http://spectrum.ieee.org/cars-that-think/transportation/systems/black-hat-2014-hacking-the-smart-car/?utm_source=carsthatthink&utm_medium=email&utm_campaign=082014, 2014. [last visit August 2014].

[6] Graeme Baker. Schoolboy hacks into city's tram system. http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html, Jan 2008. [last visit August 2014].

[7] European Central Bank. Third report on card fraud, 2014. http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf.

[8] Tom Brewste. Beware of malicious android icons in disguise, 2014. http://www.knowyourmobile.com/android-apps/android-malware/22060/beware-malicious-android-icons-disguise.

[9] Cesar Cerrudo. Hacking Washington DC traffic control systems. http://blog.ioactive.com/2014/07/hacking-washington-dc-traffic-control.html, July 2014. [last visit August 2014].

[10] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 6–6, Berkeley, CA, USA, 2011. USENIX Association.

[11] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al.

Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*, 2011.

[12] Mark Clayton. Internet-based attacks hit emergency call centers. what's the damage?, 2013. http://www.csmonitor.com/USA/2013/0404/Internet-based-attacks-hit-emergency-call-centers.-What-s-the-damage.

[13] Federal Trade Commission. Marketer of internet-connected home security video cameras settles ftc charges it failed to protect consumers' privacy, 2013. http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

[14] APWG Internet Policy Commitee. Global phishing survey: Trends and domain name use in 1h2013, 2013. http://docs.apwg.org/reports/APWG_GlobalPhishingSurvey_1H2013.pdf.

[15] ComputerWeekly. The internet of things is set to change security priorities, 2014. http://www.computerweekly.com/feature/The-internet-of-things-is-set-to-change-security-priorities.

[16] Darlene Storm (Computerworld). Hackers exploit scada holes to take full control of critical infrastructure, 2014. http://blogs.computerworld.com/cybercrime-and-hacking/23402/hackers-exploit-scada-holes-take-full-control-critical-infrastructure.

[17] Paul Cooper. Companies still falling for social engineering attacks, 2013. http://www.itproportal.com/2013/10/31/companies-still-falling-for-social-engineering-attacks/.

[18] critical-study 1. Cyber threat moving to critical infrastructure, study shows, 2014. http://www.computerweekly.com/news/2240217851/Cyber-threat-moving-to-critical-infrastructure-study-shows.

[19] National Cybersecurity and COmmunications Integration Center. ICS-CERT Monitor. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Oct-Dec2013.pdf, 2013.

[20] National Cybersecurity and COmmunications Integration Center. ICS-CERT Monitor. https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_20Jan-April2014.pdf, 2014.

[21] Gartner. Gartner says the internet of things installed base will grow to 26 billion units by 2020, 2013. http://www.gartner.com/newsroom/id/2636073.

[22] 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.

[23] Craig Heffner. Reverse Engineering a D-Link Backdoor, October 2013.

[24] Jerry Hirsch and Ken Bensinger. Toyota settles acceleration lawsuit after $3-million verdict. Los Angeles Times, October 25, 2013.

[25] Independent Security Evaluators. SOHO Network Equipment (Technical Report), 2013.

[26] Willie Jones. How Fast You Drive Reveals Where You Drive. http://spectrum.ieee.org/cars-that-think/transportation/sensors/researchers-reconstruct-cars-driving-paths-using-only-speed-data/?utm_source=carsthatthink&utm_medium=email&utm_campaign=082014, Aug 2014. [last visit August 2014].

[27] Markus Kammerstetter, Markus Muellner, Daniel Burian, Christian Platzer, and Wolfgang Kastner. Breaking integrated circuit device security through test mode silicon reverse engineering. In *21st ACM Conference on Computer and Communications Security (CCS)*, 2014.

[28] Kaspersky. Financial cyber threats in 2013, 2014. http://media.kaspersky.com/en/Kaspersky-Lab-KSN-report-Financial-cyber-threats-in-2013-eng-final.pdf.

[29] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental Security Analysis of a Modern Automobile. In *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, SP '10, pages 447–462, Washington, DC, USA, 2010. IEEE Computer Society.

[30] Infosecurity Magazine. Dhs: Critical infrastructure threats up 68% in 2012, 2013. http://www.infosecurity-magazine.com/news/dhs-critical-infrastructure-threats-up-68-in-2012/.

[31] McAfee. Cyberbullying triples according to new mcafee "2014 teens and the screen study", 2014. http://www.mcafee.com/us/about/news/2014/q2/20140603-01.aspx.

[32] Robert Siciliano (McAfee). How to protect yourself from social spam, 2013. http://blogs.mcafee.com/consumer/how-to-protect-yourself-from-social-spam.

[33] Yan Michalevsky, Dan Boneh, and Gabi Nakibly. Gyrophone: Recognizing speech from gyroscope signals. In *23rd USENIX Security Symposium (USENIX Security 14)*, pages 1053–1067, San Diego, CA, 2014. USENIX Association.

[34] Charlie Miller and Chris Valasek. A Survey of Remote Automotive Attack Surfaces. http://www.ioactive.com/pdfs/Remote_Automotive_Attack_Surfaces.pdf, 2014. [last download August 2014].

[35] Nominum. An introduction to dns based ddos amplification attacks, 2014. http://nominum.com/wp-content/uploads/Introduction-to-DNS-Based-DDoS-Attacks.pdf?aliId=84570.

[36] Nicole Perlroth. Traveling Light in a Time of Digital Thievery. http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all&_r=0, Feb 2012. [last visit August 2014].

[37] Proofpoint. Proofpoint Uncovers Internet of Things (IoT) Cyberattack. http://www.proofpoint.com/about-us/press-releases/01162014.php, Jan 2014. [last visit August 2014].

[38] John Leyden (The Register). Spamhaus-style ddos attacks: All the hackers are doing it, 2013. http://www.theregister.co.uk/2013/06/03/dns_reflection_ddos_amplification_hacker_method/.

[39] John Leyden (The Register). Hackers pose as hacks: Iranian crew uses facebook to spy on us defence bods report, 2014. http://www.theregister.co.uk/2014/05/30/fake_journos_iranian_spy_caper/.

[40] Richard Chirgwin (The Register). Team cymru spots 300,000 compromised soho gateways, 2014. http://www.theregister.co.uk/2014/03/04/team_cymru_ids_300000_compromised_soho_gateways/.

[41] ABI Research. More than 30 billion devices will wirelessly connect to the internet of everything in 2020, 2013. https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne.

[42] Symantec Security Response. Dragonfly: Western Energy Companies Under Sabotage Threat. http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat, 2014. [last visit August 2014].

[43] Homeland Security. Protecting our nations critical infrastructure from cyber threats, 2014. http://www.dhs.gov/protecting-our-nations-critical-infrastructure-cyber-threats.

[44] Mellisa Tolentino (SiliconANGLE). Pacemakers under attack: When the internet of things gets sick, 2014. http://siliconangle.com/blog/2013/08/20/pacemakers-under-attack-when-the-internet-of-things-gets-sick/.

[45] Rebecca Smith. Grid Terror Attacks: U.S. Government Is Urged to Take Steps for Protection. http://online.wsj.com/articles/grid-terror-attacks-u-s-government-is-urged-to-takes-steps-for-protection-1404672 Jul 2014. [last visit August 2014].

[46] Rebecca Smith. U.S. Risks National Blackout From Small-Scale Attack. http://online.wsj.com/news/articles/SB10001424052702304020104579433670284061220, Mar 2014. [last visit August 2014].

[47] Kaoru Hayashi (Symantec). Linux worm targeting hidden devices, 2013. http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices.

[48] Per Liljas (TIME). Teens are now bombarding airlines with fake bomb threats, 2014. http://time.com/62978/american-airlines-twitter-teen-bomb-threat/.

[49] Andrew Trotman. Volkswagen sues UK university after it hacked sports cars. http://www.telegraph.co.uk/finance/newsbysector/industry/10211760/Volkswagen-sues-UK-university-after-it-hacked-sports-cars.html, Jul 2013. [last visit August 2014].

[50] European Geosciences Union. Press Release: Using moving cars to measure rainfall. http://www.egu.eu/news/85/using-moving-cars-to-measure-rainfall/, Nov 2013. [last visit August 2014].

[51] Webroot. The wild, wild west of mobile apps, 2013. http://www.webroot.com/shared/pdf/WildWildWest_MobileAppReputation.pdf.

[52] Jonas Zaddach, Luca Bruno, Aurelien Francillon, Davide Balzarotti, and France EURECOM. Avatar: A framework to support dynamic security analysis of embedded systems firmwares. 2014.