SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Secure, dependable and trusted Infrastructures

COORDINATION ACTION

Managing Emerging Threats in ICT Infrastructures

Grant Agreement no. 216331

Deliverable D2.1.x
Threat Reports

Contractual Date of Delivery	31/03/2009
Actual Date of Delivery	15/05/2009
Deliverable Security Class	Public
Editors	Working Group Leaders
Contributors	FORWARD Consortium
Quality Control	M. Almgren, H. Bos, S. Ioannidis, E. Kirda, and K. Marakomihelaki

The FORWARD Consortium consists of:

Technical University of Vienna	Coordinator	Austria
Institut Eurécom	Principal Contractor	France
Vrije Universiteit Amsterdam	Principal Contractor	The Netherlands
ICS/FORTH	Principal Contractor	Greece
IPP/BAS	Principal Contractor	Bulgaria
Chalmers University	Principal Contractor	Sweden

Contents

Chapter 1

Introduction: FORWARD Threat Reports

This document is the compilation of the three threat reports that were produced independently by the three FORWARD working groups during the second phase of the project. These working groups were established after the first FORWARD workshop that was held in Goteborg, Sweden in April 2008. They are briefly described in the following paragraphs:

The *Malware and Fraud* working group is concerned with the malware and fraud-related threats on the Internet. It covers topics that range from novel malware developments over botnets to cyber crime and Internet fraud.

The *Smart Environments* working group is concerned with ordinary environments that have been enhanced by interconnected computer equipment. There is general expectation that a large number of small devices such as sensors and mobile phones will be interconnected. The group aims to identify emerging trends with respect to security in this domain.

The *Critical Systems* working group focuses on critical systems whose disruption of operation can lead to significant material loss or threaten human life. It attempts to identify emerging threats in this area.

For our work, we introduce the following definition of threat:

Threat - Definition : A threat is any indication, circumstance, or event with the potential to cause harm to an ICT infrastructure and the assets that depend on this infrastructure.

Our version is related to a variety of other definitions that exist in the literature, such as the ones provided by *ISO/IEC* and the *EU Green Paper for Critical infrastructure protection, 2005* [20]. In both cases, a threat is described as a event, circumstance, or incident that has the potential to cause destruction or, more general, harm to the system or organization that is exposed to the threat. We adapt our definition to explicitly refer to ICT infrastructures and assets, as this is the scope

of the project. However, we observe that the definition is reasonably general to accommodate a wide range of possible threats and scenarios. This is necessary to allow different working groups to identify interesting threats without being constrained by an overly narrow, initial definition.

Creating a list of emerging and future threats is a challenging endeavor. The past has witnessed many stunning scientific and technical advances, and these advances have transformed society and the way people use and rely on information technology. Of course, also attackers are creative and constantly invent new ways of abusing technologies and applications for financial profit or simply because they enjoy virtual vandalism. Thus, trying to imagine potential developments is always at risk of failing to accurately predict the future. Nevertheless, it is important to actively think about the potential risks and threats that emerging technologies and their applications entail. Otherwise, one would simply concede to the adversaries and, at most, react to their new attacks.

One way to think about emerging and future threats is to bring together a group of domain experts and let them enter a dialogue in which they will (hopefully) come up with a set of possible threats. This is one possible way, and in part an approach that FORWARD leverages through its working groups. However, it would be desirable to introduce a more systematic methodology to think about emerging threats. In FORWARD, we attempt to do this by introducing a number of "axes" along which developments can happen (or are currently unfolding). These axes serve as the main drivers of development in general, and allow us to set a framework in which each working group can systematically explore threats. Our four axes are the following:

- **New technologies:** With new technologies, we refer to technical advances that provide functionality that simply was not there before. Clearly, this is very difficult to predict, but there are certain drivers, such as Moore's law, that have been valid over a long period of time. Extrapolating these steady trends, we foresee much faster networks (both wired and wireless), a substantial increase in parallelism (multi-core machines), and better energy and battery technology. Also, computing devices will become increasingly smaller and cheaper. As a result, they will become more widespread, and they can support more and richer applications.

- **New applications:** New applications refer to completely new uses of technology, uses that typically did not exist before or do not have a counterpart in the real world. One important class of new applications are social networks, tools that have rapidly reached a significant fraction of the population and that support social interactions among large user groups. Another interesting class of new applications is the idea of software as a service. This buzzword characterizes a model in which applications are hosted by providers on a large-scale computing infrastructure, such as a cloud. This deployment and computing model is profoundly different from the traditional client-server model, and thus, we need to consider its security implications.

- **New business models:** With new business models, we refer to the fact that certain services or applications that might exist already in some form increasingly start to rely on a working ICT infrastructure. For example, online shopping, online banking, and even e-government would be considered new business models in our taxonomy. That is, these services did exist before (as retail stores, banks, and offices), but they are now increasingly carried out via ICT. Also, these services do not represent a fundamentally different application, since they are typically instances of well-known models of computing that are simply adapted to suit the business case.

- **New social dynamics and the human factor:** The category of new social dynamics and the human factor takes into account possible changes in the way that people approach and use technology and certain applications. For example, one can consider the fact that young people get increasingly sophisticated with ICT, but we also have to consider the trend that people are increasingly willing to entrust devices and applications with a significant amount of private information. This opens the possibility for new, emerging threats.

In each working group report, we will see the four axes as a guideline to think about possible advances. These advances will then drive the discussion and anticipation of novel threats. Moreover, it is important to observe that the reported threats are not "invented" by the project partners, but reflect the views of all experts that are members of a working group. The role of the project partners is that of moderators, scribes and guides, who steer the working group during discussions and collect and maintain their findings. The threats and discussions compiled in the threat reports originate from e-mail discussions, phone conferences, and in-person working group meetings.

In addition to the ongoing process in the working groups, we also used the second workshop as a means to checkpoint the threats in discussions with a large audience of experts (more than 100 attendees from academia, industry, and government institutions). In these discussions, we attempted to ensure that our lists of threats are as comprehensive as possible. And indeed, there were a few updates to the threats in each working group. These updates are already reflected in the following reports. This also explains why these reports are delivered after the point in time initially foreseen in the proposal. Together with the project officer, we found it useful to wait for the results of the second workshop before finishing the threat reports. This allowed us to consider the updates and outcome of the second workshop.

In the following chapters, we introduce the three threat reports that were compiled by the three working groups of the FORWARD project. In these reports, we will see how each working group has forecast possible technological and societal developments, and how the group has mapped these projected developments into emerging and future threats. It is important to note that the reports contain the

threats and the trends that the working groups have independently identified in their particular domains. As a result, some threats are similar. For example, the Malware and Fraud working group has listed mobile malware as an emerging threat. Similarly, the Smart Environments working group is also discussing this threat in its report. As some of the threats are multi-faceted, it is not surprising that there is a certain overlap between some of the threats. It is the goal of the third phase of the FORWARD project to identify such overlapping threats, by condensing them into a coherent white book. Moreover, the reports do not yet contain a risk assessment for individual threats. This risk assessment, that is, our view on the severity of each threat, is also part of the inter-working-group discussion and alignment that are part of the third project phase.

Chapter 2

Working Group: Fraud and Malware

2.1 Introduction

The Internet has become an indispensable part of our lives. Undoubtedly, Internet applications have become the most dominant way to provide access to online services. Every day, millions of users purchase items, transfer money, retrieve information and communicate over the Internet. Although the Internet is convenient for many users because it provides anytime, anywhere access to information and services, at the same time, it has also become a prime target for miscreants who attack unsuspecting Internet users with the aim of making an easy profit. The last years have shown a significant increase in the number of Internet-based attacks, highlighting the importance of techniques and tools for increasing the security of the Internet. For example, online banking web sites all over the world are frequent targets of phishing attempts and there has also been extensive press coverage of recent security incidences involving the loss of sensitive credit card information belonging to millions of customers.

The malware and fraud working group, as used in the context of the FORWARD project, is concerned with the malware and fraud-related threats on the Internet. Fraud and malware are closely related to each other as many attacks that are launched use malware (e.g., Trojans, worms) with the aim of stealing sensitive information for financial gains (e.g., credit card numbers, modification of online banking information, etc.).

2.2 About the threats

In this section, we discuss various threats that have been identified by the malware and fraud working group. As mentioned previously, we used four axis to drive our search for emerging and novel threats. In the following, we discuss the advances that we foresee, and how they influence emerging threats.

2.2.1 New technologies

We assume that the current technological trends with regards to increases in the speed of networks and the density of integrated circuits (IC) continue. This has a number of implications. For one, it is possible to build smaller devices that are more powerful. Thus, it is conceivable that mobile devices (such as smartphones) will become a major computing platform that provide anywhere access to the Internet. When the computing power of these devices increases, they will be used for more and more applications that will have access to an increasing amount of sensitive data. However, the improvements in computer hardware and networks also allow new computing models. In particular, it is possible to "outsource" computation to remote machines (such as the "cloud"). As a result, the perimeter between local data and computation is increasingly blurred, and potentially sensitive data is moved around on the Internet. Finally, we assume that IPv6 will eventually become widespread. This has implications for networks, as (a) most machines will become directly reachable and (b) the complexity increases because it is necessary to support multiple Internet protocols (IPv4 and IPv6) simultaneously.

We believe that novel technologies such as the ones outlined above provide new opportunities for malware authors. One reason is that these technologies will have defects that can be exploited. Another reason is that these technologies will increasingly transport and manipulate sensitive data that is valuable to attackers. As a result, we see emerging threats such as malware on mobile devices, malware in the cloud, and malware that exploits features of IPv6.

In addition to technological advances related to the ICT infrastructure and hardware, we also need to take into account new defense technologies. Clearly, security vendors have identified malware and fraud as one of the core problems on today's Internet, and finding more effective security solutions is a big business. This triggers an arms race in which the adversary has to improve existing attack technology to stay ahead of the game and to evade novel defense solutions.

We believe that we already see results of the arms race between security vendors and attackers. For example, cyber criminals have started and will likely continue to develop better and stealthier ways to manage botnets, and they already make use of the domain registration system to bypass IP-based blacklists and takedown attempts. In addition, security improvements on the client side (at the host level) will prompt attacks against weaker parts of the ICT infrastructure. In particular, we foresee attacks against the network management elements such as routers or switches. The reason is that controlling such a network element provides the attacker with the ability to tamper with the network traffic of a large amount of clients. Moreover, their security is unclear, and initial attempts to exploit network infrastructure devices (e.g., by the Phenoelite group) have proven to be promising.

2.2.2 New applications and business models

We see two main drivers in this domain. First, there is a substantial increase in the possibilities for people to move their social interactions (lifes) into cyber space, and people make increasingly use of these opportunities. The most obvious confirmation of this is the tremendous growth of social networks. For example, Facebook currently attracts several million new users every day. However, also other applications such as voice over IP (with Skype) or instant messaging are extremely popular. Of course, whereever people can get into contact, there is the potential for fraud. Similar to what we have seen with email, new ways to connect people can also be abused by cyber criminals to reach out to victims. A first glimpse can already be seen with spim (spam over instant messaging), but we expect a significant growth of attacks that exploit these new vectors of reaching out to people.

The second driver in the domain of new applications and business models is the substantial growth of the amount and importance of data that is exchanged and stored online. While eCommerce and online banking has been around for a while, there is work on simple and micro payment methods that allow more people to handle more transactions over the network. Clearly, this is beneficial from a business perspective, since the costs can be reduced. On the other hand, it provides an increasing number of vectors that criminals can exploit to make money. As a result of this shift of sensitive and financial information, we have witnessed the growth of a thriving underground economy and more and more sophisticated attacks against financial institutions. For example, attacks against banks started as simple phishing pages but are now typically in the form of sophisticated Trojan malware programs that intercept online transactions and redirect the money to criminals. These malware programs are so sophisticated that they will fake the balance sheet returned by the bank server in order to create the impression to the user that her transaction was carried out as expected.

2.2.3 New social dynamics and the human factor

One important new social dynamics, as mentioned above, is the shift of social interactions from the real world to online communities (be it social networks, worlds such as “Second Life,” or online games such as World of Warcraft). This can lead to an array of new possibilities for fraud. As a second, interesting driver, we witness that people are becoming increasingly aware of the risks that they are exposed to online. For example, it is not as easy for attackers anymore to have gullible victims fall for simple, mail-based fraud schemes (although it still happens far too often). As a result, the adversaries need to devise more sophisticated attacks, as can be seen when analyzing targeted attacks and spear phishing cases. That is, we expect increasingly sophisticated attacks and fraud schemes to offset the fact that users are (slowly) becoming more security aware and alert.

2.3 New technologies

2.3.1 Mobile device malware

Threat. Carrying a so-called smart mobile phone is almost like having a powerful computer today. In fact, smart phones that are sold today are as powerful as desktop PCs that were sold ten years ago. An increasing number of phones sold today include extensive online access, keyboards, and other typical computer functions. However, the power and convenience comes at a cost. Just as traditional computers face security threats, so do these mobile devices. Unfortunately, the larger the functionality becomes that these devices support, the more vulnerable they become to attacks. In the near future, it is highly probable that these devices will become susceptible to the same type of threats that plague our laptops and desktops.

The most common operating systems used by mobile phones and personal digital assistants (PDAs) are Microsoft Windows Mobile and the Symbian OS. Windows Mobile 2003 and Windows Mobile 6 are based on the Windows Mobile platform, which has a shared-source kernel strategy. Because of Microsoft's developer-friendly environment and shared-source policy for Windows Mobile, more phone manufacturers have begun to adopt it. At the same time, these same features are expected to attract more and more malware writers. The malware and fraud working group believes that malware for mobile devices should be an increasing concern for researchers and industry.

Currently, although there are known attacks against mobile devices [25, 26, 141], miscreants have not been targeting these devices on a large scale. This is probably because attacking traditional computers is easier and profitable currently. However, as users will increasingly use their mobile phones to surf, make purchases and communicate sensitive data, these devices will become interesting targets for attack. For example, some mobile network providers let their customers transfer money from their mobile accounts to other customers via SMS messages. Recently, a malware targeting mobile devices was discovered [69] that automatically transfers money to the attacker via such functionality.

The working group believes that mobile malware can be used to steal sensitive financial information if mobile devices become widespread financial instruments. Also, the working group envisions that these devices will be used in the future to track users, probably listen to their conversations (e.g., by remotely turning on the microphone), and black-mail individuals. It is also possible that mobile devices will become part of botnets once mobile Internet access becomes cheap and ubiquitous. In fact, mobile Internet access prices have been steadily decreasing in many EU countries.

Mulliner et al. [101] identified the integration of different communication techniques as a potential threat to a user. For example, integrating a GSM modem with a Wi-Fi network component into a single mobile device might open the user to the threat of malware that can cross the border of the individual transmission techniques. Such malware could infect the device through a vulnerability of the Wi-Fi

component and subsequently dial or send text messages to premium-rate numbers via the GSM modem.

In [99] the same author describes and implements attacks against current near field communication (NFC) enabled mobile phones. NFC today, is mainly used for mobile payment and ticketing. By modifying the information broadcasted by a NFC tag the authors succeeded in performing different attacks against NFC enabled phones. These attacks include denial-of-service and man-in-the-middle attacks. An attacker can perform URI spoofing with tags used for ticketing services to lure a user into calling premium-numbers instead of the legitimate ticketing number. Furthermore, the paper discusses and introduces a proof-of-concept NFC worm.

How malware targeting mobile devices propagates in mobile phone networks modeled and simulated in [30]. The propagation of malware that relies on other means of mobile communication and infection (e.g., messaging, Bluetooth) is in the focus of [14].

Possible solution(s). Current anti-malware solutions need to be adapted so that they can be used to detect and respond to mobile malware. Some work has already been going on in this area. However, the proposed solutions are still heavy weight and mobile devices still have performance and bandwidth problems.

Network service providers and GSM companies need to start thinking about how to mitigate the threat on the server-side, before it reaches the end users. To this end, Bechter and Freiling propose a mitigation strategy [8] where any application that is about to be installed on a mobile device is first transmitted to the network provider for analysis. This analysis executes the sample in a restricted environment (i.e., a sandbox) and monitors and records the behavior of the sample in terms of API calls. Such an analysis scheme closely resembles techniques applied by TTAnalyze [10] and similar tools on PC hardware and operating systems. Only if the analysis does not identify any malicious behavior in the sample it is allowed to be installed.

To mitigate the threat of mobile malware that crosses service boundaries, Mulliner et al. [101] demonstrate an approach that relies on resource labeling. During execution all processes and resources (e.g., files) on a smart phone are labeled with the network interfaces they have been in contact with. Whenever a process invokes a system call, its labels are compared against a global policy file that specifies whether the action should be allowed or not.

The Multimedia Messaging Service (MMS) is used to exchange messages between user agents running on mobile devices. Mulliner and Vigna proposed a system [100] that performs fuzzy testing of such user agent applications to reveal possible vulnerabilities. This approach identified multiple security vulnerabilities that allowed to compromise system security. In addition, they implemented a proof-of-concept attack that exploits one of the detected buffer overflow vulnerabilities to execute arbitrary code received through an MMS message.

2.3.2 Hardware security and threats

Threat. Since the early days of personal computing, malware writers took notice of the vast opportunities connected to computer hardware and certain restrictions, hardware vendors have to face in their development process. In general, malware targeted to specifically attack certain pieces of hardware has a good chance to stay undetected on the target system. However, a further categorization is necessary to properly explain the different attack vectors that will become significant in the near future.

Hardware-targeting code. Even though the attack vector in such a scenario is strongly related to common malware attacks, the target platform is a piece of hardware in the first place. A good example would be a piece of malware that reprograms the BIOS of the target machine to gain easier access. Another application would be to influence the behavior of voting-machines with a tailored firmware patch to specifically influence the outcome of an election. Whatever the final exploit may be, the hardware vendor is not automatically responsible for securing the components against unauthorized modifications. Operating system providers have to take care that these modifications are not possible but still provide a usable system. Therefore, defending against such attacks is mostly covered by today's malware research and anti-virus tools. Nevertheless, the possibly inflicted damage to the target system reaches from stealthy backdoors to damaged BIOS information, which may destroy a computer system.

Malicious hardware circuits. An even more serious attack vector is posed by the possibility to introduce whole sets of malicious hardware components. The principle behind this form of infection is quite simple. Instead of executing code on the target machine, the attacker makes sure that the implemented circuits inside the target system are already prepared to allow an attack on the target machine. Experiments have proven that is it possible to hide a backdoor circuit inside a CPU without any possibility to detect it from the same machine[72]. The backdoor was such that it allows an attacker to login as a root user after sending a magic packet to the target machine. Even though this form of an attack is deemed among the most powerful, it is not heavily used these days. The reason is that possible black hats need to gain access to the development process of large hardware suppliers such as Intel or Seagate. Then, they would need to modify the developed hardware with malicious circuits, but still keep the rest of the layout functional. Therefore, it is practically only for developers already working at such a company. Another possibility to introduce malicious circuits is by third-party vendors. Hard drive suppliers, for example, often out-source the production of the DMA controllers to low cost countries, where the integrity of the produced microchips are not guaranteed.

Ubiquitous Hardware Devices Just like malicious circuits introduced in computer systems, the threat of ubiquitous system being targeted by tailored attacks is

a very real one. In [38] for instance, the authors exploit the quite weak security structure of implantable medical devices (IMD), in this specific case a pacemaker to issue electric shocks directly to the heart of the victim. There are, of course, less critical system that are either portable, or otherwise counted among pervasive devices. With the growing possibilities to connect these devices, be it Bluetooth, WiFi, GSM or even Infrared, the implied security threats grow likewise. Exploiting these devices is pandered by their limited processing capabilities paired with the requirement to be functional and easy to use. As a result, these devices are often vulnerable to quite simple attack vectors, once their security structure is clear.

Virtualization. The fourth and last issue connected to hardware security concerns virtualization environments. An astonishing trend has become visible there. Automatic malware detection nowadays relies heavily on virtualization like VmWare or Qemu to be able to revert infected machines to safe states or properly track the changes made to the system. Consequently, malware authors try to detect their environment and refrain from executing their code when they are inside a virtual machine. Simultaneously, however, production environments also switch to virtualization tools because they provide a lot of flexibility and better resource management. As a result, a productive setup running their servers as virtual machines is already protected against a considerable percentage of malware that exists today. How this issue evolves in the future remains to be seen, but it is safe to assume that the trend will continue at least for the next two years.

Possible solution(s). There have been research initiatives that aim to identify trojaned hardware chips by launching a set of benchmark tests. Awareness needs to be raised in industry about the possible threats of hardware attacks in the future. As more and more hardware is being manufactured outside of the EU, the malicious components being integrated into chips designed in the EU is a viable threat. Therefore, techniques need to be developed that can check the integrity of hardware that is not produced in the EU.

2.3.3 Attacks against virtualization

Threat. In the last ten years, the popularity of virtualization has increased significantly. Virtualization is the method by which a ”guest” operating system is run under another ”host” operating system, with little or no modification of the guest OS. In 2005 and 2006, extensions to the x86 architectures by Intel and AMD made virtualization easier.

Virtualization is popular because it makes the maintenance of computing systems easier. Furthermore, virtualization techniques are increasingly being used in the analysis of security threats such as malware. The working group believes that virtualization technologies will be increasingly attacked in the future. For example, the attackers will be interested in finding techniques to break out of the the virtual guest in order to infect the host. In a recent paper [152] a proof of concept to this

attack was demonstrated. A flaw in the XEN virtualization environment allowed the authors to gain control of a host machine even avoiding additional security measures installed on the host system. Such an attack could be easily launched on a large scale by breaking out of a virtual machine hosted on online cloud services such as Amazon EC2. Here, a single vulnerability in a virtual machine could allow an attacker to simply rent more virtual machines, using his exploit to break out of each new, virtual host, and as a result, successively taking over the complete cloud.

Some security researchers have discussed the possibility of a "Blue Pill" attack, using a virtual rootkit similar to the one created by security researcher Joanna Rutkowska. This kind of rootkit, in theory, can hide in the hypervisor and away from the reach of today's security tools. Although blue-pill-like attacks have not emerged so far, the working group believes that stealthy malware that uses virtualization is a real threat that will emerge whenever the attackers see the need for it. That is, if security tools improve and can deal with techniques such as obfuscation (e.g., using behavior-based detection), then there will be a need for more stealthy malware.

Perhaps more problematic is the fact that intrusion detection tools cannot be deployed today to look at inter-VM traffic. As a result, as virtualization technology is used more and more to host services, the intrusion detection tools of today will be rendered increasingly ineffective.

Separation between virtual machine instances is another security problem. Even though theoretically one VM instance should not be able to inspect other virtual images running on the same host, it might be possible for an attacker to infer useful information about other instances using a side channel attack. As the hardware is shared between the instances, timing attacks like the one presented in [73] might be used to recover information about cryptographic secrets used in another virtual machine.

Also, note that malware samples are increasingly becoming virtualization resistant. That is, many malware samples have built-in checks and are testing for the presence of virtualization. If they realize that they are running in a virtual environment, often, they change their behavior. The aim of these malicious programs is to prevent the malware analysts from understanding their inner workings by running them in a virtual environment. Virtual environments are often used to analyze malware and clearly, malware authors are aware of this fact.

Possible solution(s). Awareness needs to be raised in industry to change the common belief that virtualization techniques are perfect for security. Furthermore, research is needed to make virtual malware analysis environments more resistant to evasion techniques. Virtualization providers need to provide hooks into the inter VM communication channels so that intrusion detection systems can monitor the traffic and detect attacks and also current malware detection applications have to be adapted to the new threat environments by applying for example approaches

like the one presented in [117] which allows active monitoring of running VM instances.

2.3.4 IPv6 and direct reachability of hosts

Threat. The Internet Protocol version 6 (IPv6) is the next generation network layer protocol for the Internet. The main motivation for the design and implementation of a new version of such a core Internet standard is the upcoming exhaustion of the IPv4 address space. An ongoing survey [51] currently projects that IANA's unallocated address pool will be exhausted in March 2011, and that regional registries' unallocated pool will run out a year later. Unfortunately, there is little economic incentive to deploy IPv6 before address exhaustion. Furthermore, because of "network effects," an IPv6 deployment is of little use until the rest of the Internet has also deployed IPv6. It is therefore hardly surprising that adoption of IPv6 has been slow. According to a recent Google study [37], less than 10 0.000000e+00nd users had functional IPv6 connectivity as of October 2008. None the less, rapid and widespread deployment of IPv6 will become inevitable once the IPv4 address space is exhausted.

Transition Issues. A sudden transition to IPv6, triggered by the unavailability of IPv4 addresses, may well exacerbate the security risks that are unavoidable in such a mayor upgrade of networking infrastructure. Furthermore, the transition phase itself carries its own risks. In the span of time in which IP versions 4 and 6 will coexist, network administrators will face the complex task of policing both protocols, as well as their interactions, such as the use of tunnels to send IPv6 packets over IPv4 (6to4) or UDP (Teredo). As an example, tunneling of an IPv6 packet over IPv4 could be used to avoid firewall restrictions or inspection from an intrusion detection system. Security analysis of these transition mechanisms has shown novel threats enabled by both 6to4 [130] and Teredo [61]. These include new avenues for Denial of Service attackes, and a greater ease in performing address spoofing. The inherenet complexity of the transition phase, coupled with the lack of knowledge on IPv6-related security issues on the part of network administrators, may well mean that IPv6-related misconfigurations will be one of the primary avenues of attack for Internet criminals.

Universal Addressability. Like IPv4, IPv6 has been designed to provide universal addressability for all devices on the Internet. However, the scarcity of IPv4 addresses has led to work-arounds such as Network Address Translation (NAT) that allows for machines with only a local IP address (that is not globally unique) to communicate with the rest of the Internet. While the use of local addresses and NAT was not originally a security measure, it effectively provides a very restrictive firewall that allows no incoming connections to the devices behind NAT. The IPv6 address space, on the other hand, is easily large enough to allow all Internet-connected devices to have globally-unique addresses. This has numerous technical

advantages and simplifies the development of new network applications. On the other hand, if the ingress filtering provided by NAT is not replaced by an appropriate firewall, a large number of home and corporate hosts that were previously exposed only to client-side vulnerabilities (when browsing the world wide web or using other applications) will suddenly also become a potential target for server-side attacks.

Topological Scanning. Another consequence of the huge IPv6 address space is that it will not be possible to perform a brute force scan of the IPv6 address space by simply sending packets to all (or many) addresses on the Internet. Brute force scanning will not reveal all hosts on a network to attackers or allow Internet worm to spread rapidly. None the less, other techniques may well successfully achieve these same goals. The presumed secrecy of IPv6 addresses should not lure network administrators into a false sense of security. Recent research has used mathematical models to explore the porpagation of self-replicating network worms in a hybrid, IPv4 and IPv6 network [159], as well as in an IPv6 only network [63]. The fundamental problem is that the IP address of a host is not really secret because it has to be known to any other host it communicates with. As an example, an attacker that has control of a single network node can quickly learn the addresses of all other nodes it communicates, for instance, by reading the DNS cache. Furthermore, if he is able to sniff (even encrypted) traffic between other nodes, he can harvest their addresses. This type of topological scanning may well allow more sophisticated Internet worms to spread quickly even in the future IPv6 Internet. Furthermore, any Internet service to which a user connects can harvest the user's address. The working group can imagine that Internet criminals would buy and sell IPv6 addresses just like they currently buy and sell email addresses to use as targets of phishing and spamming campaigns, especially in countries with lax privacy regulations where such commerce may well be legal.

Additional Issues. Specific features included in IPv6 may also cause security problems. IPv6 Routing Headers have been shown to be an extremely useful tool for attackers, allowing them to amplify their denial of service attacks and to perform advanced network discovery [119]. For this reason, IPv6 Routing Headers are in the process of being deprecated by the IETF [2]. The network autoconfiguration features of IPv6 may also pose a security risk. As an example, an attacker with a foothold in a network may attempt to use ICMPv6 Router Advertisement messages to establish a rogue router, re-route legitimate traffic through it and perform a man in the middle attack.

Possible solution(s). The EU has started initiatives and is trying to push IPv6. Currently, there is no large need for IPv6. However, in the near future, as the IP address space will not be sufficient to connect a large number of devices, IPv6 will become inevitable. Just like there were problems with the implementations of

IPv4 in the early days of the Internet, we will probably face IPv6-related implementation issues and vulnerabilities. This time, however, the attackers are more organized and aim to make illegal financial gains. As a result, awareness needs to be raised among ISPs as well as industry about the potential threats that will arrive with IPv6. Vulnerability analysis tools that have been used to improve IPv4 stack implementations need to be adapted for IPv6.

An early, gradual adoption of IPv6, combined with IPv6 training of network administrators and engineers, can avoid the high security exposure that we expect would be associated with a last-minute scramble for IPv6, deployed as a reaction to IPv4 address exhaustion. The security of the future IPv6 network will also depend on which of a plethora of standards and proposals for IPv6 extensions [57] will see widespread adoption. The operational and research security communities need to be involved in this transition, to make sure that the real-world deployment of IPv6 improves, rather than worsens, the security of the internet.

2.3.5 Advanced botnets

Threat. A popular tool of choice for criminals today are so-called bots. A bot is a type of malware that is written with the intent of compromising and taking control over hosts on the Internet. It is typically installed on the victim's computer by either exploiting a software vulnerability in the web browser or the operating system, or by using social engineering techniques to trick the victim into installing the bot herself. Compared to other types of malware, the distinguishing characteristic of a bot is its ability to establish a command and control (C&C) channel that allows an attacker to remotely control or update a compromised machine. A number of bot-infected machines that are combined under the control of a single, malicious entity (called the botmaster) are referred to as a botnet. Such botnets are often abused as platforms to launch denial of service attacks [95], to send spam mails [64, 124], or to host scam pages [5].

Most currently active botnets' C&C mechanism is based upon the Internet relay chat (IRC) protocol. There are various reasons for the popularity of IRC among botmasters: IRC enables small and simple client implementations in the bot software, it allows the botmaster to use off-the-shelf clients for commanding his bot army, and it allows to use publicly available, legitimate servers for hosting the C&C rendez-vous point, while at the same time offering built-in functionality for access control, to keep out security researchers, or other botmasters trying to inflict harm on their rivals. However, most importantly, IRC has been chosen as the C&C protocol in a few original bot implementations, from which an overwhelming fraction of today's active variants are still derived. A brief overview of the most important variants of IRC-based bots as well as their functionality can be found in [9].

While IRC served botmasters well in the past, the anti-malware industry, security researchers, as well as network administrators have taken advantage of several shortcomings IRC exhibits as a C&C protocol. First, compared to other application layer protocols, such as HTTP, IRC is not a main-stream protocol used by a great

number of people for serious purposes. For many, IRC has even turned into a synonym for botnet C&C. Many firewalls, especially in company networks, filter IRC traffic, an thus, render any successfully compromised machines useless for the botmaster. Second, for most of the popular variants there are network signatures that identify infections when deployed in a network intrusion detection system. Owners of publicly accessible IRC networks pay attention to identify C&C channels on their servers and take them down. Third, and most importantly, the C&C structure of an IRC botnet exhibits a single point of failure: The IRC service. The botnet is not robust to failures, caused either by technical malfunctions, or by intervention of anti-malware institutions aiming to shatter the botnet. By taking down the C&C channel, the botnet is irreversibly destroyed. For these reasons, a recent trend is that IRC is no longer considered a safe and efficient means of communication for botmasters.

While script-kiddies might continue to use IRC, and thus, the majority of botnets will likely still use it in the near future, more professional attackers have begun to explore alternative means of enabling C&C communication. These miscreants are motivated by an outlook for huge financial profit, and do not refrain from investing money and time into developing custom-tailored solutions that remove some, or all of the drawbacks that IRC brings. Recently, numerous botnets using alternative C&C protocols have been detected and monitored by the anti-malware community. The two most wide-spread alternatives to IRC as a C&C medium are HTTP, and peer-to-peer protocols, such as Overnet.

The utilization of HTTP as C&C protocol, above all, camouflages the C&C communication within a large amount of traffic transported with the most commonly used application-layer protocol existent on the Internet. Unfortunately, it is not possible to detect suspicious signs towards the presence of a bot infection in the network traffic, unless costly deep packet inspection is performed on all web traffic. Firewalls do not pose a problem, since Web traffic usually must be allowed to trespass to fulfill usability requirements. Even though HTTP botnets can be taken down by either disabling the server itself, or preventing the resolution of the domain name, bots can iterate over a list of registered domain names in order to locate a server that is active. These domain names can even be computed dynamically, based on the current time. So, even after having lost the botnet, botmasters can eventually regain control.

One of the most well-known bot implementations using HTTP is the infamous Conficker worm. More detailed information about Conficker is presented in [81]. At the time of this writing, Conficker is allegedly the world's largest botnet with almost ten million infected PCs.

Other botnets, such as the Storm worm, make use of peer-to-peer networks to communicate the botmaster's commands to the bots. By using well-established file sharing networks, such as Overnet, the botnet immediately takes advantage of a high number of peers to use as communication partners. Also, its traffic remains completely unobtrusive in front of the ubiquitous background of benign file sharing traffic.

In [35], an overview on the field of peer-to-peer botnets as well as the Storm worm is presented. A more detailed discussion on the Storm worm, including static analysis results of the worm binaries, can be found in [121]. The authors also explain how Storm leverages the widely-used Overnet peer-to-peer protocol to put in place its C&C network. In [46], the authors elaborate on tracking and analyzing peer-to-peer botnets, and demonstrate their strategies on the Storm worm. In addition, approaches for infiltration and mitigation are developed.

In addition to switching to more powerful, and less suspicious protocols, attackers make use of simple, yet powerful tools to avoid detection and retain secrecy about their intentions. By transmitting the commands in an obfuscated form, instead of in the clear-text, botmasters now successfully avoid detection by current automatic (intrusion detection) systems to identify bot infections. By using classic cryptographic methods, they can even thwart manual efforts from malware experts to decipher the commands, unless an instance of the bot software is obtained and reverse engineered.

The malware and fraud working group believes that the threat imposed by botnets will continue to increase. In the near future, botnets will be less-dependent on IRC but more on protocols such as P2P, and even instant messaging infrastructures.

Possible solution(s). While throughout the past years many efforts have been made to mitigate the botnet threat, these efforts have only been partially successful. The changes in the tools and tactics used by botmasters and malware authors clearly call for further research in order to identify, correctly specify, and filter botnet traffic. Due to the ever-increasing presence of botnets on the Internet, there is a need for automated systems aiding researchers in their work. Because of the rising diversity in the C&C structures of current botnets, completely new methods for deriving and implementing means of detection must be developed.

2.3.6 Naming, the role of domain registrars, fast-flux networks

Threat. Fast-flux DNS is a recent technique which overloads the A (address) records in the DNS server. One A record will have multiple IP addresses, making it redundant: each client will try one IP address after another, until it can successfully establish a connection.

In botnets, fast-flux techniques are used to connect to and hide the command and control servers (C&C). That is, it is used by botnets to hide phishing and malware sites behind a changing network of compromised hosts. These sites are used to deploy malware (botnet software such as Storm Worm) to unaware users. It can also refer to the combination of peer-to-peer networking, distributed command and control, web-based load-balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures.

The fast-flux networks are a group of compromised (hacked) computer systems that have a public DNS record. These records change very fast, which makes the

detection of these networks harder. Fast-flux networks have multiple (tens, hundreds, or thousands) of IP addresses assigned to it. These IP addresses in the A records are changing very fast, using round-robin IP addresses and a very short TTL. An unaware user connecting to a website might be connecting to a different infected host each time. The IP address pool is usually not the final destination. Instead, these hosts merely serve as redirectors that forward the requests to other backend servers (that provide the content). This technique is typically used for load balancing and high availability, but botnet herders have adapted this approach for illegitimate purposes. The controlling elements are called "motherships" [46]. These motherships are hidden by the front-end fast-flux nodes. The motherships host both the DNS and HTTP services, and can be configured to manage thousands of domains simultaneously on a single host. The motherships provide the information for DNS to the front-end, which then forwards it to the infected client. There are two different types of fast-flux networks: single-flux and double-flux.

Fast-flux networks are a major menace as they are difficult to take down. The problem of fast-flux networks is expected to grow in the future, resulting in a increasing interest by various security groups [48]. In [45], the authors study the significance and general principles of this kind of network service. Their experiments show a rapid increase in the use of this new technology — while earlier measurements from December 2006 [5] showed only very few online fraud campaigns to be hosting content using multiple IP addresses, their evaluation of spam-trapped data from August 2007 suggests the use of fast-flux services to be almost as high as 30%.

From the collected data, they were able to extract three key features common to fast-flux service networks. First, the number of unique `A records` returned by a DNS lookup is significantly higher than observed for legitimate hostname lookups. Alike, FFSN employ more nameserver entries than casual networks. Last, as the single steppingstones are typically widely distributed over many internet service providers (ISPs), the number of ASNs is rather high (whereas legitimate networks are usually hosted within a single system).

Based on their findings, Holz et al. propose a tool to detect networks that employ fast-flux services by calculating a `flux-score` based on observed values of the three characteristics described above. The authors of [116] extend this idea and present `FluXOR`, a tool to detect and monitor botnet networks that employ fast-flux services. FluXOR achieves its goal by monitoring a (potentially) malicious network from the perspective of a victim that is lured into accessing a resource provided by a webserver hidden behind a proxy, i.e. gathers data from `outside` the infected network.

More precisely, the tool continuously monitors (i.e. queries for) the IP addresses associated with suspicious hostnames. It then tries to extract and identify multiple features that can be used to distinguish the observed networks from casual, benign services employing load balancing or the use of mirrors to provide content.

In addition to the features presented by Holz et al., these new features mainly concentrate on TTL values associated with DNS records, the domain age and used registrar, as well as more precise ways of measuring the heterogeneity of botnet clients. The values obtained by FluXOR for a given hostname can then be compared to a training set of manually classified networks. This allows to decide if a network is hosted by a fast-flux service without having detailed information on the network's internals. A similar system that provides real-time monitoring and statistics is presented in [15].

In [104], Nazario and Holz extend work from [45] and provide more detailed information about lifetimes, sizes, and separability of fast-flux service networks. By inspecting data collected over 4 months in early 2008 they gathered that FFSN have an average lifetime of 18.5 days. The largest and longest-living network operated almost 60 days, spanning over 100.000 network nodes. By clustering for distinct set of IP addresses, the authors identified 26 distinct fast-flux botnets providing different services such as "pharmacy product" stores and sites used in phishing attacks.

In contrast to other work, Konte et al. [74] study fast-flux techniques by assigning a large set of networks to 21 distinct scam campaigns exhibiting fast-flux behavior. They investigate on common properties among and unique characteristics within the individual campaigns and compare the results to a large set of benign networks. The authors further measured the network's dynamics, i.e. the rates at which DNS mapping are changed, the speed at which the number of network nodes grows, as well as the rate of changes in the DNS hierarchy (for double flux systems). Their findings suggest that the network's dynamics pose another means of identifying malicious networks in terms of fast-flux techniques.

Possible solution(s). Domain registrars seem to be very lax when it comes to registering and selling domains. The working group believes that in order to combat fast-flux networks, cooperation by ISPs and domain registrars is inevitable. The working group believes that ISPs and domain registrars need to be held responsible, to a certain extent, for the damage that is caused by the services that they host. For example, if a domain registrar does not disable a registration after repeated complaints, there needs to be a legal mechanism that can hold them accountable. Currently, domain registrars are often lax and are not concerned as they are not liable.

2.3.7 Attacks against the network backbone and infrastructure

Threat. The steady reduction of prices in the IT industry has increased the spread of Internet access and of network-based equipment. Victims of computer attacks are now a large number of Internet users who use services such as online banking and e-mail.

Nowadays, mostly Internet providers ship to their customers out-of-the-box (self-configured) network devices such as ADSL and wireless routers. These de-

vices are quite easy to use and install. Often, they come with default settings. Unfortunately, because of their ease of use, these devices may sometimes have default configurations that may be insecure. They may have default authentication credentials, weak keys, and may allow open Internet access to outsiders. Also, note that these devices often use freely available operating systems such as Linux. Hence, the vulnerabilities that are found on operating systems may also be applicable to these devices. Since years are known to be in the wild Bot that spreads using commodity-routers' vulnerabilities. Reseachers at Symantec Corp. claims to have observed a worm infiltrating D-Link's devices through a three-years-old vulnerability [142].

Many of the attacks on the Internet today target personal computers. These computers are often not well-protected. Also, many home computers have high-Internet connectivity that can be useful for the miscreants (e.g., for launching DoS attacks or for sending spam). Hence, whereas many attacks were targeting servers 10 years ago, we see a strategic shift by the attackers who are less in interested in servers that have become more difficult to attack (e.g., because of default firewalls and automatically installed patches), but more interested in home computers.

One novel attack that will be increasingly seen is click fraud [62]. A new economic, advertising model has emerged where companies such as Google, Yahoo, and Facebook offer online advertisements. The revenue model is based on the number of people who click on the links. Unfortunately, miscreants have already started to target this revenue model. Home computers that have been compromised are sometimes used to generate fraudulent clicks. In the future, click fraud will probably become more widespread.

Also, note that attackers are already targeting the Internet backbone. Sophisticated, ad-hoc customized attacks against BGP autonomous systems have been reported and DNS root servers have also been attacked in the past. On October 21 2002, it was observed the first DoS attacks against DNS root server [148], replicated then on February 6 2007, when the attack lasted for more then five hours. ICANN stated that this second attack could have been carried out by the cybercrime organizations thanks to a Botnet [53]. Beside attacks that target the availability of network backbones, current and future malicious techniques, such as the injection of illegitimate sub-prefixes for third party ASs impact the integrity and confidentiality of data.

Finally, the DNS protocol was recently found to be vulnerable to an attack that can easily be exploited [147]. This attack is a variation of a so called "cache poisoning attack." It works because of the small value domain of the DNS transaction IDs (16-bits) and the fact that the attacker can launch multiple attempts to guess (spoof) this ID in rapid succession. Given a chosen domain name, the weakness permits to substitute the original IP address with an illegitimate one. Consequently, web traffic, email, and other important network data can be redirected to systems under the attacker's control.

Possible solution(s). Research is required on attacks that target the computing infrastructure of home users as well as the Internet backbone. Interestingly, it was known for a long time that BGP is vulnerable to attacks. However, the problem was ignored by the industry. The working group believes that the number of attacks against the Internet infrastructure will increase in the future.

2.4 New applications and business models

2.4.1 Abuse of social network privacy and trust in online communities

Threat. 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 friendships and general interests. Recently, the popularity of social networks that might focus either on business-relationship or friendship has dramatically increased. As social networking sites such as XING [154], LinkedIn [85], Facebook [28], StudiVZ [139] and MeinVZ [92] have been gaining popularity among Internet users, miscreants started to abuse most widely-used social networking sites for their nefarious purposes.

The nature of information social networking users provide by registering to the network is sensitive and attractive. Typically, users enter their real e-mail addresses and provide information on their education, friends, professional background, interests, sexual preferences and activities they are involved in. Hence, from the attacker's point of view, access to this type of detailed, personal information would be ideal for launching targeted, social engineering attacks, now often referred to as spear phishing [138, 59]. Furthermore, the collected e-mail addresses and personal information would be invaluable for spammers as they would have access to e-mail addresses that belong to real people and have information about the people using these e-mail addresses allowing them to efficiently personalize their marketing activities, tailored according to the knowledge from the target's profile.

The relation between users on the current popular social networking sites is based on strong trust. The malware authors may leverage that fact and abuse the service by using the environment as their infection medium. Obviously, if an attacker manages to build this relation between the victim, she can easily deceive him to install her malware since the victim will think the attacker is a trustworthy friend. To this end, the attacker may choose to perform impersonation attacks, which are proven to be doable not only by researchers [98] but also real-world attacks that are observed in the wild [80].

The attacks performed in the past show that the criminals started to focus on popular social networking sites such as MySpace, Facebook, Orkut and so forth. They were mainly trying to deceive users to install their malware by directing them to fake codec sites or attracting them to install some social networking site specific applications. The latest also the most interesting attack was seen in February 2009 and it was carried out by Koobface worm's latest version [75]. The malware installed after infection of the victim was trying to steal credentials of various social

networking sites. The fast evolution of the type of the attacks targeting social networking sites can be interpreted as more serious attacks can appear in the nearest future.

The more compromised users an attacker has, the more massive attacks she is able to perform. Obviously, if a feasible way to launch the social-networking attacks in an automated fashion can be found, the attacker may easily and quickly achieve her goals. To prevent attackers from automatically accessing and abusing their services, social networking sites make use of CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart). A CAPTCHA is a type of challenge-response test that is commonly used to determine whether the user of a certain application is a human being or a program. The key feature of CAPTCHA algorithms is the ability to generate tests that are at the same time easily solvable by humans, but very difficult to solve for a computer application. Clearly, using CAPTCHAs that are very difficult to be broken by programs most likely can stop emerging social networking attacks from the beginning. However, most of the popular social networking sites do not put enough effort into making automated crawling and access difficult.

Unfortunately, even if the social networking sites use CAPTCHAs that are very difficult to be solved by automated programs (e.i. reCAPTCHA [149]), the criminals who own a botnet with numerous bots may evade the CAPTCHA obstacle. In the beginning of 2009, the spammers used a botnet to crack Microsoft Live Hotmail CAPTCHAs in order to create a large amount of accounts. Similar technique can be applied to social networking sites for other malicious activities as well.

Possible solution(s). A prerequisite for being able to access personal information in a social networking site is a confirmed personal relationship with the person who is concerned. Once the attacker establishes such a connection, which is based on strong trust, he can insidiously make the user perform various attacks without her being aware of the involvement in the attack. The most challenging task for the attacker seems to be persuading the victim that a friendship request is coming from a real friend. However, recent research showed that it is not as difficult as it is thought to fool social networking users. Obviously, the user is the weakest link in social networking sites. Many are not security-aware, and there is much implicit trust. One solution that could improve the security of contact requests would be to provide more information to the receiver on the authenticity of requests.

Since it is very difficult to make all of the users be aware of authenticity and privacy issues on social networking sites, the biggest part of the work on making social networking sites more secure has to be done by the social networking providers. Recent research[reference] showed that not all of the social networking sites track anomolous behaviour such as crawling, consequtive CAPTCHA solving attempts, large number of similar activities done by one account etc. Hence, if the service provider applies anomaly detection techniques, they may stop or at least slow down propogation of the malicious activities on social networks.

2.4.2 Underground economy

Threat. Over the last few years, there has been a dramatic change in the goals and modes of operation of malicious hackers. As hackers realized the potential monetary gains associated with Internet fraud, there has been a shift from ”hacking for fun” (or bragging rights and celebrity within and outside the hacker community) to ”hacking for profit.” [144, 32] This shift has been leveraged and supported by more traditional crime organizations, which eventually realized the potential of the Internet for their endeavors.

The integration of sophisticated computer attacks with well-established fraud mechanisms devised by organized crime has resulted in an underground economy that trades compromised hosts, personal information, and services in a way similar to other legitimate economies [78, 135, 134]. This expanding underground economy makes it possible to significantly increase the scale of the frauds carried out on the Internet and allows criminals to reach millions of potential victims. Also, criminals are taking full advantage of sophisticated mechanisms, such as the service bots used on IRC channels to automatically verify stolen credit card numbers or the use of fast-flux networks [45] to create attack-resilient services.

The emerge of the underground economy has resulted in the existence of well-funded adversaries that have the incentive and the means to create better, stealthier malware. In addition, it has also led to the development of novel services that cater to the needs of the underground economy. For example, malware that steals sensitive information requires a way to leak this data back to the malware author (or controller). Often, compromised machines (so-called drop zones) are abused for this purpose [44]. Another example are trading forums (such as IRC channels, web site) that are leveraged by criminals to exchange stolen information for money [32]. Finally, there are services needed to launder or to exchange money. Recently, the use of e-casinos has become a popular means to transfer money from one party to another. To move money from party A to B, both join the same game (table) in an e-casino. Then, the player(s) controlled by A deliberately play weak and lose their bets to the player(s) controlled by B. Such transactions appear legitimate, and they are difficult to identify as illegal money transactions. The different services and novel schemes that are forming in the wake of the underground economy are of significant concern. In particular, we require actions to counter and disrupt these services and transactions to attack the underlying platform on which criminal activity thrives.

In addition to the novel services and platforms used by cyber-criminals, it is also possible (and likely) that they seek novel business opportunities. One such business model leverages the fact that a botmaster controls a large number of desktop machines that store a significant amount of possibly valuable information [22]. While it is easy (and already practice) to search this data for financial credentials, it is also possible to monetize other, more specific information. For example, one of the compromised machines might contain Word documents about a certain company that is interesting to and relevant for a competitor. To connect the data with

potential buyers, the botmaster could decide to rent his botnet to customers that are then allowed to perform a number of desktop searches on the compromised hosts. Thus, the botmaster does not require to know in advance what information is valuable. Instead, he just sells access to his data to criminals that are more specialized in looking for certain kinds of data [49].

Possible solution(s). One reason why the underground economy is flourishing is because it is very difficult to trace back the attackers [49]. Also, the cost of running illegal operations for the attackers is low. After discussions, the malware and fraud working group believes that it is important to disrupt the underground economy, possibly by using offensive techniques to increase the cost for the attackers. For example, a possible defensive solution could be to inject a large volume of false information as a response to the attacks launched by the attackers [32]. As a result, the attackers would face the problem of identifying which stolen data is valid and which data is fake, and the cost and the difficulty of the attack would increase.

Another possible offensive, perhaps controversial, defense technique could be to automatically launch DoS attacks against illegal web sites that are operated by the attackers. By making these sites inaccessible, potential victims could be prevented.

2.4.3 Attacks against the financial sector / banks

Threat. Since the advent of the web, our lives have changed irreversibly. Web applications have quickly become the most dominant way to provide access to online services. For many users, the web is easy to use and convenient because it provides anytime, anywhere access to information and services. Initially, web sites were mainly used for providing information to visitors, but today, a significant amount of business is conducted over the web, and millions of web users purchase items, transfer money, retrieve information and communicate via web applications.

Unfortunately, the success of the web and the lack of technical sophistication and understanding of many web users have also attracted miscreants who aim to make easy financial profits. The attacks these people have been been launching range from simple social engineering attempts (e.g., using phishing sites) to more sophisticated attacks that involve the installation of Trojan horses on client machines (e.g., such malicious software may be automatically installed by exploiting vulnerabilities in browsers in so-called *drive-by attacks* [96]).

An important web security research problem is how to effectively enable a user who is running a client on an untrusted platform (i.e., a platform that may be under the control of an attacker) to securely communicate with a web application. More precisely, can we ensure the *confidentiality* and *integrity* of sensitive data that the user sends to the web application *even if* the user's platform is compromised by an attacker? Clearly, this is an important, but difficult problem.

Ensuring secure input to web applications is especially relevant for online services such as banking applications where users perform money transfers and ac-

cess sensitive information such as credit card and account numbers. Although the communication between the web client (e.g., the browser) and the web application is typically encrypted using technologies such as Transport Layer Security [55] (TLS) to thwart sniffing and man-in-the-middle attacks, the web client is the weakest point in the chain of communication. This is because it runs on an untrusted platform, and thus, it is vulnerable to client-side attacks that are launched locally on the user's machine. For example, a Trojan horse can install itself as a browser-plugin and then easily access, control, and manipulate all sensitive information that flows through the browser. In this case, using an encryption technology such as TLS does not solve the problem.

In a typical client-side web attack, the aim of the attacker is to take control of the user's web client in order to manipulate the client's interaction with the web application. Such an attack typically consists of three phases. In the first phase, the attacker's objective is to install malware on the user's computer. Once this has been successfully achieved, in the second phase, the installed malware monitors the user's interaction with the web application and waits for the user to perform a security-critical operation. The third phase starts once the malware detects that a security-critical operation is taking place and attempts to manipulate the flow of sensitive information to the web application to fulfill the attacker's objectives.

Malware that manipulates bank transactions already appears in the wild. For example, several Austrian banks were explicitly targeted by Trojan horses that were used by miscreants to perform illegal money transactions [77, 122]. In most cases, the victims did not suspect anything, and the resulting financial losses were significant. Note that even though the costs of such an attack are covered by insurance companies, it can still easily harm the public image of the targeted organization and may cause subsequent damage such as the loss of customers (who may lose confidence in the organization).

The working group expects attacks against financial institutions to increase in the future.

Possible solution(s). Research is needed in secure input technologies. Also, banks and financial institutions should be encouraged to create a second, trusted channel so that if one channel is compromised, the second can be used to detect the attack or to limit the damage. Many banks in England, for example, still use only a single pair of user name and password.

2.4.4 New vectors to reach victims

Threat. In the past years, cyber criminals have constantly improved and extended their malicious operations on the Internet. Unfortunately, threats such as worms, viruses, credit card and identity theft, phishing websites and other fraudulent online activities are still on the rise.

Cyber criminals have traditionally employed a number of techniques to find potential victims. The vectors used for reaching victims include mass (spam) email,

fake web sites, social engineering, online advertisements served to benign web sites and other forms of online or offline communication. Occasionally, even real-world, hardcopy mail is used as a part of online fraud. For example, a letter might lure a victim to a fake web site and try to convince him to enter valuable, sensitive information. Another interesting example of merging the physical and virtual world has been reported by the SANS institute in February 2009 [129]. In this case, the criminals were using windshield fliers and fake parking tickets containing a link to a malicious web site. By visiting the link, the users were asked to download and install an application to be able to view the pictures of their vehicle.

For cyber criminals, a "victim" for their malicious activity can be either an unsuspecting human or a vulnerable computer system. Typically, the criminals are motivated by monetary profit. This profit can be directly related to their victims. For example, credit card information stolen via a phishing site can be used to withdraw money from the victim's bank account. On the other hand, a victim could indirectly be part of malicious activities. For example, a worm could turn the victim's computer into a malicious bot, which in term might be used by the cyber criminal to conduct illegal activities.

Spam remains very popular for cyber criminals, as it has the potential to reach a large number of victims while typically exhibiting low cost. The Spamhaus Project [137] now estimates that about 90% of the incoming e-mail traffic in North America, Europa and Australasia is spam. To evade spam filters and detection, there has been a number of improvements (from the attacker's point of view) [67]. For example, bodies of non-spam text are often inserted into spam emails to defeat statistical detection algorithms, or images containing a spam message are attached to an otherwise innocuous email.

Alternatively, cyber criminals are leveraging other communication media other than e-mail for spam. For instance, instant messaging (SPIM) and Internet telephony (SPIT) are being increasingly used by criminals to send spam or infect their targets [88, 40]. Recently, social networking websites (e.g., Myspace [102] and Facebook [28]), virtual environments (e.g., Second Life [133], Playstation Home [120]) and online games have become attractive targets for spammers, as a large number of users can be reached via these vectors.

In particular, social networks are very appealing for cyber criminals. They can easily create fake profiles and, using the internal search tools provided by the social network, they can identify their victims based on demographic segments or geographical location. To get access to private information only disclosed to the contact's friends, attackers can steal real user identities by creating profiles of real people [80] or by duplicating existing profiles in a different social networks [12]. The information collected in this way can then be used to create targeted attacks (usually called spear phishing [138, 59]). Finally, also more traditional malware infection are moving to social networks, as proven by new worm infections observed in the wild that specifically target MySpace and Facebook users [103]

Another vector that is increasingly abused to find victims are compromised, but legitimate web servers. Cyber criminals are injecting malicious code into

hacked web servers, which then triggers malicious activity on the visitors' computers. Even security aware users are easily susceptible to this kind of attack, as it abuses the trust relation between the user and the legitimate web site.

The working group is expecting alternative vectors to reach victims to increase in the future. New technologies and service ideas are constantly emerging and are expected to be quickly exploited by criminals looking for new spreading mechanism and new, more effective way to identify and reach their targets.

Possible solution(s). Existing countermeasures have to be adopted and extended to defend against these new threats, as online criminals are quickly adopting to new trends in technology and user behavior.

Finding victims is one of the first steps a cyber criminal has to undertake. The security community has identified this prerequisite for illegal operations and successfully devised a number of counter-measures. For example, spam and phishing filters are now commonly used by service providers, and anti-virus software and firewalls are easily available for most computer systems. While these systems are far from perfect, they have reduced the effectiveness of some of the malicious activities. Unfortunately, cyber criminals have reacted to these efforts, and are now extending their operations to different vectors to find victims.

New techniques have been proposed to detect IM-based spam [83] and different security companies have started integrating spam blocker functionalities into their instant messaging management systems to filter the traffic and protect the users from unsolicited messages.

There have also been research initiatives to mitigate attacks on social networking sites, both in the direction of protecting the network from the creation of a large number of fake profiles [156], and in the attempt to better protect the online privacy of users' data [36].

2.5 New social dynamics and the human factor

2.5.1 Targeted attacks, spear phishing

Threat. Most attacks on the Internet are aimed at a large number of users. Considering phishing attacks, which are performed to acquire sensitive information such as user names and passwords. It is obvious that the effectiveness of the attack increases if the attackers manage to reach a large number of users. Phishing attacks also require little or no knowledge about the fraud victim, and a single version of a mail text is sufficient to perform the attack. This phishing mail is sent to as many people as possible, hoping that some of them will be lured into clicking on embedded links.

A recent trend is that today, not all attacks are aimed at large groups of people. In recent years, a new kind of attack emerged: the targeted (or spear-phishing) attack. This attack does not target an unspecified group of users, but only a selected

group of people or even individuals. Usually, these people are part of a certain community or organization (e.g., employees of a company, a CEO, etc.). Attackers have been attempting to gain access to computers inside organizations in order to steal valuable information such as business secrets. These secrets can be worth significant amounts of money [29].

Whenever a so-called targeted, spear-phishing attack is launched, the e-mail sender information has been faked or "spoofed." Whereas traditional phishing scams are designed to steal information from individuals, spear phishing scams mainly work to gain access to a company's entire computer system. Spear phishing also describes scams that target people who use a certain product or Web site. Scam artists use any information they can to personalize a phishing scam to as specific a group as possible [93].

The number of victims in targeted attacks is usually limited. This has two main reasons. First, if a zero-day exploit is used, targeting individuals is more advantageous as there is a low risk that there will be anti-virus signatures soon that will mitigate the attack. Second, the attack and the attacker will be less likely to be detected. Furthermore, if only individuals are targeted, it is easier for the attacker to cover her tracks.

For 2008, only 0.4% of all spam e-mails were targeted attacks. However, this is a four-fold increase over the previous year, and these attacks tend to cause significantly more damage and have a higher success rate than untargeted phishing. Scammers also take advantage of e-mail reputation hijacking facilitated through the repeated breaking of CAPTCHA schemes employed by major web mail providers. A low volume scam attack sent from a trusted source (for instance, the mail server of a well-known web mail provider) is more likely to pass spam filters and go unnoticed than mass e-mails sent through a botnet [19].

A recent study has shown that the main hurdle to a successful attack is convincing the user to click the malicious link, as users who do so are very likely to divulge sensitive information on the web page they are directed to [79]. More targeted information in scam e-mails raises the probability of users following the link. For example, a user is more likely to follow an alleged link to the website of a bank she is a customer of than to a bank that she is not familiar with. Browser cache sniffing [60] can be used to reveal sites the user has visited to obtain this information.

The malware and fraud working group believes that there is large potential for more sophisticated targeted attacks in the future. As phishing becomes common knowledge among users, the attackers will shift their attention to targeting individuals and using knowledge about these users that they have acquired on the Internet. The plethora of social networking sites like Facebook, MySpace and Twitter, that have cropped up in recent years, makes the gathering of personal information from the Internet very easy for determined miscreants. These sites also create a new attack vector for so-called "Nigerian" (advance fee) scams, where a hijacked account and the personal information within is used by the attacker to impersonate the victim and ask friends for money [136]. Even when noticed by the account

owner, these attacks are hard to stop [105]. A study carried out at the University of Indiana shows that phishing victims are four times more likely to fall for the scam if they are solicited by someone appearing to be a known acquaintance [58].

Possible solution(s). Targeted attacks pose a great threat to organizations and companies. Employees have to be made aware of the fact that even e-mails that appear to come from a legitimate source such as a colleague or a boss can be a fraud. Hence, training and raising awareness is the key to solving the spear-phishing problem. First studies evaluating the efficacy of anti-phishing training programs show promising results. Training against general phishing threats also raises awareness of targeted attacks, and employees working together benefit already from having only few of them trained against phishing [79]. Furthermore, research in the areas of content analysis would be useful in detecting malicious e-mails.

2.6 Conclusions

In this chapter, we introduced a number of threats that have been identified by the malware and fraud working group. The focus is on what we consider to be novel threats or threats that are considered to become more problematic in the future. Of course, the list of threats is not intended to be completely exhaustive. Instead, we have selected those that the working group considered to be most interesting and that the working group expects be growing in the future. Also, some of these threats have not yet received much attention by the research community or by industry.

Chapter 3

Working Group: Smart Environments

3.1 Introduction

The working group on smart environments concerns itself with ordinary environments that have been enhanced by interconnected computer equipment, sensors, displays, etc. While there is no generally accepted definition of the term 'smart environment', in practice it can be fairly accurately defined negatively, by looking at what it does not address. For instance, we mostly exclude environments that are used for "traditional" computing and computer security (such as PCs and mainframes). Instead, the working group on smart environments investigates the threat landscape in areas such as intelligent houses, car networks, smartphones, and so on.

Compared to the world of PCs and servers, security in smart environments is more difficult to analyze because fewer security problems have occurred so far. Everybody is familiar with spam, viruses, and phishing attacks, but what exactly are the threats that emerge from smart parking sensors, mobile phones, and computer controlled homes?

On the surface, studying security in smart environments seems to require a crystal ball and/or a lively imagination. While we do not deny the usefulness of either, we argue that studying existing threats and trends allows researchers to form a coherent picture of (at least some of the) threats likely to emerge in the future.

For instance, we observe that mobile phones are becoming like computers with full-blown operating systems, lots of applications and (as a result) many bugs and vulnerabilities. In other words, we see increasing opportunities for hackers to attack phones. Still, we do not see many attacks on phones (yet). It is more lucrative for an attacker to hack a PC than it is to hack a phone. After all, PCs are used to enter credit card details, passwords and many other interesting potential targets that all represent value. Phones are mostly used to, well, phone people.

As a result, attacks on mobile phones are still relatively rare. However, we witness a trend that phones will be used increasingly for financial transactions, in addition to normal, PC-like, Internet access. This makes them a more interesting target for attackers. Combining the two trends – increasing opportunities and increasing incentives – allows us to predict that smartphone are much more likely targets in the future than today.

The working group on smart environments has established an online forum to discuss interesting developments and security outlooks in the field of smart environments.

3.2 About the threats

In our work, as in all the other working groups, we used the following definition of a threat.

Definition of a Threat : A threat is any indication, circumstance, or event with the potential to cause harm to an ICT infrastructure and the assets that depend on this infrastructure.

This is a variant of other definitions that exist in the literature, among them the definition found in the *EU Green Paper for Critical infrastructure protection, 2005* [20].

In this section, we discuss various threats that have been identified by the working group. The focus is on what we consider to be new threats (or new twists to existing threats), rather than threats that have already been explored extensively by researchers and industry. Furthermore, we will structure the discussion along the axes introduced earlier (new technology, new applications, new business models, and new social dynamics).

In this threat report, we use the same 'axes' for categorizing the threats as in the threat reports of the other working groups. These axes are:

New technologies New types of devices and new technology often bring new types of threats.

New applications Sometimes, the technology has not changed significantly, but new applications run on top of existing technology and introduce new threats.

New business models This is a bit less relevant for the working group on smart environments and listed mainly for completeness. Threats may be introduced because we apply new business models (like e-commerce) to existing technology and applications

New social dynamics Social dynamics change, and so do the users themselves in their use of services and applications.

Some of these axes are more relevant to smart environments than others. However, it would be a mistake to place all new threats under the banner of 'new technology', even though smart environments often employ new technology. We will see that some of the threats can be more usefully (also) placed in the other categories.

However, the boundaries between the various threat sections in general are fuzzy. This is unavoidable. For instance, we discuss security issues related to new technology like smartphones, new forms of threats against privacy, and so on. However, smartphones introduce a raft of security problems. We have already seen that gaining control over phones will be increasingly interesting for attackers, but we will see later that phones also introduce interesting new privacy problems. Moreover, the technology gives rise to new applications, new business models, and new social dynamics. As a result, the phone fits in more than one category.

Also, our list of potential future threats is not intended to be exhaustive. The set of potential threats is probably infinitely large. Instead, we have selected a few threats that the working group considered to be interesting and that have not yet received much attention in research and industry. As the threats are future threats, clearly the selection is debatable. But we did try to keep on eye on the threat level associated with each threat. Threat levels themselves are hard to assess and we will only assign appropriate threat levels in the later deliverables in the project. Nevertheless, we may expect to use such criteria as:

- Will the threat affect many people?
- Is the threat likely to occur often (either because it is unavoidable, or because there is a clear and obvious incentive for attackers)?

By these simple questions, we may rate the threat level of attacks on mobile phones as 'high', because most people have phones which are increasingly vulnerable *and* handle security sensitive data (providing an incentive for attackers). By the same token, denial of service attacks on wireless infrastructure is rated as 'low-medium': the threat is real, but it is likely to concern relatively few incidents, and the incentive for attackers is not immediately obvious. Again, in this report, we will not yet assign threat levels to the threats.

3.3 New technologies

In this section, we discuss interesting new threats that are related to the introduction of new technology, and/or substantial improvements in existing technology.

3.3.1 'Smart' phones and braindead zombies.

Threat. As mentioned earlier, smartphones are mobile phones with PC-like capabilities. We now zoom in and look at the domain of mobile phones in more

detail. We will see that while they are similar to PCs in many respects, they are quite different in others.

In addition to more traditional telephony stacks, calendars, games and address books, smartphones may run any application the user loads onto it. An increasing number of hardware vendors bring out ever more powerful models, running applications that are often similar but different from the competition on a diverse set of operating systems. The application domain of smartphones currently ranges from high-end business markets (targeted for instance by RIM's Blackberry) to consumer and entertainment markets (as targeted by the Apple iPhone, and Nokia 5800 series). In practice, smartphones are used for email, web browsing, centralized calendaring, navigation, music, etc.

In addition, phones are frequently used for commercial transactions. In other words, there are changes along the axes of business models and applications too. Apple and other companies allow applications, music and videos to be purchased online. Payment for goods and services via mobile phone is already provided by Upaid Systems and Black Lab Mobile. In the meantime, companies like Verrus Mobile Technologies, RingGo, Easy Park, NOW! Innovations, Park-Line, mPark and ParkMagic all offer payment-for-parking schemes. Others focus on mass-transit. For instance, Mobile Suica already allows passengers to use their mobile phones to pay for transport on the East Japan Railway Company, the largest passenger railway company in the world.

It is clear that the domain is widening and involves real money. Analysts predict that in the near future the smartphone will be the primary interface to the Internet and indeed the digital world in general.

The tsunami of applications engulfing what was previously a dumb device (a phone) implies that bugs and vulnerabilities to attack are on the rise also. Vulnerabilities provide opportunities for attackers, while the increasing importance of smartphones and the real money involved in the interactions provide an incentive.

Vulnerabilities in the past have allowed attackers to completely take over mobile phones via Bluetooth. Examples included phones from various vendors, such as the Nokia 6310, the Sony Ericsson T68, and the Motorola v80. The process, known as bluebugging, exploited a bug in the Bluetooth implementations. The takeover results in a "zombie" phone, completely under the control of the attacker. While these are fairly old phones, more recent models, such as the Apple iPhone have also shown to be susceptible to remote exploits. Recent examples include trojans on the Symbian OS [27] and exploitable vulnerabilities on Google's Android phone [113].

So what is new? Surely, we have seen all of this before in the world of PCs and so the threat of the future is the threat of today? Unfortunately not.

Yes, smartphones are just like PCs in processing capacity, range of applications, and vulnerability to attacks. But they are very unlike PCs in other respects, notably power and physical location. These two aspects matter when it comes to security.

First, unlike normal PCs, smartphones run on battery power. Power in mobile phones is an extremely scarce resource. For instance, one of the main points of criticism against Apple's iPhone 3G concerned its short battery life [97]. Software developers bend over backward to make core code run fast on phones, because every cycle consumes power, and every Joule is precious.

As a consequence, many of the security solutions that work for desktop PCs do not suit smartphones as they are too heavyweight. File scanning, taint analysis, system call monitoring all consume battery power. Battery life sells phones, and consumer hate recharging. The likely result is that both vendors and consumers will trade security for battery life.

Second, unlike traditional computers, phones go everywhere we go. And we use the phones for security sensitive operations in potentially hostile environment (a change along the axis of social dynamics and use). Attacks may come from sources that are extremely local (e.g., via bluetooth). A person with a laptop or another smartphone that happens to be in the same room could be the source of an attack. That means that security solutions based on in-network scanning are useless: they will never even see the bytes that are used to take over the phone, steal information, and plunder your bank account.

Worse, phones are small devices, and we do not always keep an eye on them. We may leave them on the beach when we go for a swim, slip them in a coat or shopping bag, forget them on our desks, etc. Theft of a phone is much easier than theft of a desktop PC or even a laptop. Moreover, attackers could "borrow" the phone, copy data from it, install back-doors, etc. This is an important difference with the PC you have sitting on your desk.

What would it buy an attacker to steal your phone (and perhaps return it later)? Well, having the device in your hands opens up a wide range of options for attacking the device that would otherwise not exist. Hardware attacks, for instance [6]. Attackers may use hardware debugging equipment to snoop on data traveling from and to memory, read or write keys, etc. Direct loss of private data may be an immediate result. However, another and perhaps more insidious threat is when the phone is returned to the owner with a backdoor that allow attackers to gather information for a long period of time.

Is this practical? Let us have another look at the example of bluebugging; the faulty implementation that made the earliest bluetooth phone vulnerable to remote exploits was fixed fairly quickly. However, phones could still be compromised. The only thing that was needed was that the bluebugger talked "the victim into handing over the phone, which the bluebugger manipulates to set up a backdoor attack and then hands back" [82].

We stress that the trends are not working in our favor. On the one hand, mobile phones are an increasingly attractive target for attackers. On the other hand, because of power limitations and physical exposure to hostile environments, phones are inherently more difficult to protect than traditional computers. In a future Internet, it is imperative that solutions are found to protect mobile devices that carry

valuable data. Existing paradigms, based on in-network scanning and/or traditional anti-virus software cannot be simply ported to mobile phones.

Possible solution(s). It would be interesting to explore whether security can be (almost) entirely decoupled from the phone itself. Any functionality that is applied elsewhere will not drain the phone's battery and may therefore consume more power. A simple solution in that direction is to apply anomaly-based intrusion detection systems in the network [18], but we have already argued that this approach is limited because some of the attacks stem from a local source (e.g., via bluetooth) and thus never reach the network. A radical alternative model might try to replicate the state of the phone in a dedicated security server [31]. By keeping the copy of the phone in the security server in sync with the phone, all security checks can be applied in the server and not drain the battery of the phone. A simple example of performing file scans in a set of separate servers is found in the CloudAV project [112, 111]. Yet another approach might be to apply more rigid coding practices on phones that rule out the occurrence of certain exploitable bugs by design. The problem with this solution is that it does not seem plausible that vendors will opt it in the short or medium term.

3.3.2 RFID-related threats.

Threat. Radio Frequency Identification (RFID) technology is pushed quite aggressively by industry to help create what is known as an Internet of things. RFID tags contain a tiny, miniaturized chip that is powered by means of induction. Their low cost make it possible to attach them to almost everything: key cards, public transport tickets, clothing, products in a supermarket, pets, passports, and just about anything else. Mostly they are used in supply chain management to identify products. They may also be used to identify users. In these cases, the tags typically contain a fixed code. However, they may be used to store and update a small amount of information also.

RFID introduces a host of security threats. It has been argued in [131] and [145] that RFID technology threats span much of what is known as the STRIDE threat model (originally proposed by Microsoft), which includes Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service, and Elevation of privilege.

Much of the discussion about RFID security to date has focused on information disclosure and tag replication. For instance, various versions of the Mifare chip that is used extensively in public transport have come under attack, when it was shown that the protective methods (including the encryption) can be broken easily [33]. The findings have had tremendous and quite costly consequences in many countries. For instance, they have jeopardized the introduction of the the public transport card in the Netherlands altogether.

The FORWARD project has kept a keen eye on RFID-related threats from the beginning. For instance, in the first year of the project, FORWARD researcher

Melanie Rieback from the Vrije Universiteit Amsterdam was among a group of four researchers asked to advise the Dutch parliament on the matter of the public transport card[1]. Prior to this, she appeared in many newspapers, magazines, as well as on the news on radio and television to comment on the security of RFID.

It is clear that FORWARD has been actively scrutinizing RFID security. Besides the above problems with a particular chip, we suggest that other threats should be taken more seriously also. Spoofing and tampering are particularly worrying.

Spoofing can be accomplished in two ways: attackers may spoof the identity of the reader (in which case unauthorized scanning may be performed), or attackers may spoof the identity of the tag (which may, for instance, lead to unauthorized access). Since tags are typically designed to be as cheap as possible, it is questionable whether high-grade authentication will always be applied in practice [43, 115, 39, 71].

Tampering occurs when attackers modify a tag. For instance, an attacker may modify a tag that identifies a user to something that links the user to a criminal or terrorist (see also the section on data fabrication above). The inverse is also possible, where a criminal modifies a tag so as to appear as a citizen in good standing. Modification of tags in the supply chain may disrupt business operations, or in the case of price tag modification may lead to loss of revenue [13, 71].

However, tampering may also mean the addition or removal of tags. Adding tags to a shipment may make the shipment appear to contain more items. Deleting tags may render items (e.g., products in a supermarket) undetectable.

A development that we consider interesting but not at all surprising, is that RFID tags can be used to carry and distribute malware [127].

A selection of the above threats have, in one way or another, already been discussed in existing literature. In our opinion, they *all* need to be looked at carefully, which in turn requires careful tag management (who is allowed to read or write which tags and when?). The threat or challenge is scalability. Users will not even be aware of all the tags they own and carry around. How can we make sure that the appropriate access policies are applied to things of which we are not aware?

Possible solution(s). Tag management is crucial in all security aspects related to RFID. Some researchers have proposed a guard or blocker device carried by the user that allows users to block readers from communicating with the tags in their possession [65, 126, 43]. All access may then be mediated (vetted) by a security device that makes sure that unauthorized access is not permitted. The problem with such solutions is that it may be difficult to apply specific policies to specific tags. Worse, as one might own many tags, some of which you do not know about, it is difficult to limit a policy at the same time to all your tags, and to only your tags and not someone else's. Typically, blockers prevent readers from interacting with all tags in the user's vicinity. However, the user may not own all tags in the vicinity. We may need to distinguish between important "known to be owned" tags (say the

[1] An reply letter to parliament was sent on March 10th 2008.

tag in your passport) and less important ones that may or may not be owned by you and differentiate access control accordingly.

3.3.3 Threats due to malicious hardware

Threat. Increasingly, hardware design and fabrication has come to resemble that of software: hardware logic modules (resembling software libraries) are licensed from third parties and combined in designs of greater complexity, while the fabrication is outsourced to a low-cost manufacturer or otherwise off-shored.

While this new way of constructing hardware has brought great benefits in terms of design reuse, rapid development and prototyping, and lower component and product costs, it has also introduced new vulnerabilities for high-value or sensitive users of such technologies. In particular, a sufficiently motivated adversary (or a disgruntled employee) can introduce backdoors (*Hardware Easter Eggs, or HEEs*) during the hardware design or fabrication phases. For instance, a hardware designer, by changing less than ten lines of Verilog code, can easily modify an on-chip memory controller to send data items it receives to a shadow address in addition to the original address. Such HEEs can be used in attacking confidentiality (e.g., by exfiltrating sensitive information), integrity (e.g., by disabling security checks such as memory protection), and availability (e.g., by shutting down the component based on a timer or an external signal). HEEs cannot be detected using standard state-of-the-art pre-fabrication testing techniques because the attacker is likely to delay enabling or opening the backdoors until after deployment using simple control circuits. It is even possible to create low-gate-count general-purpose HEEs that can be leveraged by attackers to launch a variety of powerful attacks against the system.

Because hardware components (including embedded HEEs) are architecturally positioned at the lowest layer of a computational device, it is very difficult to detect attacks launched or assisted by those components: it is theoretically impossible to do so at a higher layer, e.g., at the operating system or application, and there is little functionality available in current processors and motherboards to detect such misbehavior. The state of practice is to ensure that hardware comes from a trusted source and is maintained by trusted personnel: a virtual impossibility, given current design and manufacturing realities. In rare circumstances, when volumes are relatively low and the risk is high, physical inspection and verification of the hardware may be conducted. Such inspection is destructive, costly, and time-consuming, and thus can only be applied in few cases and for a small number of samples.

Establishing trust in the hardware components underlying all modern IT will likely prove a key future challenge for the security and hardware design communities. While HEE-based attacks are virtually unheard of to date, economic, technological, and social drivers make these attacks more likely than ever before, while the potential damage from such an attack is extremely high: shutting down an hypothetical adversarys cyber-infrastructure (or “just” a significant or sensitive part

of it) in the event of an armed conflict or during a period of diplomatic tensions can be an effective and cheap way of forcing the outcome.

Some early work on rootkit concealment by leveraging firmware was reported by Heasman [41] and hardware-supported rootkits were discussed by David et al. [23].

Possible solution(s). Addressing the problem requires a concerted, long-term effort in physical design and manufacturing methodologies, secure and trusted fabrication practices and operations, post-fabrication testing and verification techniques, and runtime HEE detection and mitigation. One approach might be to check VHDL code for parts of the circuit that are not active during any of the pre-fabrication tests. However, doing so may be hard and does not guard against all easter eggs inserted between the test and the actual realisation in hardware. The problem domain represents both challenges (in terms of the physical parameters, low-level of abstraction, ease of implementing certain catastrophic attacks, and lack of access to IC internal state) and opportunities (the ICs interface to the rest of the environment is limited and can be completely controlled). We believe that a combination of techniques, combined with updated manufacturing practices, can help mitigate the risks at acceptable cost, both in terms of research expenditures and manufacturing/operational practices.

3.4 New applications and business models

In this section, we discuss threats that arise not because new hardware is introduced, but rather because existing devices are used for new applications. Examples include all sorts of sensors that are increasingly ubiquitous, home automation, etc.

3.4.1 Threats due to false sensor data.

Threat. Sensors themselves have been around for years, but now they are becoming ubiquitous. Privacy is an obvious concern (and interesting new threats to privacy are discussed elsewhere in this report). However, if privacy is concerned with the undesired *leakage* of information, the opposite threat is that of data *fabrication* or *falsification*. Fabrication of sensor data is the topic of this threat section.

Suppose sensor data identify a user as having visited an embarrassing or illegal venue (e.g., the red light district, or an illegal neo-nazi rally). Can we be sure that the user really was present? To what extent can we trust sensor data connected on to the future Internet? Unfortunately, the answer cannot be unequivocally yes due to two reasons: (a) potential bugs in the devices, and (b) potential data manipulation by attackers.

Buggy devices yield wrong information. A common example of a buggy sensor is the barcode reader in the supermarket that double-charges a product. Similarly, supposedly-disabled RFID tags on clothing or other products frequently set off

alarms when a client exits the shop, often creating embarrassment. It has happened to most of us, and these are the simplest examples of what we call buggy devices. While barcode readers result in modest overcharging, other types of buggy sensors are more serious. In some places, automated parking sensors are used to identify your car, and cars are tracked on motorways to pay as-you-go. In several countries, public transport is accessed using a smart card or phone, directly linkable to you. With the increase of the number of sensors increases the probability of false reports.

Similarly, as Internet Protocol (IP) telephony becomes more popular, buggy telephones (or buggy call protocols) may misbehave and dial numbers that are embarrassing to the user. For instance, call records could indicate that employees frequently converse with the competitor (or more embarrassing, perhaps, paid sex lines). It is unclear whether an employee will be able to convince their employers that something went wrong.

Perhaps the most significant threat is that phones, sensors, or databases can be hacked, and data can be falsified. Most information is stored in centrally-controlled databases. Take, for example, your telephone company. Whether you are at home or roaming away from it, all your phone calls are logged by your provider in a huge, centralized repository. A sophisticated hacker or a person with knowledge of a company's internals can alter all the information about your phone calls. Such actions can have significant repercussions in one's life. For example, one may be framed by being linked via telephony records to criminals. Mobile tracking, shopping activities, car parking, they all can be manipulated to create a virtual clone of yourself with unknown implications. In the digital world, where everything is connected via the Internet, planting of "evidence" is both easier to do and harder to detect.

Besides data fabrication, attackers of course may also remove traces. The motivation for doing so may vary. A recurring example in movies and books is that in which potential alibis are deleted, but it is not hard to imagine other uses.

Falsifying sensor data is simply a new variant of form of traditional data tampering. Tampering with data for one's own benefit is hardly new. For instance, in the 1983 Hollywood production "War Games," Matthew Broderick was shown tampering with the school database to change his grade from a fail to a better grade. However, tampering and fabrication to hurt someone is less common, but should be taken more seriously in a world where information is stored in many places.

We have sensors and databases in hospitals, in banks, in organizations, in police and justice departments. Given the proper motive, a person with access to such information can easily incriminate someone. Or worse. Consider a determined attacker who tampers with a patient's medical records. When the patient receives treatment, the doctor consults the e-record to check the patient's medical history. The original medical record indicates a blood allergy to specific drugs. An altered medical record hides this information. Wrong treatment to the patient may have dangerous consequences. As another example, attackers wanting to hurt or embarrass someone may "invent" a serious medical condition, a poor credit history, or a

criminal past, all of which may reduce his/her eligibility to certain programs, jobs, or opportunities.

Another new application domain is vehicular networks. Sensors in cars is nothing new, however cars may in future also receive information from outside the car itself. Currently, information about congestion is broadcast along with public radio signals. This information is then used by navigation device to prevent the user from ending up in a traffic jam.

In the future we expect more of this kind of information and more importantly, distributed using local radio transmitters. Examples are information about road conditions (ice and fog) and the status of traffic lights. Even more advanced are cars sharing information about speed and deceleration. The obvious threat is that people may start broadcasting bad data.

Possible solution(s). While some progress was made in the world of sensor networks on the subject of detecting and filtering out false data [155, 158, 76], it is unlikely that we will be able to prevent falsification of sensor data altogether by means of technical solutions. As a result, the reliability of electronic data should have legal implications. In our opinion, the (un-)trustworthiness of sensor data creates a legal void that needs to be filled.

Most easy solutions are wrong. Admitting sensor data as reliable proof makes little sense if the data may be unreliable, and especially if the data can be altered. But clearly, there is a link between the sensor data and reality in most cases, so we cannot altogether dismiss sensor-based evidence either. Current legislation already looks at some of these issues (e.g., the legal status of footage from a surveillance camera), but the scale at which a multitude of sensors will track persons and objects in the future is such that re-thinking legal implications is important.

The issues that need to be taken into account ranges from evidence based on individual sensors to collections of sensors, and incorporates both agreements between sensors and anomalies. Ideally, there should be a way of establishing the reliability of sensor data. This is not easy. For instance, we cannot say that a certain sensor has a reliability of 98.5%. However, we may be able to categorize the security of devices. Arguably the most important question that needs to be answered is how people who are accused on the basis of sensor data can defend themselves.

3.4.2 Threats to system maintainability and verifiability.

Threat. Smart environments often consist of a large collection of sensors, controls, computing equipment and output devices, as well as connections between them. Most of these devices have existed for years, but now they are combined in complex configurations. Consider a smart home. It may contain a multitude of media devices and sensors, heating, lighting, phones, refrigerators, washing machines, blinds, sprinklers, and both electronic (cameras, motion sensors) and phys-

ical (locks) security devices. Ideally, it would seem, all these systems should be integrated.

It is unlikely that all these devices are made by the same vendor, so there may not be an obvious entity to go to when there is a problem. Even if they are made by the same vendor, there are many things that can go wrong. The probability of some devices malfunctioning or interacting with other devices in an undesired way is enormous due to the large number of devices (all devices in a house times all the houses).

Once there is a problem in such a smart-environment, it may be incredibly difficult to debug it. In essence, the smart home is a complex distributed environment with many nodes that all interact in unpredictable manners. Debugging such complex systems is known to be extremely hard [86]. It may be that a problem with one device (say the locks) is caused by a completely unrelated device (e.g., because a bug somewhere causes a denial of service attack against the first device).

Things become even more complicated when software or hardware is updated, added to, or removed from an existing smart environment. How can we be sure that the complete system still behaves properly? Testing a complex distributed system is exceedingly hard and exhaustive testing is probably impossible.

The real problem is that some errors do not manifest themselves until much later. Moreover they may occur only in rare situations (for instance, due to unusual race conditions, or exceptional circumstances like a very hot summer, or very cold winter).

Possible solution(s). Debugging, upgrading, testing and verification, should all feature prominently in the design of a smart environment. They should not be an after-thought. In our opinion, integration should be limited. While communication between some subsystems should be possible, the number of contact points between modules should be limited. Some subsystems may have to remain isolated from the others completely. Centralization of intelligence and standardized interfaces will also help stem the complexity.

On the longer term, we see a demand for a *simple, formally verifiable* language to express behavior in a complex environment. Verifying large systems is difficult [140]. It seems advisable, to express the “smarts” of the smart environment in this language. Verifiability should be sufficiently simple to allow verification each time the software and/or hardware configuration changes.

3.4.3 Attacks on office equipment that is not a traditional computer.

Threat. Computer security has mostly focused on traditional computers (desktops, laptops, and servers). However, much of the office equipment these days contains embedded computers, complete with full-blown operating systems, a score of processes and exactly the same sort of bugs as found on traditional PCs. While these machines are often peripheral in the sense that they are not worked on directly by employees to create security sensitive content, they may nevertheless *see*

such content. Indeed, they may see sensitive content from many users, and as such be even more attractive targets than an individual desktop PC.

This threat may fit in different categories. For instance, often the problem is exacerbated by new technology (more smarts) in existing technology. We have chosen to classify it as new applications, as the equipment is often not that different from previous generations, but there is more sharing, new and complex remote management, and different use. Attackers often aim for such equipment because they are generally not as well protected by software.

Consider a smart printer. It does not contain a word processor, spread sheet, or similar programs, but many of the documents created with such programs will eventually be sent to the printer when they are finished. A malicious printer could steal and alter the data that is printed, or it could be used by a hacker as a stepping stone for further infiltration into the network. Moreover, modern printers may contain tens of gigabytes of hard drive space, fairly fast general purpose processors, general purpose operating systems (often Linux) and even complete web servers with database backends.

In a recent edition of BlackHat [114], a security researcher called Brendan O'Connor showed how a Xerox WorkCentre Pro could be hacked and used for password snarfing, network scanning (from the inside), changing billing counters, and even changing print jobs (as an innocent example, a scanned image of a paper clip would occasionally be inserted in a print job).

Consider also the example of a network printer that got hacked by spies [42]: In 1999, an intruder hacked into a printer located at the Space and Naval Warfare Systems Command (SPAWAR) in San Diego. The intruder then re-configured routing tables on SPAWAR equipment so that files in the print queue were directed to Russia and then back to the SPAWAR printer. The hijacker could keep a copy or even modify its contents.

Like printers, routers and switches are great targets, as they see all network traffic passing through to them. PABX phone exchanges and storage devices are equally interesting to attackers.

Possible solution(s). Security auditing needs to comprise the entire networked system, including all connected devices. The problem is that often office equipment consists of closed devices. It may be hard to analyze the security of the system if insufficient information is available. Another problem is that it is difficult to track the configuration, as USB sticks, drives, cameras, and other devices are constantly connected and disconnected by users.

3.4.4 Threats to home automation

Threat. Steadily, our homes are being transformed by technology to resemble the data centers of past. With game consoles, Internet enabled televisions, media station personal computers, PDAs controlling the sound system and lighting, and with everything interconnected by wired and wireless networks. This environment

we are called upon to live in is riddled with security pitfalls and dangers. Let us summarize the causes and threats of such environments.

Home devices are generally based on embedded systems. Both the proverbial Internet-aware coffeepot, but also the widely available TiVo-style digital video recorders (DVRs) have some software that was installed on it when they were produced and are likely to be running the same exact software when they reach their end of life and they are thrown away. Without software or firmware upgrades, we run the risk of having buggy code be the target of malware for long periods of time.

As mentioned in the previous section, this concern is shared with office environments as well (e.g. networked printers, VoIP phones, but even switches and routers). Such devices may not have a lot of resources to exploit, but they can provide an important bridgehead for aspiring attackers.

What is common with such devices is that they are typically "under the radar" of security teams, they generally run old software, and their configuration may be full of security holes. For example some security features may have been disabled at some time in the past when a busy system administrator was trying to troubleshoot a problem and then forgot to re-enable them.

Particularly in home environments, there are numerous examples when support personnel (Telco, ISP, DVR etc) have instructed users to turn off various security features while diagnosing problems. Most notably, parents get locked out of their parental control features of their TV sets, so support personnel help them turn parental controls off, rather than telling them how to configure them properly.

Home devices are operated by inexperienced users. Most of us technologists have had personal experiences helping our non tech-savvy relatives, having trouble with their personal computers. In many cases trouble is due to all kinds of nasties that they have unknowingly downloaded into their computers. In a complex home network, most people run the risk of misconfiguring devices and possibly allowing outsiders into their home networks.

Home devices need to inter-operate with all kinds of other systems. Consider a typical home network and the following scenario. The kids go to bed, so, to make sure that they really go to sleep, you have to (temporarily) cut off access to the home entertainment system from their room. At the same time, your next door neighbor comes in for a chat and a coffee, bringing their laptop with them, and asks for permission to use your wireless LAN to access the Internet or to watch some movie you have in your entertainment system. How do you grant limited access to this person? How do you withdraw it later? How do you make sure that he does not access your personal videos or candid photography collection?

Every time one brings a new device into your home, how do you assign rights to it? For example, if its for the kids, it probably should have different rights than

say a device for one's spouse. If you then give it away, how do you make sure that the rights are revoked?

How do you define the limits of your home network? Even wired networks have been known to have lapses of security. For example, Ethernet ports located in the company car park for the benefit of spouses coming to pick up their relatives may be located inside the firewall, hence, providing access to the internal network to anybody who uses the car park.

With wireless networks, things are even worse as their range may well exceed the physical boundaries of a home. In fact, in cities, wireless access points often overlap, and someone can pick up a number of wireless signals most of which are protected by the inferior WEP protocol.

Possible solution(s). We believe it is possible to counter threats due to increased home automation taking a two pronged approach. User education should be part of the solution but possibly the harder to achieve since users need things to "just work" out of the box. So we must be able to offer technological solutions. Offering security out of the box is a very hard problem, but there are steps we can take. For example, devices can ship with a default secure configuration. We must design and build them in a way that guides user actions to avoid security pitfalls. Finally, we could simplify their functionality and interfaces. Simplicity is a key factor to security.

3.4.5 Threats to aviation security

Threat. An area we do not normally associate with smart environment security, but rather with physical security and fault tolerance is aviation and avionics. In principle, the technology is well-known, but it is the combination of different types of technology and novel ways of applying technologies (e.g., wireless connections for airplane control) that creates the threat. As more and more computer functionality is added to aircrafts and the underlying infrastructure, so do the risks associated with computer related failures, malicious or accidental. We split the problem into three categories:

Communication problems. This includes failures in communications between air traffic control and planes, positioning failures (for example GPS hack [123]), even failures in the communications between the airline company and the crew.

Soon aircraft will be able to plan their own routes through the skies, by inquiring the position of other planes and determining their own position via GPS and other means. In this scenario, accidental or malicious failures could threaten the safety of flights.

Avionic failures. Modern planes, such as the Airbus 330 and 340 and the Boeing 787, rely on computers to fly the plane. Gone are the physical wires linking the

pilot to the control surfaces on the wings. These are replaced by computers that receive input from the pilots and control actuators that move the control surfaces.

Things became even more complicated in planes such as the Airbus 380 and Boeing 787, that have *distributed* data acquisition and control networks, derived from optical Ethernet technology. In these planes everything is networked, and there are fears that computers at different levels of trust (avionics, lighting, in-flight-entertainment, etc.) share the same LANs, with the danger that an unforeseen failure in one subsystem may cause secondary failures to more important systems.

IT problems. This is a broad category that includes the IT infrastructure that helps the planes, crews, passengers and luggage to get to their destinations. Again and again we have seen that failures of such systems can not only cause havoc to the plans of hundreds of thousands of passengers, but can even threaten flight safety. In this category, we also include the infamous black list of suspected terrorists. Intelligence agencies use all kinds of heuristics to populate such lists. Once you are in, you are likely to suffer even if you are not a terrorist. Getting out of that list is apparently next to impossible. Hence the creation, maintenance and distribution of such lists is a threat on its own.

Possible solution(s). Addressing problems in aviation security would require a combination of solutions. As we mentioned in the previous paragraphs, aviation security touches many different planes (pun intended), physical security, network security, computing systems security, policy, etc. We could combine proposed solutions from all the above fields in an attempt to address the ever increasing complexity of aviation systems.

3.4.6 Multicore-related threats.

Threat. Paradoxically, the threat of multicore hardware is really a threat of the software. A set of isolated applications each running on its own core is not necessarily more vulnerable that in single core system. However, as soon as software starts spreading out over multiple cores (which is often unavoidable for performance reasons) concurrency problems arise.

Race conditions in software systems that may lead to security violations is not new in the security community. Typically, the attack involves some privileged program that examines the state of a resource before proceeding in a critical operation on that resource. The time gap between the check and the actual operation gives a window of opportunity to the attacker to modify some aspect of the target resource for their own benefit. The vulnerability is caused due to the belief of the privileged program that it is the sole executing entity on a system.

Currently, we are experiencing a revolutionary growth in multicore and hardware multi-threaded systems. The reason is that hardware architects can better exploit the exponentially increasing density on microchips by increasing the number of (slower) processing units than attempting to increase single-threaded per-

formance. The consequence of this is that we are opening the door for a new generation of race condition/concurrency attacks.

Let us not forget that multicore processors are not limited to use on personal computers, but are also used on phones, sensors, and so on and so forth. One may argue that personal computers, which run mostly tested operating, should be able to cope with the increased threat level. But, other devices like mobile phones and sensors, utilize simpler, embedded operating systems, perhaps with fewer facilities to combat this type of attacks.

Possible solution(s). We believe there are specific steps we can take to counter threats from the increased number of hardware processors operating in parallel. We should start by reevaluating our applications and operating environments. Applications have been mostly developed with the single threaded model in mind. Even multi-threaded applications have been designed with only a few tens of threads in most cases. Software architects should begin fundamentally changing the way they build software. On the other hand, operating systems must change to handle the more complex, and parallel hardware. Hardware virtualization is not a panacea but it will certainly help in some respects (although virtualization can also lead to problems that we will not expand in this section). To assist programmers of both applications and operating systems we must invent new programming languages that are designed for highly parallel and multiprocessor environments.

3.4.7 Threats to the wireless plane

Threats. Heterogeneous wireless networks hold the promise of empowering people through a digital environment that is aware of their presence and context, and sensitive to their needs. These wireless networks will enable application areas such as ubiquitous/pervasive computing, resiliency and quick recovery from nature and man-made disasters, and provision of safety services for a better quality of life for elderly and disabled people. Specific applications that make use of the capability of wireless communication systems to connect the physical world to the cyber-world range from monitoring bridges, roads, tunnel structures, and water quality, to controlling the temperature of our homes according to the presence and location of people.

However, the strict resource constraints of wireless networks (i.e., radio frequency bandwidth, energy), and other characteristics of such systems such as mobility and shared broadcast medium, require the use of the complex control mechanisms to conserve the system resources. This makes these control mechanisms a target of choice for denial of service attacks. We have recently shown that most wireless networks are sensitive to what we call cross-layer attacks. Such attacks focus on specific frequency carriers, at specific instants of time, with the objective to corrupt critical control messages crossing multiple layers. With very little resources, a smart attacker can cripple a complete wireless network.

Such attacks can consume four orders of magnitude less energy then previously known attacks. It is shown that these attacks apply to various forms of cellular networks (e.g., GSM, 1xEvDO, WiMAX), wireless local area networks (e.g., IEEE802.11), but also MANETs.

Possible solution(s). It is shown that cryptographic randomization, agility, and diversification, in a game-theoretic context can provide the tools for building resilient wireless networks against both external and internal attacks. Such techniques can even allow the identification of internal attackers.

3.4.8 Threats to the Internet infrastructure

So far we have been discussing attacks to end systems. However the core Internet infrastructure is also a very valuable target from the malicious user perspective. In this section we outline a series of attacks that are possible against the network infrastructure. The attacks are not new, but we expect to see a raising number in the years to come. Furthmore we expect existing attacks to target new applications that are being deployed on the Internet like VoIP, Internet TV, etc.

- Router attacks:

  Direct attacks against routers are already commonplace, albeit not openly discussed. The tendency is towards worm-based exploitation of home routers, wireless access points, and similar - typically badly secured - networking equipment. These types of attack allow for sophisticated man in the middle attacks and sniffing. Emerging threats include DNS or DHCP highjacking, with potentially serious security implications. (Example: “Symantec warns of router compromise,” `www.news.com`, 24. Jan 2008)

- Routing attacks/misconfigurations:

  The global routing system on the Internet depends on correct operation of key service providers. Currently, there is no authentication of routing information, which leads occasionally to major security problems, accidental or intentional. (Example: “YouTube IP Highjacking,” Nanog mail archive, 28. Feb 2008).

- Denial of Service:

  Although technically speaking not a new threat in itself, denial of service attacks keep making headlines (example: “DoS attacks against Estonian targets,” May 2007). While technically knowledgeable organizations are able to fight current attack patterns, it can be expected that attackers come up with new ideas on how to cause a denial of service. These attacks are likely to move up to the application level.

- Lower layer and physical attacks:

  Where physical access to fibers or networking equipment is available, many attack forms are possible, including wiretapping and router intrusions. Social engineering attacks are often successful in bypassing physical access control mechanisms. These attacks require more effort than remote attacks, but where the value of information on the Internet is increasing, this type of attack will become more popular.

- Higher layer attacks:

  As the TCP-IP layers are becoming increasingly robust and attack-resistant, attacks will not only move to the lower layers, but also to higher layers such as the application. DNS poisoning attacks (various forms) also fall into this category. Internet infrastructure is directly or indirectly also affected: Networking equipment is becoming increasingly more complex, and application layer attacks will also be seen against the network itself.

- Loss of visibility: The number of applications using various forms of tunneling or encryption is increasing steadily, both on the "good-warex" and malware side. This makes it harder to counter-act any of the above mentioned attack forms, and adds a significant burden to the network. In the future, new visibility techniques will need to be developed to support network-based analysis of traffic.

- Operational complexity: The complexity of networks has increased dramatically over the last years, and the tendency is still growing. This means that increasingly less operators really understand their network in its entirety. This increasing operational complexity will undoubtedly cause more problems in the years to come, both in accidental operational errors, as well as in deliberate attacks. New mechanisms and algorithms to control and monitor network complexity are urgently required.

Possible solution(s). There are some academic proposals to tackle some of these problems. For example, so-BGP and S-BGP could be employed to address routing attacks, but both are considered too expensive by operators. There is currently no deployable, easy solution for routing security or DDoS [56]. This could lead to major Internet outages, and even a "split" of the Internet. On the front of DNS, the most serious proposal to address attacks is DNSSEC, which will cryptographically secure DNS. While there are problems with its deployment, it is slowly gaining momentum.

3.5 New social dynamics and the human factor

In this section, we discuss threats caused by new ways in which people interact with technology.

3.5.1 Privacy threats: spyware in the bedroom.

Threat. Privacy has been a concern in ICT-environments from the outset. In this section, we identify several interesting aspects to privacy violation, rather than such well-studied topics as spyware, faulty encryption, etc. The threats are again related to new technology that brings existing threats to new environments. Typically, the problems are caused by ultra-portable devices with powerful sensors. The way we interact with the devices has changed. For instance, we now have devices that never leave our side.

We are not the first to observe the threat accompanying the introduction of ubiquitous sensors and mobile computing equipment. Security cameras, keycards, parking sensors, and RFID ranks among the conspicuous examples of such sensors, but the list is endless. In the near future, it may be difficult to engage in activities outside the home without leaving a trail of electronic footprints. Such information in the hands of attackers lends itself to abuse.

What is new is that sensors like phones, PDAs, RFID tags, and media players are increasingly with us *always* and *everywhere*. A compromised phone might be used by attackers to obtain audio and video recordings out of classified business meetings, or even our supposedly private bedrooms and bathrooms. In addition to (visible) security cameras, and other devices in the public space, we must now consider our own devices that may have been compromised and betray us. The closest analogy is that of spyware in a traditional PC that tracks our Internet interests, or gains control over the computer's webcam. However, with ultra-portable devices with a plethora of sensors, the scope for "spying" expends tremendously.

Another new development in the realm of privacy, includes RFID tags. RFID tags worn by users in clothing or "smart cards" may be read by readers close to the wearers and identify and store their presence in sensitive areas. Knowledge about where you have been, what you have done, and what your interests are can be exploited in various ways.

Possible solution(s). Beyond securing the devices that may be compromised, the working group on smart environments could find no immediate technical solution for these privacy problems. An important partial solution is to educate users about how ultra-portable devices will affect their privacy.

3.5.2 Threats due to scale

Threat. New applications on the Internet lead to a growing user base. This is not likely to change. As a result much of the technology that was designed for relatively small networks now have to cope with huge numbers of devices, users, and links. For instance, the Internet itself has grown to a 100-million node network, but most of our models and intuition of the world has hardly moved from the familiar two-node client-server model. As a result, networks are increasingly vulnerable to attacks such as puppetnets can be amplified in proportion to the num-

ber of clients and servers in the system. Similar patterns are exposed in metro-area WiFi networks [3], where minor vulnerabilities are amplified into serious threats due to deployment density, and how the change from wired to wireless brings long forgotten vulnerabilities such as DNS spoofing back to the spotlight.

In the future, we expect recurrent patterns of security vulnerabilities that come with scale. Specifically, in a 100-billion node network, composed of what we consider the traditional Internet, but also smartphones, networked vehicles, and a variety of sensors implanted in our everyday environment, will bring out and transform old vulnerabilities.

Possible solution(s). We believe there are three approaches to counter threats due to scale. Firstly, we must study and understand the interdependencies between systems. Without a clear understanding of possible side effects there is no way to move forward. Secondly, we should model larger systems in our security evaluations. It is no longer sufficient to assume systems of hundreds or thousands of nodes, we have moved firmly into the domain of tens of millions. Lastly, whenever possible we should form clear boundaries between systems. Strict isolation can break the domains in smaller, more manageable sizes.

3.5.3 Sensitive Information in Social Networks

Threat. The main threat here is that people publish sensitive data about themselves in an on-line system. To the users it appears as if they are sharing the data only with their friends. However, often this information is publicly accessable. For example, a picture of college students being drunk at a party may years later be viewed by a prospective employer.

Possible solution(s). Improve security mechanism but especially the user interface to allow people to become aware of the extent in which the information they put online is visiable and to allow them to effective control this.

3.5.4 Valuable Resources in Online Gaming

Threat. A trend in online games is that resources, such as weapons but also real estate, have a real-world monetary value. In some games, users buy the virtual money in the currency used in the game with real world money and use that virtual money to buy objects. In other case, users trade among themselves in online markets that are not connect to the game.

In both cases, theft or destruction of a user's objects represents a real loss. A related issue is that users can pay for good and services in a game using creditcards, etc. Compromising the game may put the user at a risk of online theft of his creditcard data.

Possible solution(s). Security in games has to take these threats into account. In the past the main threat was cheating players. Now, criminals may enter the game just steal objects or creditcard details.

3.6 Conclusions

In this report we presented a list of emerging threats in smart environments. The list was compiled by the members of the smart environments working group and is not meant to be exhaustive but rather reflect what the group thought as the most important threats. In this report, we have categorized these threats depending on whether they stem from new technologies, whether they are triggered due to new applications of existing technologies, and lastly whether they are caused because of new social dynamics.

Chapter 4

Working Group: Critical Systems

4.1 Introduction

Critical systems and networks constitute the critical infrastructure of society. Our everyday life becomes more dependent on their proper operation and service. The extensive use of Information and Communication Technologies (ICT) and their proliferation in many new areas, such as process control and critical infrastructures, pose substantial challenges to critical systems' security.

The Critical Systems Working Group (CS WG) views the critical system as a system or network whose disruption of operation can lead to significant material loss or threaten human life. It can be critical because it is used in a critical application or because it is part of a critical infrastructure. To limit the scope of the working group, and also better accommodate previous initiatives in the European Union Framework Program, we only consider critical systems that are highly dependent on an ICT component, or would be considered to be an ICT in themselves. Such systems will increase in the future. Modern technologies are used for industrial process control and may introduce new vulnerabilities and even be the cause for incidents. Special security measures are thus needed, which take into account the special properties of control systems. On the other hand, advanced automation is widely used in critical infrastructures through industrial control systems, which leads to new security problems. Critical infrastructures themselves expand the scale of security threats with their complexity, large connectivity, interdependency, and possible cascading effects. Even conventional cyber threats for which there are well-known remedies could have large and unpredictable impact on critical systems, since many concerns other than information security are at stake in this environment. The characteristics of critical systems thus highlight the need for security solutions *specific* to those systems and special attention has to be paid to their security. Thus, critical systems are of paramount importance to society and their security has always been a concern. With the growing use of ICT in critical infrastructures and extended application of control systems (e.g., SCADA) [34] the need for secure and resilient critical systems becomes a priority for governments,

organizations, industries, and academia. There also exist signs of a growing interest from the cyber crime community of attacks directed towards the critical infrastructure [34]. Based on the motives presented above, it was decided to investigate the threats to critical systems in a separate working group.

4.2 Outline

The Critical Systems Working Group (CS WG) considers threats against critical systems, especially threats against their supporting ICT infrastructure. Before presenting the list of emerging threats, we discuss the process of the working group in Section 4.3. Understanding how the group worked, also explains the threats we present. In Section 4.4, we give a definition of what we consider to be a *threat*. This is the same definition used by all working groups. Here, we also present a simple model of a critical system to explain how the focus of the CS WG differs from the focus of the other working groups. We then describe the special characteristics of a critical system in Section 4.5.

In Section 4.6, we describe a few typical critical systems with an emphasis on new types of systems we believe will play a major role in the future (e.g., *the connected car*). Given that such systems are being developed and not yet widely used, we expect there is time to rectify security weaknesses before wide deployment, if enough resources for security research are allocated. Particular care have been taken for also accounting for these emerging systems when considering the threat list.

This is followed by the presentation of the emerging threats in Section 4.7. At this point, we have not prioritized the list; instead our list will serve as input together with the lists from the other working groups to a final result to be presented later.

Many experts we have spoken to have also pointed out the unique role of the Internet. For that reason, we devote a section to the issue of Internet and critical systems (Section 4.8). In Section 4.9, we further discuss some particular research methodologies and techniques that we find important when considering how to mitigate the effects of the emerging threats we have presented. This is followed by a short description of related projects we find interesting in Section 4.10. Finally, the chapter on critical systems is concluded in Section 4.11.

4.3 The process of identifying threats

One of the goals of the FORWARD project is to present a list of threats that will become (or remain) significant in the future, thus allowing research efforts to focus on key areas where advances are necessary, if we are to limit the potential of these threats to wreak havoc.

However, in the absence of a “crystal ball” we have to rely on the imperfect information available today. The threat list presented later is the result of a process,

including a series of workshops with both domain experts from critical systems, government and security specialists. By taking known threats of today, in relation to trends in society such as the drive to decrease cost while still increasing the functionality of the system, we make a prediction of important domain areas that could become a serious threat in the future *unless we launch mitigating efforts*. While some of the presented problems are new, others may feel familiar to the reader. We still include the latter to emphasize that the problem is by no means solved and will grow in the future unless it is thoroughly studied.

If you are "just" presented with a list of threats, it is difficult to judge its significance. For that reason, we ask the reader to also consider the process used for creating the list of threats, as this will give a deeper understanding for why we included a specific threat.

We have used a bottom-up approach mixed with a top-down approach in our work. First, experts presented important problems they face. Based on this diverse input, we abstracted the salient features and created a first draft threat list. This list was then taken back to the domain experts and we asked if they still could find the more general problem interesting. Even though not all threats are applicable to all critical systems, we have received feedback that the threats listed are very relevant and are a cause for concern.

Finally, we asked a few domain experts to give us examples how a generic threat from the list would be manifested within their particular domain. This tangible input has also been considered in the threat description to show the reader in a concrete fashion what the threat will involve.

4.4 Modelling a critical system and its threats

In our work, we used the following definition of a threat.

Definition of a Threat : A threat is any indication, circumstance, or event with the potential to cause harm to an ICT infrastructure and the assets that depend on this infrastructure.

This is a variant of other definitions that exist in the literature, among them the definition found in the *EU Green Paper for Critical infrastructure protection, 2005* [20]. We have used an open-ended definition so as the work between the working groups could be coordinated.

In Figure 4.1, a generic ICT system is shown. It is defined as any system that delivers service to a group of users. Such a system is under a number of threats, which may influence the service delivery to the users.

At this point, we do not further define the *system* box but leave it as a black box in the diagram. A ranking of the most important emerging threats can still be performed on such a black-box system. However, by knowing more about the *system* box, we can better judge what types of emerging threats will be the most severe and therefore important.

Figure 4.1: A model of a generic ICT system.

Each working group in FORWARD concentrates on a particular area: fraud and malware, smart environments and critical systems, and within each area we use the specific structure to uniquely fine-tune the ranking of emerging threats. Simply put, each working group treats the *system* box in Figure 4.1 differently. It can be a black box, but it can also be given more structure to scaffold any discussion of emerging threats. For example, the malware group concentrates on a more general list of threats applicable to normal use of ICT by private or professional users. Their list partly serves as input to the other two groups, where more specific but still very important areas of use of ICT are studied. Formally, we see the work as using a ranking function where we, from all possible emerging threats, list a set of the most important ones based on the structure and functions of the *system* box.

Definition of Critical Systems We define a critical system (CS) as a system that delivers a critical service to a group of users. A critical system consists of a traditional critical infrastructure (CI) or a critical application (CA) and supporting Information and Communication Technology (ICT).

Note that even though there are CIs that do not depend heavily on ICT today, we believe a growing number of CIs will depend on advanced ICT services in the future. Also note that we will in this document sometimes use the term critical system (CS) to denote a CI (or CA) as well as the total CI (or CA) plus ICT system. This is for convenience and it should be evident from the context which interpretation that is relevant.

The Critical Systems working group focuses on the ICT that supports critical infrastructures in society. Understanding the emerging threats to such systems is important because the consequences can be very dire. Going back to the simple Figure 4.1, we have a system that delivers services to a group of users. In this document, we define the system as being critical if any service interruption would have severe consequences for the user group. Thus, given that the service delivery is critical we say that the system in itself is critical, when it delivers such critical service. More specific definitions of a critical system can be found elsewhere in the literature. In this document, we by purpose refrain from a very specific definition. The criterion of criticality may change over time and each professional group that discusses the issue has their own definition. A critical infrastructure to a single country is many times not critical to the EU as a whole, and the reverse is also sometimes true. Instead, we present a general model with the important salient properties that is found across many critical infrastructures. Using this model as

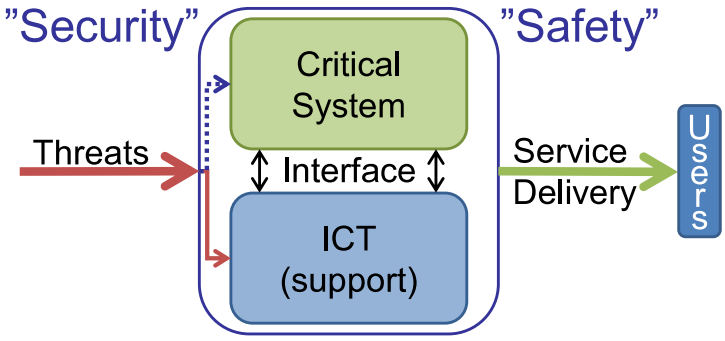

Figure 4.2: A model of a specific system for critical services. We do not consider threats directly targeting the critical system (CS) (dotted line).

the basis for our discussion, we can focus on the issues that will remain relevant in the future.

In Figure 4.2, we have expanded the *system* box first shown in Figure 4.1. Assuming a critical service delivery, we can further detail the structure of the system box based on the model of such critical systems.

We would like to emphasize the following. There are four boundaries: the outer system boundary, the two inner boundaries to the critical system and to the supporting ICT system, and the boundary (interface) between the critical system and the ICT system. This is in contrast to a normal ICT system, where there is no CS–ICT boundary. The consequences of the CS–ICT boundary will be discussed in greater detail below. The threats can then be divided into four groups according to the boundaries shown in Figure 4.2.

1. Threats targeting the whole CS / ICT.

2. Threats targeting the interface between the CS / ICT

3. Threats targeting the ICT part, especially considering the special conditions on the ICT part listed below (see Section 4.5).

4. Threats directly targeting the CS.

We do not consider threats that directly target the critical system (4), in that it is a critical infrastructure. Such threats are already discussed and accounted for in other working groups in the EU. The focus of FORWARD is on cyber threats, often directly targeting the ICT structure by their very nature. Thus, the focus is on problems related to the supporting ICT infrastructure, that is (1) – (3) in the table above. We would like to emphasize (2) in the table, as the particulars of this interface may be prone to many security vulnerabilities.

4.5 Specific characteristics of a critical system

In the Critical Systems working group, we specify the structure of the *system* box from Figure 4.1 in more detail. The result is shown in Figure 4.2. The *system* box is now divided into two parts: one part being the actual critical system (or critical infrastructure) and the second part being the supporting ICT infrastructure. In some cases, the critical system is of an ICT nature; in other cases it is a traditional process control system or something similar. Below follows a list presenting some of the specific characteristics of a critical system as shown in Figure 4.2.

1. *Critical service*. A Critical System is delivering a critical service to users, which has to be preserved and maintained even in the case of cyber attacks. The disruption of operation of such systems will lead to severe consequences.

2. *Complexity and availability*. The complex architecture of critical infrastructures hampers investigation and assessment of the impact of threats. Further complicating the issue is that many of these systems need to run around the clock all days of the year, meaning that a system cannot simply be brought off line.

3. *Many and different interfaces*. There are various types of interfaces to a critical system and it is not as structured as an ordinary system. Rather, it is the result of combining several independent systems. Thus, there are many interfaces and they differ greatly in many ways (expanded below). This affects the vulnerability of the system as a whole. Critical systems have specific and diverse relations with ICT systems and between internal systems. Further, the system mixes interactions of human operators (slow response) with computer services (fast response) through a variety of interfaces. Many times these interactions are rather complicated in that the access modes vary and the time frames between the parts are widely different.

4. *Interdependency issues (long chains of dependencies)*. One of the important issues for critical infrastructures is the interdependencies among the infrastructures. There may be long and complex dependency chains, where service 1 depends on service 2 that depends on service 3, etc. An attack against any of the services may cascade unpredictably through the system. In [128], the role of ICT in critical infrastructures is defined with the term cyber interdependency. An infrastructure has cyber interdependency if its state depends on information transmitted through the information infrastructure. Virtually all modern critical infrastructures are influenced by and dependent on the security of the information infrastructure.

5. *Data is important*. Almost always, data is important [16]. This is especially true for *financial services*. It is also true for other types of systems, such

as air traffic control in Europe, where data are underlying even the simplest decisions.

6. *An underlying physical process*. Many times, a physical process is underlying the critical system. The system has to observe time constraints which are hard to combine with certain security measures. The physical process may be a *control loop* in the physical system. Thus, critical systems have physical and possibly a very complex interaction with the environment. Security functions integrated into the critical system must not be allowed to compromise the normal functionality of the critical system [109].

7. *Real-time constraints*. The above, described in point (6), implies that critical systems are often real time, as they are determined by physical systems. They may also be considered real time in that they deliver a critical service that should not be interrupted. Depending on the specific system, the term real time may imply very different time scales; in air transportation this could be seconds, in other cases hours or even days. Critical systems are generally time critical and have to respect some acceptable levels of delay and jitter dictated by the individual installation. Some systems require deterministic responses. This may mean that they have to observe time constraints, which are hard to combine with certain security measures. High throughput is typically not essential to CS. In contrast, ICT systems normally require high throughput, and they can typically withstand some level of delay and jitter [109].

8. *Many owners, policies and domains*. Often, a critical system has many owners and this fact is emphasized through the deregulatory nature of policy decisions taken lately. The mixed ownership affects the system as a whole, in that there are artificial interfaces between the parts and each part may be governed by its own security/safety policy. For example, data is often sent over both propriety networks and Internet.

9. *The trade-off between safety and security*. Based on the tradition of safety-critical systems, safety is and has been emphasized over security. Examples exist in the industry corroborating this statement. For example, passwords are sometimes avoided by intent; it is reasoned that sometimes it is very important to immediately be able to control a process (to stop it from reaching critical mass), and a password would only slow down the operators. Thus, no regards to integrity or access control exists in such a system and such features cannot easily be added later, or added to one part of the system if another part lacks such support.

10. *Mismatch of practices between CS and ICT systems*. Operating systems (OS) and applications in critical systems may not tolerate typical IT security practices. Legacy systems are especially vulnerable to resource unavailability

and timing disruptions. Control networks are often more complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). Software and hardware are more difficult to upgrade in an operational control system network. Many systems may not have desired features including encryption capabilities, error logging, and password protection [109].

11. *The human factor plays a pivotal role for proper operation*. The human being is considered to be the weakest point in a critical system. The roles include operators in control rooms, engineers taking technical decisions, managers and decision-makers for future strategy development. On the other hand, insiders with experience of and knowledge about the critical system could be a serious threat.

Even though the emerging and future cyber threats seem common for all ICT applications, there are specific issues regarding the subdomain of critical systems. The special attention to the critical systems will help with a better understanding of the new challenges and with finding appropriate countermeasures. As can be seen, there are many differences compared with a regular ICT system.

1. *No ICT–CS boundary*. In a regular system, there is no ICT–CS boundary.

2. *No limitations from physical laws*. A regular ICT system is not normally connected to a system governed by physical laws. This implies that a regular ICT system does not have the same constraints in terms of timely input of data or a similar limitation on the types of interfaces available.

3. *No critical service delivered*. No critical service is delivered by a regular system.

4.6 Examples of critical infrastructures

When speaking about critical systems, it is important to understand the wide range of systems they encompass. Even though we spoke about the special characteristics of a critical system in Section 4.5, we will illustrate very briefly with a few practical examples.

A “traditional” critical system controls public resources such as water, electricity, and telecommunications. A SCADA system may be involved. Many security weaknesses in SCADA systems have been discussed elsewhere and there are important on-going efforts to secure such systems.

Below we describe three systems that also can be considered as critical systems but with different characteristics from the traditional ones. The *connected car* is a type of system that is growing in importance. The *data centers* follow the

trend of using the *cloud* for storage and computation, and, finally, we discuss *financial systems* where the ICT component is indistinguishable from the actual critical system.

When considering the threats presented in Section 4.7, a "traditional" CI is probably more susceptible to certain threats (old system design and hardware) than a more modern system. We also consider the *emerging* critical systems, such as the *connected car*, as systems that will grow in importance and thus, also problems related to their area will become more important in the future.

Finally, a word about the Internet and its role as a critical infrastructure. Given that the Internet (and other large networks of specific operators) has such a special role due to its special importance for everybody and everything, it is discussed separately in Section 4.8.

4.6.1 The transportation area: Connected vehicles

Road transportation is undergoing a significant technological transformation with wireless communication enabling vehicles to both communicate with other vehicles and with the infrastructure, thereby improving safety, mobility, vehicle performance, and personal convenience. Improved connectivity for vehicles allows for more effective fleet management, route planning, resource planning, reduced fuel consumption and safety. For example, hazardous goods could be routed around areas with a lot of traffic or people. To enable connected transports it is necessary to build an infrastructure of connected roads [21].

Thus, connected vehicles will play an important role in the transportation sector. This implies that information technology is entering (or has already entered) into the automobile domain and into each individual car. Most of the functionality in a car is nowadays controlled by electronics and software, and it provides electronic interfaces to its environment. The idea among automobile manufacturers is to perform administrative procedures, such as diagnostics and firmware updates over a wireless communication channel, and also to provide various services which allow hand-held devices, such as cell phones and PDAs, to interact with the vehicle. Thus, the notion of the *connected car* emerges. As a result of allowing external wireless communication to interact with a safety-critical device such as a car, a number of *safety-critical security risks* are introduced. Human lives are potentially in danger.

The vehicle domain has traditionally only dealt with safety concerns. However, the security risks create a need to consider the threats presented by an intelligent attacker, as these threats can now have a significant impact on safety. Since the wireless vehicle network will involve millions of vehicles and drivers, it will be a critical infrastructure of very high magnitude. The conclusion is that there is an imminent need to study and assess future cyber threats for the transportation area and to suggest proper security solutions.

4.6.2 Data centers

Data centers, and the wider paradigm of cloud computing, are becoming ubiquitous. As they provide data necessary for more traditional CIs, their importance will grow. A majority of the data centers available today are privately owned but accessed through open standards (often over the Internet). For several reasons, details about major data centers are scarce. For example, competitive business advantages may be involved in the construction and running of such centers [94].

We expect several problems in regards to this new type of critical system. Hiding the details of the data centers means less understanding and less control. For example, "different" backup systems could easily be served on the back-end on the same data center. Other more mundane problems can also be enumerated. These data centers store very sensitive information, and the information can be compromised or lost by physical theft of hard drives or by a lack of vigilance in managing routine processes, such as off-site maintenance and retirement of old equipment [132]. Many such exposures have already been reported and other problems are discussed in [84].

As the data center becomes a natural agglomeration of information from many places, we believe the *insider* problem (see Section 4.7.3.3) will be especially severe for data centers. No longer is only a single organizational entity at risk from an insider attack, but the problem can easily escalate across the organizational borders.

Some of the problems facing the data center can probably easily be solved with known security mechanisms (such as encryption for sensitive content). However, as the domain is relatively closed with the centers privately owned, the discussion and analysis of their function are lacking. An open approach is necessary to avoid more severe problems.

4.6.3 Financial systems

Financial systems are a back bone for trust within a society and for that reason, it is critical they work. However, the financial system (and its related data center) is very different from a more traditional critical infrastructure, such as the power or water plant.

For example, the financial system is integrated in the supporting ICT. It is difficult to view this critical infrastructure without its ICT component. Recent developments have also changed the access control model to the financial system. There are now a multitude of access points to the system: ATM, bank, cell phone, local consumer's computer for Internet banking, etc. These access points use either private or public networks to reach the bank. Regardless of the security built into the protected core of the system, these terminals might easily be attacked or replaced. This, especially, puts a focus on the *access control* mechanisms. It is not possible to have a single security perimeter when the clients are outside but still allowed access to the system.

The real-time nature of the financial system is also different from other, more typical, CIs. A slower response is accepted with a singular payment but it is critical to have instant response to close down one path into the system when malicious behavior is detected.

Even though the financial systems present new security challenges, this is also one of the areas where traditional security is extensively used and where the personnel is very knowledgeable. However, several attacks have been documented, many times targeting the customers of the bank. There are examples of criminal groups using malware to steal money from banks. See for example Nordea Heist (2006), where criminals successfully obtained the login details to the bank from several customers. This was done through a malicious program (Haxdoor) [107].

4.7 Threat list

In the sections above, we have described a simple model of a critical system to illustrate the specific properties of such a system, as well as to show the focus of this working group. A number of actual critical infrastructures has also briefly been described, to show that the area encompasses both old and traditional systems as well as new types of systems with their own unique environment.

When discussing the list of threats to include, there was a trade-off between being too general and being very specific. For that reason, the threats here are a mixture; when we use general language, we also try to show with concrete examples how the specific threat would manifest within a selected critical system. The role of economic market forces is also accounted for when considering new threats. The antagonist can come from a terrorist organization or from organized crime. Knowing the driving force of the antagonist and his possible gains also direct us to important threats.

The threats are assigned to one of three different groups to reflect various aspects on a technological / sociological scale. These groups are *New technology*, *New applications on existing technology* and *Social dynamics and human factors*. The introduction of new technologies is a challenge in any area of application, because they come with new requirements to the systems and networks. From a security viewpoint, new technologies come with their sometimes insufficient security capabilities and vulnerabilities. Moreover, not all new security measures developed for a regular system are directly applicable to a critical system. Regarding the new applications group we have included threats that emerge from different kinds of applications, whether intended or not. Thus, hidden functionality is a threat in this group. The third group is related to social dynamics and human factors. Here we have included threats that result from the different cultures between safety and security communities and the threat from human factors in general.

We realize that in some cases the grouping could be discussed and it is true that a certain threat could sometimes belong to more than one group, depending on what aspect of the threat that one finds most important. However, we believe

that the suggested grouping should facilitate the reading and understanding of the threats.

The potential *gain* of an attack has in several cases also been a driving force when discussing the threats. It is best illustrated with an example. For example, using wireless technology for control systems and connecting these very same systems to the Internet has a similar effect – it creates holes in the security perimeter and allows remote access for attackers. We could have chosen to structure the list of threats based on their effect, but we found that it was better to divide the areas as the potential mitigating solutions would be different, depending on the area.

When discussing the solutions, it is important to remember the properties of a critical system. These systems cannot easily be taken off-line. This leads to problems that face security professionals dealing with critical systems. First, they are only patched irregularly. Antivirus might be old and the systems might be running on old operating system versions. Second, larger security solutions can never be subjected to full operational testing – these systems need to run continuously and normally cannot be taken off-line.

4.7.1 New technology

4.7.1.1 Sensors as the "New Computing Class"

Threat: The convergence of control with communication and computation will make sensor networks the new dominant "computing class." This class will provide the ability for large numbers of sensors, actuators, and computational units (interconnected), to interact with the physical environment. This computational shift is going to bring a big shift also on computer security issues.

Description: In addition to the security concerns of wireless networks in general, wireless sensor networks have a number of additional ones.

- The nodes in sensor networks are in general very limited in terms of battery, storage and computational power. Therefore strong cryptography and other general security tools are of limited use, if at all available. An attacker can have much more powerful hardware than the nodes being attacked.
- Sensor networks typically reside in unattended environments where an attacker can physically destroy nodes, add malicious nodes or in other ways tamper with the hardware of the network.
- Nodes in a sensor network die for many different reasons. For example, battery can run out, nodes can break during deployment when they are deployed (thrown out from an air plane) or break during operation due to a harsh environment. It is hard to distinguish such natural failures from a malicious attack where nodes are deliberately destroyed.

There are many venues of attacking sensor networks [17, 118] including the following.

- Snooping information
- Inserting false or misleading information [89]
- Jam radio channels
- Make nodes run out of battery by never letting them sleep
- Give the impression of phantom nodes that do not exist [108]
- Give the impression of connectivity that does not exist [68]
- Make messages go through an attacking node that can selectively drop messages from the system [68].

Possible solutions: We consider the following three approaches worth further pursuit.

- Autonomic solutions where the system will continuously evolve and control its security.
- Solutions that will mask subsystem takeover.
- Combining sensor information with physical information for verifying certain operations.

4.7.1.2 New Generation Networks

Threat: New Generation Networks bring new security challenges.

State of the art: Recently, there is a general trend for carrying multimedia in the field of electronic communications. This was imposed by Internet as it is its inherent feature. Under the pressure of Internet, on the one hand, and because of the increased service requirements of end users, on the other, some telecommunication companies are migrating to the so-called Next Generation Networking (NGN).

NGN is a broad term describing some key architectural modifications in the telecommunication core and access networks that have been deployed in the last five years. The general idea behind NGN is that one network transports all information and services (voice, data, other media) by encapsulating them into packets, as is done on the Internet. NGNs are commonly built around Internet Protocol, and therefore the term *all-IP* is also sometimes used to describe the transformation towards NGN [151].

Within the Bulgarian Telecommunications Company (BTC), a project has been running since 2004 for migration of the existing national operator's telecommunication networks to NGNs. The BTC has built the so-called *converged NGN*, which provides voice services, transport services for VPN, data services, and Internet access services. The Next Generation Network combines best characteristics of

former and present communication technologies [151], [125]. In addition, similar projects to this one in the BTC are going on in KPN in the Netherlands, in Ireland [151] and in British Telecom (BT) *21CN* in the United Kingdom.

Outlook of the problem: The openness and easy access and usage of NGN lead to an increased number of vulnerabilities and extreme attention to security measures must be paid. The following is written in [146].

> As part of its responsibilities, DHS (Department of Homeland Security) created the National Infrastructure Protection Plan to coordinate the protection efforts of critical infrastructures. The plan recognizes Internet as a key resource composed of assets within both the IT and the telecommunications sectors. It notes that Internet is used by all critical infrastructure sectors to varying degrees and that it provides information and communications to meet the needs of businesses, government, and the other sectors.

This excerpt confirms the *upcoming critical role of the Internet in CI* and this trend seems unavoidable. The same basic characteristics, which make Internet so prone to evolvement and so ubiquitous, are now sufficient for considering Internet in itself a potential threat-generating environment.

On an open network such as the NGN [143], capabilities and responsibilities for providing security may reside at any level/layer or with any participant, making security an end-to-end challenge. The NGN as part of the information infrastructure, and thus as a critical asset, depends upon transport networks being highly available, reliable and tamper-free, even under stress.

Possible solutions: As described in [143], the security mechanisms on open packet networks will be very different from those of legacy telecommunication services in many aspects. In legacy networks, being circuit-oriented vertical networks, much policy management was “built into” the integrated service, comprising all aspects of the network. Security will need to be addressed differently in the NGN.

The design and implementation of NGN should meet complex requirements, which complicates its security architecture. As a consequence it is difficult to use a single standard to define it [160]. As a present security solution it was recommended in [157] to use *multiprotocol label switching* (MPLS) VPNs to construct an NGN virtual private bearer network, and thus logically separate NGN services from traditional data services.

4.7.1.3 Wireless communications

Threat: The use of wireless communications in critical industrial applications.

State of the art: Today, wireless communications are not yet widely used in practice in industrial environments. Most plants are only considering them for information gathering in the form of measurements, but not for closed-loop control [66].

However, wireless technology is compelling because of its many advantages: operator mobility, safety, access security for visualization and optimization, and the immediate benefits of their deployment [11]. There are already applications for maintenance, condition monitoring, asset management, asset tracking, etc. Such applications improve efficiency but may not be directly related to actual control or incremental measurement of processes. Based on these compelling advantages there is reason to expect a greater adoption of wireless communication in industrial control, thus with an overall growth in its market share.

Outlook of the problem: Experts from WINA and ISA [87] predict that within 10 years, even critical control communications will be wireless. Recently, following the WirelessHART and ZigBee Alliance announcements and after approving the SP100 standard for industrial wireless communications by ISA, there is already use of wireless communications in industrial and even critical applications. Despite this, the single industrial wireless standard ISA-SP100.11 does not give enough guarantees for dependability and security to critical systems and applications. It can be expected that the use of such systems and hence the problems will expand in the future.

One main security aspect of the wireless communications in general follows from the unbounded nature of radio frequency (RF) propagation. The perimeter of a wireless network cannot be limited and controlled as can be done with a wired network. There are reflected signals, which find their way out of buildings. These dispersed signals could be detected by motivated attackers that could then attempt to interfere with them if they are in physical proximity of the facility. Thus, traffic can be passively captured and an attempt to penetrate the network could be made with the aim to reach other connected enterprise networks. Both RF attacks based on frequency jamming and protocol attacks based on crafted packets can create denial-of-service situations that interfere with the operation of the LR-WPAN network [90]. Another serious security problem in using wireless communication is related to the security of the access and communication protocol itself. Here, we will face the same type of problems for wireless applications as we already see for non-wireless ones.

Possible solutions: Whereas all of the experts are convinced of the extended use of wireless communication for industrial communications in the future, some of them also comment on the risks involved, and especially emphasize the careful introduction of these technologies. The first and main consideration when addressing security of industrial wireless communications is the conformity to the ISA-SP100 Usage Classes. There are many useful recommendations like those in [90, 91], where detailed recommendations for securing wireless networks are given.

Some of these considerations for industrial environments can be as follows: depending on the problem, use of least susceptible frequency band in case of intensive electromagnetic interference (EMI), or increasing the transmit power level by using a higher-gain antenna, if the amount of electromagnetic noise is signifi-

cant. In other cases, it may be better to reduce transmission power levels or deploy directional antennas in order to reach negligible levels of the stray signals.

The use of a *frequency hopping* (FH) radio with configurable hopping channels and patterns can help mitigate/avoid interference, reduce multi-path fading, as well as provide an additional measure of security, if a non-default hopping pattern is used and also changed on a periodic basis [90], [91].

The IEEE 802.15.4 standard [54] supports an optional GTS transmission. To mitigate real-time operation problems, it is recommended to use *guaranteed transmission mode*, whenever possible. For securing the industrial wireless communication the secure mode is supported in the standard.

4.7.1.4 Unforeseen cascading effects

Threat: Interconnected systems and networks are difficult to model properly and interdependencies between them can lead to cascading effects that are difficult to foresee. This is due to the inherent complexity of the connected systems. It is claimed that nobody *really* understands a network such as the Internet anymore, let alone interconnected, heterogeneous networks. Further, testing is virtually impossible due to the complexity and, in particular, not when the system is connected connected to a critical infrastructure with real-time requirements.

Another important cascading effect occurs when, e.g., the Internet is attacked or overloaded resulting in a denial-of-service situation. This will naturally affect a connected critical system, even though the attack was not directed against the critical system per se.

Details: Large networks and systems are very difficult to understand due to their complexity. This applies to a single network infrastructure. Connecting two or more infrastructures together will make this complexity grow exponentially. Even though system complexity is an issue for all working groups, some factors related to critical systems make the issue of the complexity of systems extra severe. First, due to the deregulation of markets, critical infrastructures are often run by different organizations that need to cooperate. These organizations are seldom a single unit, but they are comprised by many smaller units as virtual organizations (see for example Figure 4.3). A complicating issue is then that part of the system may be governed by proprietary protocols while others use open standards. Different system owners may not trust each other, and different parts of the system is governed by their own safety / security policies.

Possible solutions: Development of appropriate models for the domain and an overall better, probably structured and hierarchical, architecture with a security baseline. Removing the human from the loop and introducing automation, because the seemingly intuitive action might be completely wrong and lead to large problems.

4.7.2 New applications on existing technology

4.7.2.1 Hidden functionality

Threat: One threat of paramount importance is that of hidden functionality in systems, and in particular, in software. Hidden functionality may be almost any functionality, but common examples are backdoors, i.e. secret and undocumented entries to a system, and Trojan horses. Such functionality can be introduced into the system by accident, but the most common reason is that somebody, for example the designer or maintenance engineer, enters this functionality for his own, in many cases malicious, purposes. In other cases it is introduced for commercial reasons. Regardless of its purpose, the idea is that this extra hidden functionality is not known by the authorized user and the rightful owner of the system.

It is evident that such functionality presents an enormous threat. Not only is it unknown, but it is also put into the system in such a way that it is very hard to find it. Furthermore, this functionality is totally uncontrolled and can lead to a large range of very detrimental impacts on the system.

Possible solutions: It is very hard to find solutions to this problem. Any type of remedy would imply that you must be able to prove, or at least make plausible, that no such functionality exists. Unfortunately, there are significant theoretical obstacles in proving the *absence* of something. It is certainly possible to find and remove such functionality, but to verify that there is none left after removal is extremely hard. Still, the only possible solution would be to develop better validation and verification methods and tools. A methodology for measuring security could be one of them.

4.7.2.2 Retrofitting security to legacy systems

Threat: Security can seldom be retrofitted to an existing system, but economical constraints might still make this necessary. Most critical systems are created to provide a certain functionality. Safety and control characteristics are the natural focus of such systems. Thus, applying security measures afterward instead of incorporating it in the original design could constitute a problem. For example, the in-vehicle network has historically been a closed environment responsible for the control and maneuverability and safety of vehicles. The in-vehicle network has been designed to provide this functionality, and security has not been part of the design. The connected car scenario, described in Section 4.6.1, allows external communication to interact with the previously isolated in-vehicle network. Thus, the in-vehicle network is opened up to potential attacks. Designing security solutions for the existing in-vehicle network creates difficulties as real-time constrains, protocol and hardware limitations need to be considered. In addition, security solutions must not interfere with the functionality provided, e.g., by imposing delays as this could have serious consequences from a safety perspective. Due to economical constraints it may not be possible to redesign the entire system with security in mind. Either the best possible security solutions considering the existing system

are developed and applied and as a result possibly degrading the system's performance, or good enough solutions are applied to ensure that the existing system's functionality is left unaffected.

Possible solutions: Short-term solution: a better understanding of how to best adapt security to such systems. Analysis of what new features can be added without unnecessary risk. Study the dependability of the different parts. With education and training, new architectures can be developed where security permeates all parts of the design for the long term.

4.7.2.3 The use of COTS components and systems

Threat: The use of COTS components and systems can make the critical system vulnerable to a variety of attacks. The fact that makes the threat of COTS components especially severe is that the designer has no real control over the product he is introducing into his system. The COTS product is designed (and manufactured) elsewhere and the documentation can be incomplete or faulty. There is no guarantee that there is no hidden functionality, such as back doors or Trojan horses. Nor can the absence of these be verified, as discussed in Section 4.7.2.1.

State of the art: To reduce cost and time for design, the use of COTS systems and components in critical applications seems attractive and will thus continue. COTS systems are used in industrial automation process-control systems because they are cheaper and more efficient. Going to COTS components the emphasis is on cost and new operations. In process control systems, however, the main concerns are availability and safety. There is a gap between the priorities (safety versus cheap COTS components) and this gap leads to new challenges to security and reliability.

There are some projects (e.g., DEAR-COTS [24]) where COTS components are applied to design distributed computer-controlled systems. They are organized using redundancy and design diversity to make the system dependable and secure. Some of the issues addressed in DEAR-COTS are the use of emerging information technologies to cope with heterogeneity issues while providing a dependable user-friendly man-machine interface.

Another trend that seems inevitable is the transition to ICT in process control. Proprietary solutions are replaced by open and conventional protocols and networks and security techniques and technologies have to be introduced. There are efforts to apply COTS components and open-source standards along with the standards for process control systems. The organizations from industry that develop commercial interface standards work with some military programs to include real-time and fault-tolerance requirements [150].

A real-life process control system for oil and gas is shown in Figure 4.3. The objective in this system is to introduce more automation and many ICTs will be implemented into it in the next five years. These systems will be operated remotely. The operator will be out of view of the real systems and it will be difficult to assess any special situations that may arise. For that reason, computers will control

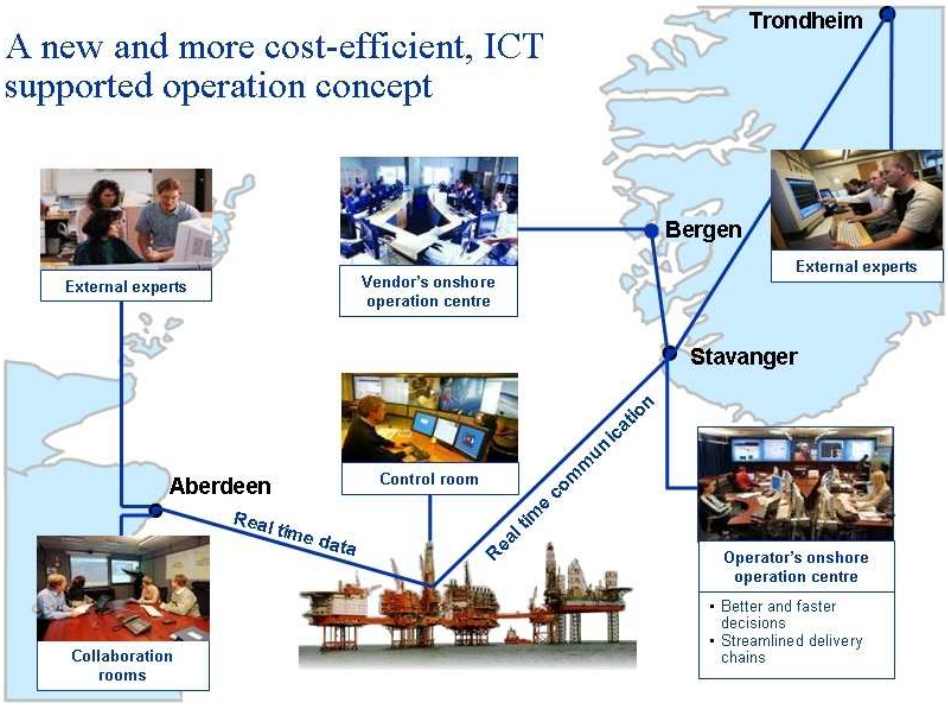

Figure 4.3: A new and more cost-efficient, ICT supported operation concept.

many functions but they are prone to virus infections. There will be remote access through connections to Internet, leading to new threats. Response management is needed, coping with incidents – recovery, isolation, and restoring the system to a working state. Forensics should be also applied to determine the responsibilities.

Possible solutions: No good solution exists, but various work-arounds, such as using COTS systems with some fault-tolerant approaches (replication, diversity approach); applying the COTS components in non-critical areas only; introduce and manage heterogeneity; or use of a compact and trusted application base.

Another possible approach is to introduce semantic technologies, i.e., to take a holistic approach to security with semantic technology (e.g., SOA). Physical components should be classified, as they have to be defined from the basis. We have to identify and decide what and how to protect, i.e., an assessment of the assets to be protected has to be done.

4.7.3 New social dynamics and the human factor

4.7.3.1 Safety takes priority over security

Threat: In the domain of critical systems both safety and security are important but in certain scenarios, safety takes priority.

Outlook of the problem: Based on the tradition of safety-critical systems, safety is and has been emphasized over security. Examples exist in the industry corroborating this statement. For example, passwords are sometimes avoided by intent. It is reasoned that sometimes it is very important to immediately be able to control a process (to stop it from reaching a critical point), and a password would only slow down the operators. Thus, no regards to integrity or access control exists in such a system and such features cannot easily be added later, or added to one part of the system if another part lacks such support.

Giving priority to safety is not just a traditional vision. It is justified by the potential losses after a safety incident. The safety of critical systems is important because of CS interaction with the physical world and the possible risks of that interaction. Security is usually considered being of less importance compared to the major safety issues of the actual CS. With the extensive use of ICT in critical systems, however, security should be considered more seriously, since security and safety are very interrelated. Problems with security can lead to safety issues. Thus, a security attack can lead to a safety problem and endanger lives.

The lack of mutual understanding between the control and security communities (discussed in Section 4.7.3.4) makes the overlooking of security a problem. Control specialists and even the management personnel of organizations are security-unaware and tend to neglect security measures and tools. Sometimes people with little experience or with different primary tasks operate the supporting IT system and they are more prone to do mistakes or ignore security alerts. All these problems stem from the vision that safety is the main priority and security is only a complementary measure to maintain the ICT supporting network properly operational.

Possible solution: As we stated previously, the understanding that safety and security are interrelated is of very high importance and will lead to improvement in overall security and safety policy. A better understanding of the domain for the IT security experts is necessary. On the other hand, the control community should be aware of the important role of security measures to safety. Security should be tailored to the specific characteristics of the CS. Some new solutions might need to be developed.

4.7.3.2 The human factor

Threat: The weakest link in the system is the human. This is especially true in critical systems where the *human – system* interaction affects safety and could have serious consequences.

The human factor plays various roles in critical systems, including roles such as operators in control rooms, engineers taking technical decisions, managers and decision-makers for future strategy development. It was estimated that in some situations, human reliability falls from 10^{-4} to 10^{-3}, whereas system's reliability is 10^{-9}. There are incorrect interactions with the system, other operator errors, and

interdependencies. The human being is a serious factor when considering overall system security.

There is a lack of understanding of the overall (critical) system, since their complexity is continuously increasing. This is growing to become a serious problem. Large networks are hard to encompass and their comprehension goes beyond the capacity of the human brain. Introducing automation could help coping with this problem.

Possible solutions: The education and training of personnel working in critical systems is a constant task that can help maintain an up-to-date knowledge on systems and networks. The awareness of security risks should be raised. There are many bad practices (e.g., running unpatched versions of software, using default configurations and passwords, etc.) that could easily be removed by making people understand the role of security measures. A sound and evolving security policy in the organizations is needed to mitigate security risks. There are approaches to model the user (*cognitive modeling*) and user-interactive properties that could be used to improve the interaction of the users with the systems.

Another approach is to model and design the systems in such a way that they are more easily comprehended and understood. This would include e.g. structural design, encapsulation, intuitive interaction interfaces, etc.

4.7.3.3 The insider threat to critical infrastructures

Threat: Insiders are employees with experience of and knowledge about the CS. The threat from the insider lies in the risk that a trusted employee betrays their employer by conducting some kind of malicious activity. Insider betrayals comprise a broad range of actions, from theft or subtle forms of sabotage to more aggressive and overt forms of vengeance, sabotage, and even work place violence. Insider activities cause financial losses to organizations, have negative impacts on their business operations and damage their reputation. It is of particular concern to the financial sector where the problem is known, but also other sectors are realizing the damaging effect an insider can have.

In [110], it is argued that the nature and seriousness of the threat requires a combined view of physical and IT security systems and policies. Although physical and cyber threats from insiders manifest differently, the concepts are quickly converging as many potential attacks bear characteristics of both physical and IT sabotage, fraud, or theft.

The “insider threat” to critical infrastructure is defined in [110] as the following:

> one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity’s security, systems, services, products, or facilities with the intent to cause harm.

One of the main findings of that particular study is that any modeling of the insider threat needs to take into account the potential of combined physical – cyber attacks. Moreover, a coordinated attack combining an insider attack with an external attack could have multiplier effects and could be much more destructive than a simple one-dimensional attack.

Some interesting results from a study on the insider threat [70] show that a negative work-related event is most likely the trigger to most insiders' attacks. Furthermore, the majority of insiders planned their activities in advance. An observation is that the majority of insiders were granted system administrator or privileged access when they started work, although less than half of the insiders had authorized access at the time of the incident. An interesting point is that both unsophisticated and relatively sophisticated methods for exploiting system's vulnerabilities were used. Remote access was used to carry out the majority of the attacks. Many times, the insider attacks were only detected when there was a noticeable irregularity in the information system or when a system became unavailable.

Possible solutions: Effective strategies for discovering an "insider" is an open research question. The recommendations from [110] include low-cost, easily implemented policy solutions for near-term effect: education and awareness, employee screening, technology policy, information sharing. In the long-term aspect, further guidance, findings, samples, and tools are needed. Some solutions for IT systems/cyber security could be the following: to use integrated IT and physical security system tools to identify rule violation patterns for potential insider threat behavior; to use dual protection access technologies (e.g. biometric, key card or encryption key verification); to use dual control access mechanisms to protect high-value systems and processes; to manage access, integrity and availability of computer systems (e.g., identity management system). Control over creation and termination of user and administrator accounts and maintaining security/access rights should be done by segregation of duties.

4.7.3.4 Cultural differences between control and security communities

Threat: Control system professionals are often not aware of security risks, since these are not considered as part of the normal system operation. The emphasis in control systems is on safety and availability aspects.

On the other hand, IT security specialists use known techniques from a normal ICT system to introduce security, but may be missing important safety and control characteristics of the specific CS. Traditional security measures are usually not directly applicable to critical systems. Delays that may be caused by the operation of security tools are not acceptable within such systems. Critical systems, especially the ones with a real-time requirement, need to be available around the clock. They cannot be interrupted or restarted to introduce software patches or implement a security mechanism. All security measures should be tested before being implemented to ensure that they do not conflict with control operations.

The first priority in critical systems is safety. Systems must be operational and safe, providing their service in an uninterrupted and safe fashion. There is a big difference in the awareness and the techniques for security used in control systems. Safety is always prioritized, while security is seen as a secondary feature that can be added afterward, or even not considered at all. Sometimes no passwords or other security mechanisms are used. There are cases when security techniques and mechanisms could slow down or impede the prompt reaction to a situation requiring fast response.

Cultural aspects are very important. Organizations are cooperating in virtual organizations, thus increasing their complexity. Personnel from several different cultures (safety, security, process control, etc.) are cooperating. We have to create trust and propose a security baseline in order to merge the different views of security of ICT people and people from other areas.

Possible solutions: As with all human-related activities, an increased awareness, training, and education can help to better illuminate the problems. A common language and exchange of experience between the safety and security communities should be built. Cultural synergy should be sought.

Some promising areas of research with respect to the human factor and cultural problems are risk and vulnerability assessment tools and methods, secure control architectures and technologies, awareness and governance of risk to society.

4.8 A discussion of the role of the Internet

The Internet is a communication environment that has become an essential part of our everyday life, in the same fashion as the electricity or the telephone network have become essential over the last one hundred years. The more products and services we access through it, the more dependent we become on its functionality and availability. Indeed, the “functionality” of the Internet has outgrown its initial goal, to transfer information between distant sites; we now expect it to transfer trust and to operate in new critical areas.

By design, the Internet is not suited for critical applications, since it was built to provide a best-effort packet relay service. Now the Internet is being used by critical applications, and, as a result, it has itself turned into a critical system. The popularity and mass expansion of the Internet encourages its use even in critical applications where it was not previously used. The Internet technologies work along with the specialized technologies for process control and if this tendency reaches the safety-critical systems in their main functionality, it could be a serious threat.

An area of potential threats is the connection of the Internet to critical infrastructures (CIs). Many CIs (e.g., banks, power stations, industrial complexes, telephony networks, etc.) use the Internet for their communication needs. The effects of the insecurity of the Internet and its vulnerabilities will increase when connected

to critical infrastructures, considering their scale, complexity, connectivity, and interdependency.

Traditionally, in the fields of hazardous industrial processes and safety-critical systems for process control, specialized real-time and fault-tolerant computer systems and communications are used with guaranteed dependability and safety.

On the other hand, according to the integrated vision on dependability and security [7], any undesired event for a system (external or internal) can be regarded as a threat. For example, if an off-the-shelf system is put into a critical application, there is high probability that a fault occurrence may lead to system failure with unpredictable consequences. Fault-tolerant systems preserve their dependability and security even when unreliable components and subsystems are used for their design. Unfortunately, such guarantees are not present in the Internet. In particular, the use of off-the-shelf components in the Internet is a common practice. Hence, when used in critical applications, problems can arise.

A possible chain of threat-causing events (threat pathology) could be as follows: (i) The use of the Internet with a critical application induces a gap between the application requirements and the capabilities of the involved Internet components, (ii) this deficiency effectively decreases the robustness of the components and (iii) in turn leads to increased risk and vulnerabilities. Therefore, the increasing and *uncontrolled* use of Internet in critical systems can be regarded as an area of emerging threats in itself.

Being part of the communication infrastructure, the Internet has the same typical vulnerabilities and is prone to similar threats. There are approaches to improve communications' robustness and availability (and those of the Internet in particular) [4]. Using the Eight Ingredients Framework of Communications Infrastructure [106], the vulnerabilities of future networks were studied systematically to determine the vulnerabilities of each of the eight ingredients. The approach relies on vulnerability analysis, since it is recognized that intrinsic weaknesses of communication infrastructures are of a finite number and can be identified by professionals in order to eliminate or mitigate their effects. Combining vulnerability and threat analysis will help improving CI security. Although it is argued that threat analysis is ineffective when the knowledge of possible threats is not certain, the identification of threats helps anticipating challenges in areas of concern that may need more research and development activity.

In the Internet of services and things, two major areas /levels can be outlined – services and humans. In the huge space of the Internet of things, many services are delivered. These things are interconnected (Figure 4.4). The scale of so many connected things that are providing service to many people makes this system critical. At the level of humans are the end-users, operators, administrators, managers. Service level controls the system at things' level. Services can be SCADA systems, public notification systems, monitoring systems, etc. We should define the properties of CIs in our view. Threats depend on the critical system. Another source of threats is the operations of individuals or between them; from outside and inside the systems/networks. Security can be viewed in relation to Service-Oriented

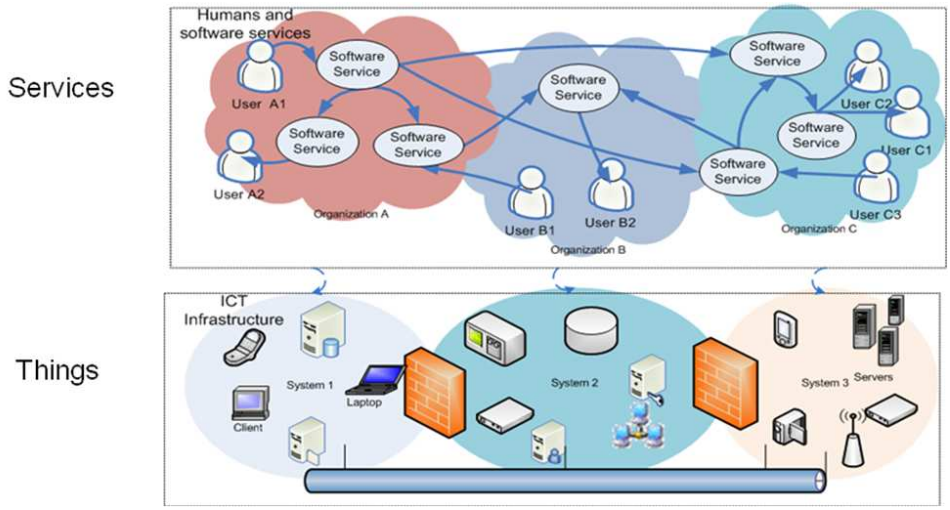

Figure 4.4: Humans and software services with the ICT infrastructure.

Architecture. Following the model of service and human levels we can identify combination threats or combined threats.

As the use of the Internet in critical applications and CIs in the near future is unavoidable, the following main suggestions could be considered.

1. Make a full decoupling of highly-critical systems (hazardous industrial processes, mission-critical tasks) and Internet

2. Control the introduction of the Internet in other critical areas (legislatively, technically and organizationally).

Some measures related to the second suggestion may be: (a) surveillance, regulation, and coordination between different sectors of CIs in the cases when they are planning the use of Internet, e.g. like these in [47]; (b) application of diversity approach when using COTS components [1]; (c) use of compact and trusted applications base; (d) use of integral approach to security (e.g., [50]).

4.9 General solutions

Security is a process. Technologies evolve, interactions among networks and infrastructures change, the view on IT security changes. New vulnerabilities are introduced with the ever-growing network complexity and old flaws still persist because of the existence of legacy systems and bad practices. Networks become more difficult to manage, they are interconnected, interdependent and heterogeneous. There is no single mechanism that can solve all security problems. For any threat there could be many ways to mitigate it. This means that security should not be a one-time effort. It is a process that adapts to the new challenges with the constant goal to protect systems from threats.

Security should be applied at all levels: technologically, organizationally, and legislatively. It is a policy that encompasses all aspects of protection.

Here we discuss briefly some more general solutions of how to counter the threats to security. They are not targeted at any specific threat, but rather organize systems' and networks' defense in a way to be able to maintain their service delivery despite the threats.

4.9.1 Resilience approach

One of the ways to counteract the increased vulnerability of critical systems and to suppress the threats that emerge as a result of the ICT application, is the resilience approach. Since 100% security is impossible and the attacks are unavoidable, the resilience approach implies that systems must be designed, built and operated in such a way that they can "be capable of surviving and delivering sufficiently dependable and secure service despite the inevitable residual development and physical faults, interaction mistakes, or malicious attacks and disruptions that their very scale, complexity and openness make more likely" [1].

As stated previously, the emerging and future threats are hard to identify, so this may be an unfeasible task. There are many threats that still remain and will be unidentified. At the same time, we can say much more about the stochastic nature of security challenges. The times of occurrence of the challenges that could affect normal operation will rapidly and arbitrarily differ and shall be in all likelihood uncorrelated. Moreover, new challenges will emerge (e.g. new application traffic loads, forms of distributed denial of service (DDoS) attacks, deployment environments, and networking technologies). As a consequence, the affected information infrastructures and delivered network services will change unpredictably. This makes unusable a set of scenarios for resilience prepared in advance and imposes the use of a dynamically reconfigurable and extensible infrastructure with context awareness capabilities. Another challenge is that often a sufficiently sophisticated DDoS attack is indistinguishable from legitimate but enormous traffic (e.g. flash crowd events) [153].

Resilience approach (RA) [1], [52] is a feasible, emergent, and integral approach that can be used for managing the emerging threats. To be successfully implemented, systems and networks have to be designed and built with RA in mind and used in compliance with RA concepts. The main idea is creating a new kind of Information Society Technologies, the resilient technologies [1], that will have and demonstrate an emergent behavior to successfully withstand and cope with the emergent and arbitrary behavior of the challenges to normal operations.

4.9.2 Defense in depth

"Defense-in-depth" is a strategy that layers security mechanisms such that the impact of a failure in any one mechanism is minimized [109]. This strategy includes measures to different aspects of a CS, starting from an appropriate security policy

for the critical system, implementation of a network topology with multiple layers (with the most critical communications occurring in the most secure and reliable layer), applying secure architectural solutions, and defining privileges and responsibilities of the personnel.

Some of the suggested best practices require logical separation between the corporate and CS networks, employing a demilitarized zone (DMZ) network architecture (i.e., prevent direct traffic between the corporate and CS networks), implementing redundancy for the critical components, designing critical systems for graceful degradation (fault-tolerant) to prevent catastrophic cascading events, etc.

Defense-in-depth strategy includes also traditional measures to security like disabling unused ports and services on CS devices after testing; restricting physical access; restricting CS user privileges; separate authentication mechanisms and credentials for users of the control system network and the corporate network; security controls (e.g., intrusion detection software, antivirus software and file integrity checking software); encryption and / or cryptographic hashes to CS data storage and communications, etc.

4.10 Related work

We are aware of a large number of activities and projects that are related to the Critical Systems working group and whose result may potentially have an impact on our studies. Therefore, we have the ambition to follow these projects to a varying degree, depending on their applicability to our work. Below is a list of projects and activities that we have found most interesting for the time being.

Protection and trust in financial infrastructures (PARSIFAL) This project is focused on protecting the critical financial infrastructure (CFI) sector and the information infrastructure connecting CFI to other critical infrastructures.

Communication middleware for monitoring financial CI (COMIFIN) This project is focused on improving the financial infrastructure protection by providing a middleware. The 9/11 attack and black-outs both in Europe and North America have highlighted the vulnerability of this sector; in some ways an unmanaged large scale network of networks.

Increasing security and protection through infrastructure resilience (INSPIRE) The resilience of critical information infrastructures will be increased by the use of traffic engineering algorithms, self-reconfiguration and diagnosis and recovery techniques adapted to networked process control systems.

Infrastructure for heterogeneous, resilient, secure, complex, tightly interoperating networks (INTERSECTION) By using an integrated security framework made from different components, the assurance of protection of heterogeneous networks can be improved. The framework includes end users to share information on attacks and other types of malfunctions.

Tool for systemic risk analysis and secure mediation of data exchanged across linked CI information infrastructures (MICIE) In this project, a Critical Infrastructure Warning Information Network will be implemented. Possible threats can in real time be identified, as well as their role on other dependent CIs. Any alarms are evaluated based on models of abstract CIs.

Semantically enhanced resilient and secure critical infrastructure services (SERSCIS) Information systems supporting critical infrastructures can have faults, be mismanaged or be attacked. By developing adaptive service-oriented technologies, such systems can automatically adapt to the requirements of the present situation. The results will be evaluated through two information-intensive critical transport infrastructures, of which both depend on a highly interconnected information technology network: air traffic control and inter-modal port community operations.

Wireless sensor networks for the protection of critical infrastructures (WSAN4CIP) Even though wireless sensor networks are not sufficiently dependable for use in critical infrastructures, many advantages can be foreseen if they could be used in such a way. This project will extend current sensor networks and nodes so that networked and process control systems can become much more secure and resilient. In particular, the management of power generation and distribution will be studied as an application area.

Worldwide observatory of malicious behaviors and attack threats (WOMBAT) To understand the emerging threats targeting Internet economy, the WOMBAT project suggests to use real time gathering of security-relevant indications and understand the collected data by a series of analysis techniques.

2009 CWE/SANS Top 25 Most Dangerous Programming Errors In the "2009 CWE/SANS Top 25 Most Dangerous Programming Errors" list, the insecure interaction between components (*CATEGORY: Insecure Interaction Between Components*) are listed as one of the most significant error types that can lead to vulnerabilities. In the future, and especially in the CI–ICT interface environment, we expect to see more such errors as many of the components (and therefore one part of the interaction) is owned by different entities, including both private and public. There are also specific problems related to the Porous Defense category, especially in regards to the use of access control in the networks. As stated before, access control may be non-existent in parts of the system even though the transport of information is through Internet.

4.11 Conclusion

We have presented a list of cyber threats that is especially relevant for critical systems and infrastructures, but that in many cases would also represent threats to any system. However, critical systems have certain characteristics that are not applica-

ble for other systems. These characteristics entail the need for security solutions that are specific to critical systems. Furthermore, critical systems are of paramount importance to society and their security is a major concern. Therefore, the Working Group for critical systems was formed within the FORWARD project. Its goal was to suggest a list of cyber threats that needed special attention in the future. This work was accomplished as follows. First, we compiled information from experts that presented important problems that they face. Based on this diverse input, we abstracted the most important features and created a first draft threat list. This list was then taken back to the domain experts for comments and approval. The resulting list has been presented in this document. We do not claim that the list is exhaustive nor that it is the final truth. There are certainly details that remain to be discussed. Still, we believe that the threat list and the related discussions give a good comprehension of the problem addressed, and that it should be of use to stakeholders in the area.

Bibliography

[1] A European Network of Excellence. Deliverable d12 resilience-building technologies: State of knowledge. `http://www.resist-noe.org/events/events.html`, 2006.

[2] J. A. Afilias, P. Savola, and G. Neville-Neil. Deprecation of type 0 routing headers in ipv6. IETF, 2007.

[3] P. Akritidis, W. Y. Chin, V. T. Lam, S. Sidiroglou, and K. G. Anagnostakis. Proximity breeds danger: emerging threats in metro-area wireless networks. In *SS'07: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium*, pages 1–16, Berkeley, CA, USA, 2007. USENIX Association.

[4] Alcatel-Lucent Technologies. The ARECI Study, Final Report, Availability and Robustness of Electronic Communications Infrastructures. PSC Europe PSCE/RD/024, Mar. 2007.

[5] D. Anderson, C. Fleizach, S. Savage, and G. Voelker. Spamscatter: Characterizing Internet Scam Hosting Infrastructure. In *Usenix Security Symposium*, 2007.

[6] R. J. Anderson and M. G. Kuhn. Low cost attacks on tamper resistant devices. In *Proceedings of the 5th International Workshop on Security Protocols*, pages 125–136, London, UK, 1998. Springer-Verlag.

[7] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. IEEE Transactions On Dependable And Secure Computing, Vol. 1, No. 1, January–March 2004, 2004.

[8] M. Baecher and F. Freiling. Towards dynamic malware analysis to increase mobile device security. In *Sicherheit 2008: Sicherheit, Schutz und Zuverlässigkeit. Konferenzband der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 2.-4. April 2008 im Saarbrücker Schloss*, pages 423–433, 2008.

[9] P. Baecher, T. Holz, M. Koetter, and G. Wicherski. Know Your Enemy: Tracking Botnets, 2007.

[10] U. Bayer, A. Moser, C. Krügel, and E. Kirda. Dynamic analysis of malicious code. *Journal in Computer Virology*, 2(1):67–77, 2006.

[11] J. Berra. Emerson first to offer WirelessHART automation products. `http://www.controlglobal.com/industrynews/2008/082.html`, 2008.

[12] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda. All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks. In *20th International World Wide Web Conference*, Madrid, Spain, April 2009.

[13] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security Analysis of a Cryptographically-Enabled RFID Device. In *14th USENIX Security Symposium*, pages 1–16, 2005.

[14] A. Bose and K. G. Shin. On mobile viruses exploiting messaging and bluetooth services. *Securecomm and Workshops, 2006*, pages 1–10, 28 2006-Sept. 1 2006.

[15] A. Caglayan, M. Toothaker, D. Drapeau, D. Burke, and G. Eaton. Real-time detection of fast flux service networks. *Conference For Homeland Security, 2009. CATCH '09. Cybersecurity Applications & Technology*, pages 285–292, March 2009.

[16] G. T. I. S. Center. Emerging cyber threats report for 2009, Oct. 2008. http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf.

[17] H. Chan and A. Perrig. Security and privacy in sensor networks. *IEEE Computer*, 36(10):103–105, 2003.

[18] J. Cheng, S. H. Wong, H. Yang, and S. Lu. Smartsiren: virus detection and alert for smartphones. In *MobiSys '07: Proceedings of the 5th international conference on Mobile systems, applications and services*, pages 258–271, New York, NY, USA, 2007. ACM.

[19] Cisco Systems Inc. Annual Security Report. www.cisco.com/go/securityreport, 2008.

[20] Commission of the European Communities. Green Paper On a European Programme for Critical Infrastructure Protection. http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf, Nov. 2005.

[21] Connected Transport - There's more to it than cars. http://www.innovits.com/public/info_/innovits/Connected\%20Transport.pdf.

[22] D. Dagon, G. Gu, C. Lee, and W. Lee. A Taxonomy of Botnet Structures. In *Annual Computer Security Applications Conference (ACSAC)*, 2007.

[23] F. M. David, E. M. Chan, J. C. Carlyle, and R. H. Campbell. Cloaker: Hardware supported rootkit concealment. *Security and Privacy, IEEE Symposium on*, 0:296–310, 2008.

[24] DEAR-COTS project homepage. http://dear-cots.di.fc.ul.pt, 2001.

[25] F-Secure. F-secure computer virus information pages: Cardtrap.a. http://www.f-secure.com/v-descs/cardtrap_a.shtml.

[26] F-Secure. F-secure computer virus information pages: Commwarrior.a. http://www.f-secure.com/v-descs/commwarrior.shtml.

[27] F-Secure. "sexy view" trojan on symbian s60 3rd edition. http://www.f-secure.com/weblog/archives/00001609.html, February 2008.

[28] Facebook. http://www.facebook.com, 2009.

[29] Federal Bureau of Investigation. SPEAR PHISHERS Angling to Steal Your Financial Info. http://www.fbi.gov/page2/april09/spearphishing_040109.html, Apr 2009.

[30] C. Fleizach, M. Liljenstam, P. Johansson, G. M. Voelker, and A. Méhes. Can you infect me now? malware propagation in mobile phone networks. In *Proceedings of The 5th ACM Workshop on Recurring Malcode (WORM 2007)*, 2007.

[31] A. Folkerts, G. Portokalidis, and H. Bos. Multi-tier intrusion detection by means of replayable virtual machines. Technical Report IR-CS-47, Vrije Universiteit Amsterdam, August 2008.

[32] J. Franklin, V. Paxson, A. Perrig, and S. Savage. An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. In *ACM Conference on Computer and Communication Security (CCS)*, 2007.

[33] F. D. Garcia, G. Koning Gans, R. Muijrers, P. Rossum, R. Verdult, R. W. Schreur, and B. Jacobs. Dismantling mifare classic. In *ESORICS '08: Proceedings of the 13th European Symposium on Research in Computer Security*, pages 97–114, Berlin, Heidelberg, 2008. Springer-Verlag.

[34] P. Gasper. Cyber Threat to Critical Infrastructure - 2010-2015. Information & Cyberspace Symposium, Fort Leavenworth, Kansas, Sept. 2008. http://www.carlisle.army.mil/DIME/documents/Cyber_Threat_to_CI.pdf.

[35] J. B. Grizzard, V. Sharma, C. Nunnery, B. B. H. Kang, and D. Dagon. Peer-to-Peer Botnets: Overview and Case Study. In *1st Workshop on Hot Topics in Understanding Botnets*, April 2007.

[36] S. Guha, K. Tang, and P. Francis. NOYB: privacy in online social networks. In *Proceedings of the first workshop on Online social networks*, pages 49–54. ACM New York, NY, USA, 2008.

[37] S. Gundersson. Global IP V.6 Statistics - Measuring the Current State of IPv6 for Ordinary Users. Technical report, RIPE 57, 2008.

[38] D. Halperin, T. S. Heydt-Benjamin, K. Fu, T. Kohno, and W. H. Maisel. Security and Privacy for Implantable Medical Devices. *IEEE pervasive computing, mobile and ubiquitous systems*, 7(1), 2008.

[39] G. Hancke. A Practical Relay Attack on ISO 14443 Proximity Cards. Manuscript, February 2005.

[40] M. Hansen, M. Hansen, J. Möller, T. Rohwer, C. Tolkmit, and H. Waack. Developing a legally compliant reachability management system as a countermeasure against spit. In *Proceedings of Third Annual VoIP Security Workshop, Berlin, Germany*, 2006.

[41] J. Heasman. Implementing and detecting an acpi bios rootkit. In *Blackhat Europe*, Amsterdam, 2006.

[42] Hewlett-Packard Development Company. Print Security and Identity Authorization. `http://www.hp.com/united-states/public_slg/spy-museum-security-presentation.pdf`, 2007.

[43] T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. OHare. Vulnerabilities in First-Generation RFID-enabled Credit Cards. In *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security*, Lowlands, Scarborough, Trinidad/Tobago, February 2007.

[44] T. Holz, M. Engelberth, and F. Freiling. Learning More About the Underground Economy : A Case-Study of Keyloggers and Dropzones. Technical report, University of Mannheim, 2008.

[45] T. Holz, C. Gorecki, and F. Freiling. Detection and Mitigation of Fast-Flux Service Networks. In *Network and Distributed System Security Symposium (NDSS)*, 2008.

[46] T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. C. Freiling. Measurements and Mitigation of Peer-to-Peer-based Botnets: A Case Study on Storm Worm. In *Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET)*, 2008.

[47] Homeland Security Advisory Council. Report of the critical infrastructure task force. `http://www.dhs.gov/xlibrary/assets/HSAC_CITF_Report_v2.pdf`, 2006.

[48] The Honeynet Project. Know Your Enemy: Fast-Flux Service Networks., July 2007.

[49] Honeynet Project and Research Alliance. Know your Enemy: Tracking Botnets. `http://www.honeynet.org/papers/bots/`, 2008.

[50] L. Horacek. Protection on demand, information security that works for you, the IBM approach to security protection from the core to the perimeter. IDC Security Roadshow Sofia, April-12-2007, 2007.

[51] G. Huston. The IPv4 Address Report. `http://www.potaroo.net/tools/ipv4/`, 2008.

[52] D. Hutchison and J. P. Sterbenz. ResiliNets: Multilevel resilient and survivable networking initiative. `http://www.comp.lancs.ac.uk/resilinets`, 2006.

[53] ICANN. Factsheet - root server attack on 6 february 2007. `http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf`, Febrary 2007.

[54] IEEE. IEEE Standard for Information technology. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&isnumber=35824&arnumber=1700009&punumber=11161.

[55] IETF Working Group. Transport Layer Security (TLS). http://www.ietf.org/html.charters/tls-charter.html, 2006.

[56] J. Ioannidis and S. M. Bellovin. Implementing Pushback: Router-Based Defense Against DDoS Attacks. In *Proc. of the Network and Distributed System Security Symposium (NDSS)*, February 2002.

[57] IPv6 Related Specifications. http://www.ipv6.org/specs.html, 2006.

[58] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer. Social phishing. *Commun. ACM*, 50(10):94–100, 2007.

[59] M. Jakobsson. Modeling and Preventing Phishing Attacks. http://www.informatics.indiana.edu/markus/papers/phishing_jakobsson.pdf, 2005.

[60] M. Jakobsson and S. Stamm. Invasive browser sniffing and countermeasures. In *WWW '06: Proceedings of the 15th international conference on World Wide Web*, pages 523–532, New York, NY, USA, 2006. ACM.

[61] H. James. The Teredo Protocol: Tunneling Past Network Security and Other Security Implications. Symantec, 2006.

[62] B. Jansen. Click fraud. *Computer*, 40(7):85–86, July 2007.

[63] Y. Jing. Fast Worm Propagation in IPv6 Networks. http://www.cs.virginia.edu/~jy8y/publications/cs85104.pdf, 2006.

[64] J. John, A. Moshchuk, S. Gribble, and A. Krishnamurthy. Studying Spamming Botnets Using Botlab. In *6th Usenix Symposium on Networked Systems Design and Implementation (NSDI)*, 2009.

[65] A. Juels, R. L. Rivest, and M. Szydlo. The blocker tag: selective blocking of rfid tags for consumer privacy. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 103–111, New York, NY, USA, 2003. ACM.

[66] H. Kagan. Interview about wireless devices adoption in the industry and the future trends. Frost & Sullivan, Nov. 2008. http://www.teknikogviden.dk.

[67] C. Karlberger, G. Bayler, C. Kruegel, and E. Kirda. Exploiting Redundancy in Natural Language to Penetrate Bayesian Spam Filters. In *First USENIX Workshop on Offensive Technologies (WOOT '07), Boston, MA*, August 2007.

[68] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. In *In First IEEE International Workshop on Sensor Network Protocols and Applications*, pages 113–127, 2003.

[69] Kaspersky Lab. Kaspersky lab reports a new malicious program for mobile phones that steals money from mobile accounts. http://www.kaspersky.com/news?id=207575728, January 2009.

[70] M. Keeney. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors Executive Summary. https://treas.gov/usss/ntac/its_report_050516_es.pdf, May 2005.

[71] Z. Kfir and A. Wool. Picking Virtual Pockets using Relay Attacks on Contactless Smartcard. In *SECURECOMM '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 47–58, Washington, DC, USA, 2005. IEEE Computer Society.

[72] T. King, J. Tucek, A. Cozzie, C. Grier, W. Jiang, and Y. Zhou. Designing and implementing malicious hardware. In *Usenix Workshop on Large-Scale Exploits and Emergent Threats*, 2008.

[73] P. C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *CRYPTO '96: Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, pages 104–113, London, UK, 1996. Springer-Verlag.

[74] M. Konte, N. Feamster, and J. Jung. Dynamics of online scam hosting infrastructure. In *PAM*, pages 219–228, 2009.

[75] New Koobface Worm Variant Spreads Across Facebook, Myspace, Hi5 And Other Social Networks. http://cyberinsecure.com/new-koobface-worm-variant-spreads-across-facebook-myspace-hi5-and-other-social-networks/, 2009.

[76] C. Krauí, M. Schneider, and C. Eckert. On handling insider attacks in wireless sensor networks. *Inf. Secur. Tech. Rep.*, 13(3):165–172, 2008.

[77] I. Krawarik and M. Kwauka. Attacken aufs Konto (in German). http://www.ispa.at/www/getFile.php?id=846, Jan 2007.

[78] B. Krebs. Shadowy Russian Firm Seen as Conduit for Cybercrime. http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html, 2007.

[79] P. Kumaraguru, S. Sheng, A. Acquisti, L. Cranor, and J. Hong. Lessons from a real world evaluation of anti-phishing training. In *eCrime Researchers Summit, 2008*, pages 1–12, Oct. 2008.

[80] L. Laursen. Fake facebook pages spin web of deceit. *Nature*, 458, 2009.

[81] F. Leder and T. Werner. Know Your Enemy: Containing Conficker, 2009.

[82] G. Legg. The bluejacking, bluesnarfing, bluebugging blues: Bluetooth faces perception of vulnerability. TechOnline http://www.wirelessnetdesignline.com/showArticle.jhtml?articleID=192200279, April 2005.

[83] Z. Li and D. Lee. Detecting and filtering instant messaging spam-a global and personalized approach. In *1st IEEE ICNP Workshop on Secure Network Protocols, 2005.(NPSec)*, pages 19–24, 2005.

[84] A. Lim. Working with Commander Data? http://www.manilatimes.net/national/2008/mar/03/yehey/techtimes/20080303tech1.html, 2008.

[85] LinkedIn. http://www.linkedin.com, 2008.

[86] X. Liu, Z. Guo, X. Wang, F. Chen, X. Lian, J. Tang, M. Wu, F. Kaashoek, and Z. Zhang. D3s: Debugging deployed distributed systems. In *NDSI'08*, page 423437, San Franciso, CA, 2008.

[87] M. T. Hoske and I. McPherson. Industrial Wireless Implementation Guide. Control Engineering, 8/1/2008, Aug. 2008. http://www.controleng.com/article/CA6584939.html.

[88] M. Mannan and P. van Oorschot. On instant messaging worms, analysis and countermeasures. In *Proceedings of the 2005 ACM workshop on Rapid malcode*, pages 2–11. ACM New York, NY, USA, 2005.

[89] M. Manzo, T. Roosta, and S. Sastry. Time synchronization attacks in sensor networks. In *SASN'05: Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 107–116, New York, NY, USA, 2005. ACM.

[90] K. Masica. Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments, Draft. http://csrp.inl.gov/Documents/Wireless\%20802.11i\%20Rec\%20Practice.pdf, April 2007.

[91] K. Masica. Securing WLANs using 802.11i, Draft Recommended Practice. http://csrp.inl.gov/Documents/Wireless\%20802.11i\%20Rec\%20Practice.pdf, Feb. 2007.

[92] MeinVerzeichnis – MeinVZ. http://www.meinvz.net/, 2008.

[93] Microsoft.com. Spear phishing: Highly targeted phishing scams. http://www.microsoft.com/protect/yourself/phishing/spear.mspx, Jul 2008.

[94] R. Miller. Google data center faq. Internet. http://www.datacenterknowledge.com/archives/2008/03/27/google-data-center-faq/, Mar. 2008.

[95] D. Moore, G. Voelker, and S. Savage. Inferring Internet Denial of Service Activity. In *Usenix Security Symposium*, 2001.

[96] A. Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy. A Crawler-based Study of Spyware on the Web. In *Proceedings of the 13th Annual Network and Distributed System Security Symposium (NDSS)*, February 2006.

[97] W. Mossberg. Newer, faster, cheaper iphone 3g. Wall Street Journal, July 2008.

[98] S. Moyer and N. Hamiel. Satan is on My Friends List: Attacking Social Networks. http://www.blackhat.com/html/bh-usa-08/bh-usa-08-archive.html, 2008.

[99] C. Mulliner. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. In *Proceedings of the 1st International Workshop on Sensor Security (IWSS) at ARES*, Fukuoka, Japan, March 2009.

[100] C. Mulliner and G. Vigna. Vulnerability Analysis of MMS User Agents. In *Proceedings of the Annual Computer Security Applications Conference (ACSAC)*, Miami, FL, December 2006.

[101] C. Mulliner, G. Vigna, D. Dagon, and W. Lee. Using labeling to prevent cross-service attacks against smart phones. In *Detection of Intrusions and Malware & Vulnerability Assessment, Third International Conference, DIMVA 2006, Berlin, Germany, July 13-14, 2006, Proceedings*, pages 91–108, 2006.

[102] MySpace. http://www.myspace.com, 2009.

[103] New MySpace and Facebook Worm Target Social Networks. http://www.darknet.org.uk/2008/08/new-myspace-and-facebook-worm-target-social-networks, 2008.

[104] J. Nazario and T. Holz. As the net churns: Fast-flux botnet observations. In *Malicious and Unwanted Software, 2008. MALWARE 2008. 3rd International Conference on*, pages 24–31, 2008.

[105] M. Neely. My Facebook Nightmare. http://infolution.com.au/?p=112, Jan 2009.

[106] Network Reliability and Interoperability Council VI. Homeland Security Physical Security (Focus Group 1A) Final Report, Issue 3. www.nric.org/fg/nricvifg.html, Dec. 2003.

[107] B. News. Bank loses $1.1m to online fraud, 2006. http://news.bbc.co.uk/2/hi/business/6279561.stm.

[108] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *IPSN'04: Proceedings of the third international symposium on Information processing in sensor networks*, pages 259–268, New York, NY, USA, 2004. ACM Press.

[109] NIST. DRAFT guide to industrial control systems (ICS) security, 2008. SP800-82, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf.

[110] T. Noonan and E. Archuleta. The National Infrastructure Advisory Council's final report and recommendations on the insider threat to critical infrastructures. http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf, April, 8 2008.

[111] J. Oberheide, E. Cooke, and F. Jahanian. Cloudav: N-version antivirus in the network cloud. In *SS'08: Proceedings of the 17th conference on Security symposium*, pages 91–106, Berkeley, CA, USA, 2008. USENIX Association.

[112] J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahania. Virtualized in-cloud security services for mobile devices. In *Proc. of MobiVirt*, Breckenridge, CO, June 2008.

[113] oCERT. CVE-2009-0475: #2009-002 opencore insufficient boundary checking during mp3 decoding. http://www.ocert.org/advisories/ocert-2009-002.html, January 2009.

[114] B. O'Connor. Vulnerabilities in not-so-embedded systems. In *BlackHat USA 2006*, Las Vegas, NV, July 2006.

[115] M. Ohkubo, K. Suzuki, and S. Kinoshita. RFID privacy issues and technical challenges. *Communication of the ACM*, 48(9):66–71, 2005.

[116] E. Passerini, R. Paleari, L. Martignoni, and D. Bruschi. Fluxor: Detecting and monitoring fast-flux service networks. In D. Zamboni, editor, *DIMVA*, volume 5137 of *Lecture Notes in Computer Science*, pages 186–206. Springer, 2008.

[117] B. D. Payne, M. Carbone, M. Sharif, and W. Lee. Lares: An Architecture for Secure Active Monitoring Using Virtualization. In *IEEE Symposium on Security and Privacy*, 2008.

[118] A. Perrig, J. Stankovic, and D. Wagner. Security in wireless sensor networks. *Commun. ACM*, 47(6):53–57, 2004.

[119] B. Philippe and E. Arnaud. IPv6 Routing Header Security. CANSECWEST, 2007.

[120] Playstation Home. http://www.playstationhome.com, 2009.

[121] P. Porras, H. Saidi, and V. Yegneswaran. A Multi-perspective Analysis of the Storm (Peacomm) Worm. Technical report, Computer Science Laboratory, SRI International, 2007.

[122] Pressetext Austria. Phishing-Schäden bleiben am Kunden hängen (in German). http://www.pressetext.at/pte.mc?pte=061116033, Nov 2006.

[123] Priya Ganapati. Researchers Demonstrate How to Spoof GPS Devices. http://blog.wired.com/gadgets/2008/09/researchers-dup.html, September 2008.

[124] A. Ramachandran and N. Feamster. Understanding the Network-level Behavior of Spammers. In *ACM SIGCOMM*, 2006.

[125] A. Rassiysky. Evolution of data networks of BTC. Cisco Expo, Oct. 2008. http://www.cisco.com/web/BG/expo/presentations/BTK_Evolution_of_Data_Networks_of_BTC.pdf.

[126] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. RFID Guardian: A Battery-Powered Mobile Device for RFID Privacy Management. In *Proceedings of Information Security and Privacy, 10th Australasian Conference (ACISP)*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194. Springer, July 2005.

[127] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. Is your cat infected with a computer virus? In *PERCOM '06: Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications*, pages 169–179, Washington, DC, USA, 2006. IEEE Computer Society.

[128] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly. Identifying, understanding, and analyzing critical infrastructure interdependencies, Dec. 2001.

[129] SANS Institute. Malware infection that began with windshield fliers. http://isc.sans.org/diary.html?storyid=5797, 2009.

[130] P. Savola and C. Patel. Security considerations for 6to4. IETF, 2004.

[131] T. Schaberreiter, C. Wieser, I. Sánchez, J. Riekki, and J. Röning. An enumeration of rfid related threats. In *UBICOMM '08: Proceedings of the 2008 The Second International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, pages 381–389, Washington, DC, USA, 2008. IEEE Computer Society.

[132] Seagate. The Threat to Data Center Hard Drives, The Case for Self-Encrypting Hard Drives. http://www.seagate.com/docs/pdf/whitepaper/Threat_TP583-1-0710USr1.pdf, 2007.

[133] Second Life. http://www.secondlife.com, 2009.

[134] ShadowServer: DigitalNinja. RBN 'Rizing' - Abdallah Internet Hizmetleri. http://www.shadowserver.org/wiki/uploads/Information/RBN_Rizing.pdf, 2008.

[135] ShadowServer: Pheh. RBN As a Business Network - Clarifying the guesswork of Criminal Activity. http://www.shadowserver.org/wiki/uploads/Information/RBN-AS40989.pdf, 2008.

[136] J. Smith. Security: Stolen Facebook Accounts Being Used to Phish for Money from Friends. http://www.insidefacebook.com/2009/01/21/, Jan 2009.

[137] The Spamhaus Project. http://www.spamhaus.org/, 2008.

[138] Spear phishing: Highly targeted phishing scams. http://www.microsoft.com/protect/yourself/phishing/spear.mspx, 2006.

[139] StudiVerzeichnis – StudiVZ. http://www.studivz.net, 2008.

[140] P. A. Subrahmanyam. Towards verifying large(r) systems: A strategy and an experiment. In *CHARME '93: Proceedings of the IFIP WG 10.5 Advanced Research Working Conference on Correct Hardware Design and Verification Methods*, pages 135–154, London, UK, 1993. Springer-Verlag.

[141] Symantec. Palm.phage.dropper. http://www.symantec.com/security_response/writeup.jsp?docid=2000-121918-4538-99.

[142] Symantec Corp. Symantec Suspects D-Link Routers for Bot Attack Vulnerability. http://news.softpedia.com/news/Symantec-Suspects-D-Link-Routers-for-Bot-Attack-Vulnerability-81730.shtmll, March 2008.

[143] The Presidents's National Security Telecommunications Advisory Committee. Next Generation Networks Task Force, Report. http://www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20Task%20Force%20Report%20-%20Appendices.pdf, March, 28 2006.

[144] R. Thomas and J. Martin. The Underground Economy: Priceless. *Usenix ;login*, 31(6), 2006.

[145] D. R. Thompson, N. Chaudhry, and C. W. Thompson. RFID security threat model. In *Acxiom Laboratory for Applied Research (ALAR) Conf. on Applied Research in Information Technology*, Conway, Arkansas, March 2006.

[146] United States General Accounting Office. Report to the subcommittee on emerging threats, cybersecurity, and science and technology, committee on homeland security, house of representatives, June 2008. http://www.gao.gov/new.items/d08607.pdf.

[147] US-CERT. Multiple dns implementations vulnerable to cache poisoning. http://www.kb.cert.org/vuls/id/800113, July 2008.

[148] P. Vixie, G. Sneeringer, and M. Schleifer. Events of 21-oct-2002. http://d.root-servers.org/october21.txt, October 2001.

[149] L. von Ahn, B. Maurer, C. McMillen, D. Abraham, and M. Blum. reCAPTCHA: Human-Based Character Recognition via Web Security Measures. *Science*, September 2008.

[150] C. J. Walter, N. Suri, and T. Monaghan. Evaluating COTS standards for design of dependable systems. Proc. of the 2000 Int. Conf. on Dependable Systems and Networks, 2000, pp. 87–96., 2000.

[151] Wikipedia. Next generation networking (NGN_all-IP), Dec. 2008. http://en.wikipedia.org/wiki/Next_Generation_Networking.

[152] R. Wojtczuk. Adventures with a certain Xen vulnerability (in the PVFB backend). Technical report, Invisible Things Lab, 2008.

[153] L. Xie, P. Smith, M. Banfield, H. Leopold, J. Sterbenz, and D. Hutchison. Towards resilient networks using programmable networking technologies. http://www.ittc.ku.edu/resilinets/papers/Xie-Smith-Banfield-Leopold-Sterbenz-Hutchison-2005.pdf, 2006.

[154] Xing – Global Networking for Professionals. http://www.xing.com, 2008.

[155] F. Ye, H. Luo, S. Lu, L. Zhang, and S. Member. Statistical en-route filtering of injected false data in sensor networks. In *In INFOCOM*, pages 839–850, 2004.

[156] H. Yu, M. Kaminsky, P. Gibbons, and A. Flaxman. Sybilguard: Defending against sybil attacks via social networks. In *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 267–278. ACM New York, NY, USA, 2006.

[157] G. Yuxi. IP Bearer Network for NGN. http://wwwen.zte.com.cn/main/include/showemagazinearticle.jsp?articleId=9559&catalogId=12165, 2005.

[158] W. Zhang and G. Cao. Group rekeying for filtering false data in sensor networks: a predistribution and local collaboration-based approach. In *INFOCOM'05*, Miami, FLA, March 2005.

[159] Q. Zheng, T. Liu, X. Guan, Y. Qu, and N. Wang. A new worm exploiting ipv4-ipv6 dual-stack networks. In *WORM '07: Proceedings of the 2007 ACM workshop on Recurring malcode*, 2007.

[160] T. Zhimeng, W. Bo, and W. Yinxing. Security Technologies for NGN. http://wwwen.zte.com.cn/main/include/showemagazinearticle.jsp?articleId=11167&catalogId=12165, 2008.