SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Secure, dependable and trusted Infrastructures

COORDINATION ACTION

forward

Managing Emerging Threats in ICT Infrastructures

Grant Agreement no. 216331

Deliverable D1.2/1.3:
First workshop report, and
First "Threats on the Internet" seminar report

Contractual Date of Delivery	31/05/2008
Actual Date of Delivery	30/05/2008
Deliverable Security Class	Public
Editor	Christopher Kruegel
Contributors	FORWARD Consortium
Quality Control	Engin Kirda Erland Jonsson Kallia 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

This deliverable summarizes the activity of the first FORWARD workshop and the first "Threats on the Internet" seminar. Note that the first FORWARD workshop was combined with the first "Threats on the Internet" seminar. This was in accordance with the EU project officer to focus the ideas and views of the attendees of both venues into a single event. To combine both events, we decided to invite a number of speakers that would give presentations at the beginning of the workshop (to reflect the "Threats on the Internet" seminar). Then, the attendees would break out into working groups to perform the necessary brainstorming to define the project working groups (which reflects the main objective of the first project workshop). That is, the initial "Threats on the Internet" presentations served as a stimulus for the subsequent working group discussions.

According to Annex 1, a total of 35 attendees was considered to be the threshold for a successful workshop (and a minimum of 20% = 7 people from industry). This threshold was significantly exceeded, with a total of 61 attendees and 27 participants from industry (about 44%). This clearly demonstrates the interest and participation from the industrial stakeholders.

A total of 30 presentations were given, 15 in the form of plenary talks, and 15 talks within the working groups. The 15 plenary talks provided stimulating input for the subsequent discussions and represented the "Threats on the Internet" part. The other 15 talks were given during five working group meetings (three each).

In this document, we first attempt to capture the discussions that were held during the five initial working group meetings. Then, we provide an overview of the talks and individual views of those participants who agreed to make their opinions and ideas publicly available (28 out of 30 speakers). Finally, we discuss the conclusions that the consortium has drawn from the workshop and briefly outline the actions that we plan to take.

Chapter 2

Working Group Summaries

Initially, there were five working group topics that the consortium selected:

1. Critical infrastructure protection: The scope of this working group was related to infrastructure that relies on ICT. For example, signaling systems, hospitals, power plants, phone systems, and transportation were discussed in this group.

2. Fraud: This working group dealt with the underground economy and the movement towards criminal profit from computer attacks. It covered threats such as phishing, online fraud, scams, credit card abuse, and extortion.

3. Large-scale systems: This working group covered both (a) large software systems that can be a combination of many others (e.g., web mash-ups, web services, component-based software, ...) and (b) many small devices that together form a large system (such as RFID, phones, and mobile devices).

4. Malware: This working group's focus was malicious code. In particular, questions are related to how malware infects targets, how it propagates, what its behavior is, and how it can be analyzed and mitigated.

5. Networks and monitoring: This working group was concerned with issues related to the infrastructure that connects devices. This includes the routing infrastructure and network monitoring aspects. Also, privacy aspects and ways to share collected traffic were in scope.

The topics of the five working groups were selected *a priori* based on the interests of the registered participants of the workshop and the intuition of the consortium members of the potentially relevant areas in which research on future emerging threats is most necessary and beneficial. In the following five sections, the findings and conclusions of each working group meeting are summarized.

2.1 Critical Infrastructure Protection

2.1.1 Introduction

The systems and networks that constitute the infrastructure of society are often taken for granted. Indeed, in our everyday life, we rely on them, possibly without even realizing that some of them exist at all. Many times people only realize their dependence on these services when there is a disruption in their operations. Yet, when such disruption does happen, it could have serious, even dire consequences.

In the past, the systems and networks of the infrastructure were physically and logically independent and separate. They were not connected, and there was little to no interactions between them. With advances in technology, however, this has changed. In each sector, the systems have become automated and interlinked through computers and communication facilities. Furthermore, the trend shows an increase of both automation and linkage, not only within sectors but also between various sectors. Thus, we expect the future will aggravate the interdependencies between systems in general, and systems related to critical infrastructure in particular, leading to a complex ”mesh of systems.”

On one hand, having the systems linked boosts the efficiency of the systems and adds new capabilities to them, thus making them more competitive. On the other hand, the interlinked capabilities also render the systems and networks much more vulnerable to disruption and attack. Not only have the possible vectors for a determined attack or simple harmful influence increased, also the detrimental effects of a service disruption in a single sector has significantly increased. What would have been an isolated incident in the past, can today cause extensive interruptions and/or failures in other sectors as well. In fact, the cascading effects might lead to a more or less global outage or malfunction, affecting systems and networks in even seemingly unrelated sectors. If such cascading effects cannot be contained, they will directly influence both the economy of society and the physical safety of its citizens.

2.1.2 Working Group Scope

One of the most important task for the working group is to understand the scope for the future work. For example, although significant experience has been accumulated in how to protect critical infrastructures (CIs) as independent entities, the automation and linkage between CIs that now take place may invalidate some of the previous solutions. The constant development and the increased complexity of the interconnected mesh and, consequently, of the interdependencies between the various CIs may mean that we need to account for new types of weaknesses in these systems. We must also reevaluate the risk of already-anticipated weaknesses of single-sector-systems as the consequences may have changed and become more severe in systems that are interconnected.

Indeed, the CI mesh as a whole is much more complicated than just the sum of its components. This complexity raises the CI protection problem to a completely new level, where we need to face and deal with threats of a very different nature from the ones that have previously been anticipated.

It is thus obvious that future research in this area is direly needed, and the participants of the FORWARD workshop agreed that the "Critical Systems" working group will indeed be important and even a must for the correct and timely identification of emergent threats within this area. It was decided that the group should continue its work, while, in line with the points made above and the goals of the project, limit its scope to issues related to the CIs that are interconnected with other systems, excluding those CIs that have, for one reason or another, retained their independence.

2.1.3 The Communication Medium viewed as a Critical Infrastructure

As stated above, the group will focus on issues related to the CIs that are interconnected, i.e., the complex "mesh of systems." The group discussed whether special emphasis should be put on the CIs that utilize the Internet as a communication medium, as this is both increasingly common, and at the same time a rather "open" case, in the sense that fewer assumptions on the communication channels, infrastructure, equipment, and so forth, can be made in advance.

It can also be argued that the interconnecting infrastructure represents a CI per se, especially when speaking about the Internet. Regardless of one's views in regards to this argument, it is clear that the interconnected infrastructure cannot and must not be ignored when considering the weaknesses of the mesh of systems. Actually, in the world of tightly and heavily interdependent CIs, a disruption in the network that mediates their interrelations might have more devastating effects than a successful attack on one of the connected CIs by itself. In this light, it becomes obvious that securing the CIs as independent entities is not going to do much good, unless the communication between them (and with other entities) is also protected diligently. Otherwise, a successful attack on a single, but central enough network device, might put several CI "to their knees."

2.1.4 More than just Technology

One factor that could easily be underestimated or even overlooked is the human involvement. Although many CIs might look like being completely automated, the human factor still plays an important role in their operation, either directly or indirectly. Members of the group shared that in their experience the disruption in interconnected networks is many times not caused by a deliberate and malicious activity, but simply by human errors (e.g., router misconfiguration.) Despite the lack of malicious intent, the consequences of such incidents might be no less dire than if they had been consciously meant to be harmful.

The human factor is a very complex issue, and it is still not clear how much attention the working group should pay to it. It could easily be projected further into various social, ethical, and legal problems that are still related to the CIs and their protection. A very good example could be the privacy issue: a complicated and even intrinsically contradictory issue; it is both a "victim" of the need for enhanced security and a "beneficiary." Considering the socio- and psychological aspects of the problem could also help for proper threat prediction. A good example here is how the motivation behind the malicious activities on the Internet has changed during the last two decades: it is no longer "Robin Hood" style with honor and glory. Today's "virtual" bad guys are truly "bad", being no less cold-blooded and money-chasing criminals than their "real" counterparts. Of course, the terrorism threat, with its specific background cannot either be ignored. And finally, it is the society that matters in the end; it is not just about technologies. If not anything else, the successful protection of the CIs will mean continued trust in the future of the information society, a key to a stable development.

2.1.5 Concrete Results

As a summary of the tangible results from this working group, we present the following items:

1. We found that the by far most critical infrastructure is the communication system that the critical system as such is connected to. In almost all situations, this is the Internet.

2. If the critical system is isolated, i.e., has no connections to other systems, then the working group should not consider it as part of their work.

3. The working group should reflect upon the importance of cooperation between different agencies when incidents happen, and suggest policies.

4. We suggest that the FORWARD project seriously consider if there is a need for creating another working group focusing on "softer" issues, such as social, legal, and privacy issues.

5. The members of this working group should keep in contact with each other through Wiki or e-mail. Using these and similar channels the work will proceed and result in a white paper on protection of critical infrastructures.

6. We will continue to be a separate working group and not merge with any of the other working groups.

2.1.6 Conclusion

The fact that the CIs today are so tightly interconnected confirms the necessity for a project like FORWARD : it has been stressed that working cross-domain is very

important, if not critical for achieving a successful end result, and the effective and efficient coordination of the efforts will play a key role in this process. This does include the identification of the threats that are emerging at the moment or are likely to emerge in the near future; as one of the participants noted, it is very helpful to have the information from different sources correlated. Indeed, it is becoming increasingly difficult to conceive the possible threats and risks just based on single-domain observations. The complex mesh of systems will have weaknesses that can only be understood from a cross-domain perspective.

Coordination might help perceive the trends better, and thus predict with greater confidence which threats are likely to become (more) important in the future. It has been noted that this also includes correctly identifying the services that will play a key role in the society and economics of tomorrow, because these will likely be either the targets (being CIs per se) or vectors of future attacks (e.g., abusing a social networking infrastructure to spread false information, possibly creating mass panic, and thus affecting other systems.) The coordination itself must be leveraged not just to inter-domain, but to inter-governmental and international in general level as well. It is not just about learning from others' experiences, it is about understanding the complete picture viewed from different angles.

In conclusion, it is important to devise a standardized, well-structured approach toward the problem: identification, assessment, management, and classification. The continuing interaction between the participants will be of utmost importance in this process, and, in defining the approach, cooperation with the other working groups is also very helpful.

This group was subsequently renamed to "Critical Systems".

2.2 Fraud

Online scams are a form of online fraudulent activity in which an attacker aims to steal a victim's sensitive information, such as an online banking password or a credit card number. Victims are tricked into providing such information by a combination of spoofing techniques, social engineering, and sometimes advanced exploitation methods. In practice, the victims often receive an email that tries to convince them to visit a web page that has been prepared by the attacker. This page mimics and spoofs a real service such as an online banking web site. Legitimately looking web forms are provided through which the attacker can harvest and collect confidential and sensitive information.

Although tricking people to make financial profit is an old idea, criminals have realized that social-engineering-based attacks are simple to perform and highly effective over the Internet. Hence, although highly publicized, online scams are still an important security problem and many Internet users fall victim to this type of attacks. Note that such attacks are not only problematic for Internet users, but also for organizations that provide financial services online. The reason is that

when users fall victim to phishers, the organization providing the online service often suffers an image loss as well as financial damage.

2.2.1 Increase in Online Fraud

In recent years, online fraud has gained attention because the numbers of attacks and their sophistication have been increasing. The Anti-Phishing Work Group detected more than 25,000 unique phishing URLs in December 2007. Also, creating a phishing site has become easier. "Do-it-yourself" phishing kits created by criminals can easily be used by technically unsophisticated attackers. Moreover, recently, more sophisticated phishing attacks have emerged.

A typical fraud-related attack may be based on several techniques, including exploiting browser vulnerabilities or performing man-in-the middle attacks using a proxy. However, the most straightforward and widespread method consists of deploying a web page that looks and behaves like the one the user is familiar with.

2.2.2 The Fraud Working Group

The FORWARD fraud working group was interested in discussing the latest attacks and trying to understand the current trends in online fraud. Then, based on the current status of fraud on the Internet, we aimed to try to define how online fraud will evolve in the near future.

In the working group, three presentations were first given by Julio Canto from Hispasec (i.e., Virus Total), Gerhard Paass from Fraunhofer (i.e., the Antiphish EU project), and Wolfgang Trexler from Bank Austria. In his talk, Julio Canto presented some statistics about the current malware-related attacks that they are seeing. Julio reported that malware-related attacks are on the rise and they are seeing more and more tool-related attacks and botnets. Gerhard Paass reported on their content analysis-based research efforts that deal with identifying phishing e-mails. Finally, Wolfgang Trexler talked about online banking fraud in Austria and described the solutions that are used in mitigating the threat.

One of the conclusions of the discussions was that cyber-crime is on the rise. There was a general consensus that cyber-crime is here to stay as the Internet has become an important part of our lives. We do not only communicate over the Internet, but also do a significant amount of online business (e.g., banking) nowadays.

According to the participants of the working group, one of the main reasons why online fraud is increasingly gaining popularity is because Internet-based attacks are difficult to trace back. Furthermore, fraud on the Internet is easy to perform as a high number of users exist that are technically unsophisticated and are still not highly familiar with the Internet technology. For example, the effort required to launch a physical attack against a bank is very high (e.g., breaking in, armed robbery, etc.) in comparison to hosting a phishing web site and waiting for victims to simply enter their sensitive information.

The discussions in the working group also revealed that law enforcement agencies are either slow to react or do not have the necessary technical skills to identify the miscreants. With respect to traditional crime, crime on the Internet is much faster and typically more "international." That is, even if the attack takes place in Europe, the servers participating in the attack (e.g., phishing sites) might not necessarily be located in the same region. Hence, cross-border communications is often necessary, which is a time-consuming and tedious process. The working group believes that the miscreants responsible for the attacks are well-organized and know very well how law enforcement and the targeted organizations operate. For example, many attacks are now launched over the weekend as the miscreants know that not many experts are at work during this time and that they will need more time to react.

2.2.3 Future Trends and Developments in Fraud

When thinking about the future of fraud-related attacks, there was general consensus in the group that fraud was not going to disappear any time soon. In fact, everyone agreed that the problem was going to be exacerbated and that the sophistication of the attacks was going to increase. One question that was thrown in for discussion was if anything would change if, for example, the spam problem would suddenly be solved. Most participants argued that even if spam would disappear, new forms of fraud would emerge. As an example, one participant mentioned that social networks were increasingly being used by Internet users. Even if users may be reluctant to install untrusted applications on their computers, these users are less considerate when installing so-called untrusted "plug-ins" on their social network web sites (e.g., such as Facebook) that may actually be malicious.

One issue that was discussed in the fraud working group was if exchanging data would help mitigate fraud-related attacks. All participants in the working group thought that this was a good idea and that it could actually help. For example, it is certainly interesting for banks to find out if there are similar attacks happening elsewhere and what solutions other organizations use. Also, organizations are interested in knowing if certain malware specifically targets them before the attack largely seen in the wild. However, it was not clear how such a data exchange should be performed. That is, while many organizations are certainly interested in getting information and data, they are less excited about giving away information as they have privacy as well as security concerns. It is clear that a common basis of trust needs to be created among organizations so that they are willing to share sensitive information. Currently, some organizations (e.g., banks) are not even willing to talk about the problems they face as they are afraid that the information that they give out can be used against them in some way. The participants believe that by holding regular workshops (such as FORWARD), a common basis of trust can be created more easily.

One interesting research challenge with respect to online fraud is to be able understand how the underground Internet economy actually works. For example,

if we were to start a botnet business, how would we actually go about and communicate with our "customers"? How would we actually sell our services and initiate money transfers? Hence, by understanding the way this new type of illegal economy functions, the participants of the fraud working group believe that solutions could be created that actually undermine this economy and significantly increase the effort required by the miscreants.

2.3 Large-Scale Systems

In the session on large-scale systems, we had three presentations, which are summarized in the following sections. First, Serdar Tasiran presented his view on an increasingly important threat: concurrency vulnerability. Next, Roland Rieke presented his view on what he views as the weakest link in security, both now and in the future: the end-user. Finally, N. Asokan talked about new developments in authentication using the trusted platform module present in some new Nokia phones.

2.3.1 The Large-Scale Systems Working Group

The working group concluded that concurrency is important, and it does seem to be a class of upcoming vulnerabilities; especially considering the fact of increasing parallelization both on the PC themselves (multi-core, ..) as well as on the network (distributed computation). No other programming errors were identified that would result in new threats. This is an important result.

Users cannot just install any software on a mobile phone, so some of the problems of the TPM on PCs (what happens if the entire system is essentially insecure) are not expected on mobile phones. Nevertheless, malware is considered to play an important role on mobile devices in the future. The reason is mobile phones are increasingly becoming multi-purpose computing platforms, and users expect that applications that can be easily installed.

During the discussion, Ming-Yuh Huang presented some of the topics that he wished to address in his keynote at the end of the workshop. His three main observations were:

- First, within Boeing, authorization is a big problem. It is very hard to make sure that access granted by the system is exactly what it should be.
- Second, building systems out of existing components is very hard. Interactions become to complex to analyze. The participants of the discussion agreed that this was an important problem.
- Third, security should be an enabling feature. Too often security is too often viewed as an add on.

Other topics that cropped up during the working group discussion included:

- We should work towards building systems that continue to operate even when they are partially compromised.
- Sensors are a new issue: what happens when sensors get bad data (e.g., are they fooled)?

2.3.2 Summary

The conclusion of the session appeared to be along the following lines. First, we have two main areas of work/research to deal with, which are not the same, and while they overlap sometimes, they generally do not. First, we have (very) large software system, of huge complexity and sometimes heavily distributed. Second, we have systems with a large number of devices (phones, RFID).

Problems in the area of large software systems include concurrency, authorization, and integration. In the area of "many devices," the issues revolve around authorization (if people have many devices at home, how do they secure those devices?), fooling sensors, and management of these systems. For both areas, there are two problems that need to be dealt with: (1) we must be able to cope with partially compromised systems, and (2) we must establish security as an enabling technology.

While some of the topics are well-known, as they are problems in existing systems also, the working group is well-advised to look at concurrency vulnerability, "fooling" sensors, and the problems surrounding the systems with many devices. These are trends that have either fairly recently emerged, or have become increasingly important, and they do not have well-established fields of security research yet.

2.4 Malware

Malicious code (or malware) is defined as code that fulfills the harmful intent of an attacker. Typical examples include viruses, worms, and spyware. Although the history of malicious code reaches back more than two decades, the advent of large-scale computer worm epidemics and waves of email viruses has turned the problem into a major security threat for computer users. Indeed, the damage caused by malware has dramatically increased in the past few years, with a financial loss estimated to be as high as 14.2 billion US dollars in the year 2005. Another indication signifying the problem is that even people without any special interest in computers are aware of malware such as Code Red or Sasser. This is because security incidents affect millions of users and regularly make the headlines of mainstream news sources.

One reason for the prevalence of malicious code on today's networks is the rising popularity of the Internet and the resulting increase in the number of available vulnerable machines because of security-unaware users. Another reason is the elevated sophistication of the malicious code itself. Unfortunately, the problem of

malicious code is growing quickly as malware writing is turning into a profitable business. Malware authors can sell their creations to miscreants, who use the malicious code to compromise large numbers of machines that can then be abused as platforms to launch denial-of-service attacks or as spam relays. In turn, a thriving underground economy has developed in which malware plays a central role to allow miscreants to make huge profits.

2.4.1 The Malware Working Group

One issue that was raised was about the behavior of malicious code and their sources. Several participants agreed that the basic functionality of malware has not changed much. The samples that are observed today either steal sensitive information (key loggers, password thieves, Bank Trojans), send spam mails, or can be used to launch denial of service attacks. More significant changes are related to the way in which the malicious code is written. There was agreement that in addition to obfuscation to evade traditional, signature-based detection, malicious code increasingly tried to evade analysis. That is, by including code that detects virtual machine environments or debuggers, human or automated analysis is made more difficult. The goal is to conceal the malicious functionality for as long as possible and to make it more difficult for anti-malware companies to develop reasonable detection strategies. Moreover, polymorphism and run-time packing is a common mechanism to quickly create seemingly different instances of malicious code that share a common semantics. Finally, malware even uses encrypted configuration files to slow down analysis. Thus, one finding of this group was that *we expect a significant increase of novel techniques that tsealthy, malicious code uses to resist analysis and thwart detection*.

Another question that was discussed was the change in the threat landscape over the last years. There was the common agreement that most malware is actually coming from a (relatively) small number of criminal groups that have a well-funded development process and a pool of talented developers. These groups use those venues that can be most easily exploited to inject their code on end-user machines. Therefore, there is a strong trend towards social-engineering-based attacks (such as mails) or browser-based exploits compared to exploiting network services. As a result, novel mechanisms for data collection might be needed. For example, a traditional honeypot might not be efficient anymore to capture the current threats. This was confirmed by numbers from VirusTotal, which showed a discrepancy between the malware that they see compared to the samples that are collected via traditional honeypots. Moreover, the adversary might have developed techniques to fingerprint and detect honeypots so that they can avoid detection. Finally, mapping out dark (honeypot) address spaces is an emerging threat. As a result, *the group saw the need to develop techniques that can accurately capture emerging threats, since a good intelligence is a prerequisite for subsequent mitigation efforts.*

Related to the previous issue, the group also discussed emerging targets of malicious code. In particular, the question was raised whether mobile devices (phones,

PDAs) might become a target. Everybody agreed that the threat has been overly hyped in the last years. However, once there is a business model behind attacking phones (i.e., it turns out to be profitable for the criminals), such attacks can be expected to appear. Also, this development will be supported by the significant growth in the number of mobile devices. This is clearly related to the other working group on large-scale systems.

2.4.2 Malware Response

A problem that is more related to malware response was also brought up. In particular, the question was discussed what infrastructure providers such as ISPs or telecom companies can do when they detect an infected machine. Here, the problem was less technical than an issue with legal regulations and market forces. The reason is that one cannot simply blacklist or turn off infected machines, since customers may instigate law suits. Also, mitigation might cost money because customers that are shut off the network call tech support and do not understand their wrongdoing. Also, many customers simply do not care about malware infections as long as their machines are still usable for normal work. Some of these problems can be solved with new service level agreements (SLA), but in general, *the group felt that legislative support will be needed to allow ISPs more rights when requiring customers to clean up their machines*. That is, more liability must be put on the customer to force them to try to secure their machines.

2.4.3 Data Sharing

Finally, the question of data sharing was raised. Here, *the group felt that technical means to sanitize malware samples must be developed*. Of course, in addition to the technical questions, there are organizational means that need to be in place to allow people to cooperate. Here, the project can play a crucial role in setting up trusted communication channels where a small group of vetted individuals can start to engage in data sharing. Based on their experience and requirements, the working group might draft a specification of the information from each sample that is needed to allow others to perform meaningful analysis while preserving the privacy of the targeted organizations. It was concluded that a mailing list with vetted access would constitute a good starting point.

2.4.4 Summary

Orthogonal to the technical questions, the group also addressed organizational issues and discussed ways to setup the working group in a fashion that facilitates active participation. In particular, it was felt that participants need to know the precise goals of the working group. Two important goals are: (a) creating a lively platform where people do share their ideas about future, emerging threats, and (b)

ensure that participants are aware of the fact that the project's outcome is supposed to be a document that can influence policy makers.

It was concluded that a Wiki is a good idea. This Wiki should start with a page that expresses what we expect from the final document, then we will draft a table of contents and ask for external help. This Wiki should have two tiers: one with public information and one with information restricted to the participants of the working group. Moreover, it should be possible to post anonymously. Finally, a mailing list will be installed to support the Wiki-centered exchange model. Nevertheless, the Wiki should be separated from the final document and serve as a scratch-pad for drafting and discussing interesting ideas. In addition to the mailing list and the Wiki, some participants strongly felt the necessity for personal meetings. Thus, in addition to the working group meeting after the first half of the second project phase, it was considered to hold monthly teleconferences. Direct interactions increase the networking factor and help to build trust between participants in this sensitive area.

2.5 Network and Monitoring

The session comprised of a diverse crowd and touched on a variety of topics. The main themes revolved around threats to the network infrastructure, be it the Internet as we know it or evolving types of wireless networks, and threats to privacy.

2.5.1 Threats to the Internet Routing Infrastructure

One important issue are threats to the Internet routing infrastructure. Internet routing (BGP) is vulnerable against attacks. In particular, false or spoofed BGP network announcements can be honored by parts of the Internet. This may result in DoS attacks against large parts of the network or hijacking of, for example, well-known web sites during the time the false information is valid. Other problems arise from mistakes made by (trusted) operators when configuring routers or entering routing information which could have similar effects upon the Internet. Yet another type of problem are DDoS attacks against BGP routers, which may have the effect of making parts of the Internet temporarily inaccessible. A single router can also be attacked and its traffic sent via a tunnel (e.g., GRE) to a remote site that can then act as a man-in-the-middle for arbitrary domains and servers.

The problems arise from the fact that the current protocol, BGPv4, is 12 years old, and it was not designed for the current Internet in mind. Furthermore, BGPv4 is here to stay for a very long time, which means that threats are going to follow us in the near and long term future. Even though solutions exist, everyone must start using them at the same time, something which is not likely to happen. Countering future threats would involve (i) motivating vendors to implement solutions, and (ii) somehow extending BGP in a backwards compatible way to make sure the new functionality is used.

More secure routing protocols exist (S-BGP, soBGP), and can be used to verify the origin and correctness of the received information. However, BGP signatures are problematic. The solution may be to move this to out-of-band systems, since all routers are CPU-limited. Also, Moore's law does not help router builders, since density and power remain as issues as more capacity is added. It seems that in the future, there will be no need to propose new routing protocols, unless they offer some really great properties, and as mentioned before, old threats will remain.

2.5.2 Private and Secure Network Monitoring and Data Collection

One problem when attempting to study network-based threats is the question of private and secure network monitoring and data collection. There is an ongoing project in FP7 called PRISM, PRIvacy aware Secure Monitoring (`www.fp7-prism.eu`) with the goal to enhance privacy when networks are being monitored with special focus on on-line services. The idea is to create a balance between the users (customers) trust of services and the need for governments and other instances to collect information from networks. Network monitoring is necessary in many environments and is often seen as a threat to the users. Insider problems are also addressed and can occur, for example, if someone decides to sell information to third parties about traffic or contents of traffic. One major challenge is how to anonymize data without losing too much information. A method was described from the Prism project where encryption and anonymization of the collected data was applied where a special data collection engine was used to access only relevant data.

2.5.3 Attacks on Wireless Infrastructures

The challenges to deal with threats on privacy in the future will be the development of better anonymization techniques. Existing systems that have to save data for legal reasons will be even more vulnerable in the future due to the growth in data collected. Also, in the future, we will (hopefully) have even greater exchange of data between network operators for better managing the network infrastructure, but this will lead to a series of possible threats.

In the future, there will be increased demand for cooperation between technical experts and legal experts, to coordinate sharing and exchange of data. This will have its own set of challenges, which is unclear at this point how one can solve. For example, more and more biometric data is being stored in governmental as well as private databases. Biometric data is extremely valuable to attackers and are also (nearly) impossible to revoke. The threats of compromising such datasets in the future will be real and pose real dangers to society. The current trend at the state level is to try to legislate our way out of the problem. But legislative solutions alone are not the answer. One can actually argue that over-legislation can be a future threat in itself.

Finally, a significant, network-based threat are possible attacks against wireless networks. The future is wireless, which means that new attacks will focus more on the wireless infrastructure in order to interact and disrupt service. Research issues could include robustness, security, and scalability in wireless environments (where the trend is limited resources and increased programmability). There are several examples of how wireless traffic (WLAN/802.11 and GSM) can be affected and that, for example, destroying one bit in a GSM time slot (in the control channel) can prevent anyone from joining the network. One working group member argued that the power consumption of such attacks is very low, is that it is hard to trace, and that it could be very effective.

Similar attacks could be spawned against a WLAN network, where a single bit in the link layer is destroyed and the whole packet will then be discarded. The attacker just has to send and destroy one bit out of 10,000 to disrupt the service. Again, power savings is the focus of such attacks ("low power jamming"). Another problem that makes WLAN/802.11 networks vulnerable to such attacks is the timing of frames (while other nodes are waiting for a free channel, the attacker can violate the timings and send some data, causing the others to back off.) Cross-layer attacks are simply the idea to destroy a few bits at the right time and place.

With the proliferation of wireless networks be it WiFi, cellular, vehicular, or other, we are bound to face an increase number of such threats in the near future. The SPREAD project tries to address these problems where agility and diversification is part of the answer. It is similar to frequency hopping but applies to the whole network stack.

2.5.4 Summary

In conclusion, the future of the Internet, wireless or wired, will be plagued by a plethora of security and privacy issues. We have existing technologies that can address some of the issues but old threats are likely to remain and be exacerbated due to the increased reliance on network services and amounts of data the flow in our networks and are stored in our end systems.

Chapter 3

Position Papers

In this chapter, we present the individual contributions of workshop participants. As mentioned previously, we had a total of 15 plenary talks and 15 talks in the working groups. We asked each speaker to provide a short abstract that summarizes the ideas and opinions that this speaker aimed to present. In many cases, we received these abstracts - in these cases, the text is included with only minor edits. In many other cases, no abstract was made available to us. In those cases, we summarized the talk based on the slides and the presentation. Some group members provided position papers after the workshop, reflecting their view of what had been achieved and how to continue. Those papers are marked "post-workshop paper".

The summaries are grouped based on the working group topic that their contents fit to most closely. We also introduced a sixth category that holds talks related to European and international coordination and cooperation efforts. Within each section, the talks are sorted alphabetically. Also, note that two speakers decided that they do not wish to have the contents of their talks appear publicly (because of the restrictions emposed by their organizations). Thus, we have listed only 28 abstracts (instead of 30).

3.1 Critical Infrastructure Protection

F. Kargl: Security and Privacy in Inter-Vehicular Networks

Inter-vehicular communication (IVC) is a recent research trend found especially in the US, Europe, and Japan. Starting from initial research projects like Fleetnet or VSC, we currently have a number of second generation projects (e.g., Fleetnet, VSC, Network-on-Wheels, VII, CVIS, Safespot). In parallel, standardization groups have started to work on common standards (e.g., IEEE 802.11p and 1609.x, ISO-CALM, C2C Communication Consortium). By enabling cars to communicate with each other or with roadside equipment, exciting new applications become possible that make driving safer, more efficient and comfortable, but also help in car

production or maintenance. As a simple example imagine two vehicles involved in an accident. These will start sending periodic broadcast messages warning nearby vehicles of the danger. As those vehicles receiving the warning will also rebroadcast it to their neighboring vehicles, drivers approaching the site of the accident can be warned hundreds of meters away, even if there is fog or no direct line of sight. IVC research focuses on applications and efficient information dissemination strategies, but also on security and privacy aspects. Regarding the later two topics, the European SeVeCom project has an outstanding role, as it is the only project focusing exclusively on those aspects.

Topics addressed in SeVeCom include key and identity management, secure communication protocols, tamper-resistant hardware and cryptosystems, in-vehicle intrusion detection, malfunction detection and data consistency, privacy, secure positioning and security user interfaces. Huge databases containing traces of every vehicle on our streets are a privacy nightmare that could come true using IVC mechanisms. PRECIOSA is a new project that addresses especially those issues and tries to come up with technologies and guidelines to ensure privacy also in future transportation systems.

In contrast to earlier research on security and privacy in generic mobile ad-hoc or sensor networks, IVC has a unique set of properties that heavily influences security and privacy solutions. Scalability of security to millions of vehicles, high relative speeds, real-time constraints in many applications, or the possibility to create detailed personal position traces of drivers are only some examples. Communication is not focusing on unicast but instead uses patterns like beaconing, Geocast, or position-based routing. Newer approaches like Gossiping, Context-adaptive Message Dissemination, or aggregation mechanisms further strengthen the trend and lead to the observation that those forms of communication already provide an astonishing degree of resistance against attacks. In contrast to many routing protocols, there is (nearly) no signaling between nodes that an attacker could exploit. Essentially, an attacker is constrained to Denial-of-Service attacks or modification/forging of information. To counter such attacks, we need a new way of context-sensitive or organic security that constantly monitors the received information, checks it for plausibility, and leverages the redundancy of information transmitted from different entities in the network. Additionally, real-world sensors and domain knowledge can be used to discard incorrect information from the network and rate-limits can restrict the effects of Denial-of-Service attacks. SeVeCom has started the exploration of such mechanisms and initial results are very promising.

E. Nordin: Go with the safe flow

The increased globalization means that information, money, and people flow worldwide, not limited by national borders or regulations in the same way as before.

New means of communication and transportation mean new threats. Many critical services in our society are more and more dependent on secure IT-solutions and reliable, trustworthy communication. This makes us vulnerable to new kinds of threats.

Most of us have a pretty good idea of what the threats against the Information and Communication Technology infrastructure are: terrorism, malicious code, hackers, eavesdropping, system failure, environmental disasters and malicious acts or wrongdoing from users. Criminals move more towards computer-related crimes. This is a natural development because criminals move to where the money and other critical resources are. It is also easier today to anonymously find information about different types of systems. It is also a fact that production systems very often are connected to other networks or to the Internet in one way or another. One can make a long list of critical societal functions that can be jeopardized, but the list can also be as short as "everybody." Just imagine the consequences if critical infrastructures like energy, transportation, or water systems would be targeted by malicious attackers. A worrying fact is that the security monitoring of many critical infrastructure systems today is non-existing.

As of today, we can not foresee what an attacker will do. First of all, we have to be prepared for likely attacks and secondly, use an incident handling procedure to stop the attack and salvage what can be saved. These are a few areas where Combitechs information security experts have extensive knowledge and long experience from: source code analysis, establishing IRTs, Common Criteria (CC), penetration tests, log analysis and computer forensics.

A. Pasquini: Security and Dependability Perspectives in Air Traffic Control

Systems used in air traffic control have always been characterized by a limited sensitivity to dependability problems and to possible malicious attacks, which could possibly impair their integrity. It has been stated that the current systems base their functions on data provided by radars that serve a local community of air traffic controllers. As a consequence, these systems are well-confined and protected from incorrect interactions with the external world, whether unintentional or deliberately malicious.

Simultaneously, it is the humans who are at the center of the decision process, with the automated systems ensuring only some support in form of information filtering and presentation, forecasting possible traffic evolution, and providing alerts about traffic conflicts. So, most of the safety problems are caused by human errors, air-ground communication problems, and/or degradation of technical and human services combined with adverse atmospheric conditions.

However, it has been further presented, there are several recent developments that will considerably change this situation:

The control systems are becoming more and more open to the external world, and thus, are more likely to come under malicious attacks or even just have unintentional damaging influence. An example was given that there was a clear trend towards the automatic exchange of information between the air traffic control centers and the controlled aircraft to increase the communication capacity and avoid communication misunderstanding between pilots and controllers. Upcoming systems of this type include the *Controller-Pilot Datalink Communication (CPDLC)*, considered a key component of the future Air Traffic Management evolution, and the systems that allow down links to the controllers of the Resolution Advisories produced by the *Airborne Collision Avoidance System* (commonly referred to as *TCAS*,) which help pilots to avoid collisions in emergency situations.

Another example was presented with the rise of new control concepts based on aircraft identification and location through satellites, which bring an increased need for communication and interactions between different categories and classes of systems. In all these cases, exchange of data will be controlled by software, using a mix of proprietary and public communication channels. This, of course, raises concerns about possible new security and dependability issues.

The *Single Sky* initiative, recently launched by the European Union and Eurocontrol, aims at achieving a more effective and integrated air traffic management architecture, ensuring that this architecture is based on demand driven service provision. European airspace will be restructured as function of the traffic flow, rather than according to national borders, thus increasing the overall efficiency of the air traffic management system, creating additional capacity, and increasing safety. This, however, will require an increased exchange of data and a better coordination between the various control centers, and also homogenization of the different local practices and equipment.

The conclusion was that there was a growing concern about the effects of the increased dependability and the possible new security problems, related to this more open and automated environment towards which we are heading. Especially troubling is the limited awareness of the problem and of the possible solutions amongst the providers of Air Traffic Services. While flying is still extremely safe, it may not be so much in the future, unless proper attention is paid to these issues.

A. Stefanini:
Towards measures to support the Security of Control and Real-Time Systems

Networked computers reside at the heart of plants and systems on which our daily life depends, such as power, manufacturing, oil and chemical plants, and the related delivery infrastructures. Today, many of these systems are far too vulnerable to cyber-attacks, which can inhibit their operation, corrupt valuable data, and expose private information. Some of these attacks might actually have catastrophic consequences on the environment and the safety of the population.

It was noted that there had been a qualitative leap in the last years in the need to safeguard such installations against malicious activities that could have resulted from acts of terrorists, organized crime, or violent extremists. The intensive use of ICT brings a constant influx of new vulnerabilities, and this in a scenario where security threats are, in fact, increasing as well.

For these purposes, the JRC has developed an approach for the systematic assessment of the security of those installations. This could help in evaluating and strengthening the current systems and might support the design and development of new ones. The presentation specifically concentrated on the experience made with GRID, a coordination action about ICT vulnerabilities of the power grid, to overview the current landscape of security threats against supervisory and control systems.

A very indicative shift in the industrial cyber-incidents was demonstrated. During the period 1982-2000 the charts showed 69% of these to be either internal (inappropriate activity by employees, disgruntled employees, etc.) or accidental, with only the remaining 31% of external origin, after the year 2000, the share of the latter has increased to as much as 70%, far surpassing the other types. It was further demonstrated that the major local source of incidents was the business network, but at the same time direct physical access still played a very important role.

It is very worrisome that critical systems have already been indeed hacked into, some of these attacks being accompanied by extortion attempts, and some having even resulted in true service disruptions. Unfortunately, there are many possible vulnerable targets for such attacks, and some of the attacks could cause damage that would take months to fix.

It has therefore been emphasized that it was very important to establish consensus on the key issues involved in the ICT power systems vulnerabilities. Focused R&D is required on the relations between the ICT functions and the power system. The investigation must focus on the control architectures and technologies upgrade. Furthermore, the difficulties or barrier before the integration of innovative control technologies must be overcome, and a new control paradigm based on the use of decentralized intelligence must be devised. There is a strong need to increase the awareness on control and ICT vulnerabilities where a basic and widespread education on risk is lacking. It is also very important to achieve consensus on risk governance structures, and especially vital to establish standards and platforms for risk assessment. It was noted that Europe is lagging behind the US, and the perceived lag was described as ”broader than 2 years.”

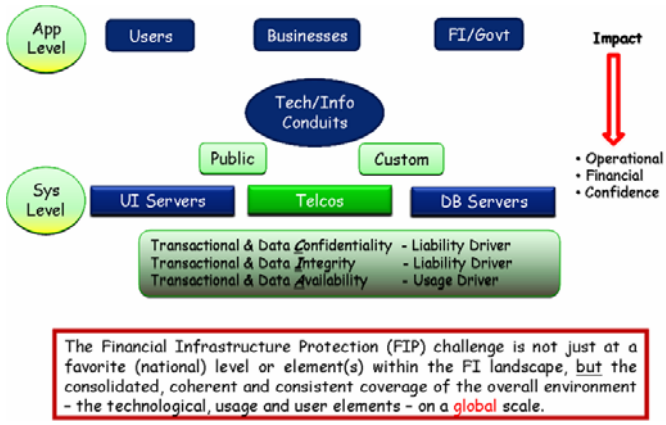
J. Clarke, N. Suri: Financial Infrastructure Protection (post-workshop paper)

An area of coverage we would like to have included in this working group is Financial Infrastructure Protection. This is crucial to ensure stability, availability, and

continuity of the key financial markets and individual businesses worldwide. Traditional approaches have focused on protecting individual financial domains (such as banks or brokerage firms) while ignoring the threats arising from the cross-domain interactions as well as those originating from remote, seemingly unrelated critical infrastructures. With todays crumbling organizational boundaries, and the emerging trends towards fluid, globally integrated enterprises, these approaches are no longer adequate and needs to be addressed by the RTD communities.

Within the STREP CoMiFin (ICT-SEC-2007-225407 starting 1. Sept. 2008), we aim to develop a comprehensive approach to the financial infrastructure protection. In contrast to the existing work, we will not restrict our attention to protecting each individual financial domain, but rather focus on the entire financial ecosystem as a whole. Our specific objective in the CoMiFin timeframe will be to devise a scalable distributed monitoring subsystem that will provide the relevant IT components of each participating financial domain with early notifications about faults and other potentially malicious activity originating at remote sites (possibly belonging to other critical infrastructures), thus, enabling those components to trigger the necessary protective mechanisms in a timely fashion. It is envisaged that these outputs can be fed into this working group of FORWARD.

As shown in the following figure, the challenges for protecting these infrastructures must be addressed from the perspective of the overall environment the technological, application and system levels, middleware level, usage and user elements AND on a global scale. The FP7 Coordination Action INCO-TRUST will be addressing these global issues.



F. Holgersson, E. Nordin: Additional Thoughts on Critical Systems Infrastructures (post-workshop paper)

Critical infrastructure has traditionally been represented by water, food and power distribution systems. Aside from this, logistics, (both human and material) is -

and has been - of critical importance. Information distribution systems, such as communication networks, have not until recently been considered to be of critical importance. However, this is now a fact.

When looked upon as carriers/distributors of public information, communication systems have a very real risk of creating mass panic or otherwise adversely affect decision makers into making the wrong decisions. If relied-upon communication networks are violated, information received from them will most likely be considered to be valid, thereby risking important decisions to be based on invalid grounds.

In the world of today almost everything is interconnected, or is on the verge of becoming so. If we are to allow power grids and water distribution plants to be connected to an accessible communications network, then we must be able to say with a high level of certainty that this connection can not adversely affect normal operation. When we connect existing resources to a new medium, we also expose them to every single threat that exists on that medium. This has to be taken into account before critical assets are exposed to threats which they are not equipped to handle. For example:

- What could happen if the cooling system of nuclear reactors would be accessible from the outside world?
- What could happen if the power grid could be controlled from the outside in the middle of the winter?
- What could happen if traffic lights would be accessible from the outside?
- What could happen if the air traffic control system would be accessible from the outside world?

Critical systems of today are not as easily defined as they were only a few years ago. Today, almost everything is interconnected, exposing every system to the risks of every other system.

Potential threats could be:

- Pharmaceutical companies: What would happen if their production lines would be violated? What could there be in a common paracetamol?
- Road traffic control systems: What happens when every traffic lights shows green?
- What happens when two bridges as the well as the tunnel of Gothenburg are not accessible? The traffic system would literally go down. If the traffic system would go down, then so would almost every industry in the Gothenburg area. Most major cities have choke points such as these.

F. Kargl:
The Trend towards Decentralization in Critical Systems (post-workshop paper)

In distributed systems, we face a constant trend towards decentralization. Whereas in former times, critical systems were mostly composed of one single host, later these hosts were interconnected by dedicated networks, which are nowadays more and more replaced by the Internet. Today, many critical systems are in fact systems of systems that are not controlled by a single instance any more. This has major implications for the security and reliability of those systems. More partners need to get involved, making policy-making and administration much more complicated. Furthermore, there is no clearly defined inside-outside boundary any more that could be protected by simple means like firewalls or encryption. VPNs, IDSs, personal firewalls, distributed firewalls, web-services security, etc. are all examples of mechanisms addressing the problems of those decentralized systems. However, extrapolating the trend towards decentralization into the future will raise security and reliability issues that are by magnitudes more complex and will require a substantial different approach to be addressed.

The vision of ubiquitous computing paints a picture of the future where each and every thing in our world will contain small computers that are all interconnected by wired or more often wireless communication. It is not too likely that those devices will not be part of critical systems. Two examples of such systems include vehicular ad-hoc networks (VANETs), vehicles communicating wirelessly to inform each other about e.g. dangerous driving situations or the traffic situation, and wireless sensor networks (WSN), miniature systems including processing, sensing, and communication capabilities to perform all kinds of monitoring tasks. Prototype implementations of such systems are actually already used in field-trials or for research purposes. From a security and reliability point of view, those systems are extremely heterogeneous, dynamic, often including mobile nodes that are owned by a lot of different persons or organizations. As all those nodes contribute data and computations to the overall application, new security challenges arise:

- As so many participants are involved, trust in persons or organizations gets replaced by trust in data.

- As the systems are very heterogeneous, dynamic, mobile, proactive prevention of attacks becomes hard and reactive security that detects attacks and reacts by appropriate measures, e.g. by discarding unreliable data, enhancing redundancy of message dissemination, etc.

A. Pasic:
Contribution from Atos Origin (post-workshop paper)

Some important issues which need to be addressed and could be included in the scope of this WG are:

1. Technical measures, and more specifically trust, security and dependability solutions that should be adapted or introduced in order to facilitate the implementation of the Critical Infrastructure Warning Information Network (CIWIN), the cross-border European Critical Infrastructure Protection (CIP) and CIP information sharing processes. and the identification and analysis of interdependencies.

2. Identify cross-infrastructure and external dependencies, as well as effects of it; tools and technologies for prevention, simulation, modelling...

3. Scenario building and "lightweight" risk assessment that involves collection of relevant threat, vulnerability, and consequence information (historical, publicly available data or simply based on assumptions that can be used for illustrative purposes). This would involve cross-domain cutting criteria developed on the basis of the severity of the threat propagation, disruption or destruction of the CII.

Regarding the aim of this WG, having in mind that most of this WG members comes from research community, we suggest to focus on future and emerging protection requirements that will have to take into future ICT and socio-economic concepts and contexts (let us call them "challenges") such as:

- Changes in the infrastructure stakeholders (e.g. providers, operators, intermediations etc)
- Changes in devices and network elements (e.g. sensors, handheld devices, virtualization, etc)
- Changes in the requirements (e.g. cross-border connectivity, performance, end-to-end protection, etc)
- Changes in threat models (e.g. risk of corruption or failures stemming from malware or malicious code, identity fraud, etc)
- Other forthcoming changes in CII

Atos Origin role

Atos Origin is the coordinator of PARSIFAL (Protection And tRuSt In FinanciAL infrastructures) coordination action that is scheduled to start in September 2008. PARSIFAL will dedicate special attention to the relation between protection of CII and trust, which is the key business requirement in the financial world.

PARSIFAL will match technological challenges to the future financial service scenarios (e.g. international services that run on Critical Financial Infrastructures). The results of these activities will feed into the EU policy process and research agenda.

H-L. Truong and S. Dustdar: On Protecting Networks of Services (post-workshop paper)

In our view, todays and future critical ICT infrastructures are managed by networks of software services belonging to possibly different organizations. We consider that such networks of software services are (parts of) critical systems. Examples of these networks include critical information systems supporting crisis managements, sensor Web for monitoring environments, collaboration services for networked enterprises. Although services can be provided in various forms, we believe that the mainstream of critical systems will be built around Web services technologies. To protect critical systems equals protecting networks of software services. We believe protecting critical systems is not only to protect the software (to ensure the software functions as in its design) but also to integrate human in the loop because there are various tasks which cannot be done by software in critical situations. In this sense, critical systems will include also humans, constituting the so called "mixed systems of humans and software services". Furthermore, we believe that we should not focus solely on the "defence" of critical systems but also on the response to the crisis of critical systems. Networks of software services in critical systems typically are managed by different organizations. Thus, the protection of critical systems should be coordinated across the boundaries of single organization because a critical system can be attacked from any point in the system's network. We, therefore, propose this working group to focus on the following topics:

1. To develop software engineering techniques supporting the design of critical systems to work on failure conditions. The services in critical systems and the systems themselves should be self-managed. This requires a multidisciplinary effort as we need to provide techniques at multiple levels, from networks to middleware to applications.

2. To develop monitoring techniques and infrastructure for large scale networks of services across various organizations. The prerequisite for this is that services must be monitorable at runtime. The monitoring of such networks require standardized data presentations, protocols, large scale and distributed storage, access controls, to name just a few. Here we stress that the monitoring is not only at the network level but also at the application level and we should target to the monitoring of large scale networks of Web services with the focus on providing information for threat management.

3. To develop tools and policies to support the correlation and mining of monitoring data of critical systems on the fly. We need to detect threats and patterns of threats which are associated with services and humans based on different types of interactions such as service-to-service, human-to-service, and human-to-human. The key challenge here are the technique and policy to support the correlation monitoring data gathered from different organizations.

4. To develop techniques and tools for supporting the response to the crisis of critical systems. We need crisis management systems and tools to support collaborative works in crisis situations. Furthermore, we need a mechanism to integrate humans into critical systems, making humans as a part of critical systems who can readily react to and solve activities that software services cannot do in critical situations.

3.2 Fraud

D. Chavarri: Current and future trends on e-crime

There are currently different types of online fraud that are updated as fast as new swindling techniques emerge. Phishing continues to be an important danger on the Internet, but the most popular type of attack consists of introducing malware (malicious software) in computers with the intention of stealing passwords directly usually using spy programs and trojans, while allowing third parties to take total control of a computer remotely and building botnets.

Malicious code authors used to be smart people, eager to learn new techniques and show their skills. However, some years ago, criminal organizations realized how powerful the Internet is for committing online fraud. They learned to take advantage of the Internet's weaknesses and set up a lucrative business. The e-crime business includes different roles: Pen-testers, network and system administrators, C&C developers, malicious code developers, herder, mules, and spammers. Outsourcing one or many elements of the business chain is usual.

The probability of being infected depends on several factors: most of the infection vectors work by exploiting a vulnerability in the victim's computer. The most common infection methods detected by S21sec include browser exploits (65%), email attachments (13%,) operating system exploits (11%), downloaded Internet files (9%), and other methods (2%).

People behind this threat are not teenagers any longer, but experienced criminals. Why are they interested in controlling so many computers? Because they can provide the following "services": distributed denial of service attacks (DDoS), financial online fraud, further stealth attacks, spam, malicious code distribution,

click fraud as well as new business models (the entire infrastructure can be rented or sold).

Security technology providers will have to face new e-crime technological advances:

- New infection methods and new usages. For instance: worms that use IM networks like MSN or Skype to distribute themselves, malicious code targeting mobile devices: worms that distribute themselves by using MMS (e.g., Commwarrior) or SMS, and Bluetooth communications, malicious code targeting new devices (game consoles, Media Centers...)
- Heterogeneous customers connection (unknown wireless networks, different connection technologies) makes ISP efforts effectless.
- Diversity and innovation in trojans and C&C connections (covert channels with DNS, ICMP, P2P...) makes filtering too difficult. There are also other interesting techniques like DNS records that are constantly changing, use of reverse proxies to redirect the user to another compromised computers, etc...
- Improvement of attackers' security measures to avoid detection. Use of public key cryptography, distributed VPN, PHP encoding, JavaScript obfuscation, kernel packers, covert channels, and auto-removal once they notice something strange.

L. Corrons: Panda Security: The Business of Cybercrime

In his talk, Luis Corrons asked if there is a real business behind all the malware that is appearing every minute. Whereas early malware was not focused on making a financial profit, unfortunately, this is not the case anymore. The success of the web and the lack of technical sophistication and understanding of many web users has attracted criminals, who are well-organized and who aim to make easy money. As a result, the number of malware instances discovered in the wild continues to increase at an alarming rate. To defend against the flood of malware samples, the anti-malware industry has to invest significant effort to develop effective signatures. Unfortunately, the problem of maintaining a signature database and keeping it up-to-date is not trivial.

Luis reported that the number of new malware samples has increased exponentially, and he has argued that the malware problem is about to get out of control if the appropriate steps are not taken.

One of the new developments in the malware scene is that attackers are increasingly making use of toolkits to launch their attacks. For example, web toolkits exist (e.g., MPack) that the attackers can use to easily create exploits. In fact, Panda tracked MPack for 2 months and discovered that 41 servers were running MPack and more than 300,000 pages and more than one million users were infected.

In an analysis that Panda performed, it was discovered that even simple attacks could result in large profits. In one case, the attackers were making up to $840,000 per month. Also, attackers were also openly advertising their "services" on web sites. For example, one could simply go to a web site and buy spam or botnet services.

It looks as if money transactions are mainly being handled by so-called money mules. These are unsuspecting users who are made to believe that they are working for a legitimate organization. The stolen money is sent to these users who then withdraw the money and send it to the attackers (e.g., via Western Union). The money mule can keep a certain percent of the money that is being transferred. Whenever an attack is uncovered, the money mules are usually the first people to be arrested. Unfortunately, these people are often naive and do not know for whom they are really working. They have simply been tricked into making easy money.

Luis also reported that the criminals behind these schemes are so well organized that they even have their own conferences nowadays. That is, they meet regularly to celebrate their profits and to talk about future scams.

Hence, one interesting research challenge is to try to understand these hidden, underground economies. By understanding how the criminals operate, we can come up with solutions to undermine their efforts and to mitigate the attacks that they launch.

G. Paass:
AntiPhish: Detection of Phishing Emails to Secure Communication Infrastructure

In the last years, email traffic has shown a rapid expansion of phishing, the practice of luring users to fraudulent websites. In a typical phishing attack the phisher sends out emails pretending to come from a reputable institution, e.g., a bank. In the email or on a linked website, unsuspecting online users are asked to reveal passwords, account numbers, social security numbers or other personal information. Phishing has increased enormously over the last months and is a serious threat to global security and economy. In October 2007, about 46 new phishing sites were detected per hour. The average time for phishing sites to be online is only 3.1 days; many sites disappear within hours. Recent investigations show that a quarter of Internet users are not familiar with simple characteristics of phishing emails and up to 90% of users are fooled by good phishing websites.

One approach of phishing prevention concentrates on filtering websites when they are rendered in a web browser. In the Mozilla Firefox browser, for instance, each web page requested by a user is checked against a blacklist of known phishing sites. This list is automatically downloaded to the local machine and updated in regular intervals. As new phishing sites appear frequently, the effectiveness of blacklisting is limited. Whitelist approaches, which maintain a list of "good"

URLs, have also been implemented. However, it turns out that it is very difficult to register large numbers of variants of legitimate sites.

An alternative is the filtering of email content and associated web sites. This is the main approach followed in the AntiPhish project. In this project, the members have developed a flexible architecture for the extraction of features from emails. Based on comprehensive training sets of spam emails, phishing emails and legitimate emails advanced machine learning algorithm and classifiers are trained to distinguish between these email categories. The outcome of these learners are combined to improve efficiency and reduce computational effort. Recently, more and more images appear in spam and phishing emails which contain the actual message. Therefore, AntiPhish uses optical character recognition to reconstruct the message text, which subsequently is forwarded to the message filters. In the same way, the text and structural properties of linked websites are exploited to decide whether an email has phishing content. Using a combination of these techniques the AntiPhish approach has a better filtering reliability than all other published approaches on published benchmark datasets. In addition, it was able to increase the filtering performance on real-world email streams to a very high level.

A special problem is the continuous appearance of new types of phishing emails which use new ways to disguise their contents. Specific ”salting tricks” are, for instance, white text written on white background or the arbitrary placements of words and symbols on the page to change reading order. AntiPhish has developed new methods to detect such tricks. Using this information the existing phishing filters may be updated. Together the combination of the mentioned technologies is able to detect a very high percentage of phishing emails without eliminating legitimate emails.

G. Vigna:
Undermining the Underground Economy

Recent years have witnessed 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” to “hacking for profit.” 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. 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.

Recent research has mostly focused on the visible aspects of the underground economy, such as botnets, spam, and phishing. Little has been done to understand

this economy as a whole, to analyze and model its characteristics, and to undermine its pillars. What is needed is a holistic approach to the study and analysis of the underground economy that includes all aspects of the criminal process. Only by clearly identifying the different roles among the phases of a criminal endeavor, the actors involved, and the service infrastructure necessary for its execution, is it possible to create effective countermeasures to these criminal activities.

Therefore, there is a need for novel techniques and tools to analyze the underground economy and obtain a comprehensive picture of the complete criminal process. More precisely, first of all it is necessary to create models of the underground market, its actors, the processes and interactions between actors, and the underlying infrastructure. Then, it will possible to devise techniques that leverage these models to disrupt parts of the criminal process and support the fight against computer crime.

Our approach is based on the insights that we have gained from our previous research on botnets, malware analysis, and phishing. We propose to extend the scope of our research to encompass the entire fraud process, from the compromise of a victim's information to the collection of goods and money. The analysis of the underground economy will proceed along the following three axes.

The first axis is to understand the actors that participate in the underground economy as well as their different roles. As a first step, we will identify the places on the Internet where different actors meet and exchange goods and services. This will allow us to infiltrate these marketplaces by placing probes that monitor activity on a large scale. Then, we plan to determine those actors who offer particular types of services and commodities, and those who request them. Moreover, we plan to understand the relationships between actors. That is, we propose to infer social connections between different actors (e.g., two entities who are frequently engaged in transactions), as well as different channels or venues that are visited by the same entities. This will allow us to identify influential groups or trend-setters within the underground.

The second axis is to understand how transactions are performed in the underground economy, and how information and goods flow between different actors. Similar to other economies, the concept of a division of labor is also present in underground markets. For example, a phisher typically does not use stolen bank login credentials directly. Instead, he sells this data to other criminals. As part of this research, we propose to create a model that characterizes the flow of information and goods within the underground economy. This model will capture the ways in which different roles within the economy interact.

The third axis is to understand the infrastructure that is used by criminals to carry out their operations. We plan to monitor the underground economy to obtain more details about the platforms that are used to exchange information, the servers that are used to host malware or phishing pages, the machines that are used to send spam, the points from which commands are injected into botnets, and the "bullet-proof" hosting services supporting organized crime. We plan to leverage the information gained from these analyses in order to devise novel techniques to

undermine the underground economy by influencing the trust-building processes, creating certain forms of inflation, and by leveraging the non-automatable, human-intensive steps of the criminal process.

3.3 Large-Scale Systems

N. Asokan: On-board credentials

Username/password is by far the dominant mechanism of user authentication on the Internet. It is cheap, easy to deploy, and platform-agnostic. It is currently the only general-purpose user authentication mechanism that can scale to a large number of users. At the same time, it is also annoying and leaves the users more vulnerable by being susceptible to various kinds of attacks.

Hardware tokens are used in specific application domains. GSM/UMTS is the most widely deployed system using hardware tokens for subscriber authentication. Some enterprises and banks use one-time password tokens for employee and customer authentication. Hardware tokens are usually more secure and more intuitive than purely software mechanisms. But they tend to be more expensive, and harder to deploy. Their biggest drawback in practice is their inflexibility. Technically, the same hardware token can be used for multiple services from different service providers. In practice, this rarely happens because the token issuer tends to control which services can use their tokens. As a result, users end up carrying different hardware tokens for different services.

A new development has been taking place in the last few years, which can help provide a solution that occupies a middle-ground between the extremes of software-only authentication mechanisms and hardware tokens. Several types of general-purpose secure hardware are starting to be deployed: e.g., Trusted Platform Modules (TPM) and Mobile Trusted Modules specified by the Trusted Computing Group and other platforms like M-Shield and ARM TrustZone. All these platforms enable, to different degrees, a strongly isolated secure environment, consisting of secure storage, and supporting secure execution where processing and memory are isolated from the rest of the system. TPMs are already available on many high-end personal computers. Several Nokia phone models are based on hardware security features of the M-Shield platform.

Nokia research has designed a platform for ”On-board Credentials” (ObCs) which can be realized on such general-purpose secure hardware. ObCs combine the flexibility of virtual credentials with the higher levels of protection due to the use of secure hardware. They have prototyped the ObC architecture on various secure environments including mobile phones based on M-Shield. The primary component is the ObC interpreter, which runs in the secure environment. Credential logic can be implemented in the form of “credential programs,” which are scripts that can execute on the interpreter. The interpreter has exclusive access to a

device-specific master key called the ObC platform key (OPK). The interpreter provides sealing and unsealing functions using which credential programs can protect credentials for persistent storage. The key used by the sealing/unsealing function depends on OPK and a digest of the code of the credential program that invokes the function, thereby inherently isolating persistent data of one credential program from another.

A strong point of the architecture is that anyone can be allowed to write and provision credential programs for the ObC platform because the platform isolates credential programs from one another. By using device-specific keypairs, the system also enables anyone to provision secret credential data securely to any given set of credential programs. Such an open provisioning architecture can lower the barrier for service providers to deploy usable and secure user authentication and thus bring to fruition the vision of a mobile device as a personal trusted device that can be used by its owner to securely authenticate to a variety of services, both digital and physical.

D. Mutz: Scalable Development of Secure Software

The modern business environment demands software engineering teams move quickly to meet new and ever-changing product requirements. In the case of web-based applications, this often means that a large volume of newly written software stands between critical user data and the Internet at large. In order for security requirements to scale in proportion to the functional requirements of software, security mechanisms and idioms must be accessible to software engineers with no specialized training in security. In this way, the task of preserving security guarantees in the application is distributed across the development team.

Virgin Charter is an online marketplace for buyers and sellers of charter jet travel. Buyers express demand on the site in a way that is analogous to search operations on web-based travel agencies such as Expedia and Travelocity. Sellers issue quotes against buyer demand, and buyers are then able to select the most competitive of the quotes they receive and make a purchase. The jets chartered using the web site range from turboprops and light business jets to airliners.

Security is a significant requirement for Virgin Charter. In addition to the high expectations consumers have of the Virgin brand, the clientele of the company intersects heavily with business executives, celebrities, and other high net worth individuals. Therefore, preserving the confidentiality of the clients financial information and travel itineraries is of particular importance for Virgin. Storing financial data of customers additionally implies conformance with legislative (e.g., California AB 1950 and SB 1386) and payment card industry (PCI) security requirements.

Like many organizations with critical security requirements, Virgin has met the challenge with a strategy of defense in depth. The rapid pace of application development, however, has presented a particularly acute, ongoing challenge for

security. The company has met this challenge with a variety of software artifacts that make the path toward secure programming concise and idiomatic for all software developers in the organization. In this way, the organization has scaled the security of its system with the rapid pace of development. Three artifact examples are summarized below:

1. **Well-factored input validation.** Extensions to the input validation library allow developers to specify restricted character sets and length restrictions on a per-field basis in a single line of code. These character sets are defined in a single location and used across the system. For example, both web forms and SOAP requests are validated using the same input validation implementation.

2. **Transactionally-backed state machines.** Leveraging the transaction guarantees of the database, the organization has defined a state-machine model that can be customized to represent virtually all business flows in the system. This abstraction allows the common practice of modeling business rules to be considered separately from the specialized problem of enforcing those rules correctly in the face of concurrency.

3. **Aspect-oriented access control.** The Virgin system employs the model-view-controller architecture, in which user functions are represented as methods in controller classes. This approach allows access control checks to be factored into method decorators and are applied with a single line annotation to class methods.

In his talk, Darren Mutz has argued that the rapid pace of application development in the modern business environment calls for distributing the task of preserving application-level security guarantees across the development team. This is enabled via purpose-built software artifacts, allows security requirements to keep pace with functional requirements, and reduces the degree to which specialized security teams become a bottleneck for the rapid evolution of software.

R. Rieke:
Upcoming information security threats - an end-user perspective

One of the main points to take away from this presentation is that in both old and new threats, the weakest link appears to be the end-user. Prevention and mitigation of the misuse of infected hosts would protect not only the end-user, but in fact the entire Internet as a whole.

Rieke starts by using Viviane Reding's classification to identify the various stakeholders involved in securing computers and networks: the EU member states and their public administration, the private sector, the citizens, the academic and research community. They all have to act.

Member states should secure their own networks and give the example of good practice to other players. While it is not immediately clear what is part of the public administration, presumably both the police force and justice departments should play a role in this. The private sector should start considering security as an asset that provides a competitive edge, rather than an overhead. Citizens should be educated to understand that their home systems are critical for the overall security chain. The academic and research community make a significant contribution to the foundation of security.

Rieke focuses explicitly on the end-user. He first discusses new threats to ICT infrastructures. Specifically, he mentions attacks that exploit mobile networking and leverage the increasing availability of mobile networking technology, threats that target novel types of services (MMS, VoIP, TV over IP, e-Health service), new types of physical transportation (malware spreading by way of mobile devices as carriers that leverage syncing mechanisms and USB connections), and blended threats (e.g., new bot architectures with convenient plug-in interfaces allow attackers to easily extend a bot's features).

He continues by discussing some scenarios in a bit more detail. One threat that he sees on the horizon is that of Vehicular Ad hoc NETworks (VANETs), which opens the door to vehicle intrusion threats, which in turn create threats to the overall car safety functions. What is needed to analyze the VANET concepts, according to Rieke, are models: high-level traffic simulation models, models of WAVE security services for applications and managed messages, and plausibility and belief-change models. The security goals in this domain are both privacy (e.g., to ensure non-traceability) and integrity (secure operation in untrusted environment). This is partly addressed in EU the FP7 EVITA.

He also highlights an example in e-Health, which is representative of novel, complex e-Service architectures. Attackers may appear in various places (e.g., between services, as a man in the middle between a broker and an e-Health services, etc.), but according to this talk, confidentiality is the weakest link. In other words, the system at the end-user (doctor/pharmacist) is the most likely point of attack.

Possible results of attacks on such large systems that attackers may make:

1. to trace vehicles (and possibly trigger accidents);
2. to eavesdrop encrypted data and store the data for many years until decryption is possible;
3. to control the flow of *things*, not just information (for instance, using RFID);
4. to make attacks that may cross infrastructures therefore causing domino effects (SCADA).

The technical challenges are thefore as follows:

1. to understand the general principles of systemic intervention, disruption and infection in highly interconnected complex ICT systems and to predict the

effects of threat prevention, detection, and mitigation strategies in current and future attack scenarios.

2. to develop novel concepts, tools and mechanisms that prevent and mitigate malware epidemics enabling efficient and adequate countermeasures and offering assistance to the affected end-users

3. to improve usability of security while not sacrificing privacy; end-users' legal responsibility for unintentional attacks requires that the current situation and the impact of possible courses of actions is fully understood

More specifically, in order to understand the system's behavior and predict effects for very large systems, we need novel modeling, simulation and visualization techniques. Abstraction is key.

For security analysis, and enforcement, we need: (a) Identification (is this possibly an attack?, (b) Containment (avoid its spreading), (c) Eradication (kill and erase the source and all its entities), and (d) Distilling the Lessons learned (what can I learn for future attack identifications and share with my friends).

What is needed is collaborative, distributed defense.Complementing existing security solutions and taking into account parts of the network currently not integrated; in particular end-users and their systems is necessary. Making use of distributed knowledge across network infrastructures to enable co- operative reasoning and response is crucial.

To conclude, the challenges are: to understand the general principles of threats to old and new highly interconnected complex ICT systems and to predict the effects of mitigation strategies, to develop novel technical and organizational concepts, tools and mechanisms to prevent and mitigate malware epidemics, and to improve usability of security while not sacrificing privacy. And we should keep reminding ourselves that the weakest link is the end-user.

A. Sabelfeld: Emerging Threats: A Perspective from Mobius

As computing devices are becoming increasingly autonomous, interconnected, and extensible, they are becoming increasingly vulnerable to large-scale attacks.

The main theme of Mobius, an EU integrated project of 16 partners, is the security of mobile devices. Mobius' approach to securing potentially untrusted code on these devices is via the paradigm of proof-carrying code (PCC). The PCC architecture accommodates security certificates as formal proofs of security. Mobius covers a wide range of advanced security policies such as information-flow and resource control. At the heart of Mobius technology we find type systems and program logic, reducing security-certificate validation to type and proof checking.

Of particular focus in Mobius investigations is the security of Java-enabled devices. Especially important in this context is a specific platform, the Mobile

Information Device Profile (MIDP) of the Connected Limited Device Configuration (CLDC) of the Java 2 Micro Edition (J2ME). At least, one third of the mobile phones in the world support MIDP.

The talk at the the FORWARD meeting provided a general overview of Mobius activities, including those related to the threat model of MIDP.

S. Tasiran: Program Analysis and Verification for Identifying Concurrency-Related Vulnerabilities

The main observation is that concurrency attacks are a tremendous problem that is likely to grow worse, rather than better. First, concurrency attacks have serious consequences and a high success rate. Second, with the trends towards multicore and more parallelism, concurrency is becoming part of most software parcel. In other words, concurrency must be a primary concern.

The other part of the message is that to detect vulnerabilities and errors, we need coordinated research in program analysis, verification and monitoring tools. To remove or prevent such vulnerabilities we need hardware, OS and runtime support for safe concurrency.

In practice, many of the detectable errors in modern operating systems are due to concurrency errors. For instance, for the Windows 2000 hot fixes, 26% of defects analyzed (14 out of 52) were races or deadlocks. In the Windows 2003 late cycle defects, synchronization ended second in the ranking of errors, after buffer overflows.

One of the challenges here is that concurrency errors are hard to detect. For instance, the August 2003 power blackout in the US (costs: $6-10 billion) was caused by a race in alarm and event processing code; code that had been running in excess of three million operational hours.

The common concurrency vulnerability pattern is the race condition which leads to a windows from time of check to time of use (TOCTOU). A usual scenario is that a program checks for authorization (permission, value or whatever) and if a condition holds, the resource can be used. The check and use should be atomic. In reality, however, an attacker in a concurrent process changes the value of the critical variable between check and use.

A race condition is symptomatic of a bug, but removing the race condition does not always remove the bug. Other concurrency errors may exist, e.g., atomicity violations, and refinement violations.

Several methods exist to fix, and guard against concurrency errors:

- Local fixes: Lock, make certain code blocks atomic
- Re-architect the system: Message passing between components instead of shared memory? (Example: Singularity operating system)

- Safe concurrency: Transactional memory?

In addition, there are several approaches to detect and recover from such errors at runtime:

- Concurrency-error aware, instrumented run-time environments (Example: Goldilocks, DataRaceException)
- Hardware support for instrumentation, tracking
- Use multi-cores for monitoring

The important message is that concurrency is and should be a primary concern for the security of systems.

3.4 Malware

J. Canto: HISPASEC: Malware Trends

Malicious code (or malware) is defined as software that fulfills the deliberately harmful intent of an attacker. Malware analysis is the process of determining the behavior and purpose of a given malware sample (such as a virus, worm, or Trojan horse). This process is a necessary step to be able to develop effective detection techniques and removal tools. Currently, malware analysis is mostly a manual process that is tedious and time-intensive. A number of analysis tools have been proposed that automatically extract the behavior of an unknown program by executing it or analyzing it in a restricted environment. However, the most important line of defense against malicious code are still virus scanners. These scanners typically rely on a database of signatures that characterize known malware instances. Whenever an unknown malware sample is found in the wild, it is usually necessary to update the signature database accordingly, so that this novel malware piece can be detected by the scan engine. Hispasec Spain offers a service that allows users to submit samples that are then analyzed using a large number of commercial virus scanners.

In his talk, Julio Canto from Hispasec Spain presented some statistics about the current malware-related attacks that they are seeing. Julio reported that malware-related attacks are on the rise, and they are seeing more and more tool-related attacks and botnets.

Hispasec has conducted studies and has seen that a phishing site was online for about 3 days on average. In the most extreme case, a site was up for 21 days. One problem with phishing seems to be the fact that it takes a long time for authorities to shut down sites. In one extreme case that involved a bank, it took 4 days for the ISP to bring the phishing site down.

Also, attackers have been using a combination of compromised computers (e.g., botnets) and servers to host their phishing web sites. Often, the DNS servers that the miscreants use are located outside of the country where the attack takes place. Hence, it is impossible or it takes a long time to shut down these servers.

Obviously, time is crucial when dealing with such online fraud attempts. Unfortunately, there is clear evidence that the attackers are aware of how the legal systems in certain countries operate and how IT systems are generally defended. For example, many attacks are launched during weekends as the attackers know well that many security professionals are not in office. Hence, by timing their attacks properly, the attackers ensure that there is a long window of vulnerability for victims.

Julio also reported that the attacks they are seeing are becoming more complicated every day. He argued that he expects the sophistication to continue to increase as Internet attacks are still easy to launch and difficult to trace back.

E. Contreras: BruteScan: Malware and Security Measures Sampler for End-user Computers

Since last year, Hispasec has been actively participating in the study on Information Security and e-Trust in Spanish households, carried out by INTECO1 (National Institute of Communication Technologies). To this end, they use a tool called BruteScan. Many malware variants are discovered in the wild every day, and these samples can have a variety of purposes, ranging from stealing confidential information (credit card numbers, account passwords, etc.) to denial of service. But no exact or experimental information about the prevalence of malicious code in end-user homes is available at the moment. This raises many important questions, such as: how many of these malware specimens are really affecting end-users? What are the infection vectors of these samples? Does the use of antivirus, firewalls and other security measures really have a noticeable impact on the infection status of end-user computers? Do end-users regularly apply security patches, and what is the impact of this behavior on malicious code incidents? Our tool is an attempt to give answer to these and other questions.

Goebel et al introduces Blast-o-mat, a system deployed at RWTH Aachen University to detect infected machines based on honeypots. While this approach has the advantage of being capable to passively listen to large networks seeking for malware activity, it is very limited in the sense that it may only detect code with scanning functions and only in the case of hitting the honeypot-based system. In order to circumvent the problem of detecting infected machines, Hispasec has adopted an active approach that involves sampling end-user PCs with their consent.

BruteScan samples PCs on a monthly basis. The sampling involves seeking for malware and recovering information related to security configuration and habits

(patching state of the system, antivirus presence, firewall presence, registry configuration regarding ActiveX controls, auto-loading of removable devices, etc.). All files on the system are compared with VirusTotal's database, and if more than five antivirus flag the sample as a threat, the system is considered to be hosting some sort of malware. A taxonomical classification of the specimens found in the end systems is also performed based on the signatures given by five of the most reliable antivirus engines in the light of our experience. In this way, the deployment of this tool on a large amount of end user PCs can reveal certain infection trends such as a greater presence of Trojans and an ever decreasing rate of virus infections.

The efficiency of the tool is based on the brute-force power of VirusTotal. VirusTotal is one of the biggest malware stores of the world, and it has the advantage that for each of the samples, there exists a characterization by more than 30 Antivirus Engines. It is thanks to the power of VirusTotal's database that a PC can be, with a noticeably degree of certainty, flagged as hosting malicious code.

Note that BruteScan is by no means an antivirus itself, it is just a monthly sampler capable of discriminating possible malicious code based on a database of information built with the results provided by the different antivirus engines present in VirusTotal.

The tool has been collecting data for over a year now. It has revealed daunting results: 80% of the sampled computers hosted some sort of malware, 50% specifically hosted a Trojan, 40% Adware, 24% malicious tools, etc. Surprisingly enough, 87% of the households had an active antivirus. 74% of the computers without antivirus held malicious code vs. 72% in the case of those that did have an active antivirus. Many other correlations and trends have been observed.

Even though BruteScan has important limitations (polymorphic code not indexed in VirusTotal, malware not detected by more than five engines, etc.), it depicts a situation that in the best case is as bad as as shown, in the worst case it can be much worse.

Hispasec believes it is time to go broad with the study and carry it out at an European level. Indeed, it might reveal interesting cross-country patterns that may illustrate what certain countries are doing wrong/right in comparison to others, what are the emerging threats and what is the penetration degree of these threats.

Thorsten Holz: Challenges in Honeypot-based Research

A *honeypot* is an information system resource whose value lies in unauthorized or illicit use of that resource. These tools are electronic decoys that pretend to be normal system, but are actually waiting to be attacked and compromised for the purpose of tracking attackers and learning more about their proceedings. *Honeynets* are networks of honeypots and have proven to be an effective tool in learning more about Internet crime like worms, botnets, credit-card fraud, and other areas of network-based attacks.

As attacks in communication networks evolve, the design of honeypots also needs to evolve. For example, we observe more and more attacks against client applications like web browser or office applications. Traditionally, honeypots are designed to collect information about attacks against server systems. We thus need to develop honeypot solutions that can be used to learn more about client-side attacks. Honeypot systems like HoneyMonkey by Microsoft Research is a first step in this direction.

In the near future, IPv6 will be introduced on a larger scale to overcome the shortage of IPv4 addresses. This change in the networking area will presumably result in changed attacker behavior. For example, nowadays bots and worms commonly search for other vulnerable systems with the help of different network scanning techniques. However, in an IPv6 environment, scanning will become inefficient due to the large address space. We need to develop new honeypot techniques that can capture information about network-based attacks in an IPv6 environment.

The increased mobility of users is another challenge in the future. For example, a mobile phone is a fully-featured computer that is constantly connected to the Internet. This device has an intrinsic mobility and will connect to many networks during a typical day. Learning more about attacks against such systems is an important area and classical honeypot techniques need to be redesigned. A similar area is virtualization: since virtual machines become more common, we need new honeypot systems to learn more about attacks against these systems. High-speed networks are a third field in which we need new honeypot designs and implementations.

Furthermore, current honeypot systems are often not able to detect targeted attacks. Since honeypots are network decoys, an advanced attacker can fingerprint them and avoid attacking them. The concept of stealth, shadow honeypots should be extended to enable detection of targeted attacks using honeypots.

A. Keromytis: Race to the bottom: Malicious Hardware

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.

This new way of making hardware has brought great benefits in terms of design reuse, rapid development and prototyping, and lower costs, but 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, integrity and availability. 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 to launch a variety of powerful attacks against the system.

Because hardware components (like HEEs) are architecturally positioned at the lowest layer of a computational device, it is theoretically impossible to detect at a higher layer attack launched or assisted by them. Also current processors and motherboards lack the functionality to detect such misbehavior. The state of practice is to ensure that hardware comes from and is maintained by trusted parties: a virtual impossibility, given current design and manufacturing realities. Physical inspection and verification of the hardware may also be applied, but it is destructive, costly, and time-consuming. So it is only applicable in rare cases, when volumes are relatively low and the risk is high.

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.

Addressing the problem requires a concerted, long-term effort in physical design and manufacturing methods, secure and trusted fabrication practices and operations, post-fabrication testing and verification techniques, and runtime HEE detection and mitigation. The problem domain represents both challenges and opportunities. 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.

E. Markatos:
The future of malware: From fun and profit to physical harm

The number and diversity of malware samples is growing at a much faster rate than our existing defenses are able to cope with. Even though the technical aspects of malware have been extensively studied and analyzed with hundreds of defense systems being introduced, what has not been systematically investigated is (i) the impact of malware, (ii) how it evolves over the years, and (iii) what its potential risks are for the future.

Early malware authors were mostly motivated by fun and by the quest for peer recognition. However, the appearance of the first computer worm revealed that

malware can also have a strong financial and social impact, as recovering from a worm outbreak costs both in terms of money and human effort. Up till now we have been measuring the impact of malware primarily in terms of their financial fallout. Botnets, denial-of-service attacks, and XSS attacks at popular sites demonstrate the effectiveness of malware to wreck financial havoc.

It is very likely that in the future malware will have a much more profound impact on the well-being of humans themselves. For example, if organizations of vital importance, such as hospitals and fire departments, power grids and emergency services, become victims of attacks, they may stop providing their services to the public. For instance, if botnet nodes are instructed to repeatedly call a hospital through a VoIP system, they may easily jam all communication channels to the hospital. In turn, the hospital personnel will end up receiving thousands of calls, unable to serve any real requests for help. The consequences of such an attack put lives in danger, and may even be fatal. Attackers may also use more subtle methods to deliver fatal blows. For example, consider that an attacker acquires the capability to access and modify medical records stored in a hospital or a doctor's tablet or PDA. Modifying such records can lead to wrong diagnoses and, therefore, incorrect medical treatment.

The integration between digital and real world offers attackers a new operation arena and the consequences of this integration to human lives have not been adequately studied yet. As more and more facilities and services become reachable through the Internet, they are increasingly exposed to the associated dangers, which, unfortunately, may not be visible, until the outbreak of the first major incidents. We believe that it is of paramount importance to start considering such scenarios and begin working towards finding appropriate solutions.

F. Veysset: Botnet, malware and traffic analysis

For the last ten years, there have been some tremendous changes in Information and Communication Technologies (ICT). Always-on devices, always-on Internet access (xDSL, cable, WIFI/WiMax, 3G...) have huge impacts on the Internet, and more particularly on the nature of new threats. 2007, and its infamous "Storm Worm," have highlighted new kind of malware and botnets. The Storm worm event could have been far worst, as the design could have been better, but this worm is probably one of the first large-scale P2P based C&C botnet. The impact of the Storm worm in 2007 has been quite strong, at least from a telco / ISP point of view:

- Numerous customers have been infected
- Good strategy against anti-virus. Very fast signature changing, code obfuscation, C++ and multi-threading, advanced anti-debugging mechanisms...

- High raise of SPAM activities
- Quite some overload on the infrastructure, and particularly on DNS servers (lots of MX request)

Monitoring DNS server (or other parts of the network) can provide us with valuable information to analyze the threats. For example, MX request evolution is a very good indicator of the infection rate, as regular customers tend to have a low MX rate. Unfortunately, legal constraints tend to make monitoring hard. In many countries, including France, monitoring this kind of traffic is unlawful as this will be considered as profiling / privacy violating. Monitoring will be allowed only for infrastructure protection and reaction against acknowledged risks.

We can fear that in the near future (it might have already beginning), malware will tend to be more and more stealthy and effective. Anti-virus technologies will probably betotally ineffective against those threats soon. Next generation malware will be much more "professional," nearly undetectable, and be able to perform many tasks with one target: be as much lucrative as possible for their authors. This opens the door to many new annoyances, including SPAM over any new form of media (for example, SPIT and SPIM become easy if you abuse end-user PCs, but IMS attacks from authorized user desktop is also an option). Fighting against this threat is not an easy task, and we can expect difficult problems to solve, both from a technical point of view, but also from a legal point of view.

3.5 Network and Monitoring

M. Behringer: Emerging Threats to the Internet Infrastructure

End system security is important - however, the majority of today's research and industry initiatives focuses on the end system; the infrastructure of the Internet itself needs more attention and research. Emerging threats against the Internet infrastructure include:

- 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). There are academic proposals (so-BGP, S-BGP) to tackle the problem, but both are considered to expensive by operators. There is currently no deployable, easy solution for routing security. This could lead to major Internet outages, and even a "split" of the Internet.

- 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-ware" 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 raising 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.

E. Boschi: Towards privacy preserving network monitoring

Passive network monitoring is required for the operation and maintenance of communication networks as well as to detect anomalies and attacks. Raw packet-level traffic traces are collected and fed to monitoring applications for analysis. Gathering and uncontrolled processing of traffic information poses significant risks for the legitimate privacy rights of the network users. Not only payload information may often contain sensible used data, but also collected header information can be exploited to indirectly identify and profile natural persons.

The PRISM project aims to show that it is technically possible to devise a privacy-preserving network monitoring system where carefully designed data protection and access control mechanisms can coexist with suitably adapted monitoring applications. PRISM is exploring two complementary technical approaches to achieve this goal:

- data protection mechanisms devised to allow monitoring applications to operate over protected data;
- a semantic access control middle-ware devised to restrict and regulate access to the data according to the specific purpose for which the data information is collected.

These two technical approaches are combined into a comprehensive monitoring infrastructure based on a two-tier system. The first front-end tier of data protection mechanisms is directly enforced at the traffic probes. Data may be protected on-the-fly, exported, and stored using the standard for IP flow information export, the IPFIX protocol, with the goal of providing interoperability and standard interfaces to the different architecture components and to analysis tools; Collected (and possibly already protected) data are delivered to a second back-end tier, which is implemented as a privacy-enforcing role/purpose-based access control middle-ware and provides an additional level of protection to enable data access from and/or data sharing with external parties.

PRISM poses a great attention not only in carefully following the requirements set forth by applicable data protection and security regulation, but also in providing their actual enforcement through technical solutions. First, in full adherence with recent legal directives, the envisioned architecture functionally decouples the entity in charge of enforcing data protection from the one in charge of running the actual monitoring applications and analyzing the relevant results. Second, the system is being designed with the intent of enabling the selective and controlled

reversion of part of the data protection mechanisms set forth, for both system operation reasons (such as reaction to attacks and anomalies) as well as for regulatory-imposed conditions (such as that mandated by data retention and legal interception laws). Finally, PRISM is devised to explicitly include regulatory requirements in the system architecture in the form of technically-enforceable statements, such as semantic (ontology) statements and consequently derived policies.

J. Ioannidis: Internet Routing

The integrity of the Internet routing infrastructure is of paramount importance. Unfortunately, there is an increasing number of outages, mostly caused by misconfigurations, accidents or even intentional attacks. For the Internet to scale, it follows a hierarchical structure. At the first layer of this structure, the Internet is a collection of over 27,000 *Autonomous Systems (ASes)* interconnected through *border routers (BRs)*. Because there is no central database of the existing ASes and how they connect, BRs run the *Border Gateway Protocol (BGP)* to determine existing network paths and chose the "best" among them for the forwarded packets.

BGP was originally designed for a much simpler Internet topology. In the last fifteen years, BGP has been repeatedly extended to meet the ever-increasing requirements of the Internet Service Providers for policy routing. This resulted in a very complex protocol that keeps getting extended in order to accommodate newer operational requirements. Security is always at odds with complexity, and each additional feature creates new opportunities for problems (accidental or intentional).

Many of the security problems of BGP stem from the fact that it relies on trust between BRs. Each BR makes a routing announcement for each IP prefix of their AS. However, upon receiving an announcement for a prefix, a BR has no way of knowing whether the originating network had the right to make it *(Origin Authentication Problem)* or if it is true *(Path Validation Problem)*. No generic methods for detecting and filtering such errant announcements exist today.

A somewhat less obvious problem is that each BR announces to its upstream neighbors only the "best" path to a specific destination. Moreover, the announced subset of "best" routes is "censored" to conform to a route export policy. This enhances the scalability of the routing process but also prevents global path optimizations and may lead to aberrant behavior. Even worse, a BR has no way of knowing whether previous BRs in the path have abided by their declared policies or by the intended policy of the originator. So, when something goes wrong network administrators frequently have to guess the reason that triggered the BGP announcements they are actually seeing. We call this the *Information Hiding Problem*.

Additionally, BGP is known to suffer from a *Policy Expressiveness Problem*. Policy decisions come into play when a path must be picked among a number of available paths based on constraints that have to do with agreements between ISPs. Policies in BGP are expressed as a set of BGP path attributes. This severely

limits the policies that ISPs can currently use and frequently leads them to use very contorted ways of casting the policies they want.

A final, fundamentally hard to defend against problem is that of *Anomaly Containment*. BGP has no mechanism for preventing incorrect information to propagate through the network. If everybody in the Internet were running a routing security protocol, most anomalies caused by badly-configured or compromised routers could be stopped within one hop. However, this is unlikely to happen, so the part of the Internet that is actually running more advanced security mechanisms has to protect itself from the rest.

M. Koyabe: Defence Against Next Generation ICT Infrastructure Threats

As the future use of Information Communications Technology (ICT) infrastructure increases and evolves, incidents of technology-enabled crimes are likely to continue. Some of these technology-enabled threats include infrastructure risks, the use of wireless and mobile technologies, sophisticated malware, Web 2.0 vulnerabilities, identity theft, computer- facilitated fraud, intellectual property infringement, outsourcing and industrial espionage. Mitigation of these threats, on a large-scale especially in the electronic layer, will increasingly become a challenge. Information carrying capacity is now exceeding a terabit per second and doubling every twenty months, whereas information processing capacity is already in the region of 10 gigabit per second and doubling every thirty-six months.

Implementing security algorithms to mitigate these threats for large volumes of information or traffic using electronic processing will become a challenge. Scaling of high-end middle-boxes (including IPS, IDS and Firewalls) in large-scale ICT infrastructures is becoming untenable as data rates and processing requirements increase. Efficient power handling and low environmental impact of larger and faster processors is becoming a high priority for a number of network carriers and network service providers. The ability for next generation security platforms to consolidate, virtualize and simplify security services delivery, while preserving the choice of best-of-breed security applications at very high-speeds, will become a key component in mitigating future ICT infrastructure threats.

The development of simple level wire-speed optical processing to act as primary information/traffic filter in front of these middle-boxes (e.g. IDS, IPS and firewalls), might be ideal in addressing future limitations of electronic processing of large volumes of traffic. Security algorithms deployed in optical hardware can enable scalable mitigation against next generation ICT infrastructure security threats.

A number of research groups (such as EU IST WISDOM - WIrespeed Security Domains using Optical Monitoring- project) are currently investigating best approaches in designing scalable and effective photonic-firewalls. WISDOM aims to design photonic sub-modules (algorithms) that will expand the functionality avail-

able today at wire speed, based on high- speed (greater than 40 Gb/s) optical logic gates and processing circuits. These new algorithms will also provide security analysis based on the knowledge of both the limited wires-peed optical processing (currently available), and additional functionality which will be developed in the project.

G Noubir:
Cross-Layer Attacks in Wireless Networks and Countermeasures

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 networks. Such attacks can consume four orders of magnitude less energy then previously know attacks. We have 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. We have also 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.

A. Nyre:
SINTEF: Privacy Controlling Personal Information

Privacy is popularly defined as the right to be let alone, meaning that users should always be given the choice not to provide any personal information. However,

many services require personal information (such as name and address for billing purposes) or will improve usability if additional information is provided. Consequently, there is often a trade-off between privacy and usability needs. Acceptable privacy requires that the user herself retains control of personal information, in particular allowing information to be deleted or revoked.

The problem is that the lack of privacy on the Internet poses a serious threat to users, organizations and governments. Information aggregation, online personal social network services, web site extensive logging and the vast amount of information available, makes it impossible for originators to retain control of personal information usage and distribution. On the Internet there is no guarantee that provided or collected information is not distributed to third parties; that security measures for storage are adequate or that information will be deleted on request. In general, users are left with the option of manually consulting the privacy policy of the web site, if available, and then rely on experience, own judgment and recommendations when assessing to what degree the website is likely to comply with the policy. Clearly, there are few informed decisions being made about ones privacy.

There are clear indications that the future of the web will involve semantics and machines in one way or the other. The semantic web was proposed to help users manage the overwhelming amount of information on the web more efficiently. By creating machine understandable information, agents are able to perform automated search and retrieval of relevant information, to discover and interact with services to perform tasks and adapt to user preferences and experiences. Unfortunately, these scenarios implicate serious privacy concerns. With machine automated search and retrieval, information aggregation is far easier than on the current web. The use of context information for service discovery (e.g., location awareness) would enable through tracking and logging of user activity. The use of automated service interaction forces the user not only to trust the agent performing the task, but also to trust its assessments regarding remote services and how they handle personal information. Providing user privacy is of paramount importance for successful migration to the semantic web.

SINTEF is currently involved in a FP7 EU proposal that will develop a privacy management infrastructure for use with semantic technologies. The envisioned infrastructure will be user- centric and provide mechanisms for privacy and trust management as well as access control.

3.6 Cooperation and Coordination Efforts

D. Bruschi:
Computer Security in EU: What is it lacking?

The take-away message of Danilo Bruschi's presentation is that Europe is sadly lacking in expertise in system security. It needs to act now, if it wants to be a player

in the field, rather than remain dependent on expertise and technology developed elsewhere.

Since the Internet worm in 1988, the trend in computer attacks has been that it has been constantly growing regardless of the metric you wish to consider (e.g., number of attacks, complexity, hosts involved, costs, etc). These days the phenomenon is apparently assuming its definitive characterization: a criminal activity perpetrated mostly against millions of unaware citizens. Thus, in the near future, typical attacks in the network will be a natural evolution of the current attacks, improved by more sophisticated forms of social engineering as well as very advanced technical means. We will see botnets which will survive the shutdown of most of their bots, stealthy spyware, undetectable viruses, as well as attacks on any "intelligent" device. Combating these new forms of attacks will be a very hard task and in all the cases it will require a fundamental ingredient: a very strong body of knowledge.

This body of knowledge, usually referred to as *system security*, however, is built on a deep understanding of system internals, a kind of knowledge that historically has been developed outside of Europe and that Europe is hesitant, if not reluctant, to acquire. As a consequence, most of of the information that is actually used for fighting computer crime and for building new and stronger security systems is produced outside Europe. Given this, Europe is currently strongly dependent on external information sources in the computer security field. The lack of a cultural perspective in this area has also negative consequences on the ability, and possibility, of our continent of being active in the production of proactive tools and also on the quality of education provided in the field, as high quality advanced education cannot exist without the support of research.

If Europe wishes to become a prominent or at least an independent actor in the computer security field (which is one of the most strategic fields for the development of the information society), such a situation has to evolve and improve. A strategic choice has to be made for promoting this area; specific initiatives and support have to be provided to the few groups, both industrial and academic, that are truly involved in this discipline, in order to enable them to compete at international level with corresponding realities.

J. Clarke and N. Suri: International Co-operation in Trustworthy, Secure and Dependable ICT infrastructures

In November 2006 and April 2007, two workshops were held, mainly with EU and US Researchers engaged within ICT Trust, Security and Dependability (TSD), but also with participation from Australian, Japanese and Canadian colleagues. The workshops were highly successful in their mission of identifying and scoping research areas that require and will benefit from international collaboration between EU researchers and those within other industrialised nations.

Following the success of these events, a Coordination Action (CA) proposal "International Co-operation in Trustworthy, Secure and Dependable ICT infrastructures (INCO-TRUST1)" was submitted to the first call of EU ICT FP7 on secure, dependable and trusted ICT global infrastructures and partnerships.

During these two workshops, the organising committee requested position papers from the participants and a list of questions to the participants. Following this process and during the workshops, a number of the participants, both from the EU side and the other nations, identified emerging global risks as one of the areas where global collaboration would be mutually beneficial. This included early identification and protection mechanisms for emerging global risks as the digital systems evolve, where the threats and types of attacks also change.

In order to accomplish this, it was agreed by the participants that this could not be done in isolation but needed global efforts and needed to be done in a twin tracked approach. First, it is advisable to permanently survey and identify the new possible attacks, the potential vulnerabilities due to complexity or just-in time services. Second, it is also advisable to look for new emerging risks, while being conscious of the incompleteness and the limitations of all these analyses.

Examples of these emerging risks at the global level discussed amongst the participants are dealing with the ever increasing scourge of SPAM, denial of service, excessive disclosure of private information, bullying, identity theft and squatting and predators masquerading. Other areas for global partnerships in research and development identified in the second workshop included aspects related to attack distribution "information concerning possible attacks, who or what is responsible for the attack, the extent of the attack"[1], information gathering; tracking and tracing for forensics to enable prosecution of cyber criminals; and balancing technological challenges with legal aspects and privacy of individuals.

With these in mind, the synergy between the FORWARD CA and INCO-TRUST CA is then quite fruitful because the INCO-TRUST CA can provide the contacts of the knowledge base already uncovered during these previous works in order to pair the EU researchers with the "right people" in the participating countries.

B. Daskala: Towards assessing and managing emerging and future risks

We identify emerging and future risks (EFR), considering present, emerging and future applications and technologies. Current risks are relevant from the present up to one year, and are basically posed by existing or even some emerging applications and/or technologies. These risks are the subject of all the existing RM/RA methodologies. Emerging risks are relevant from one year to five years into the

[1]Taken from Infosec Research Council Hard Problems List - see http://www.infosec-research.org/docs_public/IRC-HPL-as-released-990921.doc

future and may be posed by emerging or new technologies and/or applications. Future risks are relevant risks created in the future (at least five years into the future) by an existing application and/or technology or by a future technology, which we may not know yet.

The accelerated pace of development of new technologies and applications in an increasingly interconnected society with its growing reliance on computers and networks in almost every aspect of human life, poses significant risks and raises many serious concerns. In this context, there is a need to appropriately identify and assess those emerging and future risks, so that they may be effectively addressed and mitigated, thus promoting a proactive approach to addressing risks (e.g., security and privacy by design). Risk management methods and tools are inter alia used to identify risks, calculate their impacts and mitigate existing and possible risk realization; however, the majority of RM/RA methods and tools are designed to tackle risks within the time frame of contemporary risks. Therefore, and in order to tackle the challenge of emerging and future risks, RM/RA experts have to use variations of existing methods as well as mixed or new approaches to identify, calculate impacts and mitigate emerging and future risks. ENISA being aware of this fact and identifying the need for an early and accurate identification of such risks.

Considering the nature of the emerging and future risks, we have identified the use of scenarios as the most appropriate means towards initially identifying the problem, the issue, that could then be analyzed. Such a scenario could for example resemble the dark scenarios identified in the SWAMI project [D. Wright, S. Gutwirth, M. Friedewald, E. Vidjiounaite, Y. Punie (eds.) (2008) Safeguards in a World of Ambient Intelligence. The International Library of Ethics, Law and Technology 1, Springer publications]. The problem described in the scenario will be derived by the use of one or more specific emerging and/or new technology and/or application. Following the scenario analysis, a risk assessment or management methodology can be used in order to identify and assess the risks pertaining to the particular scenario. At every step, results will be validated. At this point, it is important to highlight the necessity for an appropriate and on-going trend analysis regarding technologies and applications to be included in the approach, which will provide for a better identification and building of the scenarios.

Chapter 4

Conclusions

The consortium feels that the workshop was a large success. Not only was the planned number of participants significantly exceeded, but we also received positive feedback that demonstrated the need for an initiative such as FORWARD and a great momentum that we can build upon in the future.

Based on the concrete feedback received during the workshop, it was decided to form three working groups for the project. The decision to shrink the number of working groups was to focus the efforts of WG participants and to avoid unnecessary fragmentation. Also, several WGs showed a substantial overlap in the topics that were discussed during the workshop.
The final working group topics are the following (in parenthesis, the responsible partners - the organization that is the WG leader is shown first):

1. **Smart environments (FORTH, VU)**: This working group addresses security problems that emerge because of the growing numbers of small, networked devices (such as cell phones, PDAs, or RFID sensors) that increasingly become part of our immediate environment.

2. **Malware and fraud (IEU, TUV)**: This working group addresses threats related to the thriving underground economy, fraudulent activity on the Internet (such as phishing and spam), and malicious code.

3. **Critical systems (Chalmers, IPP)**: This working group addresses threats that are faced by ICT systems that are relied upon to carry out critical tasks (this includes topics such as critical infrastructure but also large-scale, mission-critical enterprise software).

In the weeks following the workshop, each partner is actively recruiting members for their respective working groups by mail and starting to build the working group community. It was agreed that three different levels of access to working group material should be provided:

- **Public** - Content viewable for everybody

- **Restricted** - Content can be viewed by the consortium and all members of any working group
- **Private** - Content can only be viewed by the members of one particular working group and the consortium. This level of access is beneficial when incidents or other sensitive material should be exchanged. This might also require that access to certain working groups is restricted. To get access to private working group material, a new member must be vetted. This vetting process will be defined by each working group individually.

Chapter 5

List of Participants

Carl-Johan Akerblom, ICT Turku / CONNECT, Finland
Magnus Almgren, Chalmers Univ. of Techn., Sweden
Spiros Anonatos, Institute of Computer Science, Greece
N. Asokan, Nokia Research Center, Finland
Leif Axelsson, Volvo Technology, Sweden
Michael Behringer, Cisco, France
Ralf Benzmueller, D Data Software AG, Germany
Kristina Bjelkestal, Volvo Cars, Sweden
Cedric Blancher, EADS Innovation Works, France
Elisa Boschi , Hitachi Europ, Switzerland
Kiril Boyanov, IPP-BAS, Bulgaria
Danilo Bruschi, Universit degli Studi di Milano, Italy
Julio Canto, Hispasec Sistemas, Spain
Daniel Chavarri, S21sec, Spain
Massimo Ciscato, European Commission, Belgium
James Clarke, Waterford Inst of Techn., Ireland
Luis Corrons, Panda Security, Spain
Marc Dacier, Symantec Research Labs Europe, France
Barbara Daskala, ENISA, Greece
Ruth Fochtner, Technical University Vienna, Austria
Artan Halimi, Telekom Austria TA AG, Austria
Ingvar Hellquist, SEMA, Sweden
Fredrik Holgersson , Combitech AB, Sweden
Thorsten Holz, University of Mannheim, Germany
Philip Homburg, Vrije Universiteit, The Netherlands
Ming-Yuh Huang, The Boeing Company, USA
Luchesar Iliev, IPP-BAS, Bulgaria
Sotiris Ioannidis, FORTH, Greece
John Ioannidis, Packet General Networks, USA
Erland Jonsson, Chalmers Univ. of Techn., Sweden

Frank Kargl, Ulm University / SeVeCom, Germany
Angelos Keromytis, Columbia University, USA
Pradeep Khosla, Carnegie Mellon University, USA
Engin Kirda, Institute Eurecom, France
Martin Koyabe, British Telecom (BT), UK
Christopher Kruegel, Technical University Vienna, Austria
Hakan Kvarnstroem, TeliaSonera AB, Sweden
Evangelos Markatos, FORTH-ICS, Greece
Emiliano Martinez, Hispasec Sistemas, Spain
Darren Mutz, Virgin Charter, USA
Erik Nordin, Combitech AB, Sverige
Bosse Norrhem, Lindholmen Science Park, Sweden
Guevara Noubir, Northeastern University,, USA, FR
Asmund Nyre, SINTEF, Norway
Tomas Olovsson, Chalmers Univ. of Techn., Sweden
Gerhard Paass, Fraunhofer IAIS, Germany
Aljosa Pasic, Atos Origin, Spain
Alberto Pasquini, Deep Blue, Italy
Christian Platzer, Technical University Vienna, Austria
Roland Rieke, Fraunhofer SIT, Germany
Andrei Sabelfeld, Chalmers Univ. of Techn., Sweden
Thomas Skordas, European Commission, Belgium
Alberto Stefanini, Joint Research Center of th EC, Italy
Neeraj Suri, TU Darmstadt, Germany
Serdar Tasiran, Koc University, Turkey
Wolfgang Trexler, Bank Austria, Austria
Philipp Trinius, University of Mannheim, Germany
Hong-Linh Truong, Technical University of Vienna, Austria
Philippas Tsigas, Chalmers Univ. of Techn., Sweden
Franck Veysset, France Tlcom / Orange, France
Giovanni Vigna, University of California, Santa Barbara, USA