SEVENTH FRAMEWORK PROGRAMME

Information & Communication Technologies
Trustworthy ICT

NETWORK OF EXCELLENCE

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

System Security Research in Europe: A Research Roadmap

Abstract: During its first year of operation, the SysSec network of excellence has created a roadmap for System Security Research. This white paper presents a summary of this Roadmap along with its expected impact on the European industry, the European Citizen, and Society in general. In addition, this document describes the procedure we propose to maintain the roadmap and update its content at the end of each project year.

The *SysSec* consortium consists of:

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

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

1 Introduction

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

This document is a summary of the Roadmap defined by SysSec [2]. The role of this document, and therefore of the research roadmap, is (i) to analyze the current status of each threat, (ii) to outline the research that needs to be done to mitigate it, and (iii) to list the impact this research is expected to have on the European industry, the European citizen, and the European Society in general.

1.1 Roadmap Definition Process

The collaboration with external experts, both through the project's mailing list and the participation to the face-to-face meetings, helped us to achieve a more general and precise view of which areas of system security need to be better investigated in the near future. One of the outcomes of our brainstorming activity is a list of driving factors that are responsible for changing the IT world, and that can give us a possible direction toward which we need to focus our effort. The result of the brainstorming can be summarized by the following few, important keywords: *mobility*, *increasing lack of privacy*, *24/7 connectivity*, and *cloud computing*. The starting point for the meeting discussion was the *White Book* [1] published at the end of the FORWARD Project. The document contained a number of recommendations for future research based on the likelihood and severity of a number of identified upcoming threats. The main difference between the result of the white book and the content of this document is in the scope of the document.

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

In addition to the White Book, we refined our roadmap by taking into account the content of similar roadmaps and strategic documents recently published in Europe and in the United States (for a more comprehensive overview of such previous work please refer to the complete project Deliverable [2]).

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

2 Privacy: Give me back the Control of my Data!

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

Such a large amount of information requires to be carefully protected and regulated in order to preserve the citizens' privacy. One might think that encryption might be the solution to this problem: after all, storing data in an encrypted form prevents all attackers from accessing them. Unfortunately, this is not the case as users frequently can not use encryption to protect their data (such as in social networks). On the contrary, we believe that we should invest in the system research aspects related to the users' privacy.

2.1 Recommendations and Research Directions:

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

2.2 Expected Impact

- Increased confidence by EU citizens in a privacy-preserving use of ICT.
- Increased societal acceptance of ICT through the assured protection of basic privacy expectations.
- Increased support towards the protection of the right of privacy for ordinary citizens.

3 Targeted Attacks: Looking for the Needle in a Haystack

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

actors with significant resources at their disposal [3]. The attack clearly showed how our current defense tools, policies, and infrastructures failed in front of a threat that was designed to focus against a specific target instead of blindly targeting the entire community.

Malicious hardware can also be used as a very subtle vector to perform extremely hard to detect attacks against critical infrastructures, large corporations, and government organizations. However, targeted attacks do not necessarily need to be extremely sophisticated and, even in their simplest forms, can pose a very serious threat against normal users. Targeted SPAM, for example, is extremely effective in phishing users credentials. We envision ad-hoc banking trojans could be developed in the near future to avoid detection by targeting only a restricted group of individuals.

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

3.1 Recommendations and Research Directions:

We believe it is very important for researchers to develop new techniques to collect and analyze data associated with targeted attacks. The lack of available datasets, in addition to the limitation of the traditional analysis and protection techniques, is one of the weak points in the everlasting war against malware. In this area, the problem is often to find the needle of the targeted attack in the haystack of the traditional attacks perpetuating every day on the Internet.

In addition, researchers should also focus on new defense approaches that take into account alternative factors (such as monetization), and large scale prevention and mitigation (e.g. at the Internet Service Provider's (ISP) level).

3.2 Expected Impact

- Significant improvement towards the protection of Critical Infrastructures.
- Winning significant ground against sophisticated cyber attackers.
- Design of new detection and protection techniques to mitigate cyber-espionage attacks against governments and large organizations.
- Improved collaboration with international research and operational stakeholders.

4 Security of New and Emerging Technologies: Hey You! Get out of my Cloud!

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

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

Cloud Computing - The Cloud is quickly changing the way companies run their business. Servers can be quickly launched and shut down via application programming interfaces, offering the user a greater flexibility compared to traditional server rooms.

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

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

Smart Meters - This new class of devices is a clear example of a new technology that has been rapidly deployed without the required security protection mechanisms. Studying and fixing these devices in particular, but also extending previous work done in more general sensor networks should therefore be one of the goals of system security researchers.

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

4.1 Recommendations and Research Directions:

Securing new and emerging technologies before it is too late is one of the main priorities of the system security area. In this

direction, it is important to sponsor activities and collaboration between academia and the industrial vendors to maximize the impact of the research and reduce the time required for the analysis and the experiments.

4.2 Expected Impact

- Increased adoption of, and placing trust in, emerging technologies by ordinary citizens.
- Reduced costs associated with security incidents.
- Lower barriers for mobile operators and application developers to provide accessible and affordable mobile services to their customers.

5 Mobility

We are currently witnessing the penetration of mobile devices in every facet of our society. These devices have varying characteristics but their underlying common features are: ever-increasing computational capabilities and continuous connectivity, be it Ethernet, WiFi, GSM, 3G, 4G LTE, Bluetooth, or even infrared.

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

5.1 Recommendations and Research Directions:

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

5.2 Expected Impact

- Increased adoption of mobile devices for commercial use by ordinary citizens.
- Improved European industrial competitiveness in mobile phone applications in all realms of life.

6 Usable Security: Focusing on the Weakest Link

The SysSec consortium yearly invites international experts to brainstorm about new threats. The importance of human factors was one of the main points that emerged from the last brainstorming activity between the members of the consortium and the international experts.

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

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

6.1 Recommendations and Research Directions:

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

6.2 Expected Impact

- Empowering users to play a more effective role in securing cyber space.
- Provide increased support to end users so as to make better decisions when accessing the ICT infrastructure.
- Increase the end-user adoption of security-related software and monitoring systems.

7 Roadmap Update Process

As previously explained in Section 1.1, the process we adopted to define the initial roadmap was based on a number of brainstorming activities conducted by the members of the SysSec consortium and several international experts. To bootstrap the process, we started from the list of future threats identified at the end of the Forward project, and published in the Forward *White Book*.

In the next three years, we plan to refine and extend the initial roadmap to reflect changes in the system security landscape. In particular, we can

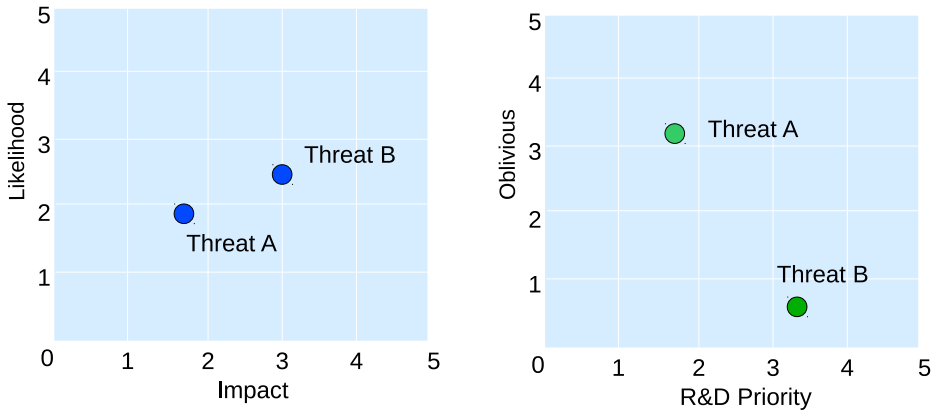

Figure 1: Example of Landscape Graphs used to estimate the potential characteristics of each threats

identify four main reasons that can lead to modification of the roadmap's direction:

- New threats and attacks are discovered that need to be addressed by the research community (e.g., the security of Smart Meter devices)
- Existing threats are mitigated by deployed products, changes in the underlying technology, or new defense mechanisms (e.g., the use of random tokens has been successfully adopted as countermeasure against cross-site request forgery attacks)
- Existing threats, even if unsolved and still potentially harmful, lose interest because of changes in the underground ecosystem or in the criminal motivations (e.g., flash worms were replaced by more lucrative botnets).
- Changes in the existing technology or in the available services suddenly increase the likelihood and severity of some previously unlikely attacks (e.g., spear phishing boosted by the spread of Social Networking sites, or mobile malware by the new widely available smarthphones)

In order to make our approach more systematic, we propose a simple yet effective procedure to update the roadmap. First of all, at the beginning of each year we collect information from several sources: scientific papers published in top venues in system security, statistics about current and future threats reported by antivirus and security companies in their public reports, and opinions of international experts discussed in blogs, talks, whitepapers, or public panels. We then use the collected information to redact an internal

draft including new candidates for the future roadmap, as well as previously identified areas that can be removed from the new version.

In the third step of our update process we will involve a number of external experts invited to participate to our working group meetings. In particular, we will ask each expert to position each threat (both from the previous roadmap and from the list of new candidates) on a number of two-dimensional graphs [5] (for example, on the impact-likelihood and R&D-obliviousness landscapes depicted in Figure 1). This experiments, inspired by the approach adopted to redact the *Global Risk 2012* document published by the World Economic Forum, will allow us to support the collected data and to put on a 5-point Likert-like scale [4] the different threats.

Finally, to conclude our approach, we will merge the collected graphs and distill their content to capture variations between the questionnaire answers and trends between different threats over time. The results will be summarized and presented in the yearly edition of the research roadmap.

8 Conclusions

In this document we presented a short roadmap for the research in the system security area. One of the primary goals of this document is to serve as a guideline for researchers in the field, and more specifically to guide the work in the three technical workpackages of the SysSec project. Our first version of the roadmap can be summarized in five topics:

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

These topics will be evaluated again during the following years of the projects, according to the update methodology we described in Section 7.

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

References

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

[2] The SysSec Consortium. Deliverable d4.1: First report on threats on the future internet and research roadmap, September 2011. http://www.syssec-project.eu/media/page-media/3/syssec-d4.1-future-threats-roadmap.pdf.

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

[4] R. Likert. A technique for the measurement of attitudes. *Archives of psychology*, 1932.

[5] Z. Minchev and V. Shalamanov. Scenario generation and assessment framework solution in support of the comprehensive approach. In *Proceedings of SAS-081 Symposium on Analytical Support to Defence Transformation, RTO-MP-SAS-081, Sofia, Boyana, April 26*, 2010.