Future Research in Systems Security

Evangelos Markatos and Davide Balzarotti* , eds

The SysSec Project
contact@syssec-project.eu

Abstract. During its first year of operation, the SysSec network of excellence has created a roadmap for System Security Research. This short paper presents a summary of this Roadmap along with its expected impact on the European industry, the European Citizen, and Society in general.

1 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 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. 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

* The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no 257007.

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 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 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 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 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