Emerging threats and actors

BIC Discussion Paper **22 June 2012**

Sotiris Ioannidis [1]

1 FORTH, Greece

This project is supported within the portfolio of the European Commission's DG-CNECT Unit H.4, Trust and Security, and has received funding by European Commission's Seventh Framework ICT Programme under grant number 25258655 for the period January 2011 to December 2013.

Introduction

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 defence 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.

Security of New and Emerging Technologies:

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 international cooperation and new and emerging technologies, which need to be studied from a security point of view:

1. **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.
2. **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.
3. **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.
4. **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.

About the Author

Sotiris Ioannidis is a researcher with the Institute of Computer Science at the Foundation for Research and Technology (FORTH) in Crete, Greece. He has been very active in the research community participating to the FP7 WOMBAT[2] and SYSSEC[3] projects.

Sotiris Ioannidis presented the current situation on threat actors and provided an overview of their capabilities, threat models and assessment of the consequences of breaches or disruptions and their criticality. The full presentation can be found at http://www.bic-trust.eu/files/2012/04/wg2_si.pdf

[2] http://www.wombat-project.eu/

[3] http://www.syssec-project.eu/