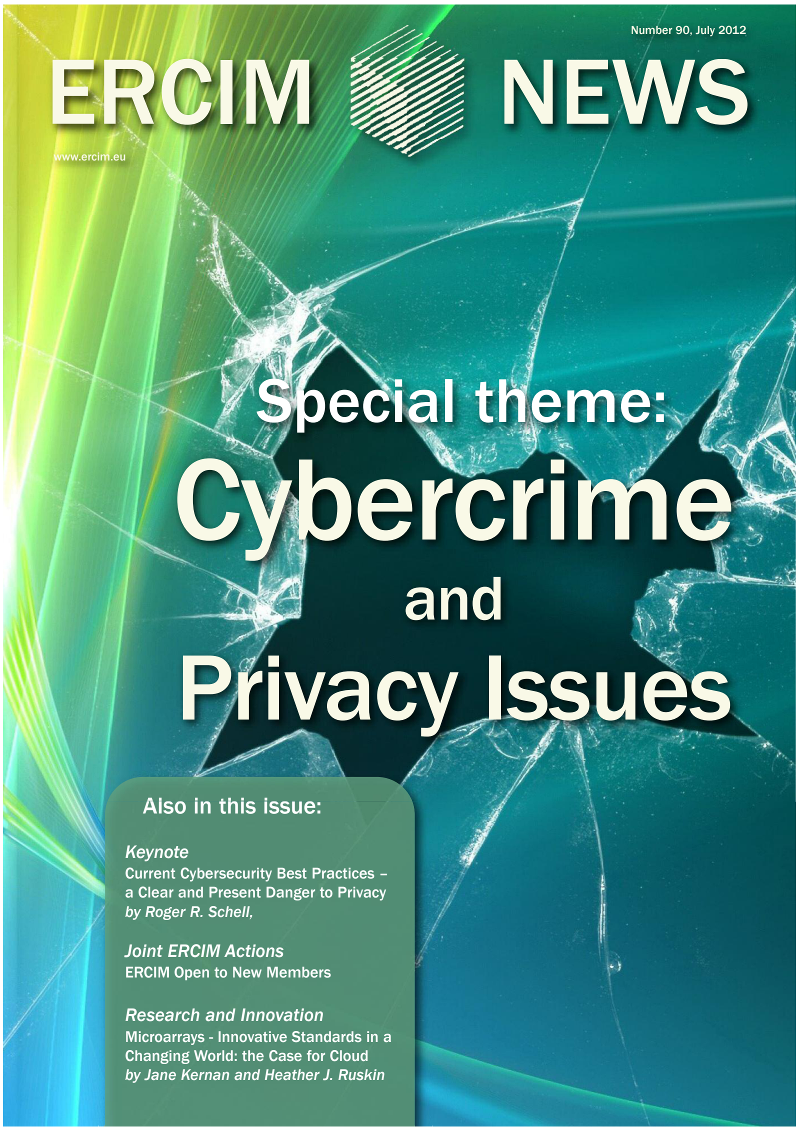

Number 90, July 2012

ERCIM NEWS

www.ercim.eu

Special theme:

Cybercrime and Privacy Issues

Also in this issue:

Keynote
Current Cybersecurity Best Practices – a Clear and Present Danger to Privacy
by Roger R. Schell,

Joint ERCIM Actions
ERCIM Open to New Members

Research and Innovation
Microarrays - Innovative Standards in a Changing World: the Case for Cloud
by Jane Kernan and Heather J. Ruskin

SysSec: Managing Threats and Vulnerabilities in the Future Internet

by Evangelos Markatos and Herbert Bos

For many years, cyber attackers have been one step ahead of the defenders. The asymmetric nature of the threat has led to a vicious cycle where attackers end up winning. SysSec, a new Network of Excellence in the area of Systems Security, attempts to break this vicious cycle and encourages researchers to work not on yesterday's attacks but on tomorrow's threats, to anticipate the attackers' next move and to make sure they are prepared.

Over the past decade we have seen a large number of cyber attacks on the Internet. Motivated by financial profits or political purposes, cyber attackers usually launch attacks that stay below the radar, are difficult to detect, and exploit the weakest link: the user. We believe that the core of the problem lies in the nature of cyber security itself: in the current practice of cyber security, most defenses are reactive while attackers are by definition proactive. Cyber security researchers usually chase the attackers trying to find one more defense mechanism for every newly created attack. Thus, we are facing an asymmetrical threat: while attackers have all the time in the world to choose when and where to strike minimizing their cost, defenders must respond fast, within narrow time constraints, and at a very high cost. Each new round of attack-and-defense drains energy from the defenders, leading them down a vicious cycle which will eventually wear them out. It seems that the only way to build effective defenses is to break this cycle, by changing the rules of the game, by anticipating the moves of the attackers, and by being one step ahead of them, through (i) identifying emerging vulnerabilities, and (ii) working towards responding to possible attacks before they appear in the wild. In this aspect, the recently created SysSec Network of Excellence takes a game-changing approach to cyber security: instead of chasing the attackers after an attack has taken place, SysSec studies emerging

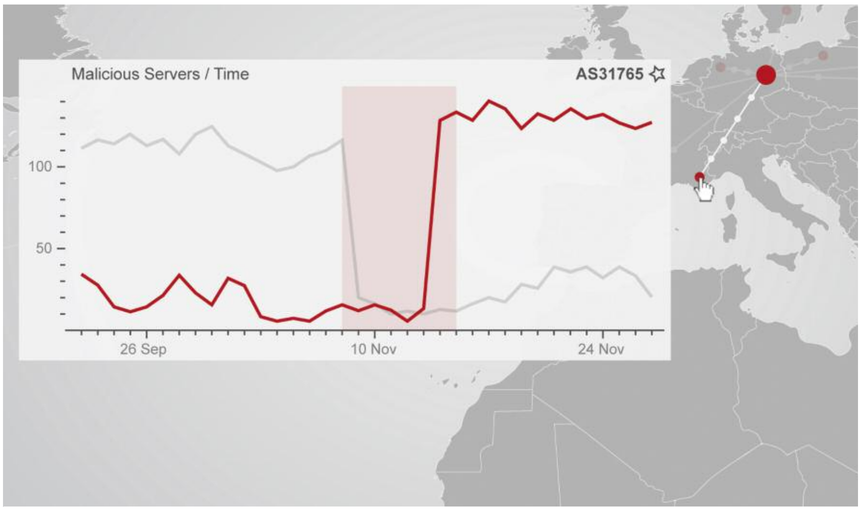

Figure 1: SysSec's BURN interface visualises malicious activities in autonomous systems---in this case, the number of malicious servers as a function of time for a network in Germany exhibits a sudden drop, whereas we find a specular sudden step in a network in France. BURN makes it easy to correlate this type of events visually.

threats and vulnerabilities ahead of time. The network's main thrusts are to identify a roadmap to work on threats and to build infrastructure to boost education in system security—to provide the expertise needed to deal with these emerging threats.

Roadmap

With the collaboration of the research community, SysSec has already produced a research roadmap (http://syssec-project.eu/roadmap1) which outlines some of the important areas the community feels we should focus on. In the first year, the project selected five categories:

1. Privacy. SysSec urges researchers to investigate how to protect users against sophisticated attacks that aim to disclose 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. Targeted attacks. It is 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 current weak points of the war against malware. The problem is often to find the needle of the targeted attack in the haystack of the traditional attacks perpetuated every day on the Internet. In addition, researchers should 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 Providers (ISP) level).
3. Security of emerging technologies, in particular the cloud, online social networks, and devices adopted in critical infrastructures (like smart meters). Security in 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. Mobility: develop new tools and techniques that can be deployed in current smartphone systems to detect and prevent attacks against the device and its applications.
5. Usable security: We believe that a study of the usability of security measures is 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 fields (including engineering, system security, psychology, etc.).

With the help of experts organized in working groups, SysSec updates its roadmap yearly to reflect new threats and priorities.

Education

Having realized the lack of educational material in the area, SysSec further aims to establish a center for academic excellence in the area and has started designing a common curriculum on cyber security, focusing mostly on the production of slides and lab exercises, which are particularly hard to design and set up. A first version of the curriculum along with course material is expected to be ready by September 2012. It will be open to universities throughout Europe and will help to set up a state of the art cyber security curriculum to train the next generation of experts.

We underline that besides SysSec several other projects aim to map the research landscape in cyber security. However, with a clear focus on system security and the development of usable course material, we believe SysSec occupies a unique and valuable niche. SysSec may be contacted at contact@syssec-project.eu, may be followed in twitter (twitter: syssecproject) and may be found in Facebook (http://www.facebook.com/SysSec).

References:

Privacy-Preserving Social Plugins

[1] G. Kontaxis, M. Polychronakis, A. D. Keromytis and E; P. Markatos. “Privacy-Preserving Social Plugins”, In the Proceedings of the 21st USENIX Security Symposium, 2012.

[2] F. Maggi, A.Volpatto, S. Gasparini, G. Boracchi, S. Zanero. “POSTER: Fast, Automatic iPhone Shoulder Surfing”. In the Proceedings of the 18th ACM/SIGSAC Conference on Computer and Communications Security (CCS), 2012.

[3] C. Rossow, C. J. Dietrich, C. Kreibich, C. Grier, V. Paxson, N. Pohlmann, H. Bos and M. van Steen. “Prudent Practices for Designing Malware Experiments: Status Quo and Outlook”. In the Proceedings of the 33rd IEEE Symposium on Security & Privacy (Oakland), 2012.

Please contact:

Herbert Bos, VU University
Amsterdam, The Netherlands
Tel: +31-20 598 7746
E-mail: HerbertB@cs.vu.nl

Evangelos Markatos
FORTH-ICS, Greece
Tel: +30 2810391655
E-mail: contact@syssec-project.eu