CLEARER: CrySyS Laboratory Security and Privacy Research Roadmap

Levente Buttyán Márk Félegyházi Boldizsár Bencsáth
Laboratory of Cryptography and System Security (CrySyS Laboratory)
Department of Telecommunications
Budapest University of Technology and Economics
www.crysys.hu

***Abstract*—The Laboratory of Cryptography and System Security (CrySyS) is dedicated to conduct research in the field of computer security and user privacy. This paper shows a research roadmap of the CrySyS Lab from its inception in 2003 until today. We will present the major achievements in the past with a particular emphasis on the research and teaching curriculum in security and privacy. We will discuss network- and wireless system security, the core competences of CrySyS. Building on the research foundation and competences in these areas, we will lead the laboratory into new territories of security and privacy in wireless embedded computing systems and the future Internet.**

***Keywords*-system security; network security; privacy enhancing technologies; economics of security; trust; wireless networks; embedded computing; Internet of Things; Future Internet**

I. Introduction

The Laboratory of Cryptography and System Security (CrySyS) was created with the purpose of conducting high-quality research on security and privacy of computer networks and systems, and to teach security and privacy at the Budapest University of Technology and Economics (BME). From its inception in 2003, the laboratory has gone a long way: our members have participated in international research efforts with widely-recognized research results in wireless network security, and in order to transfer the obtained research expertise, we bootstrapped a curriculum in the security of telecommunication systems that include courses on network and system security, privacy, cryptography, and the economics of security and privacy.

Our existing research results are centered around security and privacy problems in wireless embedded systems, notably in different types of sensor networks and vehicular communication systems. However, we are aware and keep track of the continuous evolution of other types of computing systems and communication networks too. We have witnessed such an evolution in recent years in terms of the core Internet infrastructure, end-devices and the software services relying on them. The core infrastructure is facing the major shift from legacy protocols to future Internet design. Naming and addressing, and the corresponding security mechanisms have to adapt to this change. For the end-devices, mobility and the integration of embedded systems bring a fundamental change in the way of communication and the capabilities of the communication devices. There is a significant paradigm shift at software services too; more and more functionality is concentrated at content providers who consequently started to develop infrastructure-based software services (e.g. collaborative software services).

Besides continuing our research in security and privacy in networked embedded systems, we are dedicated to contribute to the design of security and privacy solutions for the future Internet. The objective of this paper is to define a research roadmap to realize this goal.

II. Where we are?

The Laboratory of Cryptography and System Security, in its current form, was established in 2003. In terms of institutional organization, it is part of the Department of Telecommunications of the Budapest University of Technology and Economics. The lab currently has 4 faculty members, 1 post doc researcher, and 5 PhD students. This research team is currently led by Levente Buttyán, associate professor.

The research activities of the CrySyS Lab have been centered around security and privacy issues in wireless networked embedded systems. We successfully contributed to joint European research efforts by designing a security toolbox for sensor networks in the UbiSec&Sens Project (www.ist-ubisecsens.org), by applying sensor networks in the domain of critical infrastructure protection in the WSAN4CIP Project (www.wsan4cip.eu), by developing high-bandwidth and secure mesh networks in the EU-MESH Project (www.eu-mesh.eu), by designing a security architecture and location privacy enhancing mechanisms for communicating vehicles in the SeVeCom Project (www.sevecom.org), and recently, by developing secured e-health services based on body area sensor networks in the CHIRON Project (www.chiron-project.eu). We have published a number of papers on these topics in prominent journals and conferences (see our publication list on our web site at www.crysys.hu), and established a good reputation in the European ad hoc and sensor network research community.

In terms of teaching, our scope is broader, encompassing (i) an MSc level base course on Information Security, covering a wide range of security and privacy issues in IT systems and networks in general, and (ii) a special MSc program on Security in Telecommunication Systems, containing 3 mandatory courses and 1 elective course on Cryptography, Secure Protocols, Security in E-Commerce Systems, and Network Security in Practice, respectively, a number of laboratory exercises, and various offerings for semester and diploma level student projects.

III. Where we want to go?

Networked embedded systems (ubiquitous computing, Internet of Things) play an increasingly important role in IT, and therefore, their security and privacy issues remain an important research direction in the CrySyS Lab. However, besides the embedded world, we also intend to extend our research activities to the next generation Internet. In this section, we briefly summarize our research goals within the areas mentioned above.

A. Security and privacy in embedded systems and networks

1) Code attestation and code execution integrity for embedded devices: Similar to other computing systems, embedded devices are also controlled by software, which can contain vulnerabilities that can be exploited by malware. Indeed, some possible malware based attacks on sensor motes [1], RFID systems [2], implantable medical devices [3], and vehicles have been recently published, and more are expected to appear in the future. In addition, the recent incident caused by the Stuxnet worm shows, that malware targeting industrial embedded control systems exists already in practice. Smart phones will also be attractive targets for malware [4], as people store more and more sensitive information on them. At the same time, the resource limitations of embedded systems and their often specialized operating conditions make it difficult to protect them with existing anti-malware approaches known from the PC world.

In this context, remote code attestation and code execution integrity verification appear to be interesting security building blocks that help to increase the trustworthiness of embedded computing systems. Remote code attestation can assure a remote verifier that code loaded for execution is not tampered with, while code execution integrity verification in addition allows for checking that a given piece of code was executed as intended on the remote embedded execution platform. Both approaches help to detect the presence of malware.

While some hardware root of trust seems to be indispensable for remote code attestation and code execution verification, the general problem of hardware based approaches is that they cannot be applied to legacy and embedded systems that lack required hardware extensions. Purely software based solutions to attestation and verifiable execution of code running on legacy or embedded platforms have also been proposed in [5], [6] as good trade-offs between security and practical applicability. Unfortunately, some potential vulnerabilities in the most prominent software based code attestation solutions have recently been identified in [7]. This led to some debate among researchers [8], [9] that resulted in the conclusion that while software based code attestation is a useful security primitive, its design principles are not yet fully understood.

In our future research activities, we intend to develop a know-how on software based remote code attestation and code execution verification on various embedded platforms, and to design and analyze novel protocols for code attestation and code execution integrity protection. It is also our objective, to look into the possibility of applying formal modeling and reasoning for establishing some correctness proof for existing and future protocols. Our research in this area aims at increasing the trustworthiness of embedded computing systems and the services that they provide.

2) Privacy in cooperative networks of embedded devices: Cooperative networks based on the interconnection of various types of embedded devices with each other and to the Internet open the possibility to create new, highly-innovative services and applications. Embedded devices may be static, deployed at fix locations in the environment and in living spaces, or they may be mobile, carried by people or vehicles. In both cases, embedded devices can be used to sense and to control the environment, and to collect and provide various types of information about and to human users, respectively. Examples of such cooperative networks of embedded devices include wireless sensor and actuator networks, smart metering applications, vehicular networks, opportunistic ad hoc networks of personal mobile devices, or RFID based systems.

Mobile phones can also be considered as embedded computers, and they play a particularly important role, because they are usually equipped with different types of sensors (e.g., GPS based location sensors, accelerometers, cameras, microphones, thermometers, etc.), and at the same time, they have access to the Internet through WiFi or 3G connections. Hence, mobile phones are communication devices, end-user terminals, and they are also capable for continuous capturing of additional context information about the user (e.g., his physical location, the type of activity he is involved in).

While such global networks of embedded devices open new horizons in the domain of context aware services, they also create serious privacy problems. In particular, sensed data and the associated context information may leak private information about the individual sharing them.

Third party service providers who have access to such data may misuse them for tracking the location and the activities of the individual. Another aspect of the privacy problem concerns those users that want to access the shared information: their searching and downloading activities may reveal their personal interest profiles to other parties.

Therefore an important research objective of our lab is to design and analyze new privacy enhancing techniques for the sort of cooperative embedded networks described above, including both aspects of privacy, i.e., privacy enhancing techniques for information providers (who share sensed data and context information) and for information consumers (who search and download information).

B. Building trust in the Future Internet design

As the Internet transformed from a small computer network used by researchers to a global communication infrastructure the trust relations between the participants diminished. As a consequence of the disappearing trust relations, security became a fundamental issue. Unfortunately, Internet protocols were originally designed for the trusted networking environment and its rapid growth prevented computer scientists to redesign the networking protocols with security in mind. Instead, networking experts started to develop complementary solutions that could fix the original design weaknesses.

There exists a vast amount of Internet security protocols applied in practice to solve various problems and an even larger literature of academic security protocol design. There is however a substantial difference between the theoretical design of security protocols and their application in practice. The purpose of security solutions is often jeopardized by economic factors: the limited knowledge of users, the lack of incentives for users and companies to adopt appropriate security solutions or asymmetric information between participants in the security defense mechanisms. In recent years, the economic issues surrounding security problems received a significant amount of attention. Anderson and Moore [10] argued that the economic factors largely contribute to the inefficient application of security protocols. Following this observation, the field called economics of security emerged. We believe that the economics point of view of security and privacy, including the analysis of incentives using game theoretic tools, will be a key element in the design of new trust establishment mechanisms. Our research agenda covers the economics of security defense mechanisms as well as risk management issues as follows:

1) Economics of domain name registrations: Service providers play an important role in the online economy and their services are often misused by cyber-criminals. But, the service providers might not have the incentives to prevent such abuse especially if they do not suffer the consequences of misuse. In order to improve security incentives for service providers, it is important to understand how their existing infrastructure works. The online economy surrounding domain name registrations is quite complex and misused by criminals. Anecdotal evidence suggest that most of the new domain registrations serve malicious purposes [11]. Indeed, a recent study [12] has shown that a specific behavior called typo-squatting, where miscreants register domains that are reached by mistyping well-known domain names, gain momentum in domain registrations. To understand the incentives in this economy, one has to understand the purpose of domain names and the incentives of domain registrars. Our goal in this study is twofold. First, we aim at understanding how the current domain registration practices evolve and what type of domain names become popular. This is very relevant in the security context. Second, we will study how the practices of a competitive service provider market can be improved either by regulation or by designing an appropriate reputation mechanisms.

2) Trust and reputation in security defense mechanisms: Security defense relies on establishing trust between the communicating parties and blocking access of untrusted parties. Keeping usability is the main goal in mind, most existing defense mechanisms allow all unknown traffic to go through by default, observe the communication pattern and filter out communication that is deemed to be malicious. Reputation systems provide a key ingredient in defense mechanisms by sharing relevant observations with other defenders. This sharing component is crucial as it prevents the malicious traffic to penetrate widely on the Internet. Miscreants found a way to dynamically change their network identifiers and the defense mechanisms have answered with a more aggressive and reactive blocking of these identifiers resulting in an arms-race between attackers and defenders. We hypothesize that existing security mechanisms that are fundamentally based on exclusion will not be able to cope with the dynamically changing environment. Hence, there is a need to deploy more efficient reputation schemes and increasingly rely on greylisting techniques. Unfortunately, the situation is likely to escalate further with major architectural changes in the Internet architecture.

Our goal is to design reputation mechanisms that are able to keep up with the changing infrastructure while maintaining the convenient use of the protected services. We believe that this requires a transition from the traditional blocking-based security protocols to trust-building evaluation mechanisms. The main principle of the novel protocols is the incremental development of trust between Internet participants.

3) Cyber-insurance and risk management: Improving security practices on the Internet is difficult if the rules governing the interaction of participants are unclear or

weakly enforced. Cyber-insurance was proposed as a catalyst for improving security [13]. The assumption is that insurance companies in a future cyber-insurance market have a natural incentive to mitigate risks and motivate their clients to pay better attention to their computer systems. The cyber-insurance market has not yet taken off in large scale and there are several factors that hinder its widespread introduction [14]: interdependent security, correlated risks and asymmetric information jointly contribute to the difficulty of the problem. Because of these limiting factors insurers have a hard time to quantify risks and develop cyber-insurance products for complex IT systems.

We will focus on developing cyber-insurance mechanisms that fuel the improvement in network security practices. The recent example of University of California [15] has shown that clearly communicated security requirements enable an insurance company to develop an insurance products for seemingly uninsurable systems. Our research is to developing security mechanisms that provide clear guidelines for self-protection and serve as a basis of insurance products to mitigate risks that cannot be (or difficult to) protected against. We will integrate options to mitigate the adverse effects of interdependent security, information sharing and asymmetric information. We will pay a special attention to data management issues as these types of breaches have significantly increased in recent years.

IV. How we want to get there?

In order to reach our objectives, we will, on the one hand, leverage on our existing know-how and expertise in security and privacy in wireless embedded systems, and we will, on the other hand, take advantage of the background of our newly hired faculty members to progress on the new research domains described in this roadmap. More specifically, we will establish a new group with 2-3 PhD students, led by Márk Félegyházi, that will be dedicated to work on security and trust problems of the future Internet and that will follow an economics-based approach to tackle those problems. Besides that, we keep our group dedicated to security and privacy of embedded networked computing systems, and we will hire new PhD students to reach our goals in this domain. In order to obtain research funding, we are actively seeking opportunities to participate in related EU project proposals in the current and in the upcoming framework programs.

References

[1] A. Francillon and C. Castelluccia, "Code injection attacks on harvard-architecture devices," in *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, 2008.

[2] M. R. Rieback, B. Crispo, and A. S. Tanenbaum, "Is your cat infected with a computer virus?" in *Proceedings of IEEE Pervasive Computing and Communications (PERCOM)*, 2006.

[3] K. Rasmussen, C.Castelluccia, T. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, 2009.

[4] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? – revealing the nuts and bolts of the security of mobile devices," in *Proceedings of the IEEE Symposium on Security and Privacy*, 2011.

[5] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: Software-based attestation for embedded devices," in *Proceedings of the IEEE Symposium on Security and Privacy*, May 2004.

[6] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla, "Pioneer: Verifying code integrity and enforcing untampered code execution on legacy systems," in *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, 2005.

[7] C. Castelluccia, A. Francillon, D. Perito, and C. Soriente, "On the difficulty of software-based attestation of embedded devices," in *Proceedings of ACM Conference on Computer and Communications Security (CCS)*, 2009.

[8] A. Perrig and L. van Doorn, "Refutation of On the difficulty of software-based attestation of embedded devices," http://sparrow.ece.cmu.edu/group/pub/ccs-refutation.pdf, 2010.

[9] A. Francillon, C. Castelluccia, D. Perito, and C. Soriente, "Comments on Refutation of On the difficulty of software-based attestation of embedded devices," http://planete.inrialpes.fr/~ccastel/PAPERS/2010_CCS_attestation_comments_on_rebutal.pdf, 2010.

[10] R. Anderson and T. Moore, "The economics of information security," *Science*, vol. 314, no. 5799, p. 610, 2006.

[11] P. Vixie, "Taking Back the DNS," http://www.isc.org/community/blog/201007/taking-back-dns-0, Jul 29 2010, retrieved on Feb 27, 2011.

[12] T. Moore and B. Edelman, "Measuring the perpetrators and funders of typosquatting," *Financial Cryptography and Data Security*, pp. 175–191, 2010.

[13] L. Gordon, M. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," *Communications of the ACM*, vol. 46, no. 3, pp. 81–85, 2003.

[14] R. Böhme and G. Schwartz, "Modeling Cyber-Insurance: Towards A Unifying Framework," in *Proceedings of GameSec 2010*, 2010.

[15] K. Eft and A. Goldblatt, "New cyber insurance program at UC," http://inews.berkeley.edu/articles/Oct-Nov2010/cyberinsurance, Aug 9 2010, retrieved on May 31, 2011.