Laboratory of security and applied cryptography Faculty of Informatics, Masaryk University Brno, Czech Republic

Position paper for the Workshop of the development of EuroSOUPS

Vashek Matyas
matyas@fi.muni.cz

Marek Kumpost
kumpost@fi.muni.cz

1. Introduction of the participant

Laboratory of security and applied cryptography (in Czech **La**boratoř **B**ezpečnosti a **A**plikované **K**ryptografie - LaBAK) is one of the laboratories at the Faculty of Informatics, Masaryk University. It has been established in 2006 and the principal supervisor is Vashek Matyas. Currently, the LaBAK team consists of five employees, nine Ph.D. students, 5-10 bachelor or master students and two external co-workers.

The laboratory enables both graduate and pre-graduate students to gain practical experience with current security and crypto solutions and technologies. The main areas of interest are computer network security (for both wireless and metallic networks), smart card security and related cryptographical applications, user privacy, biometric authentication and the use of cryptography for creation and operation of secure systems. More specific areas of interest are selected with respect to current developments and in accordance with senior members' current research focus. Our goal is to create an environment that allows students to get hands-on experience with the available technical solutions. Lab work is to a large extent supervised by our doctoral students. The laboratory is open to students who work on their projects and theses. The laboratory also has a long experience in cooperation with commercial and governmental partners as well as other academic institutions.

2. Research in the field of privacy

We participated in the FIDIS (Future of Identity in the Information Society) project – a 5-year Network of Excellence research grant of the EU 6th Framework Program (www.fidis.net). Its objective was to research the changes that the concept of identity has been undergoing in the developing European information society. We were leaders of a work package primarily oriented on privacy models and their applicability and user profiling (our research on user profiling finished as a dissertation of one of the members of our laboratory). We also organized a European Wide study about the price of private data (geo-location being observed via mobile phones). All documents and deliverables are accessible via the project home page. There is also a book published by Springer [1].

Currently, we are involved in the PICOS (Privacy and Identity Management for Community Services) EU project. The objective of the project is to advance the state of the art in technologies that provide privacy-enhanced identity and trust management features within complex community-supporting services that are built on Next Generation Networks and delivered by multiple communication service providers. The approach taken by the project is to research, develop, build trial and evaluate an open, privacy-respecting, trust-enabling identity management platform that supports the provision of community services by mobile

communication service providers. We contributed primarily to the architecture of the communication platform.

3. General research in the field of security

The main security research areas of our laboratory are security of computer networks (both wired and wireless), research on generation of (pseudo)random number generators (especially for the mobile environment – see [4, 5]), use of cryptography to build secure systems (e.g., writing secure code) and authentication of users in computer network environment. In the field of security, we started (2002) research for the Czech National Security Authority in the area of smartcard security (and related cryptographic applications) and this cooperation is still active.

Research in the area of wireless sensor network security has taken an important part of our lab activities since 2006, resulting in a book chapter [2] and proposition of new (inter)national grant projects proposals. Ongoing research on biometric authentication and privacy protection resulted as an encyclopaedic publication (in Czech) [3], book chapter in [1] and participation in the EU funded PICOS project (see above).

4. Ideas on how to develop EuroSOUPS

Very simply:

1. In a close coordination with the SOUPS Steering Committee.
2. With the aim to create a symbiotic pair like Crypto and Eurocrypt.
3. By timing the EuroSOUPS event at least 4 months apart from SOUPS.
4. If possibly, in the same place and week as another HCI or security/privacy event in Europe.

References

[1] Gilliot, Maike - Matyáš, Václav - Sven, Wohlgemuth - Kumpošt, Marek. Privacy and Identity (Privacy and Identity). In *The Future of Identity in the Information Society - Challenges and Opportunities*. SRN : Springer Verlag, 2009. p. 351-390, 40 pp. Springer Verlag, 1st issue. ISBN 978-3-540-88480-4.

[2] Švenda, P.,Matyáš, V. Authenticated Key Exchange with Group Support for Wireless Sensor Networks, Chapter 15. In From Problem to Solution: Wireless Sensor Networks Security. Nova Science Publishers, 2008. 23 p. Distributed, Cluster and Grid Computing book series. ISBN 978-1604564570.

[3] Rak, R., Matyáš, V., Říha, Z. et al. Biometrics and human identity - in forensic and commercial applications. Prague : Grada Publishing, a.s., 2008. 664 p. ISBN 978-80-247-2365-5.

[4] Krhovják, Jan - Švenda, Petr - Matyáš, Václav. The Sources of Randomness in Mobile Devices. In *Proceeding of the 12th Nordic Workshop on Secure IT Systems*. Kringlan 1, 103 Reykjavik : Reykjavik University, 2007. pp. 73-84, 163 p. ISBN 978-9979948346.

[5] Bouda, Jan - Krhovják, Jan - Matyáš, Václav - Švenda, Petr. Towards True Random Number Generation in Mobile Environments. In *LNCS, Identity and Privacy in the Internet Age*. 5838/2009. Berlin : Springer, 2009. pp. 179-189, 12 p. ISBN 978-3-642-04765-7.