Special Issue on Applied Cryptography – Guest Editorial

Václav (Vashek) Matyáš, Zdeněk Říha, and Petr Švenda

THIS special issue focuses on the area of applied cryptography, bringing up selected papers from Santa's Crypto Get-Together (SantaCrypt), a workshop that runs since 2001 as an annual Czech and Slovak workshop aiming to facilitate closer cooperation of professionals working in the field of applied cryptography and related areas of security.

The first paper "Attacking Scrambled Burrows-Wheeler Transform" of Martin Stanek of a recent proposal for a modification of the Burrows-Wheeler transform (BWT). The BWT is a commonly used transform in lossless compression algorithms. The BWT does not compress the data itself, instead it is usually the first step in a sequence of algorithms transforming an input data into compressed data. The modification – Scrambled Burrows-Wheeler transform is an attempt to combine encryption and data compression. The paper shows that the proposed approach is insecure, presents chosen plaintext and known plaintext attacks and estimates their complexity in various scenarios.

The second paper "Two Improvements of Random Key Predistribution for Wireless Sensor Networks – Revised Version" of Jiri Kur et al. won the student KEYMAKER competition at SantaCrypt, and its first version was presented at the 8th International Conference on Security and Privacy in Communication Networks. This work deals with the area of random key predistribution in wireless sensor networks. Two novel improvements enhancing security provided by the random key predistribution schemes are proposed and analyzed. The first improvement exploits limited length collisions in secure hash functions to increase the probability of two nodes sharing a key. The second improvement introduces hash chains into the key pool construction to directly increase the resilience against a node capture attack.

The third paper "Privacy Scores: Assessing Privacy Risks Beyond Social Networks" of Michal Sramka focuses on the concept of privacy scores that were proposed in the past to provide each user with a score – a measurement of how much sensitive information a user made available for others on a social network website. This paper discusses their shortcomings, and shows several research directions for their extensions. The author also proposes an extension that takes the privacy score metric from a single social network closed system to include background knowledge, and argues for the need to include publicly available background knowledge in the computation of privacy scores in order to get scores that more truthfully reflect the privacy risks of the users.

The last paper "Accelerating Biometric Identification" of David Naccache et al. deals with biometric identification. As opposed to biometric matching, biometric identification is a relatively costly process because it involved a number of template comparisons. The paper discusses the problem of the optimization of biometric identification. The main idea is to test the most probable candidates first.

Václav (Vashek) Matyáš is a Professor at the Masaryk University, Brno, CZ, and serves as a Vice-Dean for Foreign Affairs and External Relations, Faculty of Informatics. His research interests relate to applied cryptography and security, publishing over a hundred peer-reviewed papers and articles, and co-authoring six books. He was a Fulbright Visiting Scholar with Harvard University, Center for Research on Computation and Society, and also worked with Microsoft Research Cambridge, University College Dublin, Ubilab at UBS AG, and was a Royal Society Postdoctoral Fellow with the Cambridge University Computer Lab. Vashek was one of the Editors-in-Chief of the Identity in the Information Society journal, and he also edited the Computer and Communications Security Reviews, and worked on the development of Common Criteria and with ISO/IEC JTC1 SC27. Vashek is a member of the Editorial Board of the Infocommunications Journal and a Senior Member of the ACM. He received his PhD degree from Masaryk University, Brno and can be contacted at matyas AT fi.muni.cz.

Zdeněk Říha is an Assistant Professor at the Masaryk University, Faculty of Informatics, in Brno, Czech Republic. He received his PhD degree from the Faculty of Informatics, Masaryk University. In 1999 he spent 6 months on an internship at Ubilab, the research lab of the bank UBS, focusing on security and usability aspects of biometric authentication systems. Between 2005 and 2008 he was seconded as a Detached National Expert to the European Commission's Joint Research Centre in Italy, where he worked on various projects related to privacy protection and electronic passports. He was involved in the ePassport interoperability group known as the Brussels Interoperability Group. Zdeněk has been working with the WG 5 (Identity management and privacy technologies) of ISO/IEC JTC 1/SC 27. Zdeněk's research interests include smartcard security, PKI, security of biometric systems and machine readable travel documents. Zdeněk can be contacted at zriha AT fi.muni.cz.

Petr Švenda is an Assistant Professor at the Masaryk University, Faculty of Informatics, in Brno, Czech Republic. He received his PhD degree from Masaryk University, working in the area of the cryptographic protocols for restricted environments such as wireless sensor networks, with focus on automatic generation of cryptographic protocols with the help of evolutionary algorithms. In 2008, he worked at TU Dresden on secure logging for the AN.ON anonymity service. He is also interested in practical aspects of security in cryptographic smartcards and their resistance against side-channel attacks and properties of random number generators available on smartcards and mobile devices. Petr can be contacted at svenda AT fi.muni.cz.