

Swiss army knife in cryptography and information security - cryptographic hash functions  
Prof. Danilo Gligorovski (Norwegian University of Science and Technology, Norway)

In the first part of the talk I will briefly present the importance of cryptographic hash functions. In cryptography and information security, hash functions are considered as the "Swiss army knife". They are used in countless protocols and algorithms such as: building digital signatures, checking data integrity, commitment schemes or for password protection. They are also used as a basic security mechanism for local file systems or for decentralized file systems, for P2P file-sharing, decentralized revision control tools and for intrusion detection systems. They are also used in popular software package tools such as Microsoft CLR strong names, Python setuptools, Debian control files, Ubuntu system-integrity-check, and "Hashcash" – software for fighting spam.

In the second part of the talk I will talk about the latest scientific developments in the area of cryptographic hash functions. Namely, in 2005 we have witnessed significant theoretical breakthrough in breaking the current cryptographic standard SHA-1. Although there is another family of standardized hash functions called SHA-2, ready to replace SHA-1 hash function, at the end of 2007, the National Institute of Standards and Technology (NIST) decided to start a 4 year world-wide competition process for choosing the next cryptographic hash standard SHA-3.