ThinkBS 304 Innovative Techniques for Data Security - Cryptography (Advanced)

Offered in University Politehnica of Bucharest

by:

The current real world has two components: the physical world and the virtual world. The current threats can be divided into terrestrial threats, maritime threats, aerial threats, space threats and cyber threat, respectively. The first 4 threats are governed by the laws of nature and the 5th threat is human induced. If we look at the history of virtual media, then we can say that the first means of virtual communication was the radio (Guglielmo Marconi). It took the radio 38 years to reach 5 million users. The next landmark in virtual communication was television (Boris Lvovich Rosing), which, in order to reach the same number of users, took 14 years. The means of virtual communication used today is the Internet (Sir Timothy John), reaching the same number of users in 5 years. Throughout history the above-mentioned means of communication have been used for disinformation actions (the current term used is fake-news): the incident at the German radio station Sender Gleiwitz was a pretext for the outbreak of World War II, the Romanian insurection from 1989 it has been maintained with the help of television, also in the case of elections in various states, or through the use of social networks in electoral processes. In this new reality, characterized by the virtual component, new categories of cyber threats appear to be managed. The pace of development of new technologies has led to the misalignment between IT (which owns the infrastructure) and the security team (which owns cyber security, the controls and processes that protect the business). To manage this threat, we are inviting you to attend at the lectures given by University Politehnica of Bucharest on INNOVATIVE TECHNIQUES FOR DATA SECURITY.

The course INNOVATIVE TECHNIQUES FOR DATA SECURITY consists of two strongly interconnected modules. The first module A VIEW OF THE CRYPTOGRAPHIC ALGORITHMS IN A VIRTUAL WORLD is dedicated to cryptographic algorithms and the second module APPLIED CRYPTOGRAPHY IN INFORMATION SECURITY to the security assessment from the perspective of the two reference standards in the field of cryptography (FIPS 140-3, equivalent 19790), respectively to ensure a common level of trust (ISO 15408).

Module 1 of the course Cryptographic algorithms in a virtual world is focused on symmetric algorithms, asymmetric algorithms (integer factorization, discrete log theory, elliptic curves theory) and hybrid systems. Also, the lectures covers algorithm standards such as Advanced Encryption Standard. There are discussed some relevant example of cryptographic algorithms such that: RSA and Chinese remainder theorem, block ciphers, Merkle-Hellman cipher system, Galois computation, ElGamal encryption and signature system (classic and elliptic curves based), key exchange protocols, subliminal channels, side channel attacks and software resources.

Module 2 is industry oriented and is focused on INFOSEC Standards, Cryptographic standards (FIPS 140-2 and ISO 15408), Case studies covers Vulnerabilities on RSA encryption algorithm, examples and real world problems. Last minute current issues such as the impact of the NIS and GDPR on the design of information systems are also discussed.

The lecturers of this course are as follows: SIMONA BIBIC, CORINA CIPU, CARMINA GEORGESCU, MIHAI REBENCIUC, EMIL SIMION and ANTONELA TOMA from the Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering “Traian Lalescu” (CiTi), University Politehnica of Bucharest.