International Cooperation on Cryptology – Bart Preneel

Speaker: Bart Preneel is a full professor in the research group ***COSIC*** of the ***Electrical Engineering Department*** of the ***Katholieke Universiteit Leuven*** in ***Belgium.*** His main research area is information security focussing on cryptographic algorithms and protocols as well as their applications to computer and network security and mobile communications.

Professor Bart Preneel presented the **ECRYPT II** project[1], a Network of Excellence project in Cryptology with 11 partners and 25 associate partners (1 from Taiwan). *ECRYPT II,* which stands for *European Network of Excellence for Cryptology II,* is a 4-year network of excellence funded within the Information & Communication Technologies (ICT) Programme of the European Commission's Seventh Framework Programme (FP7) under contract number ICT-2007-216676. It falls under the action line *Secure, dependable and trusted infrastructures*. ECRYPT II started on 1 August 2008 and runs until the end of 2012. Its objective is to continue intensifying the collaboration of European researchers in information security.

The main objective of ECRYPT II is to ensure a durable integration of European research in both academia and industry and to maintain and strengthen the European excellence in these areas. In order to reach this goal, 11 leading players and 20 adjoint members to the network propose to integrate their research capabilities within three virtual labs focusing on symmetric key algorithms (SymLab), public key algorithms and protocols (MAYA), and hardware and software implementations (VAMPIRE). ECRYPT II has been publishing widely used yearly report on algorithms and key lengths.

Some of the technical objectives of ECRYPT II include improving trade-offs between cost (footprint, power and/or energy consumption), security and performance**;** development and analysis of advanced cryptographic protocols for distributing trust**;** and secure hardware and software implementations**.**

The ECRYPT II research roadmap for the next 10 years is motivated by the changing environment and threat models in which cryptology is deployed and has a focus on Crypto for Internet of Things including the need for low energy crypto; Crypto for cloud computing including distributed cryptography; fully homomorphic encryption; cryptology for use in applications (in part driven by regulation) e.g. privacy for smart grid; privacy for road pricing; e-voting; and advertising.

In terms of the key elements required for the cryptology area on an international level, there is a need for an integrated policy at EU level and international collaboration is required across academia, industry and government agencies and there is a significant need for collaborative research and its interaction with policy. To build an international strategy for INCO, there is a need for collaboration on cryptographic algorithms with the forging of open competitions with shared governance; effective standardization and continual updates of a key lengths and parameters document (management of standards). Collaboration also should take place on cryptographic protocols motivated by distribution of trust and privacy (key component in privacy by design) and joint research also need to occur in these areas. We can be more effective by avoiding duplication and increasing impact on both the technology and policy levels. Professor Preneel concluded by saying it was good to see that Cryptology is included in the research agenda presented earlier within the identified BIC topics.

---

[1] **http://www.ecrypt.eu.org/**