The 2016 IEEE International Conference on Software Quality, Reliability and Security
QRS 2016

Vienna, Austria, August 1-August 3, 2016
http://paris.utdallas.edu/qrs16

Keynote Speech

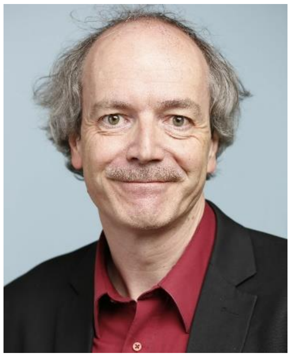
New Threat Models for Cryptography

Bart Preneel
Computer Security and Industrial Cryptography (COSIC) Research Group
Electrical Engineering Department
Katholieke Universiteit Leuven, Belgium
http://homes.esat.kuleuven.be/~preneel/

Abstract

Traditionally cryptography is used to protect communications and stored data. The cost of strong cryptography has been decreasing and today cryptography is used in tens of billions of devices. However, it has become apparent that ever more sophisticated attacks are launched to undermine or bypass cryptography: these attacks include compromising end systems, exploiting vulnerabilities in key management procedures, and inserting backdoors in cryptographic standards. We conclude by analyzing how these new threat models affect future research in cryptology and information security.

About the speaker



Bart Preneel is a full professor at the KU Leuven; he heads the COSIC research group, that is a member of the iMinds Security Department. The COSIC research group currently has 70 members, including 5 professors, 20 postdoctoral researchers, and more than 40 PhD students. He was visiting professor at five universities in Europe. He has authored more than 400 scientific publications and is inventor of 5 patents. His main research interests are cryptography, information security and privacy. Bart Preneel has participated to more than 40 EU projects, including several projects on privacy and identity management. He has coordinated the Network of Excellence ECRYPT 2004-2012, 250 researchers) and is coordinating ECRYPT-CSA and the Marie-Curie ITN ECRYPT.NET. He has served as panel member and chair for the European Research Council and has been vice-president and president of the IACR (International Association for Cryptologic Research). He is a member of the Permanent Stakeholders group of ENISA (European Network and Information Security Agency), of the Academia Europaea, and of the Belgian Privacy Commission (subcommittee national register). He has been invited speaker at more than 120 conferences in 50 countries. In 2014 he received the RSA Award for Excellence in the Field of Mathematics and in 2016 he received the Kristian Beckman award from IFIP TC11.

In 2013 he testified in the European Parliament for the LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens.