"End-to-end encryption" - real perspective or danger in cryptography?

Gyöngyvér MÁRTON

Department of Mathematics-Informatics, Sapientia Hungarian University of Transylvania

mgyongyi@ms.sapientia.ro

Nowadays, end-to-end encryption, preventing people from wire-tapping, receives more and more attention. This happens because some cryptographers revealed situations, when private communications were secretly monitoring by authorities. But on other side, end-to-end encryption, also protect communications from "bad guys". So a serious question arises from this situation: researchers, developers are allowed to use end-to-end encryption so that no one, but legitimate users can access their private data or developers should require the authorities to built escrow keys in their encryptions system. In this lecture firstly we shall present those primitives, which contribute to end-to-end encryptions, secondly we shall show our results.

References

[1] Keys under doormats: mandating insecurity by requiring government access to all data and communications. Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter, and Daniel J. Weitzner. Journal of Cybersecurity (2015)

[2] Message authentication using hash functions: The HMAC construction. Mihir Bellare, Ran Canetti and Hugo Krawczyk. CryptoBytes 2(1), Spring (1996)

[3] AES Proposal: Rijndael. Joan Daemen, Vincent Rijmen, National Institute of Standards and Technology. p. 1. (2013)

[4] New directions in cryptography. IEEE Transactions on Information Theory 22 (6): 644654. W. Diffie, M. Hellman. (1976)

[5] Elliptic curve cryptosystems. N. Koblitz. Mathematics of Computation 48 (177): 203209. (1987)

[6] Key escrow from a safe distance: looking back at the Clipper Chip. Matt Blaze. ACSAC '11 Proceedings of the 27th Annual Computer Security Applications Conference (2011)