”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`

September 2–4, 2019

Nowadays, end-to-end encryption, which protects the communicating parties from any eavesdropping, receives more and more attention. Since the Snowden affair in USA, when it was revealed that many cryptosystems have deliberately built back-doors, one of the most important goals for cryptographic researchers has been to bring high-security cryptographic systems to the public and expose primitives that are inadequately secure.

However, eavesdropping can have many different purposes which is often not directed against the privacy of the individual, but rather for the protection of the existing state apparatus which, of course, indirectly guarantees the safety of citizens.

So a serious question arises from this situation: whether developers can agree with the authorities to built escrow keys in their encryptions system, or they must cover up any attempt to protect the personal privacy of users.

In this lecture firstly we shall present the capabilities of the end-to-end encryptions, secondly we shall show our opinion, our results.

References

[1] Daniel J. Bernstein, Tanja Lange, and Ruben Niederhagen. Dual EC: A Standardized Back Door. Cryptology ePrint Archive, Report 2015/767. http://eprint.iacr.org. 2015.

[2] Bruce Schneier et al. Surreptitiously Weakening Cryptographic Systems. Cryptology ePrint Archive, Report 2015/097. http://eprint.iacr.org/. 2015.

[3] Daniel J. Bernstein, Tung Chou, Chitchanok Chuengsatiansup, Andreas Hulsing, Tanja Lange, Ruben Niederhagen, and Christine van Vredendaal. How to manipulate curve standards: a white paper for the black hat. Proceedings of the Second International Conference on Security Standardisation Research - Volume 9497 Pages 109-139. Springer-Verlag. 2015.

[4] David Wong. How to Backdoor Diffie-Hellman. Cryptology ePrint Archive, Report 2016/644. http://eprint.iacr.org/. 2016.