Secure Group Key Establishment
Course Abstracts

M.I. González Vasco

Lecture 1. The key distribution problem

In this lecture, we will try to understand the importance of securely generating, managing and distributing secret keys. Further, we will discuss the basic strategies towards secure key generation and distribution from both secret and public key cryptography tools. Focusing in the two party setting, we will explain early solutions in this direction, and review some basic key transport protocols like the Needham-Schroeder Protocol or Kerberos. As basic references, we will use material from [3, 6].

1 Lecture 2. Key exchange constructions for the two party case

We will review the main goals for authentication and key establishment and discuss the formal security notions desirable for a (two-party) key exchange protocol. Further, we will describe in detail some design principles for key exchange protocols, and explain in detail some basic two party protocols for key establishment, building on the well known Diffie-Hellman key establishment and some of its variants. In turn, we will discuss the Katz-Yung compiler for adding authentication to a basic unauthenticated construction (see [5]).

2 Lecture 3. Group key establishment protocols

This lecture will focus on group (also known as *conference*) key establishment protocols. We will start by explaining the basic Burmester-Desmedt protocol and further explore on different variants, security models and compilers that allow for the construction of group key exchange protocols with different security properties (see [1]).

3 Lecture 4. Advanced Constructions

We will give a brief summary of key establishment protocols designed for specific application scenarios, focusing on different advanced security goals: *anonymity, privacy, key compromise impersonation resilience, robustness* ect. The goal of this final lecture is to discuss a few non-standard constructions (v.g., [4, 2]) and understand the main tools at hand for such designs, as well as the different choices that can be made when specifying a security model and detailing the corresponding proofs.

References

[1] Michel Abdalla, Jens-Matthias Bohli, Maria Isabel Gonzalez Vasco, and Rainer Steinwandt. (password) authenticated key establishment: From 2-party to group. In Salil P. Vadhan, editor, *Theory of Cryptography, 4th Theory of Cryptography Conference, TCC 2007, Amsterdam, The Netherlands, February 21-24, 2007, Proceedings*, volume 4392 of *Lecture Notes in Computer Science*, pages 499–514. Springer, 2007.

[2] Jens-Matthias Bohli, Maria Isabel Gonzalez Vasco, and Rainer Steinwandt. Secure group key establishment revisited. *Int. J. Inf. Sec.*, 6(4):243–254, 2007.

[3] Colin Boyd and Anish Mathuria. *Protocols for Authentication and Key Establishment*. Information Security and Cryptography. Springer, 2003.

[4] Dario Fiore, Maria Isabel Gonzalez Vasco, and Claudio Soriente. Partitioned group password-based authenticated key exchange. *Comput. J.*, 60(12):1912–1922, 2017.

[5] Jonathan Katz and Moti Yung. Scalable protocols for authenticated group key exchange. *J. Cryptology*, 20(1):85–113, 2007.

[6] Mark Manulis. *Provably secure group key exchange*. PhD thesis, Ruhr University Bochum, 2007.