Social Key Exchange Network – From Ad-Hoc Key Exchanges to a Dense Key Network

Dirk Achenbach David Förster Christian Henrich Daniel Kraschewski
Jörn Müller-Quade

Institut für Kryptographie und Sicherheit (IKS), Fakultät für Informatik,
Karlsruher Institut für Technologie (KIT)

{achenbach,henrich,kraschewski,mueller-quade}@kit.edu
david@dfoerster.de

Abstract: Security of public key cryptography is steadily threatened by advancements in algorithmics and computing power. In this work we propose a novel approach to long-term secure key exchange based on security assumptions that are independent of strong complexity assumptions.

We present a key propagation scheme that sets up a network of distributed keys. Whenever two parties meet, they exchange new keys (e.g. using near field communication) and pass on all keys received so far. This establishes a dense key network growing and spreading with each meeting of protocol participants. Even two parties that have never met in person can use this network to obtain a common secret. A notable security feature of our scheme is the anonymity of the established keys, making it hard for an adversary to track movements of protocol participants.

Keywords: Key Propagation, Mobile Ad-Hoc Networks, Key Exchange.