LABORATORY FOR COMMUNICATIONS AND APPLICATIONS LCA

Key Establishment and Key Management in Decentralized Wireless Network

As the popularity of mobile devices such as PDAs, laptops, and mobile phones increases every day, users tend to rely more on them in a growing number of situations. In many situations, users either have no access to a central authority or simply do not want to relay on any central authority. These trends ask for the development of scalable and decentralized security solutions. On this page, we present solutions that are specifically targeted at issues of key establishment and key management in decentralized wireless networks, where users have no access to the central authority.

Inspired by PGP, in Self-Organized Public Key Management for Mobile Ad-Hoc Networks [5,6], we have shown how the need for a trusted authority can be relaxed. In this proposal, we let users to maintain a certificate graph in a fully distributed way. This approach is fully self-organized, even in its initialization phase. However, it relies on the assumption that trust between users is transitive; certain mechanisms are proposed to cope with this issue.

In order to avoid relying on *trust transitivity*, in Mobility Helps Peer-to-Peer Security [3,4], we have shown how mobility can be exploited to set up security associations (i.e., authenticated keys) among users. Thus, as users move around, they authenticate each other by visual contact and by the activation of an appropriate *authentication channel* of their personal device.

In Key Agreement in Peer-to-Peer Wireless Networks [1,2], we have presented and analyzed different mechanisms (protocols) to realize *low-bandwidth authentication channels* between the personal devices of two users in visual contact. We have considered the problem in a demanding scenario: the two devices share no authenticated information prior to their meeting. We have proven the security properties of our proposals using well-established methodology.

Publications

[1] Integrity (I) codes: Message Integrity Protection and Authentication over Insecure Channels
M. Cagalj, S. Capkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava and J.-P. Hubaux
IEEE Symposium on Security and Privacy, Oakland, California, USA, 2006

[2] Key Agreement in Peer-to-Peer Wireless Networks
M. Cagalj, S. Capkun, J.-P. Hubaux
Proceedings of the IEEE (Special Issue on Cryptography and Security), 2006
[pdf]

[3] Mobility Helps Peer-to-Peer Security
S. Capkun, J.-P. Hubaux, L. Buttyan
IEEE Transactions on Mobile Computing, January, 2006
[pdf]

[4] Mobility Helps Security in Ad Hoc Networks S. Capkun, J.-P. Hubaux and L. Buttyán
In Proceedings of MobiHOC 2003
[pdf]

[5] Self-Organized Public-Key Management for Mobile Ad-Hoc Networks
S. Capkun, L. Buttyan, J. P. Hubaux
In IEEE Transactions on Mobile Computing (January-March 2003)
[pdf]

[6] The Quest for Security in Mobile Ad Hoc Networks
J.-P. Hubaux, L. Buttyán, and S. Capkun
In Proceedings of MobiHOC 2001, Long Beach, CA, USA, October, 2001
[ps]

PEOPLE

Prof. Jean-Pierre Hubaux
Mario Cagalj

Collaborators

Dr. Srdjan Capkun
Prof. Levente Buttyan

RELATED

At EPFL

Secure Vehicular
Communication

Projects

Secure Positioning (SPOT)
webpage

| © 2017 EPFL tous droits réservés