Mobility Helps Peer-to-Peer Security

We propose a straightforward technique to provide peer-to-peer security in mobile networks. We show that far from being a hurdle, mobility can be exploited to set up security associations among users. We leverage on the temporary vicinity of users, during which appropriate cryptographic protocols are run. We illustrate the operation of the solution in two scenarios, both in the framework of mobile ad hoc networks. In the first scenario, we assume the presence of an offline certification authority and we show how mobility helps to set up security associations for secure routing; in this case, the security protocol runs over one-hop radio links. We further show that mobility can be used for the periodic renewal of vital security information (e.g., the distribution of hash chain/Merkle tree roots). In the second scenario, we consider fully self-organized security: Users authenticate each other by visual contact and by the activation of an appropriate secure side channel of their personal device; we show that the process can be fuelled by taking advantage of trusted acquaintances. We then show that the proposed solution is generic: It can be deployed on any mobile network and it can be implemented either with symmetric or with asymmetric cryptography. We provide a performance analysis by studying the behavior of the solution in various scenarios.

General information
State: Published
Organisations: System Security, Department of Informatics and Mathematical Modeling
Contributors: Capkun, S., Hubaux, J., Buttyan, L.
Pages: 43-51
Publication date: 2006
Peer-reviewed: Yes

Publication information
Journal: IEEE Transactions on Mobile Computing
Volume: 5
Issue number: 1
ISSN (Print): 1536-1233
Ratings:
BFI (2018): BFI-level 2
Web of Science (2018): Indexed yes
BFI (2017): BFI-level 2
Scopus rating (2017): CiteScore 4.93 SJR 0.82 SNIP 2.456
Web of Science (2017): Impact factor 4.098
Web of Science (2017): Indexed yes
BFI (2016): BFI-level 2
Scopus rating (2016): CiteScore 4.97 SJR 0.976 SNIP 2.84
Web of Science (2016): Impact factor 3.822
BFI (2015): BFI-level 2
Scopus rating (2015): CiteScore 4.78 SJR 1.198 SNIP 3.219
Web of Science (2015): Impact factor 2.456
BFI (2014): BFI-level 2
Scopus rating (2014): CiteScore 4.92 SJR 1.192 SNIP 3.538
Web of Science (2014): Impact factor 2.543
BFI (2013): BFI-level 2
Scopus rating (2013): CiteScore 5.15 SJR 1.424 SNIP 3.868
Web of Science (2013): Impact factor 2.912
ISI indexed (2013): ISI indexed yes
BFI (2012): BFI-level 2
Scopus rating (2012): CiteScore 4.67 SJR 1.513 SNIP 3.461
Web of Science (2012): Impact factor 2.395
ISI indexed (2012): ISI indexed yes
Web of Science (2012): Indexed yes
BFI (2011): BFI-level 1
Scopus rating (2011): CiteScore 4.81 SJR 1.373 SNIP 3.819
Web of Science (2011): Impact factor 2.283
ISI indexed (2011): ISI indexed yes
BFI (2010): BFI-level 1