



Authenticated Trusted Server Controlled Key Establishment

By Astha Keshariya

LAP Lambert Academic Publishing Sep 2012, 2012. Taschenbuch. Condition: Neu. Neuware - Any business or financial transaction over an unsecured network demands some level of trust between the communicating parties. Establishment of a key through cryptographic mechanism becomes crucial when they must be able to authenticate each other in the absence of any prior association. Certificate based Public Key Infrastructure (PKI) has been the source of many radical advances in the evolution of security solutions to provide: authentication, authorization, confidentiality, integrity and accountability. The book presents a new trusted server based key establishment protocol, AK-protocol that makes use of Certificate-based authentication. An analysis and resilience of AK-protocol for various properties that a key establishment protocol must exhibit, along with practical scenarios when under different attack situations like Replay, Impersonation, DDoS attacks, etc., is demonstrated. A proof-of-concept on the practical implementation of AK-Protocol in financial domains while integrating it with 3-D secure protocol is also envisaged. 180 pp. Englisch.



READ ONLINE
[2.18 MB]

Reviews

This publication can be really worth a go through, and a lot better than other. It is actually written in straightforward words and phrases instead of confusing. I discovered this pdf from my dad and i suggested this publication to learn.

-- Jackeline Rippin

A high quality book and also the font employed was intriguing to read. I was able to comprehend every thing out of this created e book. You won't really feel monotony at whenever you want of the time (that's what catalogues are for concerning should you check with me).

-- Prof. Johnson Cole Sr.