Abstract

With the rapid growth of computer networks, more and more users access the remote server's service in a distributed computing environment. Due to the fast development of the Internet and wireless communications, many activities like online-shopping, online banking, online voting are conducted over it. Authentication is one of the essential security features of network communication. The authentication process ascertains the legitimacy of the communicating partners in communication. In the authentication procedure, the promoter of the communication and the defendant derives some identification codes of each other prior to start of the message transaction. Sundry methods have been introduced regarding the authentication process from
An Estimated Model of Risk Analysis of Attacks on Smart Card Authentication Schemes

time to time. The static approach authentication schemes are vulnerable to different types of
attacks. The growth of smart card systems faces security threats to both the card and its
environment. Issues related to readers, protocol implementations, the smart card’s hardware
security features or a combination of logical and physical attacks is of legitimate concern. All the
elements of a smart card system have their own specific behavior. They could be attacked in
various ways. In this paper we analyze the smart card attacks through a noncyclic attack graph.
Noncyclic attack graphs provide an intuitive aid in threat analysis. We dissert that such a formal
interpretation is indispensable to precisely understand how noncyclic attack graphs can be
framed up during design and analysis. We provide an educational semantics, based on a
mapping to attack stack, which abstracts from the internal structure of a Noncyclic attack graph,
we study transformations between Noncyclic attack graphs, and we study the attribution and the
projection of a Noncyclic attack graph.

References

- Bruce Schneier: 'Secrets and Lies'; attack trees:
- Terrance R. Ingoldsby: Understanding Risk Through Attack Tree Analysis, CSI
- Bruce Schneier, Adam Schostack: Breaking Up Is Hard To Do: Modelling Security
  Threats for Smart Cards, Usenix Workshop on Smartcard Technology, February
- David Corcoran: Security-related Exposures and Solutions in Smartcards, Information
- Zoltán Kincses: On avoidance of attacks against the pin error counter of smart cards,
  (CS) – The Fourth Conference of PhD Students in Computer Science 2 Szeged, Hungary, July
  2004. Abstract on pp. 68:
- Michael Lamla: Hardware attacks on smart cards – overview, Eurosmart
- Wolfgang Rankl, Wolfgang Effing: Overview about Attacks on Smart Cards,
  2003, Munich, from their own &apos;Smart Card Handbook&apos;&apos; (John Wiley & Sons, ISBN:
  0-470-85668-8).
- P. Kocher and B. Jun, Differential power analysis,&apos;Proceedings of Crypto
  under the threat of power analysis attacks,&apos;IEEE Transactions on Computers, vol. 51,
  no. 5, pp. 541-552, 2002.
  1995, Volume: 14 Issue: 5 pp. 385-389 (5 pages)
- P. Urien, &apos;Internet card, a smart card as a true Internet node&apos;&apos;; Computer
  Communications, 2000, pp. 1655-1666.
- Verschuren T., Smart Access: Strong Authentication on the Web, Computer Networks
  and ISDN system 1998, pp 1511-1519
An Estimated Model of Risk Analysis of Attacks on Smart Card Authentication Schemes

Index Terms

Computer Science

Security

Keywords

No Cyclic Attack Graph  Authentication  Integrity