{tag}

{/tag}

IJCA Proceedings on National Level Technical Conference X-PLORE 2014
by IJCA Journal

XPLORE 2014

Year of Publication: 2014

Authors:
Nilesh M. Shidurkar

{bibtex}xplore1413.bib{/bibtex}

Abstract

A Secure digital conference scheme allows a group of people to communicate safely in different way. Dynamic participation is a key feature of the secure conference schemes that allows new conferees to join and the old conferees to leave. The conference key distribution scheme (CKDS) enables three or more parties to derive a common conference key to protect the conversation content in their conference. In this paper we study a conference scheme for mobile communications and find that the scheme is insecure against the replay attack. With our replay attack, an attacker with a compromised conference key can cause the conferees to reuse the compromised conference key, which in turn completely reveals subsequent conversation content.

Refer

ences

- H. C. Williams, "A modification of the RSA public key encryption procedure," IEEE Trans. Inform. Theory, vol. 26, pp. 726–729, Nov. 1980.
- I. Ingemarsson, D. T. Tang, and C. K. Wong, "A conference key distribution system," IEEE Trans. Inform. Theory, vol. IT-28, pp. 714–720, Sept. 1982.
- K. Koyama and K. Ohta, "Identity-based conference key distribution system," in Proc. CRYPTO'87, Santa Barbara, CA, Aug. 1987, pp. 194–202.
- M. J. Beller, L. F. Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," IEEE J. Select. Areas Commun. , vol. 11, pp. 821–829, Aug. 1993.
- M. S. Hwang andW. P. Yang, "Conference key distribution schemes for secure digital mobile communications," IEEE J. Select. Areas Commun. , vol. 13, pp. 416–420, Feb. 1995.
- M. S. Hwang, "Dynamic participation in a secure conference scheme for mobile communications," IEEE Trans. Veh. Technol. , vol. 48, pp. 1469–1474, Sept. 1999.
- D K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Trans. Wireless Commun. , vol. 2, no. 2, pp. 400-407, Mar. 2003.
- X. Yi, C. K. Siew, and C. H. Tan, "A secure and efficient conference scheme for mobile communications," IEEE Trans. Veh. Commun. , vol. 52, pp. 784-793, July 2003.
- X. Yi, C. K. Siew, C. H. Tan, and Y. Ye, "A secure conference scheme for mobile communications," IEEE Trans. Wireless Commun. , vol. 2, pp. 1168-1177, Nov. 2003.
- Feng Bao, "Analysis of a secure Conference Scheme for mobile communication," IEEE Trans. Wireless Commun. , vol. 5, no. 8, Aug. 2006.

Index Terms

Computer Science Mobile Communications

Keywords

Mobile Communications Conference Scheme Security Dynamic Participation