
Multicast security: Literature review

Lakshminath Dondeti
IRTF GSEC RG meeting
March 18 2003, San Francisco

Introduction

- **Plan to have a lit. update at GSEC meetings**
- **A list of papers we come across**
 - After the agenda announcement, received message(s) to include papers
- **We will summarize at a very high level**
 - One or two slides per paper
 - Abstract and comparison to other work
 - Authors are welcome to present their own papers as always

Recent papers in group security

- **A. Pannetrat, R. Molva. “Multiple Layer Encryption For Multicast Groups,”** In Proceedings of The 6th IFIP Communications and Multimedia Security Conference, Portoroz, Slovenia, September 2002.
- **Yongdae Kim, et. al., "Secure Group Services for Storage Area Networks,"** First IEEE International Security In Storage Workshop, December 11th, 2002, Greenbelt, MD
- **Adrian Baldwin and Simon Shiu, "Encryption And Key Management In A SAN,"** First IEEE International Security In Storage Workshop, December 11th, 2002, Greenbelt, MD, USA
- **Alain Pannetrat, Refik Molva. “Real Time Multicast Authentication,”** NDSS, San Diego, February 2003.
- **Donggang Liu and Peng Ning, “Efficient Distribution of Key Chain Commitments for Broadcast Authentication in Distributed Sensor Networks,”** NDSS, San Diego, February 2003
- **S. Zhu et. al., “Performance Optimizations for Group Key Management Schemes,”** to appear in ICDCS 2003.

A few to be discussed today

- **Did not have time to read all!** ☹️
- **These are of interest to me; not attributing any importance**
- **One application paper (Storage area networks)**
- **One on key distribution**
 - Since others have covered authentication schemes
 - Adrian at MSEC and Hovav earlier today

Securing storage area networks

- **Yongdae Kim, et. al., "Secure Group Services for Storage Area Networks," First IEEE International Security In Storage Workshop, December 11th, 2002, Greenbelt, MD**
- **Yongdae plans to present this work in Minneapolis later this year**

Secure group services for storage area networks