Secure Spread: Providing a Secure Infrastructure for Collaborative Applications

Y. Amir, Johns Hopkins University
Y. Kim, University of Minnesota at Twin Cities
C. Nita-Rotaru, Purdue University
J. Stanton, George Washington University
Gene Tsudik, University of California Irvine

Why Group Communication Systems?
- Applications operating based on a group paradigm, requiring:
  - Efficient message dissemination to groups
  - Reliable and ordered (causal order, global order)
  - Membership service
  - Fault-tolerance
- Collaborative applications: computing, white-boards, video-conference
- Distributed transactions and database replication
- Cluster management and monitoring
- Highly available servers

What About Security?
- Secure group communication:
  - Authentication and admission control.
  - Access control to system resources.
  - Key management to bootstrap other security services.
  - Encryption algorithms and integrity mechanisms.
- More challenging in a group setting:
  - Group membership changes over time.
  - Many parties can cause asynchronous events.

Robust Contributory Key Management
- Based on GDH Merge
  - Uses membership service to make consistent decisions
  - AGREED order delivery service used to ensure correctness

Integrated Architecture
- Secure Spread Library
  - Encryption for group key management
  - Key Agreement Algorithms

Encryption Overhead

Group Key Management
- Computation:
  - One member selects the key (centralized)
  - All members contribute a share to the key (contributary)
- Distribution (Transport):
  - One entity distributes the key (centralized)
  - More members can be involved, the goal is to minimize the number of secure channels (distributed)
- What is a "good" key management?

System Deployment

Group Key Agreement Properties
- Backward Forward Secrecy: compromise of the group key does not compromise previous/subsequent group keys.
- Key Independence: compromise of any subset of group keys does not compromise other group keys (includes Backward and Forward Secrecy).
- Perfect Forward Secrecy: compromise of the long-term private keys does not compromise any previous group keys (in contrast to most key distribution schemes).

Impact
- Secure Spread Library (over 500 downloads) available at: https://www.cnds.jhu.edu/securespread/
- One of the 6 technologies selected by DARPA for a Red Team Experiment involving BBN and SRI.
- Secure Spread Library used by other researchers to develop and test their own protocols or to develop their own applications: Yalta project (NCSU/MNC), Rome Labs, SRI - formal verification mutCAPSL, UC Irvine – group admission control.