MLS Security Analysis Status

Karthikeyan Bhargavan

IETF 104, Prague

Protocol Components

Key Exchange

- ART (draft-00), TreeKEM (draft-01), Blank Nodes (draft-02)

Sender, Message, Key Authentication

- Credentials, Signatures + MAC

Message Protection

- Key Schedule, Application Message Encryption, Handshake Encryption

Ongoing Analyses

Symbolic Analyses

- Tamarin (Cohn-Gordon et al, Barnes), F* (Bhargavan, Beurdouche)

Cryptographic Definitions and Proofs

- ART (Cohn-Gordon et al), TreeKEM (Alwen, Dodis et al), …

Verified Implementation

- F* (Beurdouche)

Status: Security definitions and proofs for core key exchange

A Process Proposal

- Problem: The protocol evolves very fast, so analyses become out of date
- Suggestion:
  1. Designate certain sections of certain drafts as *ready for analysis*
  2. Informally freeze these sections for major revisions until next(?) IETF
  3. Minor details (wire formats) and other sections are still free to change

- Problem: The security model and goals require a lot of work to make precise
- Suggestion:
  1. When proposing a change or feature, state an explicit security and/or performance goal, pointing to architecture doc if possible
  2. Explain, informally, why prior design fails this goal and new design succeeds
  3. Explain, informally, why the proposal does not break other stated goals