OVERVIEW

1. The High Level Take Away
2. Defining “Secure”
3. Critical Components of MLS
4. Where To Go From Here...
HIGH LEVEL TAKEAWAY

• Strong confidence in the following security properties of MLS:
  • Privacy of content
  • Authenticity of content
  • Transcript consistency
  • Consistency of Group Management

• Against adversaries that can:
  • Man-in-the-middle all traffic (including owning the Delivery Server)
  • Insider: Participant as legit user in multiple groups
  • Compromise participants devices leaking all their state
  • Register Arbitrary Keys in the Key Services
DEFINING “SECURE”

• To make “Secure” precise we must fix:
  • Communication Model
    • For Availability: With Delivery Service
    • For Security: The adversary IS the network (and the delivery service).
  • Adversarial Capabilities
  • Security Goals
    • E.g. Privacy, Authenticity, Group State, History
  • Assumption
    • Ciphersuite is secure.
    • PKI
    • Good source of randomness
CRITICAL COMPONENTS OF MLS

• MLS is big and complicated.
  • TreeKEM, Exporter Keys, Propose & Commit, PSK, Exporter Keys, External Commits, Add only Commits,…

• To keep things tractable identify critical core components...
  1. PCS across concurrent groups : Especially signature key management & update policies.
  2. Key Derivation Paths (TreeKEM + Key Schedule)
CRITICAL COMPONENTS OF MLS

3. **Continuous Group Key Agreement**

= E2E Group “management” protocol. Gives a fresh symmetric group key per epoch

= MLS with out Application Messages, Symmetric Key Schedule, PSKs, External Commits


ANALYZING “FULL” MLS

1. MLS Protocol draft 7
   • [BBN19] K. Bhargavan, B. Beurdouche, P. Naldurg - *Formal Models and Verified Protocols for Group Messaging: Attacks and Proofs for IETF MLS*. [https://hal.inria.fr/hal-02425229](https://hal.inria.fr/hal-02425229)
   • Automated Proof Tools!

2. MLS Protocol draft 11 (Analyzes MLS Design paradigm: CGKA + MAC + Signatures + ... = MLS)
STRONGEST ADVERSARIES: INSIDERS

- Most Powerful / Complete adversaries considered so far: Malicious Insiders
  - MLSv5: Full Protocol [BBN19]
  - MLSv11: CGKA [AJM20]
DEFINING “SECURE” [AJM20]

• Strongest Attackers Considers: “Insider Security”
  • Network: Fully controls network & delivery server
  • Insider: Participates in many groups as legitimate user
  • PKI: Control’s key server. Can register any keys they want on behalf of any account.
  • Adaptive: Decisions made on the fly
  • Drives the Execution: Tell parties which action to take next.
  • Corrupt Users: leak entire local protocol state from clients
  • Attacking RNGs: Can set output of RNG at will.

• Limits of Insider
  • Can’t create fake certificates to authenticate signature keys
  • Can’t break the crypto in the ciphersuite
  • Can’t mount timing attacks, exploit coding vulns.
WHERE TO GO FROM HERE...

• Metadata security analysis...
• Update automated analysis to MLSv11
• Post-quantum analysis when using PQ ciphersuite
• Analyze more advanced features: PSKs, External Commits, Ciphersuite/protocol version upgrade...