SECDISPATCH
@IETF125

Security protocols that are optimized for non-web and PQC

draft-kohbrok-mls-two-party-profile
draft-housley-tls-using-mls-handshake
draft-kohbrok-mls-tls
draft-tian-quic-quicmls

Presenter: Russ Housley, Vigil Security

Motivation

- Many Operational Technology (OT) or IT/OT use cases have restricted bandwidth and/or computational limitations. Some also have capability imbalance between the sending and receiving devices (e.g., sensors).

- Today’s network security protocols are optimization for web environments, not the challenges of such environments.

- The overhead associated with post quantum cryptography (PQC) increases such challenges, where the alternative is (generally insecure) use of long-term pre-shared keys.

- **Goal: Security protocols that are optimized for non-web and PQC.**

IETF

Key Management Requirements

The Key Management MUST:
Support Layer 3 and Layer 4
Asynchronous Key Updates
Post-Quantum Cryptography (PQC)
Forward Secrecy (FS)
Post-Compromise Security (PCS)
Protocol Formal Analysis

The Key Management SHOULD:
Asynchronous Communication
Support groups and peer-to-peer protocols

Continuous Key Agreement

Continuous Key Agreement (CKA) provide a means to start a session once and perform asynchronous key updates thereafter.

- CKA allows for more control regarding when key updates happen.
- CKA avoids synchronous (e.g., interactive key updates) after the initial key establishment.
- CKA allows **amortization** of PQC overhead (e.g., Signal-style sending some bytes with each message), bringing PQC overhead down to almost classic crypto levels.
- CKA can be used as an alternative handshake with many protocols.

MLS implements CKA and meets the requirements on the previous slide.

IETF

Approaches to using MLS Key Management

- Looking at TLS as an example, both approaches follow the two-party profile.
  - draft-kohbrok-mls-two-party-profile

- Approach 1: TLS handshake extension for MLS key Management, followed by TLS Record protocol.
  - draft-housley-tls-using-mls-handshake

- Approach 2: MLS handshake on its own port, followed by TLS Record protocol.
  - draft-kohbrok-mls-tls

Hoped dispatching outcome

- New IETF mail list to continue the discussion
- Full BoF session at IETF 126 to consider the approaches, new WG, or best WG to do the work

Community Discussion

Backup slides

Design Requirements

MUST

- Support Layer 3 and Layer 4
- Asynchronous Key Updates
- Post-Quantum Cryptography (PQC)
- Forward Secrecy (FS)
- Post-Compromise Security (PCS)
- Protocol Formal Analysis

SHOULD

- Asynchronous Usage
- Support groups and peer-to-peer protocols

Asynchronous Key Updates

- One party can update keying material and send messages without waiting for a response from another party.

Post-Quantum Cryptography (PQC)

- Looking forward, so PQC is absolutely needed
- Cryptographic algorithm agility is needed; more PQC algorithms are already on the horizon

Forward Secrecy (FS)

- Access to all encrypted traffic history combined with access to all current keying material will not disclose messages older than the oldest compromised key.
- Clients have to delete keys as soon as they are no longer needed.

Protocol Formal Analysis

- Experience with TLS 1.3 and MLS shows that formal analysis uncovers security problems during the design phase.
- It is much cheaper to resolve problems in the design phase; resolving problems after wide deployment is expensive.

Asynchronous Communication

- Do not require parties to be online at the same time.

Support groups and peer-to-peer protocols

- Ideally, the same key management approach can support groups (multicast) and peer-to-peer (unicast).
- Peer-to-peer is a group of two parties.

Proposed IETF Work (Part 1)

- Today, none of the Layer 3 / Layer 4 security protocols meet *all* of these security goals

- MLS Key Management meets the security goals
- Proposal is to apply MLS Key Management at Layer 3 and Layer 4
- Could be accomplished with an extension to the existing security protocols or a new protocols altogether

Proposed IETF Work (Part 2)

Already chartered in MIMI WG:

- Specify MLS key management with group chat

Possible approaches:

- Specify MLS key management with TLS Record Protocol
- Specify MLS key management with QUIC
- Specify MLS key management with IPsec ESP

[Each could extend the existing key management protocol *or* specify a new one.]