Use-cases and Properties

for Integrating Remote Attestation with Secure Channel Protocols

Ionut Mihalcea

Background

- **Why does this document exist?**
  - Direct response to questions raised during the Expat BoF.
  - Fulfills one of the SEAT charter milestones.
- **What is the document's purpose?**
  - Build consensus on what scenarios we are building for (the Use-Cases).
  - Establish a common set of requirements for SEAT protocol designs (the Properties).

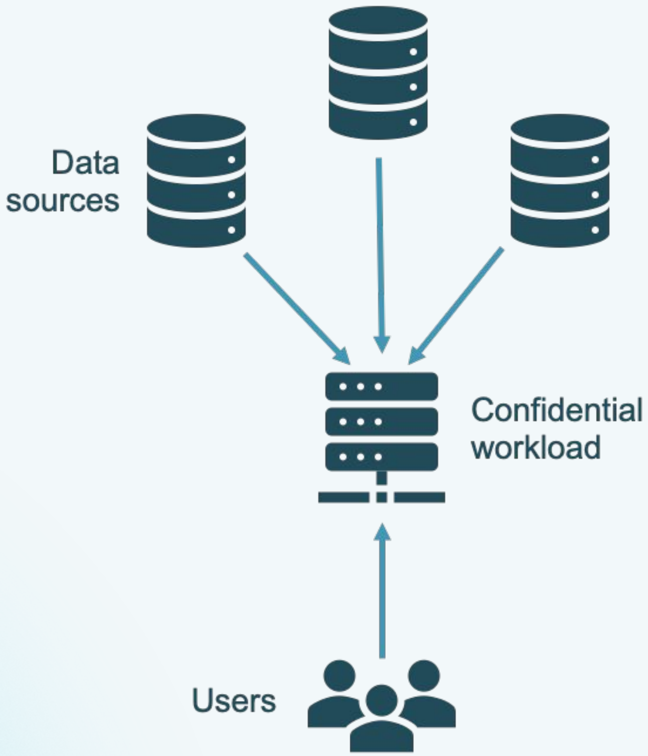
Overview

- Use Cases
  - Confidential data collaboration
  - Secure provisioning and high-assurance operations
  - Network infrastructure integrity
- Properties
  - Binding and freshness (cryptographic bindings, attestation credential freshness)
  - Protocol mechanics (negotiation, flexibility in how the two mechanisms interact)
  - Lifecycle and non-functional (credential lifecycle, privacy, performance)

Use-Cases

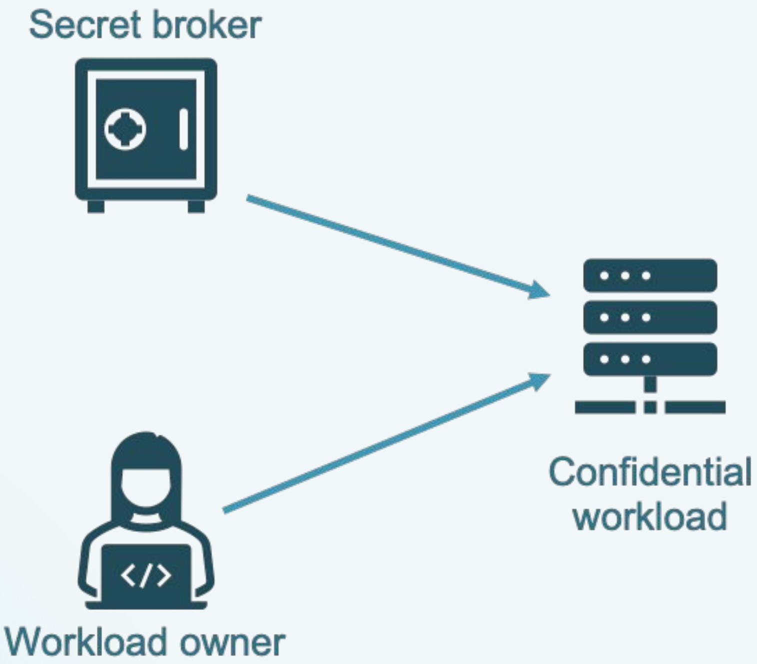
Confidential data collaboration

- **Patterns**:
  - Data clean rooms
  - Secure multi-party computation
- Data providers verifies the peer application before entrusting it with sensitive data.
- Users verify the application to trust the results it produces.



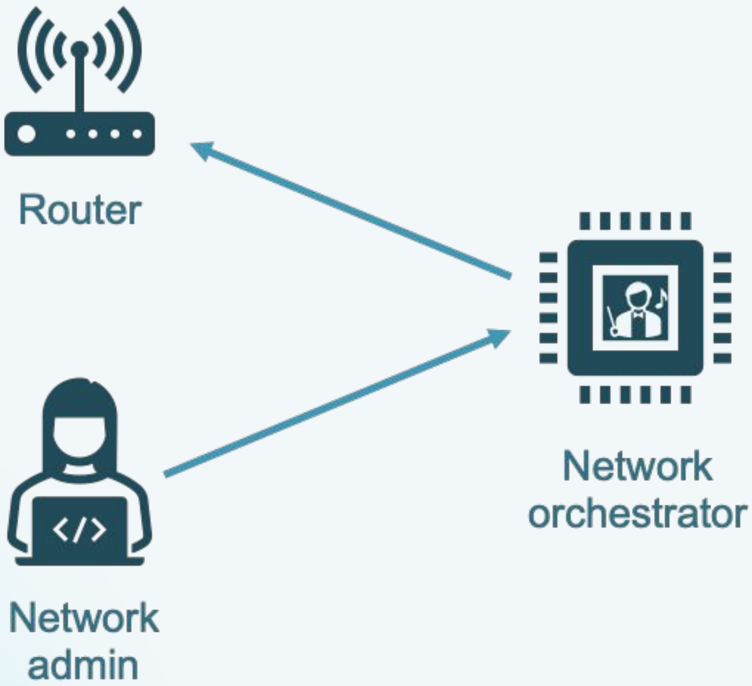
Secure provisioning & high-assurance ops

- **Patterns**:
    - Runtime secret provisioning
    - High-assurance command execution
- Workload or device owner verifies the software and its state before sharing credentials or executing critical commands.



Network infrastructure integrity

- **Pattern**: Verifying the integrity of networking devices.
- Network orchestrator verifies the state of a router or firewall before allowing it to join the network.
- Administrator verifies the state of the management endpoint before connecting.



Properties

Binding and freshness

- Cryptographic binding to communication channel
  - Attestation credential must be bound to secure channel session.
  - Prevents relaying of attestation credentials.
- Cryptographic binding to machine identifier
  - Attestation credential must be bound to the infrastructure-provider machine ID.
  - Prevents diversion attacks.
- Attestation credential freshness
  - Attestation credential must include some form of freshness proof.
  - Prevents replaying of stale credentials.

Protocol mechanics

- Negotiation and capability discovery
    - Peers must agree on support for RA, and any other relevant parameters.
    - Enables interop and graceful fallback.
- Attestation model flexibility
    - Designs must support both RATS Background Check and Passport models.
- Interaction with peer authentication
    - RA must integrate with existing authentication mechanisms, and may feature as the sole authentication method.

Lifecycle and non-functional

- Credential lifecycle management
  - Re-attestation on long-lived connections without a large performance penalty should be possible.
- Privacy preservation
  - Privacy level of secure channel protocols must not be degraded.
- Performance and efficiency
  - Designs must not add prohibitive latencies or overhead.

Next steps & call to action

- Please read the draft and provide any feedback on SEAT WG mailing list or Github repo!
- Key questions for WG:
  - Are these use-cases representative? Any critical use-cases missing?
  - Are the properties at the right abstraction level? Do they cover everything we'd need?
- Questions?