Cloud Security

Secure Systems Group, Aalto University

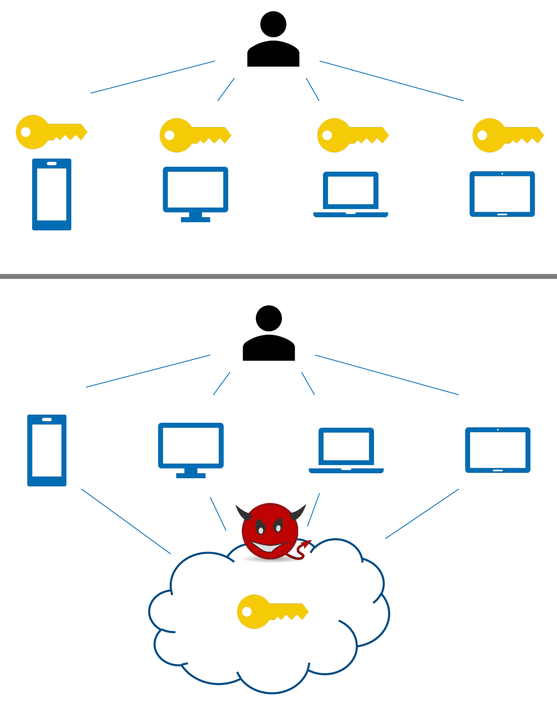
Arseny Kurnikov, Andrew Paverd, Mohammad Mannan, N. Asokan

Keys in Clouds: Auditable Multi-device Access to Cryptographic Credentials

- Managing personal cryptographic keys is challenging, especially when used from multiple devices.
- Centralized storage raises security concerns in case of a malicious cloud provider.
- Trusted Execution Environments (TEEs) provide security guarantees and enable new features.

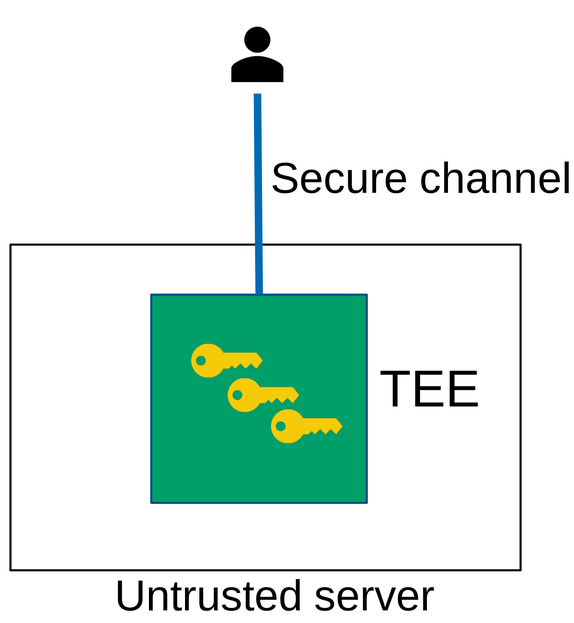
Design

- Store keys in a TEE that provides hardware-based isolation from all other software, including OS and hypervisor.
- Keys are encrypted (sealed) before leaving the TEE.
- Remote attestation assures remote users of the precise code being executed in the TEE.



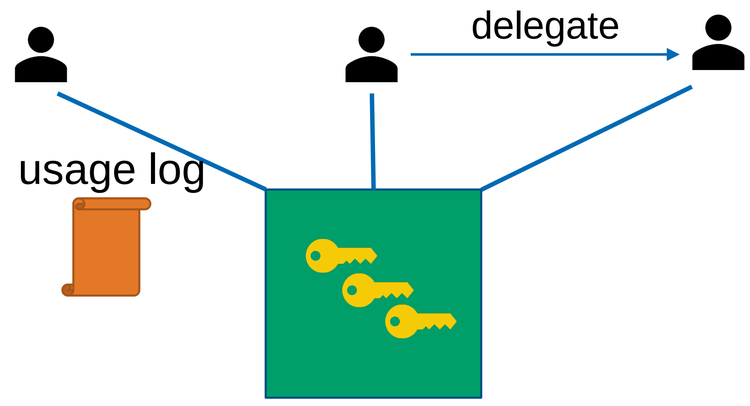
New Features

- Policy-based access control: key owner defines key usage time period and/or number of uses.
- Key delegation: user can delegate access to other users of the same CKS for a specific time or number of uses.
- Key usage auditing: CKS logs every operation performed using the protected keys, and user can audit these logs.



Implementation

- Open source server implementation using Intel SGX with password-based access control and rate-limiting.
- PC client integration with GnuPG.
- Android client integration with OpenKeychain.



Performance Evaluation

- 6,000 signatures per second on a single desktop PC.
- 100 Megabytes of heap memory to serve 100,000 users.
- Signing: 1,2 seconds for a smartcard vs 24 ms for a CKS.

To appear in SECPID 2018

Aalto University

Université Concordia University

intel Collaborative Research Institute for Secure Computing

cloSer