Portable trusted file encryption service

Chun Hui Suen Maximilian Loy Tobias Knothe
Institute for Data Processing
Technische Universität München

Overview

- Goal:
  - Trusted, secure portable storage solution
- Trust
  - Integrity of system is ensured
- Secure
  - Authentication and encryption of files

Demonstration

Content

- Introduction
- Components
  - Attestation
  - Protocol
  - Key management
- Conclusion
- Demo

Introduction - Scenario

- A portable storage device
  - eg. USB stick, USB harddisk, etc
- Usable on multiple trusted platforms
  - Office machine, home machine, trusted 3rd party
  - Trust based on known integrity

Introduction - System

- A portable storage device
- eg. USB stick, USB harddisk, etc
- Usable on multiple trusted platforms
- Office machine, home machine, trusted 3rd party
- Trust based on known integrity

- Validation
- Authentication
- Key & security image management

- TPM
- Integrity measurement

Background – What is a TPM?

- Based on specifications from Trusted Computing Group (TCG)
- TPM is not (only) DRM.
- Hardware chip that provides:
  - Integrity measurement early in boot process
  - RSA Key generation and management
  - And others ...

Attestation (1)

- Using a Trusted Platform Module(TPM)
  - TPM "Quote" operation
- Shared knowledge (set-up)
  - User's private security image
  - Privacy CA public key
  - Attestation Identity Key (AIK) certificate
  - Valid PCR values

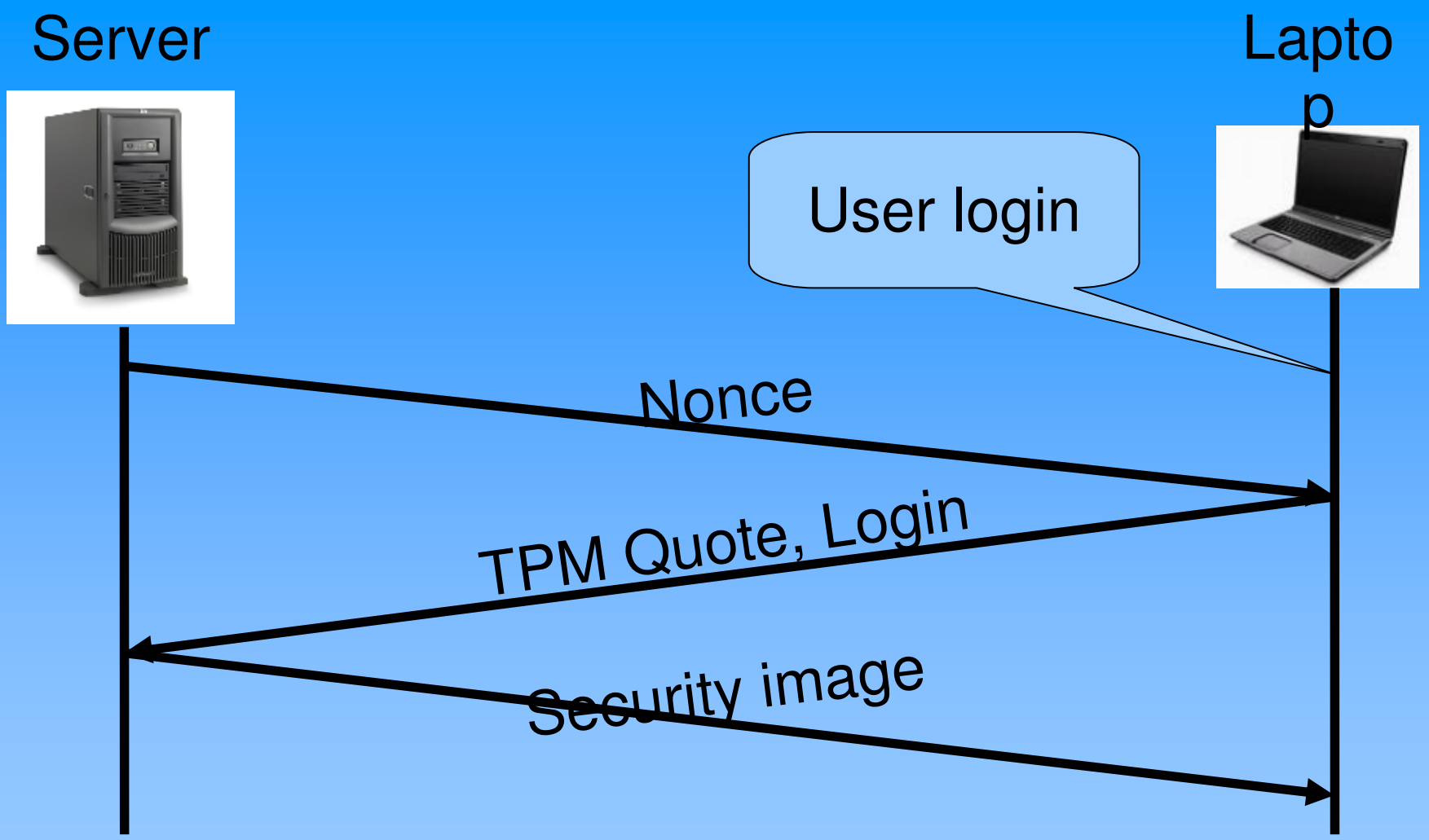
Attestation (2) – Chain of Trust

- Client ⟶ Security image ⟶ Server
- Server ⟶ Privacy Certification Authority (PCA)
- PCA ⟶ TPM Manufacturer ⟶
  Endorsement Key(EK) ⟶
  Attestation Identity Key (AIK) & certificate
- System integrity ⟶ Signed by attestation key

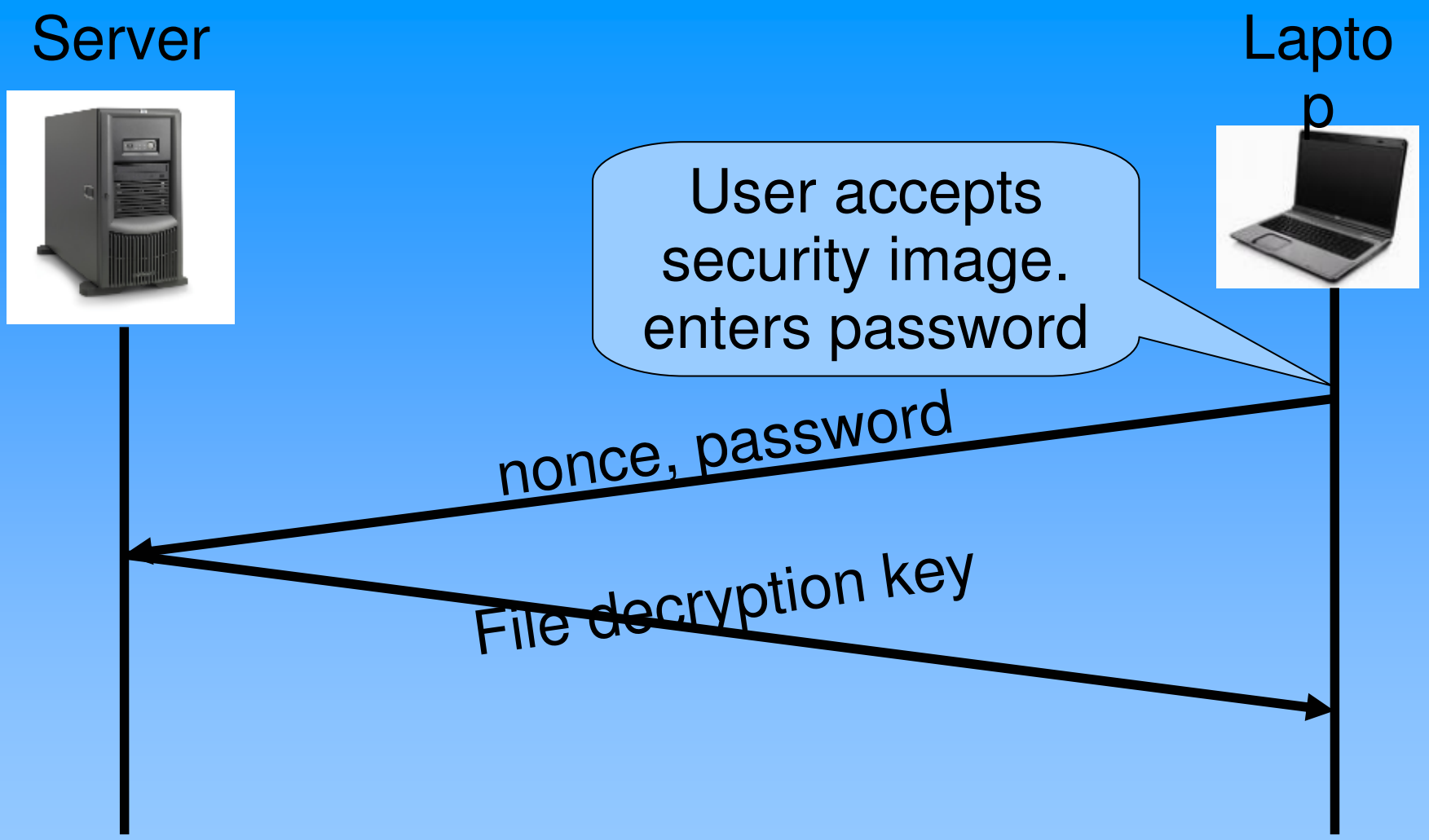
Protocol (1)

- Remote attestation(using TPM) over https
- Nonce generated by server, used in TPM quote and as session identifier

Protocol (2)


Server
Laptop
User login
Nonce
TPM Quote, Login
Security image

Protocol (3)


Server
Laptop
User accepts security image. enters password
nonce, password
File decryption key

Key Management

- MySQL database on server
  - List of known good PCR values
  - User credentials
  - Decryption key
  - Session management

Open issues & future work

- File decryption key embedded on storage device
  - Server only sends a demasking key
- Integrity measurement versioning ??
- Robust integrity measurement ??

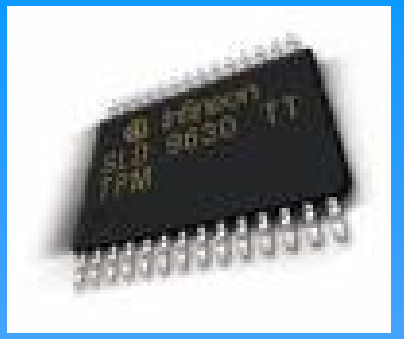
Conclusion

- Working implementation of remote attestation
- Possible “Read-only” system
  - Easy verifiability
- Useful use-case for corporate/mobile computing

Questions ?

TPM Measurement

- BIOS sends bios measurement
- BIOS sends Bootsector measurement
- Bootloader (tGRUB) sends kernel and initrd measurement
- Kernel sends rootFS measurement ?



PCR 0
PCR 1
PCR 2
PCR 3
PCR 4

.
.
.