

Enterprise-wide Security with Cryptographic Hardware Assistance

Joshua D. Guttman

781-271-2654 • guttman@mitre.org

MITRE Sponsored Research

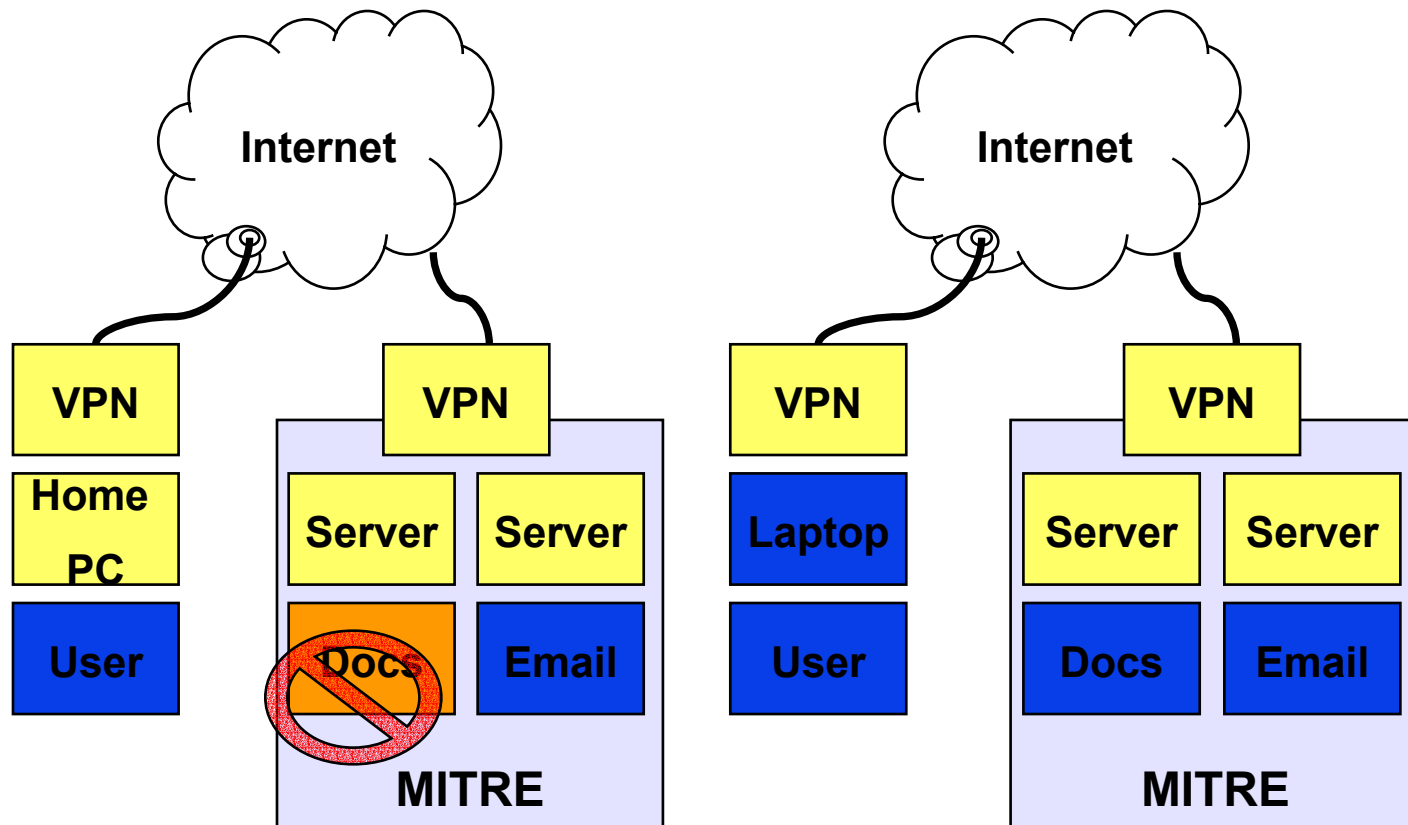
The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

MITRE
Technology
Program

Problem

- **“SSL is like an armored car delivering to someone living in a cardboard box.”**
- **General-purpose hardware does little for *end-to-end* trust.**
- **Enterprise-wide security requires cryptographic support.**
 - **Trusted Platform Module (TPM) to be widespread**
 - **How to provide manageable services?**

Background



Remote access policies: do you trust the remote system?

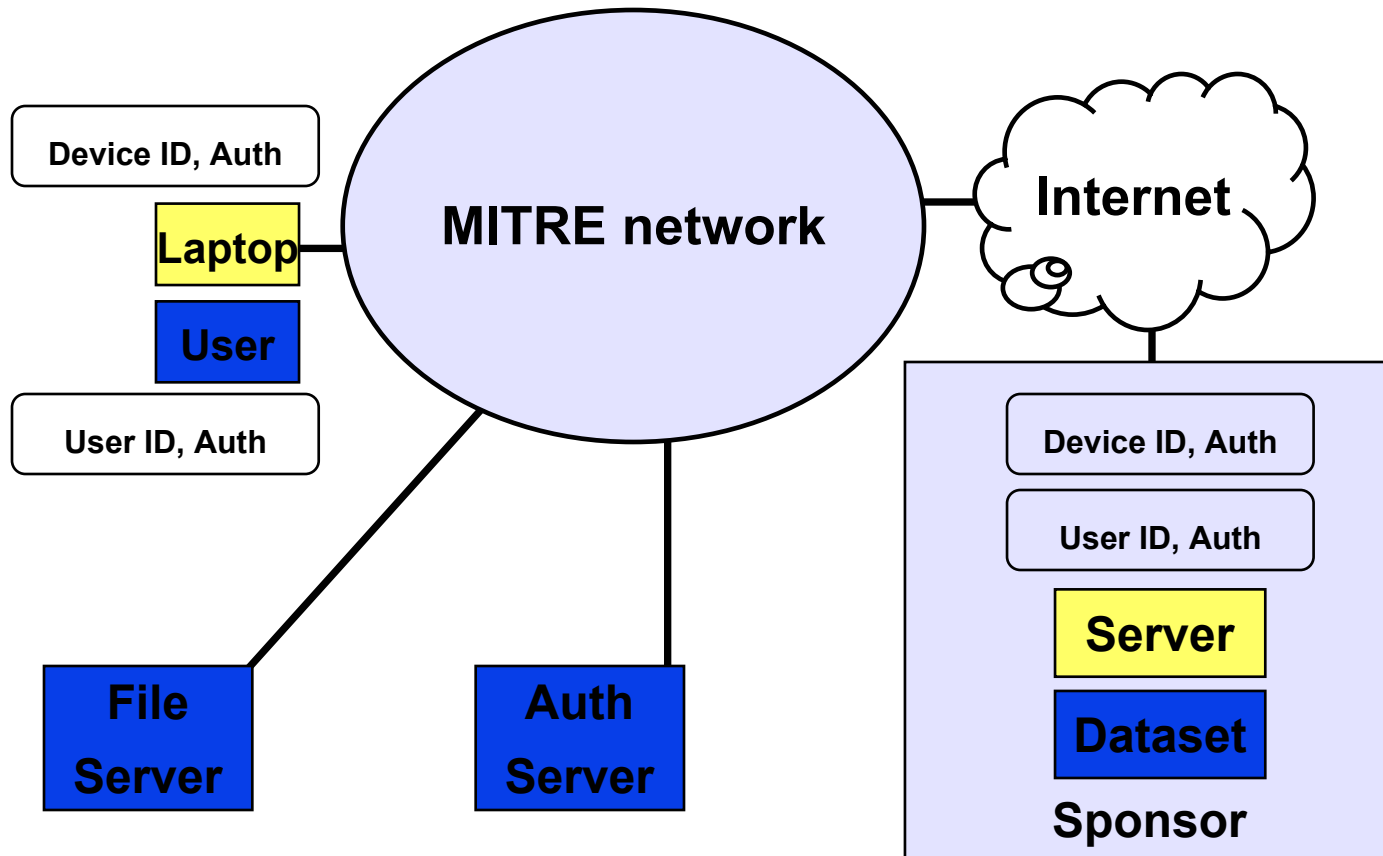
Objective

- **Achieve manageable trust using**
 - **TPM-supported protocols**
 - **Trust management**
 - **Integrity measures**

Activities

- **TPM access from Security-Enhanced Linux**
- **TPM-based protocols for authentication**
 - **Hardware identity, software configuration**
- **Trust management engine**
 - **Policy-based authorization**
- **TPM/IPsec integration for network layer enforcement**

Highlight

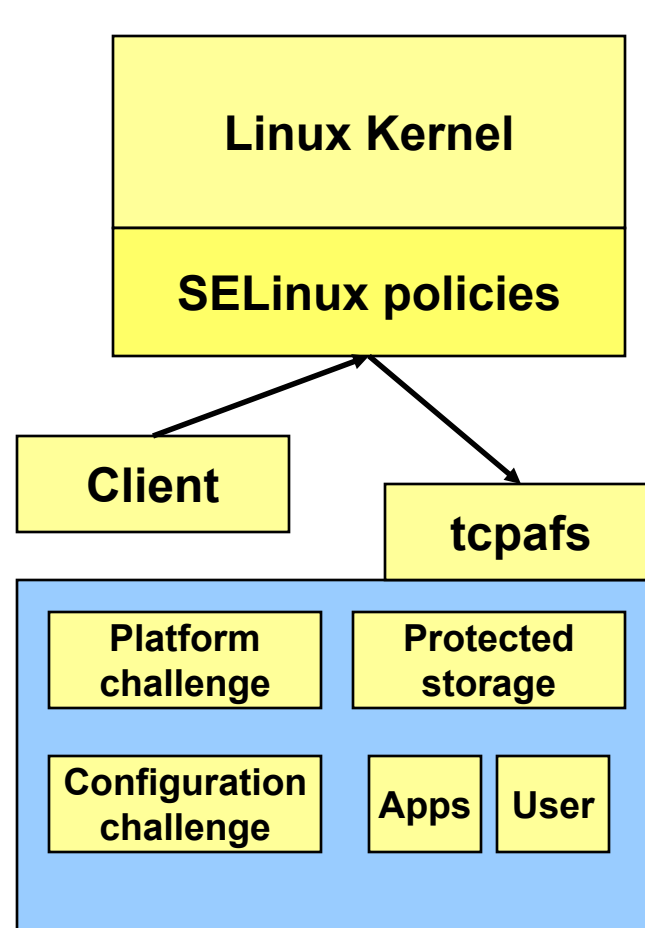


Authorizing a sponsor-owned laptop for use at MITRE

Demonstration

FS->L: MSIS, Req', N
L->MSIS: HSIS, Req', K_L
MSIS->HSIS: K_L, N
HSIS->MSIS: [K_L,N,group]K_HSIS
MSIS->L: TPMchallenge
L->MSIS: [challenge]K_L
MSIS->L: [K_L,N,group]K_HSIS
 [K_L,TPM ok]K_MSIS
 [K_HSIS, peer]K_MSIS
L->FS: Request + credentials

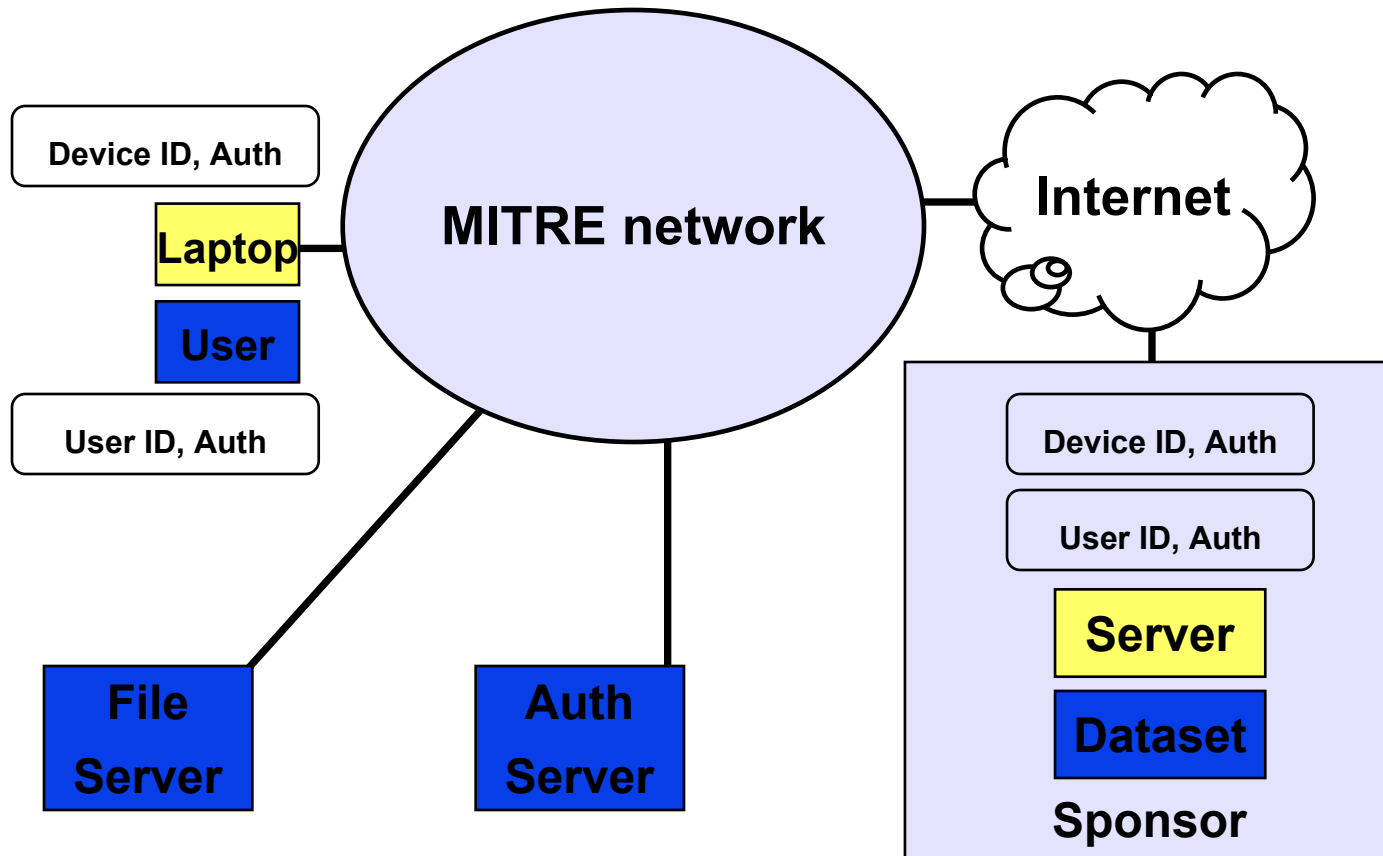
Protocol, client protection



Impacts

- Demo combines TPM, new protocols, trust management software, SELinux
- Collaborative relationships with TPM-based computer vendors
- Project goals support multiple sponsors
- Academic publications expected late FY03

Future Plans



Full mutual authentication, IPsec protection on data flows