

Enterprise-wide Security with Cryptographic Hardware Assistance

Joshua D. Guttman

781-271-2654 • guttman@mitre.org

Jay Carlson

781-271-2378 • nop@mitre.org

MITRE Sponsored Research

**MITRE
Technology
Program**

MITRE

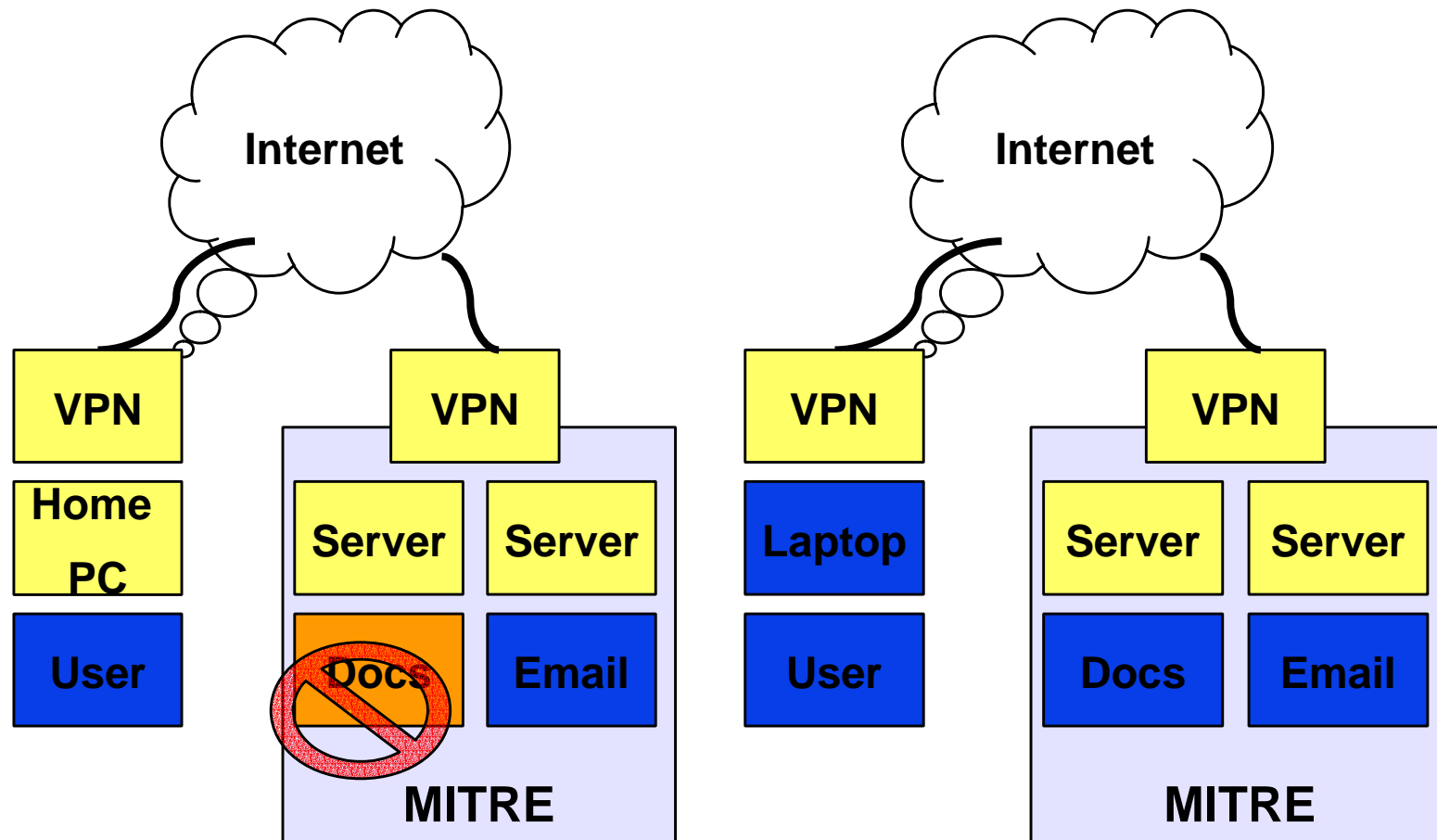
© 2004, The MITRE Corporation

Problem

- **“SSL is like an armored car delivering to someone living in a cardboard box.”**
- **Enterprises need *end-to-end* trust.**
- **Need cryptographic support and trust management**
 - **Trusted Platform Module (TPM) to be widespread**
 - **How to provide manageable services?**

Background

Access should depend on user, device, network path



Remote access policies: do you trust the remote system?

Objective

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

Activities

- **New trust management protocols for authentication**
 - **Hardware identity, software configuration**
 - **Implemented via TPM**
- **Theory for trust/protocol interaction**
 - **Protocol as trust coordination mechanism**
- **Collaborated with NSA, HP, IBM, and others**

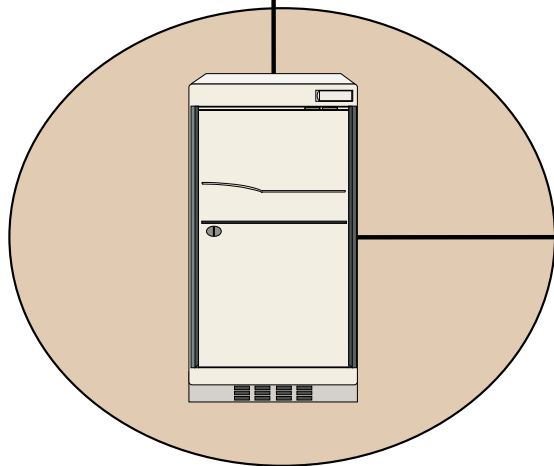
Highlight



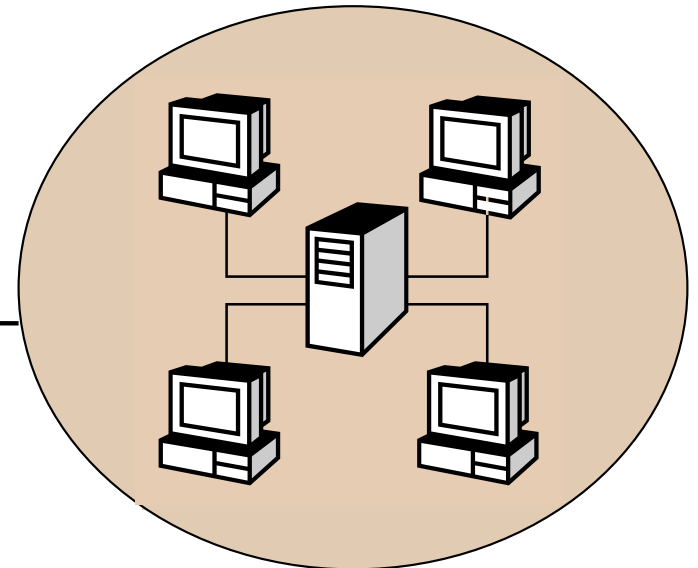
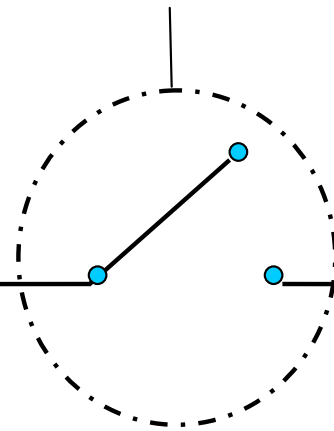
Assure laptop properly configured before providing access to corporate network

Anti-Virus Software

Up-To-Date?



Quarantined LAN

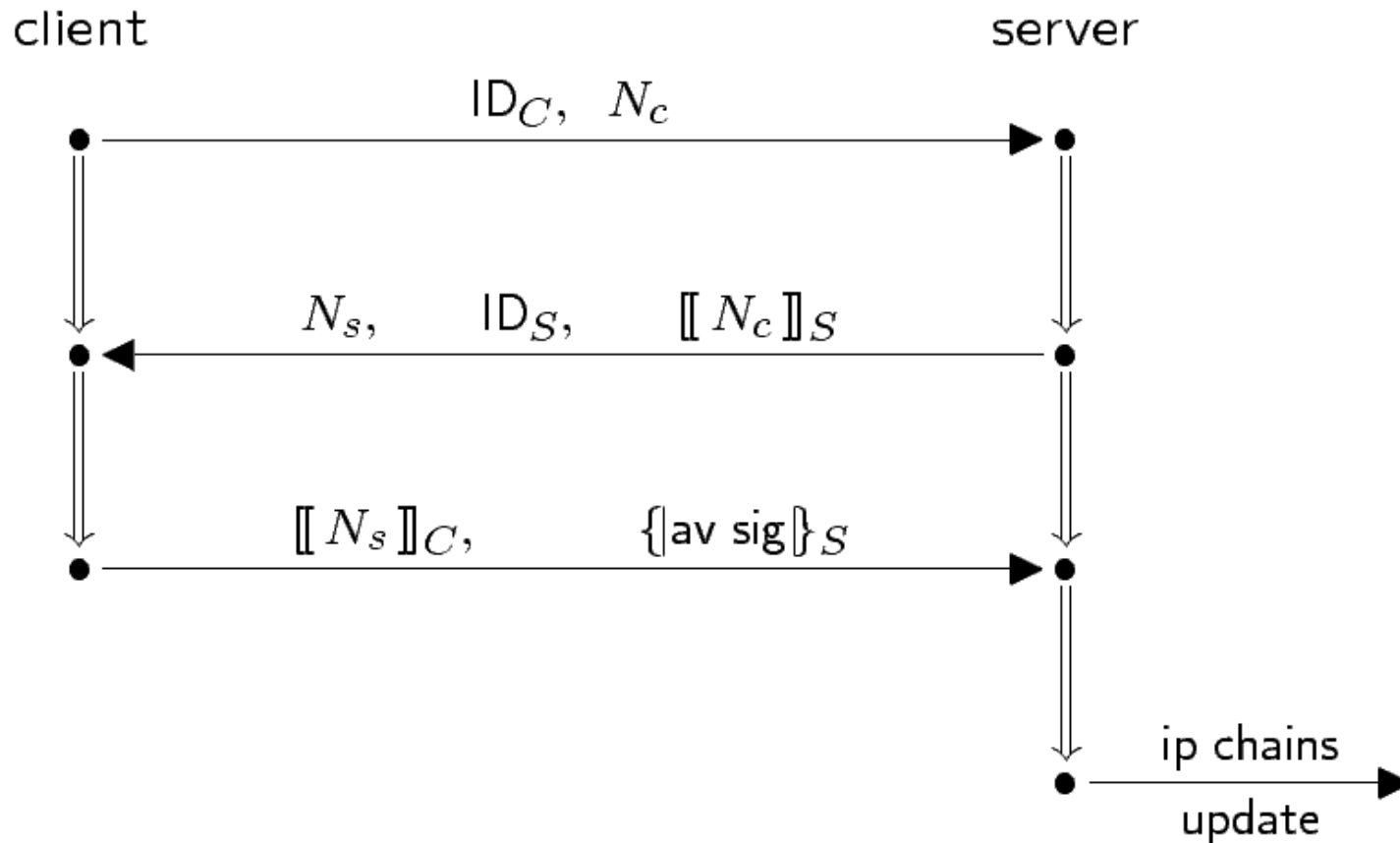


Corporate Network

MITRE

Demonstration

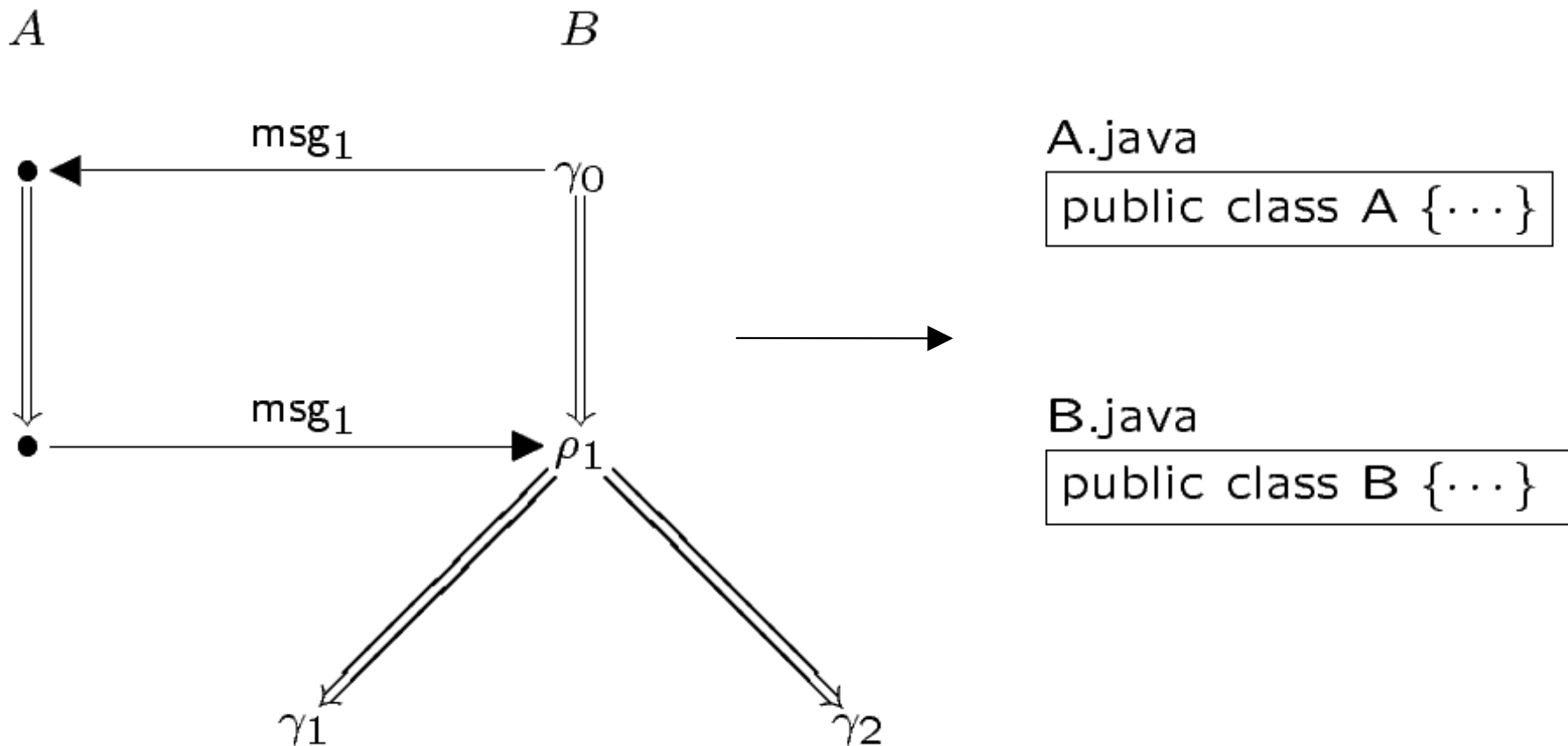
Protocol for laptop to prove antivirus up to date



Impacts

- **Demonstration combines TPM, new protocols, trust management software**
- **Collaborative relationships with TPM-based computer vendors**
- **Project goals support multiple sponsors**
- **Academic publication, lectures**

Future Plans



Compiler for cryptographic protocols with trust annotations