

Enterprise-wide Security with Cryptographic Hardware Assistance

Joshua D. Guttman

781-271-2378 • guttman@mitre.org

MITRE Sponsored Research

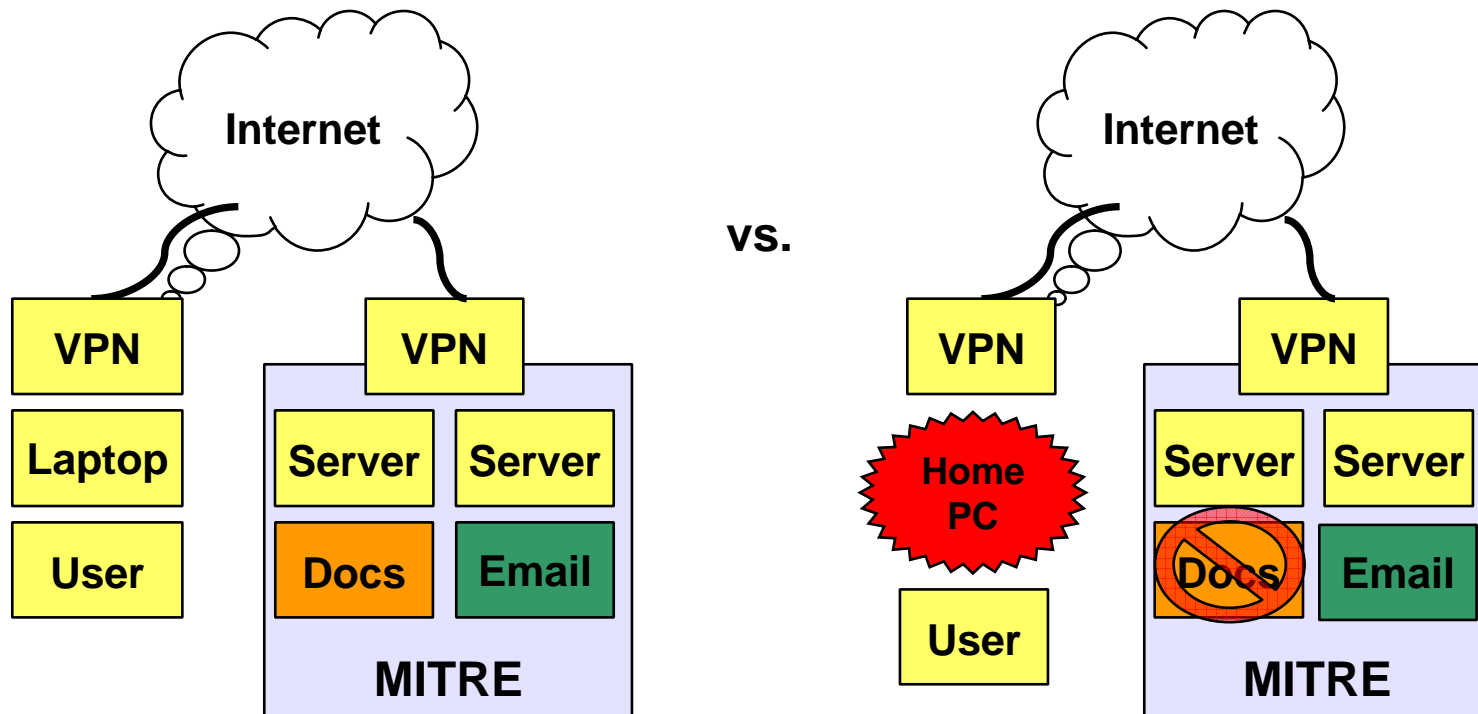


Problem

- “SSL is like an armored car delivering to someone living in a cardboard box.”
- Enterprise security needs *end-to-end* trust
 - Weak link: insecure hosts
- Need to base access-control decisions on host identity and configuration
 - Somehow combine with user, role, etc.
- How provide manageable services?

Background

Access should depend on user, device, network path



Remote access policies: do you trust the remote system?

MITRE

© 2005, The MITRE Corporation

Objective

Trust engineering

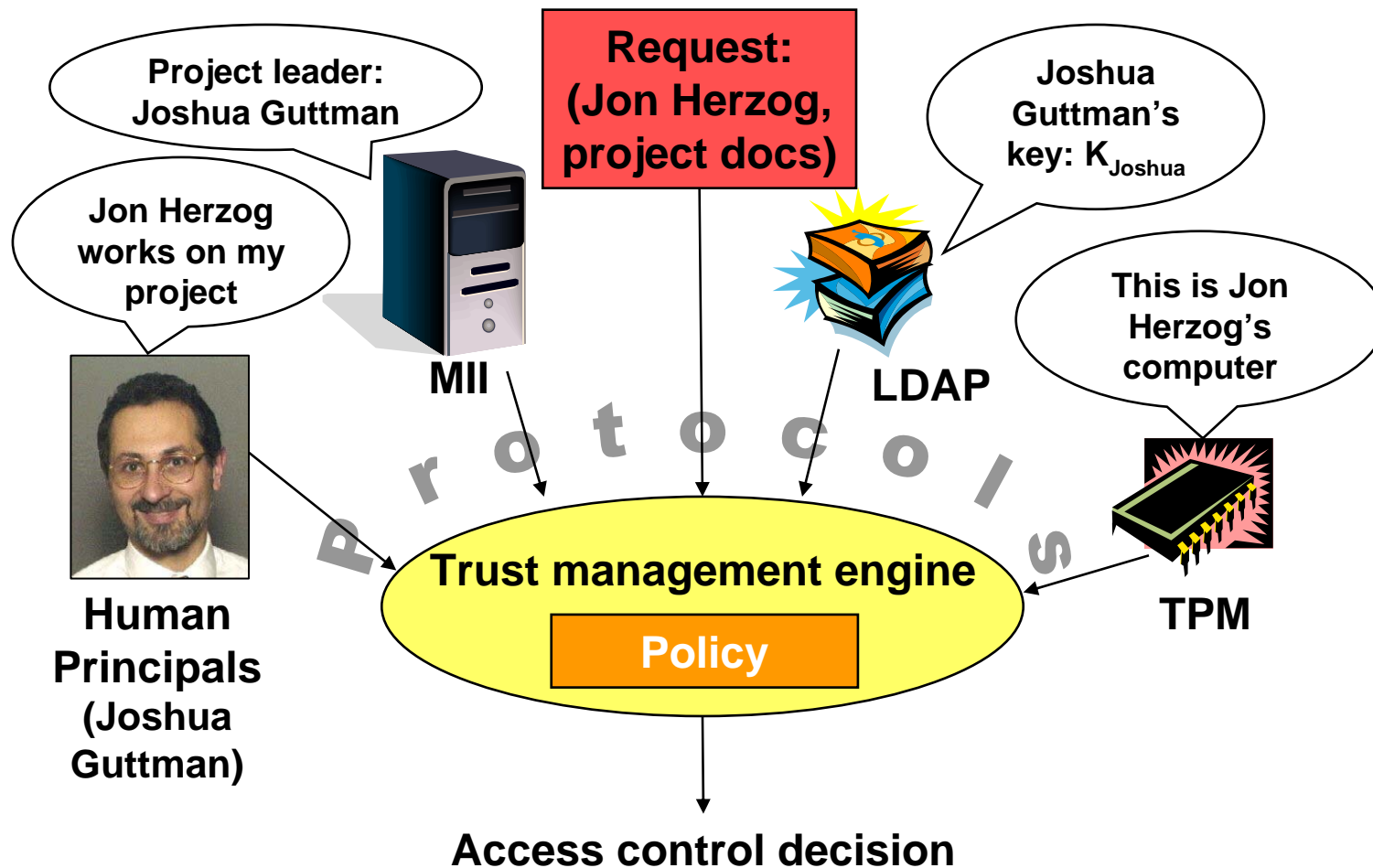
- **Anchor cryptographic protocols in trusted hardware**
 - TPM: Trusted Platform Module
- **Bind access control to protocols**
 - Authentication, confidentiality
 - TPM as trusted principal
- **Craft policies to reflect trust relationships**
 - Enterprise security goals determine access

Activities

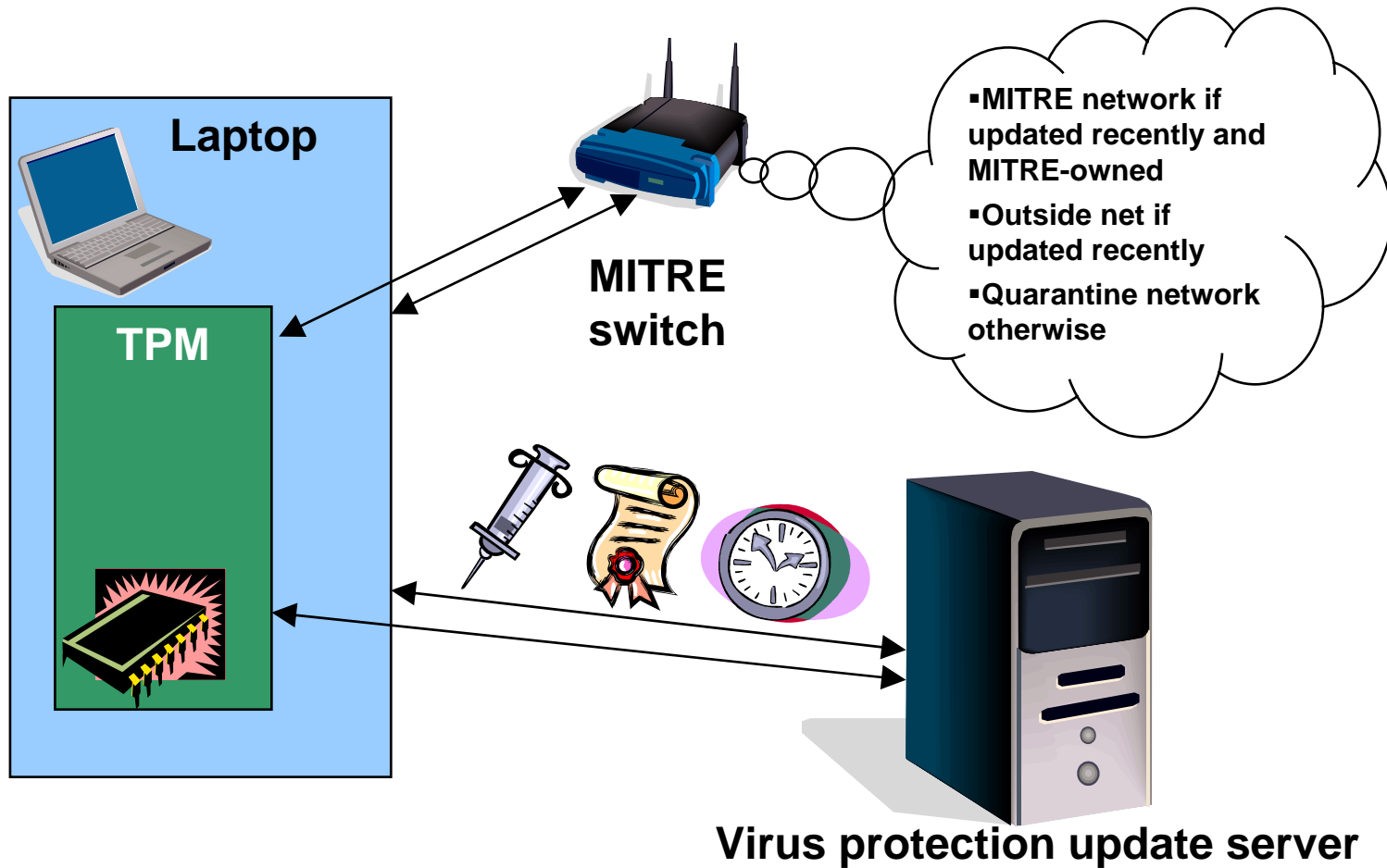
Cryptographic protocol programming suite

- **Cryptographic Protocol Programming Language (CPPL)**
- **Compiler**
- **Trust-management engine**
- **TPM access**
- **Solid grounding in theory**
- **Extensive vendor and academic contact**

Highlight



Demonstration



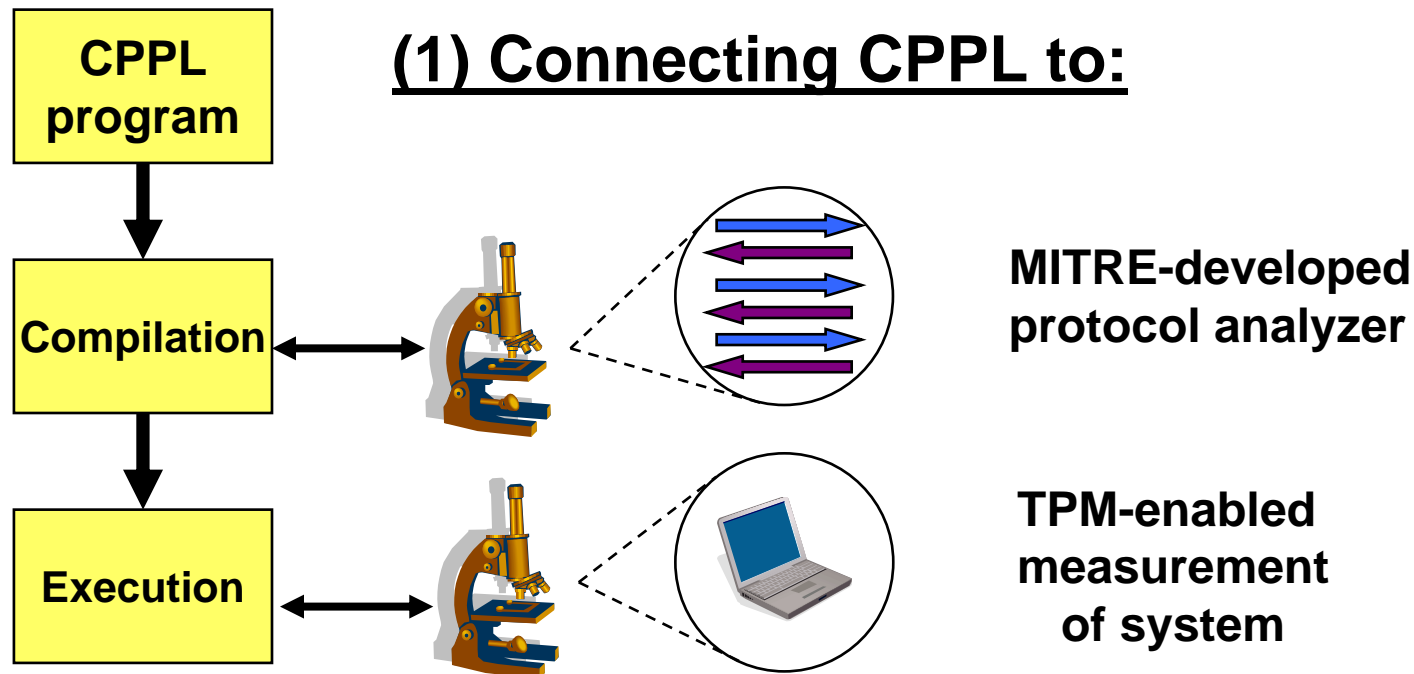
MITRE

© 2005, The MITRE Corporation

Impacts

- Usable programming language and compiler for cryptographic protocols
- Published papers and academic presentations
- Extensive conversation with vendor research labs
- Close interaction with new sponsored work

Future Plans



**(2) Tech transfer to research community,
sponsored work**