



# Systems and Internet Infrastructure Security

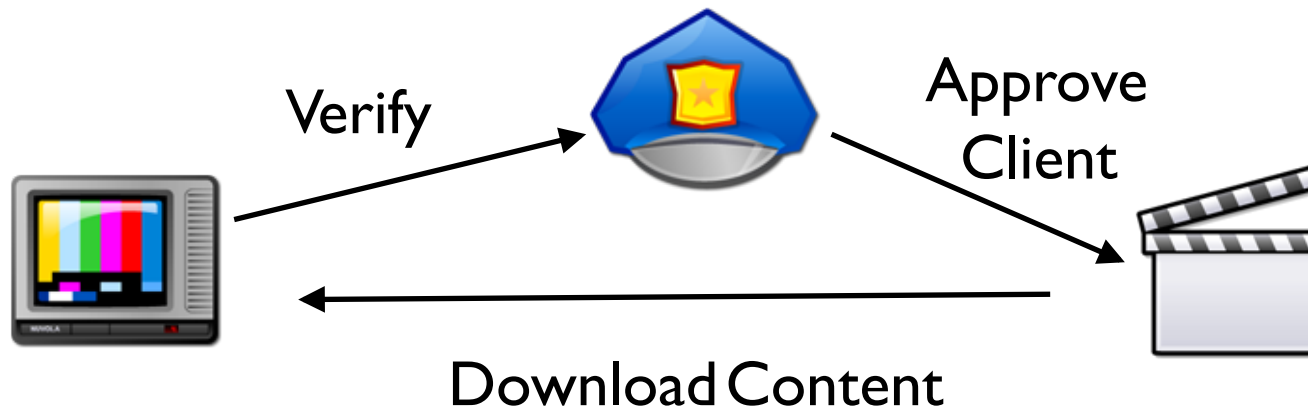
Network and Security Research Center  
Department of Computer Science and Engineering  
Pennsylvania State University, University Park PA

## Towards Practical Attestation: Challenges and Opportunities

Joshua Schiffman  
Trusted Infrastructure Workshop  
June 10, 2010

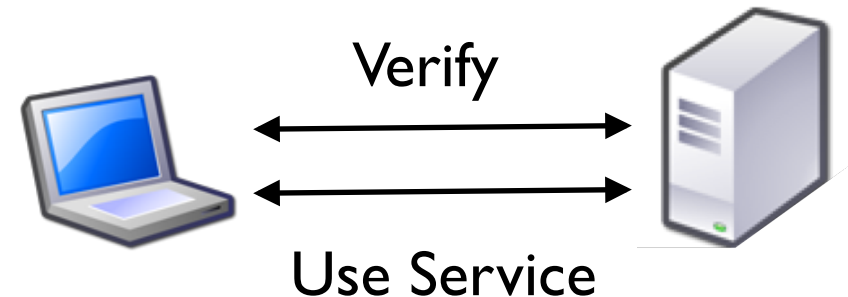
# What is it good for?

- TC originally designed to monitor **clients**
  - ▶ Monitor special purpose systems (media players)
  - ▶ Establishing trust in the client's environment
- Required the user to participate
- Lacking a PKI to identify machines



# Verifying Servers

- Servers have a **greater incentive** to use TC
  - ▶ Proof of the service's correctness
  - ▶ Supplement SSL Certificates
  - ▶ Large companies can manage internal PKI
- Adoption challenges
  - ▶ Performance
  - ▶ Privacy concerns
  - ▶ Don't want to be restricted by complicated processes



# Defining Integrity Goals

- Must first build *secure systems* before we can verify
- **Challenge**: Extract meaningful security properties from system configurations.
- What is a *secure system* or *high integrity*?
- Establish higher level properties
  - ▶ We can guide our design from *integrity models*
- Support various mechanisms

- **Challenge:** Verifying the **initial state** of the entire attestation framework
- Potentially large TCB to verify
  - ▶ Code and data
  - ▶ Need methods for assessing **dynamic** data
- Provenance of system to a **trusted origin**
  - ▶ Root of Trust for Installation [ACSAC '07]
- Alternative is to assess the impact of the data

- **Challenge**: Balancing verification and enforcement of security-sensitive events
- **Record** events for later verification
  - ▶ Verify after the fact
  - ▶ **Difficult to evaluate without context**
- **Enforcement** can reduce verification effort
  - ▶ Must verify enforcement **mechanism** and **policy**
- VM systems are even more complicated

- **Challenge:** Eliminating performance bottlenecks
  - ▶ ~ 1 second for TPM Quote
  - ▶ Late-launch requires substantial setup time
- **Must move hardware off of the critical path**
  - ▶ Use derived primitives, asynchrony, etc
- **Examples:**
  - ▶ Spork Web Server [ACSAC '09]
  - ▶ TrustVisor [S&P '10]

- Develop high level properties to verify
- Create attestation frameworks that are complete, but also simple to verify
- Build upon the TC primitives to improve performance

# Thank you

Joshua Schiffman ([jschiffm@cse.psu.edu](mailto:jschiffm@cse.psu.edu))

<http://www.joshschiffman.org/>

*SIIS Laboratory (<http://siis.cse.psu.edu>)*