Problem

- Internet services are on the rise
  - Local computing is becoming marginalized
  - We trust more remote systems with our data
- How do we protect ourselves from malicious input?
- SSL / IPsec
  - Protect our data in flight
  - Identify channel endpoints
- What about the integrity of those services?
Secure Communication

- SSL / IPsec gives us several protections
  - Confidentiality and integrity of data *in-flight*
  - Authenticity of endpoint

- Problems with those?
  - Identity assumes protection of secret key / good CA
  - Authentic malicious systems are still malicious
  - Protecting bad data still gives bad data
Verifying system integrity

• What would you do?
  ‣ Nothing
  ‣ Proof by authority (Certificates)
    • Tells you who, but not what
  ‣ Constrain the system (Secure Boot)
    • Effective, limiting, but proof is implied
  ‣ Inspect the runtime state (Authenticated Boot)
    • Flexible, attestable, but difficult to prove semantics
Secure Boot

- Check each stage in the boot process
  - Is code that you are going to load acceptable?
  - If not, terminate the boot process
- Must establish a **Root-of-Trust**
  - A component trusted to speak for the correctness of others
  - Assumed to be correct because errors are **undetectable**
Authenticated Boot

- Secure boot enforces requirements and uses special hardware to ensure a specific system is booted
  - Implied verification (Good because it is)
- By contrast, we can measure each stage and have a verifier authenticate the correctness of the stage
  - Verifier must know how to verify correctness
  - Behavior is uncertain until verification
  - Can you verify yourself?
- What is our root-of-trust?
TPMs

- Trusted Platform Module
  - PCRs, Keys, Counters, Crypto
- Remote attestation provides a report of the current system state
- Verifier checks if this is a trusted system state
Linking Integrity to Identity

- Assigned paper discusses several problems that arise when merging these two concepts together
  - Missing Link (cuckoo attack)
  - Compromised SSL Key
  - Verifying Multiple Certificates

- Virtualization

- How do these solutions revoke invalid certificates

- What does an invalid certificate mean?
Beyond Attestation

- Attestations only give a snapshot of system integrity

  - Attestations only give a snapshot of system integrity
  - Ideally, we should prove long term integrity
  - Why is this hard in general?
  - What must be true for this property to hold?
Take Away

• Secure communication alone does not prove data integrity

• Integrity measurement gives a client a view of the system’s integrity

• Linking the identity and integrity is possible

• Proving that integrity is long-lived is difficult