Topics in Systems and Program Security

Trent Jaeger
Systems and Internet Infrastructure Security (SIIS) Lab
Computer Science and Engineering Department
Pennsylvania State University

November 21, 2008
Evaluating Papers

• Due 12/5 5:00pm

• I want to know which three papers you found most valuable

• Value: contribute to your research
  ▶ Foundational techniques
    • How can these techniques be applied to your work?
  ▶ The content of the paper inspired new projects
    • What is the project and what results are envisioned based on this paper?

• Identify three such values – max one page each
Foundation

- What is the foundational concept?
  - Be precise

- How would you apply this concept to your work?
  - Outline the resulting system
  - Should make sense – architecture

- What difference would it make (potentially)?
  - What would you evaluate?
  - How might you evaluate?
New Project

• What concept in the paper did you find inspirational?
  ‣ Be precise
  ‣ Could be inspired because something could be improved – must be worthy of improvement

• What project do you have in mind?
  ‣ Outline the resulting system
  ‣ Should make sense – architecture

• What difference would it make (potentially)?
  ‣ What would you evaluate?
  ‣ How might you evaluate?
Bind Platform to TPM

• Key Requirement
  ‣ Need to be sure that the computation and the attestation originate from the same platform (physical machine)

• PGP public key distribution
  ‣ PGP Key Server
  ‣ Slips of paper

• Options for obtaining TPM public keys given physical access to the device
  ‣ Attach a code to the device – enables retrieval via Key Server or directly provides public key check
What about remote computers?

• Cannot obtain mapping to public key via physical access

• What is the requirement?
  ‣ TPM quote is from platform
  ‣ Computation is from platform

• Both must be verifiable as being from the same platform
  ‣ What do we need?
Secret with a platform

- We need to be able to authenticate the platform, so the platform statements can be associated.

- Option: Physical Unclonable Functions (PUFs)
  - Idea: manufacturing process introduces components that execute with random behavior (e.g., due to tolerances).

- Support challenge-response authentication
  - Stimulus==challenge: provide PUF with a stimulus and PUF responds with a unique response.
    - How do we verify that a challenge-response is valid?
    - How do we link two challenge-responses together?
    - How do we know that the two computations were done on the same platform?