CSE 490K

Physical Security and Computer Security

Dan Halperin, Jonathan Hsieh, Tadayoshi Kohno

Security Mindset

- The "security mindset" is > 1/2 of computer security; maybe much more than 1/2
  - Informal, heuristic, but seems to be true
  - Technical tools help, but are ineffective if used improperly
  - Need to think like the "bad guy"
    - But don't be bad (recall the Ethics Form)!
    - Every single line of code may be the target of an adversary
    - Adversaries may be foreign nations
    - Adversaries only need to find one way to "win"
    - …
  - Goal: Think like the "bad guy" -- at least spot problems, even if don't know how to fix

The "Bad Guys"

- Different types of bad guys
  - "Script kiddies"
  - ...
  - "Specialists"
- They think differently
- Suggestion: Study what the specialist might do, then scale back

The "Bad Guys"

- Specialists
  - Fully study the system
    - Don't attack system "randomly," but understand the inner workings
    - May have insider knowledge, collaborations
    - E.g., understand crypto, software security, how all the pieces of a "complex system" fit together
  - Think "outside the box"
    - Lots of "what ifs"
    - Anytime you see a line of code, or an interaction in a protocol, or some design, ask "What if...."
    - Recall: Many times a system will exhibit an unexpected behavior

Today

- Relate physical security to computer security
  - Locks, safes, etc
- Why?
  - More similar than you might think!!
  - Lots to learn:
    - Computer security issues are often very abstract; hard to relate to
    - But physical security issues are often easier to understand
  - Hypothesis:
    - Thinking about the "physical world" in new (security) ways will help you further develop the "security mindset"
    - You can then apply this mindset to computer systems, ...
  - Plus, communities can learn from each other

Picking Locks with Cryptology: Computer security meets the physical world

Matt Blaze

(Scientist, Safecracker)

University of Pennsylvania

mab@crypto.com

Not Online

- The following slides will not be online
- But if you're interested in the subject, I suggest reading
  - Blaze, "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks"
  - Blaze, "Safecracking for the Computer Scientist"
  - Tool, "Guide to Lock Picking"
  - Tobias, "Opening Locks by Bumping in Five Seconds or Less"