COMP7370 Advanced Computer and Network Security

Cold Boot Attacks on Encryption Keys (4)

Topics:

1. NSF CCLI-TUES'11 Conference
2. Homework 1, Question 1
3. Countermeasures

Topic 1: CCLI-TUES'11 Conf.

- About CS conferences/workshop
- CCLI-TUES'11 -> Conf. in other disciplines
- Feedbacks/Survey
- Computer Security: more than 20% projects
- CCLI-TUES Type 1 -> Type 2
- How to collaborate?

Topic 2: Homework 1, Question 1

- Features
- How to present your comparison table

Topic 3: Countermeasures

- Computer Security Research:
  - Many projects: < 10% motivation/threat model; > 90% solutions
  - Few projects: > 90% new threat models; < 10% solutions
  - How to determine which types of projects are better?
    - To copycat:
    - To innovate: Apple vs. Microsoft

- How to come up with good countermeasure solutions?
  - Understand threat models/problems
  - Understand attacking procedures
  - Break the link of an attacking procedure
  - Make a step in the attacking procedure difficult for hackers to launch attacks
  - Pros/Cons of each proposed countermeasures

- Scrubbing memory: (**5-min Discussions**)

Question: Describe three countermeasure ideas related to scrubbing memory?

  - Do not save keys in memory
  - Do not page out key to disks
  - Clear memory at boot time
  - **Attacker** moves DRAM to another PC

- Limiting booting from network or removable media
  - Boot from primary disk. Is it safe? No
  - **Attacker** swaps out this disk

- Suspending a system
  - Lock screen. Is it safe? No
  - Sleeping and hibernating modes. Safe? No if pwd is in RAM
  - Safe way: Key in DRAM = encrypt(External pwd)

- No precomputation
  - Precomputation speed cryptographic oprations
  - Keys are vulnerable (attack subkeys = redundant key information)

- Key expansion
  - Make it more difficult to reconstruct keys
  - How? More key transforms

- Physical defense
  - Physically protect memory (lock)

- Encryption in disk controller
  - No software, no key in DRAM
  - Key register in disk controller
  - Safe? When OS is booted, key must be erased in disk controller