CS 161: Computer Security
Midterm 2 Review

Part 2

November 1, 2006

Isolation and Sandboxing

Techniques for isolation

Sandboxing: Run code in a separate, isolated environment

- Like a kid in a sandbox: can build and destroy all he/she wants without affecting anything outside the sandbox
- Examples: virtual machines, physical isolation, interpreted code, chroot jail

Decomposition: Separate functions into independent modules

- Each module has minimal necessary privileges
- Modules do not trust each other
- Example from class: qmail

System call interposition: Intercept system calls

- Can allow or deny them based on policy
- Have full control over interaction with system

Random Number Generation

Randomness and crypto

- Basic requirement: unpredictability
- More than just statistical randomness
- Randomness necessary for crypto but hard to get right
- Numbers can’t depend on previous value, guessable value

Truly random vs. pseudorandom

Truly random

- From unpredictable source
- For example: radioactive decay, current fluctuations, low bits of high-precision clock
- Usually in short supply

Cryptographically secure PRNG

- Turn short seed into long sequence of bits
- Not distinguishable from truly random (or break crypto)
- For example: AES-CBC(seed, 0^n)
- Seed should be true random value w/enough bits (e.g. 2^{128})

Multilevel Security

Military model

- Document has three types of label:
  - *Classification:* Unclassified, classified, secret, top secret
  - *Compartmentalization:* Additional labels restricting access by topic/relevance
  - *DAC:* Distribution lists
- Bell-LaPadula model:
  - No information flow from high to low
  - Subjects/processes read down, write up
  - “Star property”: everything a subject touches is brought up to its security level

Covert channels

- Problem with Bell-LaPadula: other information leaks
  - Resource utilization, choice of values, timing, sound, etc.
  - Example: Morse code via CPU load
  - (Covert channels are also called side channels)
- Can’t remove entirely, but can restrict bandwidth
- This means systems run slower!

Miscellaneous

Other topics to brush up on

- Access control (MAC vs. DAC, etc.)
- Secure hash functions
- Fiat-Shamir zero-knowledge protocol (lecture 7)
- Needham-Schroeder (revised) protocol (lecture 9)