Final Review

Chengyu Song

Slides modified from
Administrivia

- Final exam
  - Wednesday, December 13, 7pm-10pm
  - Covers OS, network, web security and crypto
    - 1-1.5 hrs amount
  - Based on lecture and supplementary materials
    - Indicated as Preparation on the class schedule
    - Except those marked as Optional
  - Closed book. No additional sheets of notes
Types of questions

- Multiple choice
- Short answers
Final grade

• Breakdown
  • Lab: 45% (no change)
  • Homework: 2 x 7.5% = 15% (instead of 3 x 5%)
  • Midterm: 20% (instead of 15%)
  • Final: 20% (instead of 25%)
  • Participant: 5% bonus

• Based on percentile
Topics

- Malware
- Vulnerabilities
- Software Security
- Compartmentation
- OS Security
- Web Security
- Communication
- Cryptograph
- CIA
- Network Security
Security guarantees

• Confidentiality
  • Execution, data (memory, files), communication, etc
  • Attacks?
Security guarantees

• Confidentiality
  • Execution, data (memory, files), communication, etc
  • Attacks?
    • Process level: information leak
    • OS level: access control error
    • Network level: eavesdrop
Security guarantees

• Confidentiality
  • Execution, data (memory, files), communication, etc
  • Attacks?
    • Process level: information leak
    • OS level: access control error
    • Network level: eavesdrop
  • Defense Techniques?
Security guarantees

• Confidentiality
  • Execution, data (memory, files), communication, etc
  • Attacks?
  • Defense Techniques?
    • Memory safe, information flow control, etc
    • Better access control (software and hardware)
    • Encryption
Security guarantees

• Integrity
  • Execution, data, communication, etc
  • Attacks?
Security guarantees

• Integrity
  • Execution, data, communication, etc
  • Attacks?
    • Control-flow hijacking, injection attacks
    • Man-in-the-middle
Security guarantees

• Integrity
  • Execution, data, communication, etc
  • Attacks?
    • Control-flow hijacking, injection attacks
    • Man-in-the-middle
  • Defense techniques?
Security guarantees

• Integrity
  • Execution, data, communication, etc
  • Attacks?
  • Defense techniques?
    • Memory safe, input validation/escape, etc.
    • Hash, digital signature
    • Isolation (access control)
Security guarantees

• Authenticity
  • Access control, communication, etc
  • Attacks?
Security guarantees

• Authenticity
  • Access control, communication, etc
  • Attacks?
    • Confused deputy
    • Impersonation
  • Defense techniques?
Security guarantees

- Authenticity
  - Access control, communication, etc
  - Attacks?
- Defense techniques?
  - Capabilities, security token
  - Password
  - MAC (message authentication code), certificate
  - Biometrics
Security guarantees

- Availability (Not covered)
  - Attacks?
    - Denial-of-service
  - Defense techniques?
- Privacy (Not covered)
  - Attacks?
    - Tracking
    - Inference
  - Defense techniques?
OS security

• Compartmentation
  • Isolation
  • Principle of least privilege
• Access control
  • Complete mediation, tamper proof, correctness
• Defense in depth
• Keep it simple
Cryptography

- Perfect secrecy
  - One-time pad
- Block ciphers: PRPs and PRFs
- Modes of Operation: ECB, CBC, CTR
- Hash and collisions
  - MAC and HMAC
- Public-key encryption
Network security

- Protocol security
- Firewalls and IDS
- Off-path side-channel (will not examined)
Web security

- Password
- Background and same-origin policy
- Injection attacks
- Cross-site attacks