Secure Computer Systems

Midterm Review

Mustaque Ahamad, Ph.D.

Professor; Associate Director – Educational Outreach, Institute for Information Security & Privacy

College of Computing

Topics Covered so far & How to Demonstrate Mastery of Covered Topics

Georgia Tech

Before We Begin

Midterm Assessment Expectations

- Assess that you not only know and comprehend the concepts covered in class but can also apply, analyze and evaluate them
- Reading materials may seem to be overwhelming but should read them for deeper understanding
- We will briefly review all topics and look at sample exam questions

Getting Started, Design Principles, Memory Protection and Virtualization

Georgia Tech

Midterm Topics & Papers

Getting Started

- **Trusted Computing Base (TCB) & Requirements**
  - Tamper-proof, complete mediation and correctness
  - Reference monitor
- **What does "trusted" mean in TCB?**
  - Reflections on trusting trust
  - TCSEC paper
  - Attestation

Midterm Topics & Papers

- **Design Principles**
- All design principles discussed in lectures
  - What they are?
  - How they help in secure system design?

- Protection of Information Systems Paper, Section I

Midterm Topics & Papers

Memory Protection & Hardware Supported Isolation

- **Address spaces and address translation**
  - Processor execution modes
  - Privileged instructions
- **Segmentation and paging**
  - Hardware supported memory protection: SPL/PPL
  - Control transfer between privileged and non-privileged modes
  - Memory protection in 32 and 64-bit architectures

Midterm Topics & Papers

- **Memory Protection & Hardware**
- **Supported Isolation (TCB Requirement)**

- How does the hardware provide isolation for TCB from untrusted user code?

Midterm Topics & Papers

Virtualization

- Why virtualization?
- Type I and type II VMM
- Virtualization requirements

Hardware support for virtualization (VT-x)

- Root and non-root mode
- Address translation with VT
- Control transfer with VT (VM exit and entry)

Readings

- Virtualization paper available from Canvas
- Pentium virtualization paper – First 3 sections
- SGX Explained – up to page 15

Authentication

Midterm Topics: Authentication

- Basics including entropy, authentication methods, their implementation and evaluation
- Password hardening
    - Secret Sharing-based Implementation
    - Security Analysis
    - Entropy Estimation
- Smart card protocol outline
- Challenges of Biometric Authentication

Midterm Topics: Authentication

Authentication Readings

- Password hardening paper except sections that implement secret sharing with polynomial interpolation, exponentiation and vector spaces (basically, math)
- PIN-and-CHIP paper (Section I and II)

Access Control

Midterm Topics

- **Discretionary Access Control - DAC**

- Access Control Matrix
- ACLs and C-lists, their tradeoffs
- Access control implementation in Unix, Linux, Windows
- Setuid: Motivation and usage
- Java access control (Principals, Stack Introspection and doPrivilege Sections)
- Introduction to capabilities in Hydra

Midterm Topics

- **Discretionary Access Control – DAC**
- **Readings**

- Protection by Lampson
- Sections 1-6 of Unix paper
- Sections 1-3 of Windows paper
- Section 1-4 of Setuid Demystified paper (only Linux)
- Java paper (Policy Files, Stack Introspection and doPrivilege Sections)
- Sections 1-6 of Hydra chapter (Objects and Capabilities, Sharing, Revocation and Protection Problems)

Midterm Topics

Mandatory Access Control - MAC

- Motivation
- Labels, Comparison etc.
- BLP Model
- Biba Model
- RBAC
- Clark-Wilson Policy
- Chinese Wall Policy

Readings

- Sections 6.3 to 6.5 of Gasser book, RBAC and Clark-Wilson papers

Sample Questions on TCB, Design Principles and Virtualization

Sample Question 1

Q1: TCB Requirements

- Tamper-proof, complete mediation and correctness
- Rowhammer allows user code to flip a bit in system data so tamper-proof requirement is violated

Sample Question 2

- **Q2: Design principles**
  - Least privilege – process must execute with the fewest privileges with which it can complete its execution
  - Fail-safe default – deny unless explicitly granted
    - Least privilege does not imply fail-safe defaults. Just because you need access to a resource (thus, no conflict with least privilege) does not mean you can have the access right when it is not granted

Sample Question 3

(a) X86 protected mode: Any data and code cannot be accessed when CPL = 0 but RPL is set to a higher value. Max (CPL, RPL) <= DPL of target segment. Kernel data/code have DPL = 0

(b) Type I hypervisor runs in ring 0 in the absence of virtualization so OS cannot run in ring 0. With virtualization, it is possible because hypervisor runs in ring -1 (or ring 0 of root mode)

(c) Enclave code in SGX runs in ring 3. Hardware protects enclave memory from access by non-enclave code, including hypervisor

(d) CR3 cannot be loaded by non-privileged instructions. EIP can be loaded as it is updated on user call function calls and returns

Sample Questions on Authentication and Authorization

Georgia Tech

Sample Question 4

(a) Access to a sequence of instruction tables does not allow inference about distinguishing features because both columns are updated after each login.

(b) 32 bits of entropy from password. Number of features will be 15. Best case 15 bits of hardening entropy. Worst case no added entropy if everyone has the same feature vector. Thus, 47 bits or approximately 32 bits.

(c)

- I – Record and replay audio
- II – No
- III – Liveness detection. Ask to say a new phrase (called text dependent)

Sample Question 5

(a) Real id could be different when another process P’ has access to execute F. Effective UID will be U.

(b) Negative ACEs can be ordered ahead of positive access ACEs. Hashing does not follow such order. Answer is no.

(c) We will need *n* common objects, one for each other users with which we share the object, for selective revocation from any subset of the sharing users.

Sample Question 6 Pt.1

(a) Simple: Reader's label must be the same or it should dominate the label of the object that is to be read

Star: Writer's label should either be the same or it should be dominated by the label of the object being written

- Checkout should be treated as a read. Thus, simple property applies
- Check-in should be treated as a write. Thus, star property applies
- Explain the answers for full credit.

Sample Question 6 Pt. 2

(b) Chinese Wall Policy addresses conflict of interest (CoI)

- Documents have company labels
- Conflicting companies must be identified (e.g. Bank of America and Wells Fargo)
- Storage server must keep track of companies whose documents a user has accessed.
- For a checkout request, it must be granted only when the requested document belongs to a company that does not conflict with companies of documents that have been checked out by the requestor.

Summary

Summary

**Start with slide decks and videos,
read suggested sections of papers for
deeper understanding**

Midterm Assessment Goals

- Recognize and Recall topics covered in lectures
- Apply, analyze and evaluate the concepts covered in lectures