Final Review Guide

Logistics

- Finals Week Monday, June 6th, 11:30am - 2:30pm
- On Gradescope
- Zoom + Camera
- Open course material (notes, lecture slides, discussion slides, etc.)
- Close Internet (no Google, etc.)
- Use Piazza for clarification
- Final will cover everything

TL;DR

- PAs
  - Should be able to re-do and explain everything
- Attack
  - What is it attacking? What is its goal?
  - Prerequisites?
  - How does it work?
  - How to mitigate?
- Mitigation
  - What is it mitigating?
  - How does it work?
  - Any trade-off?
- Concept
  - Definition
  - Example

The Security Mindset

- Assets
- Properties (CIA triad)
- Adversaries, Risk assessment (Threat Model)
- Countermeasures
- Costs/benefits
- Should be able to analyze these for most attacks/defenses learned in this quarter

Low Level Security

- Stack layout
- Stack vs. Heap vs. Data vs. Text
- Some x86 instructions
- Purpose of common registers
- C function calls
- Exploits in PA1
  - What are the bugs?
  - How to exploit those bugs?
- Should be able to re-do PA1

Low Level Security Common Attacks and Defenses

- Return-Oriented-Programming (ROP)
- User-After-Free (UAF), Dangling pointer
- Canaries
- ASLR
- W^X
- Should be able to describe
  - Their purpose
  - How they works

More Low Level Defense (Not on final)

- Control-Flow Integrity
  - Makes sure control can only flow to legitimate places
  - Coarse grained vs. Fine grained
- Shadow Stack
  - Separate control stack and data stack
- Both are supported by latest CPU hardware

Isolation

- Six Principles of Secure System Design
    - Definition
    - Example
- Process memory isolation
- Unix permission system (ACL and uids)
- ACL vs. Capabilities
- Software-Fault-Isolation (SFI)
    - Kernel
    - Browser
    - VM
- Should be able to give definition and examples

Side Channel

- Cache timing side channel attacks
  - Basic idea
- Mem and Time hack in PA2
  - Should be able to describe steps
- Mitigation
  - Name a few

Web

- HTTP
  - Methods
  - Common/security-related headers
  - Common status code
- Cookie
  - Purpose
  - How to set and use
  - SameSite

Web

- Browser
  - Load and execute content
  - Frame and iFrame
  - Document Object Model (DOM)
  - DOM and JS
  - Same Origin Policy (SOP)
- HTML
  - Just some common tags and attributes

Web Attacks and Defenses

- Phishing
- Client-Side Injection
  - Cross Site Scripting (XSS)
- Server-Side Injection
  - SQL Injection
    - SQL basics
    - Mitigations
- Cross Site Request Forgery (CSRF)
- Should be able to do these by hand

Network

- Layers
  - Application
  - Transport
  - Network
  - Link
  - Physical
- IP
  - Addresses
  - IPv4 vs. IPv6
- TCP
  - 3-Way Handshake
- Basics of other protocols mentioned (ARP, BGP, UDP, etc.)
  - Purpose and layer
- Common ports

Network

- DNS
  - Purpose
  - Hierarchy
- Basics of attacks
  - Eavesdropping
  - Injection
  - Spoofing
  - Misdirection
  - etc.

Network

- Basics of defenses (basic idea + pro/con)
  - Firewalls
    - Default allow/deny
  - NIDS
  - Honeypots
- NAT
  - Purpose
  - Pro/Con

Crypto

- Symmetric-key
  - Block Ciphers
  - Hash Function (MD5, SHA1, SHA2, SHA3)
  - MAC
  - What property do they give?
- Public-key (should be able to do these by hand)
  - Diffie-Hellman Key Exchange
  - RSA
  - RSA Signatures
  - Bleichenbacher RSA Signature Forgery

Crypto

- TLS, SSH, IPsec
- Constructing a secure encrypted channel
- Public Key
  - Trust On First Use (TOFU)
  - Certificate Authority (CA)
  - Web of Trust (e.g., PGP)
- TLS + DH key exchange

Authentication

- Protecting Password
- One-Time Passcode
- Biometrics
- Good/Bad Examples + possible attack

Privacy & Law

- Kinds of privacy
- Anonymous Communication Challenges
- PGP
- TOR
- Principles
- CFAA, DMCA, etc.