CSC 481/681/781 Principle of Computer Security Review

01 Terminology and Goals

Key points

- CIA Goals (**1 multiple choice, 1 Short Answer questions**)
- Secure Design Principles (**1 Short Answer questions**)
- Basic Terminology (**1 multiple choice**)
    - Vulnerabilities
    - Threats
    - Attacks & Attackers
    - Security Model
    - Defenses

02 Security (Access Control) Models

Key points

- Basic Terminology (**1 multiple choice**)
    - Subjects
    - Objects
    - Actions
    - Permissions
- Policy-based access-control models (**1 Short Answer questions**)
    - Bell–LaPadula (BLP)
    - Biba Model
    - Chinese Wall (Brewer-Nash)
- Non-policy-based access-control models (**1 multiple choice**)
    - Access Control Matrix Model
    - Role-Based Access Control (RBAC)
    - Capability-Based Model

03 Cryptograph

Key points

- Foundations
    - Common Attacker Capabilities (**1 multiple choice**)
        - Ciphertext-Only Attack (COA)
        - Known-Plaintext Attack (KPA)
        - Chosen-Plaintext Attack (CPA)
        - Chosen-Ciphertext Attack (CCA)
    - Brute Force (**1 multiple choice**)
        - Number Sizes
        - Brute force time/keysizes Computation
    - Probability Theory
        - Birthday Problem
        - Shannon's entropy & Guessing entropy
    - Indistinguishability in Cryptography (**1 multiple choice**)
        - A Chosen Plaintext Game
        - A Chosen Ciphertext Game
- Classical Cipher
    - Permutation Cipher
        - Scytale Cipher
    - Substitution Cipher
        - Caesar Cipher (Single-table Substitution)
        - Vigenère Cipher (Polyalphabetic Substitution)
    - One-Time Pads (OTP)
- Secret Key Cryptography (Symmetric Ciphers) (**1 Short Answer questions**)
    - DES, AES
    - Different modes
        - Electronic Codebook (ECB)
        - Cipher Block Chaining (CBC)
        - Counter (CTR)
    - Padding Oracle Attack
- Public Key Cryptography (Asymmetric Ciphers)
    - Public Key Characteristics
    - Diffie-Hellman Key Exchange (DHE)
    - RSA (**1 Problem-solving question**)

- Hash Functions (**2 multiple choice**)
    - Hash Collisions
    - Message Authentication Code (MAC)
    - Hash Function Properties
        - Preimage resistant
        - Second Preimage resistant
        - Collision Resistant
    - MD5, SHA-512
    - Brute-Force Attacks
        - Rainbow Table Attack

04 Physical Security

Key points:

- Physical Security for Storage Devices
- Physical Security Controls (**1 multiple choice**)
    - Deterrent controls
    - Detective controls
    - Preventive controls
- Data Backup (**1 multiple choice**)
    - Full backup
    - Incremental backup
    - Differential backup

05 Operating System Security

Key points:

- Separation concept (**1 multiple choice**)
    - Protection rings
- Process Memory (**1 multiple choice**)
    - Virtual Memory
- Buffer overflow
- Attacks on Boot Sequence
    - Blue Pill
    - Mobile: Unlocking bootloaders
- Filesystems
    - Access control
- Isolations

    - Sandboxes
    - Virtual Machines
    - Modern Containers: Docker

06 Software Security

Key points:

- Basic Terminology (**1 multiple choice**)
    - Software bugs, Software vulnerabilities
    - zero-day vulnerability
    - Software security
- Secure Software Design Principles
- Stack Smashing Protections (Buffer Overflow) (**1 multiple choice**)(**1 Problem-solving question**)
    - Don’t return if return address has been overwritten
        - Canary
        - Write-protect memory to monitor writes
    - Make it so uploaded data is non-executable data
        - Return-Oriented Programming (ROP)
    - Make it so attacker doesn’t know address of attack code
        - Address Space Layout Randomization (ASLR)
- Integer Overflow
- Static Analysis
    - Symbolic execution (**1 Problem-solving question**)
    - Dataflow analysis
- Dynamic Analysis
    - Fuzz Testing (**1 multiple choice**)
        - Mutation-Based Fuzzing
        - Generation-Based Fuzzing
        - Evolutionary Fuzzing
- Malware (**1 multiple choice**)
    - Virus, Worm, Trojan Horse,Botnets

07 Web Application Security

Key points:

- Web application structure
- HTTP - Slow Loris Attack
- Static HTTP Page Request
    - DocumentRoot
    - VirtualHost
    - Permissions
- HTTP “State” (**1 multiple choice**)
    - Cookies
        - Session Hijacking
- HTTPS
    - SSL/TLS
    - HTTPS Client Authentication
- Document Object Model (DOM)
- Same-Origin Policy (SOP) (**1 multiple choice**)
- Cross-Site Scripting (XSS) (**1 multiple choice**) (**1 Short Answer questions**)
    - Stored XSS
    - Reflected XSS
    - DOM-based XSS
- SQL Injection

08 Network Security

Key points:

- Types of Networks:
    - PAN, LAN, CAN, MAN, WAN
- TCP/IP model (**1 multiple choice**)
    - Hub
    - Switch
        - MAC address
        - MAC table
        - MAC Flooding Attack
    - Internet Addresses (**1 multiple choice**)
        - IPv4, IPv6
        - Address Resolution Protocol (ARP)

        - ARP Spoofing
        - Smurf Attack
    - UDP
        - UDP flood DDoS attacks
    - TCP (**1 multiple choice**)
        - The 3-way handshake
        - SYN Flooding
        - Predictability attack
        - The Mitnick Attack
    - Domain Name System (DNS) (**1 multiple choice**)
        - Cache Poisoning
    - Firewalls (**1 multiple choice**)
        - Stateless
        - Stateful