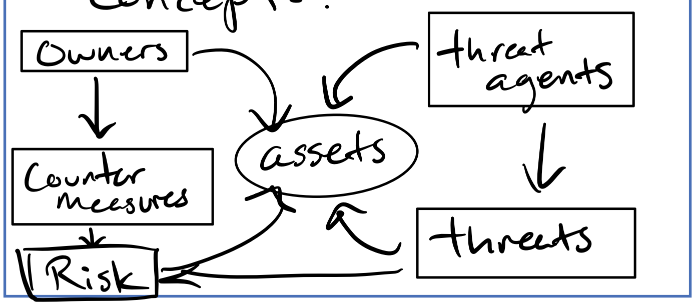
CPSC 253 Review Session Topics

Ch. 1. Fundamental Security Concepts:



- Security Concepts & Relationships
- Threats & Attacks
- 3 states of data: at rest, transit, in use
- types of storage: hot, cold, archive
- Security Policy, Implementation, Evaluation

Ch. 2 Cryptography & Encryption

RSA: $m = c^d \bmod(n)$

- Asymmetric vs. Symmetric Encryption and their algorithms
- Stream Ciphers
- Hashing
- Public-key Infrastructure
- Random v. Pseudorandom
- Cryptographic methods
- RSA formula

Ch. 3 User Authentication

x5;G721

(Superman)_(batman)_(flash)

$\frac{H(\text{Superman})}{55}$ $\frac{H(\text{batman})}{900}$ $\frac{H(\text{flash})}{20}$

- user has, is, knows, does
- Authentican Principles
- Password-based, token-based, biometric, remote auth
- MFA
- Password vulnerability & cracking
- Bloom Filters

Ch. 4 Access Control

ACM:

	user 1	user 2	user 3
File1	write	owner	execute
File2	read	execute	owner
File3	owner		read

- Types of access controls
- File/Perm. access control (rwxrwx) unix 777
- IAM: Identify & Access Management
- Identity Federation & Providers (IdP)
- Open Identity Trust Framework
- How cybersecurity applies in Identity
- Access Control Matrix
- Whitelist v. Blacklist
- user v. application permissions

Ch.5 Data Center & Database Security

- What is DMS? What is Relational DB?
- SQL, SQLi, SQLi countermeasures
- Database encryption
- Requirements of TIA-492
- Primary key v. Foreign key
- SQL commands (SELECT, DROP, ...)
- inferential, out-of-band, blind attacks

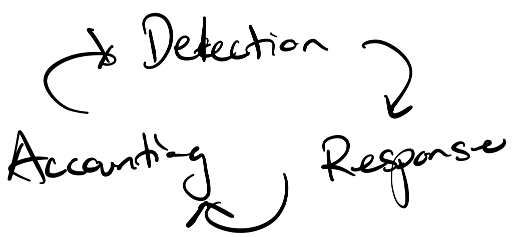
Ch.6 Malicious Software

- Types of Malware
- APTs : Advanced Persistent Threats
- Propagation Types
- Social engineering, watering hole, phishing
- Morris Worm & why its signifcant
- Logic Bombs (conditional viruses)
- Countermeasures
- Wanna Cry, Stuxnet

Ch.7 DDos (Denial of Service Attacks)

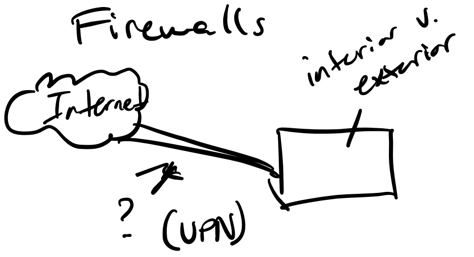
- What is Dos? What is DDos?
- Flooding (ICMP)
- Bots & botnet (zombies)
- Control & command

Ch.8 Intrusion Detection



- Intruder behavior
- Anomaly Detection
- Signature & Heuristic Detection
- IDS (NIDS, HIDS, hybrid)
- Logging, Syslog
- SIEM, SOARS, Snort
- Honeypots

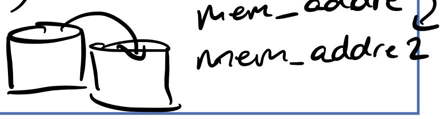
Ch.9 Intrusion Prevention & Firewalls



- Types of Firewalls
- Circuit-Level Gateways
- Host-based firewalls v. Physical firewall
- DMZ & VPNs
- IPS (HIPS, NIPS, hybrid)
- Snort can be IPS too

Ch. 10 Buffer Overflow

```
int[] = new int[9]
 read(10!)
[0][1][2][3][4][5][6][7][8]
read(   )
```



- What is Buffer Overflow
- Defenses on Buffer Overflow
- Heap Overflows

Ch.11 Code Security

- Handling Inputs
- Error Handeling
- Input Validation
- Safe Coding Practices

Ch.12 OS Hardening/Security

- System requirements & planning
- User account configuration
- Backups
- Patch management, logging, chroot jail
- Windows v. Linux security
- Sandboxxing w/ virtualization

(Not be tested for Final)

Ch. 13 Cloud Security, IoT

EX??

- Cloud Service Models
  - Cloud Types (public, private, commun)
- Security approaches to cloud
- What is IoT? (Internet of Things)
- IoT vulnerabilities

Ch. 14 IT Security Management & Risk Assessments

- What is baseline?
- Types of approachs to Risk assessment
- what is risk appetite?
- Categories /areas of risk (classification)
- Analyze, Evaluate, Treat Risks ←
- Plan - Do - Check - Act Process Model

Ch. 15 IT Security Controls, Planning, Procedures

- IT Security Plan
- Security Awareness Training & why
- Incident Handling
- Security compliance
- Security controls : operational
management
technical

↳ preventive, detective, supportive

Ch. 16 Physical Security

- Physical Security Threats
- Environmental threats
- Disaster Recovery from Physical
- Logical, Physical, Premises securities

Ch. 17 HR security

- Email Practices of Security
- Disgruntled employees
- Incident Response Teams
- Awareness v. Training v. Education
- Policy development
- Information flow

Ch. 18 Security Auditing

- Security Audit & why?
- Audit trail
- Logging functionality
- Compliance & regulatory obligations

Ch. 19 Legal & Ethics

- cybercrime
- law enforcement responses
- IP (intellectual property) & its laws
- Privacy & its laws
- Ethical Issues in Security
- Black v. Gray v. White Hat
- trademark v. copyright v. patent

Ch. 20 Symmetric Encryption

- Symmetric Encryption Types
- ECM (electronic codebook model)

focus w/ ch 2

Ch. 21 Public Key Cryptograhy

- SHA hashs
- Salting
- Diffie-Hellman Key Exchange
- RSA algorith

- overlaps w/ ch 2

Ch. 22 Internet Security Protocals (IPSec)

- TLS (transport layer security)
- TCP / UDP
- SSL (Secure Socket layer)
- IPv4 v. IPv6 securities
- Transport & Tunnel modes
- Port & protocals (know the common ones)
- DKIM (Domain-Keys) [Email]

Ch. 23 Internet Authentication Applications

- Kerberos Protocal
- Public key auth.

Ch. 24 Wireless Security & mobile security

- Wireless security threats & measures
- 802 protocals & infrastructure
- wireless types
- Discovery, Authentication, Key management
- PSK (pre-shared keys)

Ch. 25 Linux Security

- File permissions
- Terminal vs. GUI operations
- differences between UNIX & Windows

refer to OS Hardening topics

Ch. 26 Windows Security

- Registry
- User privilidge escalation (UAC)
- Windows vulnerabilities
- windows-only measures (e.g. BitLocker) TPM
- Trusted Platform Module

refer to OS Hardening topics

(not in final, maybe EC??)

Ch. 27 Trusted Computing (Models)

- Bell-LaPadula model
- what is a computing model?
- Biba Integrity Model
- Chinese wall model
- Clark-wilson model
- Trojan Horse Defence

Miscellaneous / lecture (Labs/HW)

- Active Directory & its role
- explain what VMNet10 was & why?
- lab tools (Kryptos, John the Ripper, ...)
- bash scripting (eg. shebang)