

Final Review

Spring 2009

Topics covered this half

Security & Risk Assessment – Chapter 10

Crypto Part I

Distributed Systems Authentication (Diffie Hellman /

Network Admin Security

Database Admin Security

New Access Control Paradigms (Java)

Pen Testing

Crypto – DES & AES

Information Warfare

Software Security

Security Evaluation

Know definitions:

Trusted Computing Base

Evaluation / Certification / Accreditation

Orange Book Classes (pp.174-175)

Common Criteria – Evaluation Assurance
Levels (EAL1-7) (pp.180-181)

Diffie Helman

Man-in-the-middle attack (p.216)

Replay attack (aka Denning-Sacco attack)

Kerberos Security (p.220)

Diffie Helman – be able to “work it” for a simple prime example with provided generator

Network Security

Threat models

- organizational threat modeling (sum of the parts)

Firewalls

- what is “stateful inspection”
- Describe “perimeter security”
- what is the problem with perimeter security?
- what is the function of a DMZ?

IDS vs. Firewall

- network-based IDS vs. Host-based IDS

What is the weakness of IDS? (signature-based – same as Virus-detection)

Database Security

How does a “View” help security?

Difference between “OS Access Control” and “DB Access Control”?

Describe a “statistical attack”

New Access Control Paradigms (Java)

Difference in Access Control (what is the “principal” vs. what is the “object”?)

What is a “Sandbox” intended to do?

What is a “Cross Site Script” (XSS)

Splitting the Reference Monitor

Policy administration point (PAP): creates a policy or policy set.

Policy decision point (PDP): evaluates applicable policy and renders an authorization decision.

Policy enforcement point (PEP): performs access control, by making decision requests and enforcing authorization decisions.

Policy information point (PIP): acts as a source of attribute values.

Pen Testing

Using Google for “pre-testing”

Explain: Foothold > Stronghold > Domination

Port-scanning

Vulnerability Testing

SQL Injection

InfoWar

In DOD Terms, these are the parts to CyberWar:

Military Deception (MILDEC)

Operational Security (OPSEC)

Computer Network Operations (CNO)

Computer Network Defense (CND)

Computer Network Exploitation (CNE)

Computer Network Attack (CNA)

Crypto – DES & AES

What is a “Block Cipher”?

How was AES chosen? Why was that “a good thing”?

Software Security

Know the 7 Pernicious Kingdoms – Be able to match an example from each – see Software Security Powerpoint

What is a “Race Condition?”

Why is “Input Validation” so important?

Software Security

Graduate Essay Question:

<http://cwe.mitre.org/top25/>

Choose one of the **Mitre/SANS Top25 Most Dangerous Programming Errors** explain what it is, how it is harmful, and how to avoid it