

Information Assurance: Review Topics for Exam 1

Introductory Concepts

Reading: Chapter 1

Concepts

- Security services: Confidentiality, Integrity, Availability
- Threat Classes: Disclosure, Disruption, Deception, and Usurpation
- Threat techniques: Snooping, modification, spoofing, Repudiation of origin, denial of receipt, delay, denial of service.

Access Control Matrix – Chapter 2

Reading: Chapter 2 and some of Chapter 3

Concepts

- Access Control concept and syntax.
- HRU primitives and command structure
- Safety

Policy

Reading: Chapter 4

Concepts

- Purpose of policy
- Policy versus mechanism
- High level, low level, and natural language

Confidentiality Policy

Reading: Chapter 5

Concepts

- Bell-LaPadula model
- *-property, simple security condition
- Basic Security Theorem

- Tranquility – strong and weak
- McLean’s dagger property and system Z

Integrity Policy

Reading: Chapter 6

Concepts

- Lipner’s 5 requirements of system integrity
- Three Biba models: low-water-mark, Ring, and Strict
- Lipner’s Integrity Matrix Model
- Clark-Wilson Model

Trusted OS

Reading: Lecture Notes, Data General discussion in Chapter 5, and links to OS documentation

Concepts

- Different MAC models: Pitbull LX, Pitbull Foundation, SE Linux MLS, SE Linux MCS, and SE Linux Type Enforcement
- Tricky implementation bits
 - Partitioned directories
 - Privilege Issues
 - Network data

Risk Analysis

Reading: Chapter 2 of Peltier copies handed out in class and scanned on compass.

Concepts

- Two types: Quantitative and Qualitative
- Both work with: Assets, Threats, Vulnerabilities, and Controls

Laws

Readings: Chapter 2 of McNamara copies handed out in class and scanned on compass. [Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives](#) handed out in class. [Web based CyberLaw lessons](#) reinforces the same ideas.

Concepts

- Privacy versus national interest
 - 4th amendment
 - US Patriot Act
 - Wiretapping
 - Pen-register and tap-and-trace compared to full content tap
 - ECPA
 - CALEA
 - FISA
 - Patriot Act
- Computer Crime
 - CFAA
 - Economic Espionage Act
 - Cryptography Issues
 - International Law
- Laws governing security of federal computers: FISMA, NSD-42, and NCS
- Laws governing business: HIPPA, Grahm-Leach-Bliley, Sarbanes-Oxley