Software Reliability and Security

Module 8

Winter 2017

Outline

- Security Types
- Computer Attacks and Defenses
- Attack Defense – Intrusion detection systems and testing
- Security Engineering
- Software Engineering for Security

Presentation/Lecture Schedule and Report Due Dates

- Presentation 1
  - Related background paper
  - Jan 27, Feb 1, 3
- Presentation 2
  - Project proposal
  - March 1, 3, 8
- Presentation 3
  - Final project report
  - March 24, 29, 31

- Lectures

  Jan 13, 18, 20, 25, 27

  Feb 1, 3, 8, 10, 15, 17

  March 1, 3, 8, 10, 15, 17, 22, 24, 29, 31

- Project Proposal Due

  Tuesday, February 28

- Final Project Report Due

  Monday, April 10

- Final Exam

  Wednesday, April 12, 10:00am

Security Types

- Computer security
- Program security
- Software security
- Network security
- Application security
- Cybersecurity
- Information security / Computer security
- Internet security
- …

Security Types – contd.

- Security (Bosworth et al., 2009)
  - Free from danger or exposure due to attacks
    - Hard Security - access control, authentication, etc.
    - Soft Security - trust, reputation
- Trust (Josang et al., 2005; McKnight, 1996)
  - A directional relationship between two entities
  - The degree of dependence of one entity (trustor) on another entity (trustee) in a given scenario
- Privacy (Pfleeger, 2006)
  - Controlling somebody who knows something (communications, activities etc.) about others
  - Major aspects: data sensitivity, affected parties, controlled disclosure

Security Types – contd.

- Computer security (Brinkley and Schell, 1995)
  - A field of computer science to maintain confidentiality, integrity, and availability of resources (computers and their affiliated devices)
  - Includes program security, software security, network security, application security, etc.
- Program security (Pfleeger, 2006)
  - Security at program level
  - Protect computing resources against program security flaws
  - Program (security) is a part of software (security)

Security Types – contd.

- Software Security (McGraw, 2006)
  - A field of "computer security" that focusses on software that operate normally under attacks - mainly about building secure software
- Software Security Engineering (McGraw, 2006)
  - Building Secure Software – security risk analysis, security requirements specification, secure design, and security testing
  - May include the security aspects of programming languages and O/Ss
- Application Security (McGraw, 2006)
  - Software and system protection after the development is complete
  - May include sandboxing, malicious code protection, run-time detection, enforcing security policies

Security Types – contd.

- Network Security (Bishop, Dowd, et al.)
  - A field of computer security that protects networks and their applications against attacks
  - Maintain CIA with respect to all network elements
  - Includes intrusion detection, traffic analysis, network monitoring, cryptography
- Cybersecurity (Dunn)
  - A set of technical and non-technical controls
  - Protect computers, networks, other related hardware and software along with their software and data
  - Also includes the protection of other aspects of cyberspace, from all threats (including national security)

Computer Attacks and Security Defense

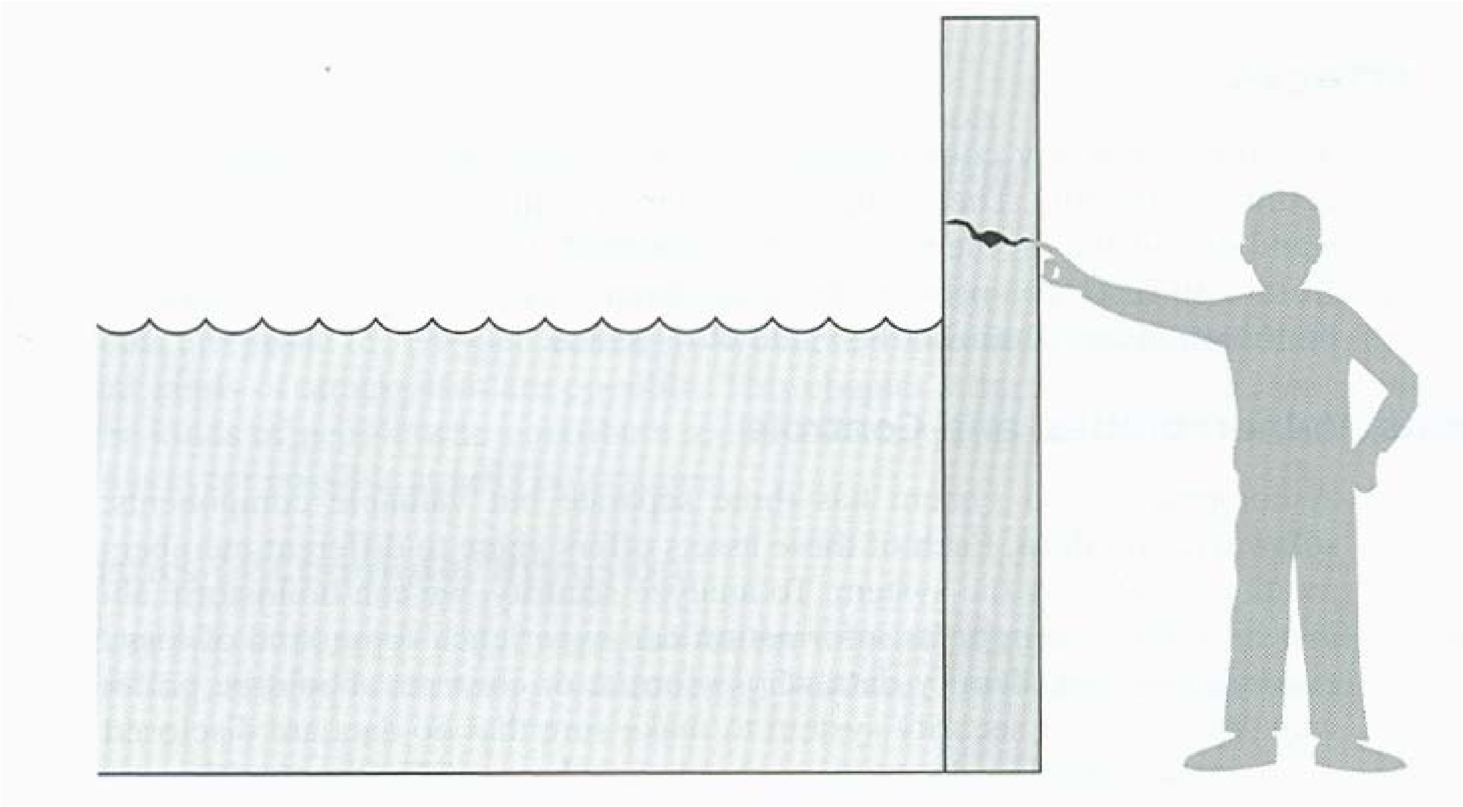
- Attacks - Threat, Vulnerability, and Control
- Methods of Defense
- Security Goals, Concepts, and their Relationship
- Attacks – Malicious code

Attacks in Computer System

- Attacks - a specific formulation or execution of a plan to carry out a threat
  - Threats – acts that have the potential to cause harm
    - Interception
    - Interruption
    - Modification
    - Fabrication
  - Vulnerabilities – an exploitable weakness in a system to break security
  - Controls – Methods and tools to reduce or protect due to a vulnerability

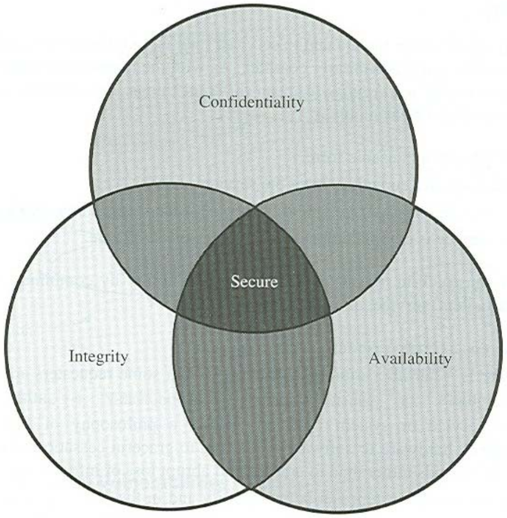
Threat, Control, and Vulnerability

A threat is blocked by control of a vulnerability



- **Precondition for an Attack - MOM (Method, Opportunity, and Motive)**

Security Goals

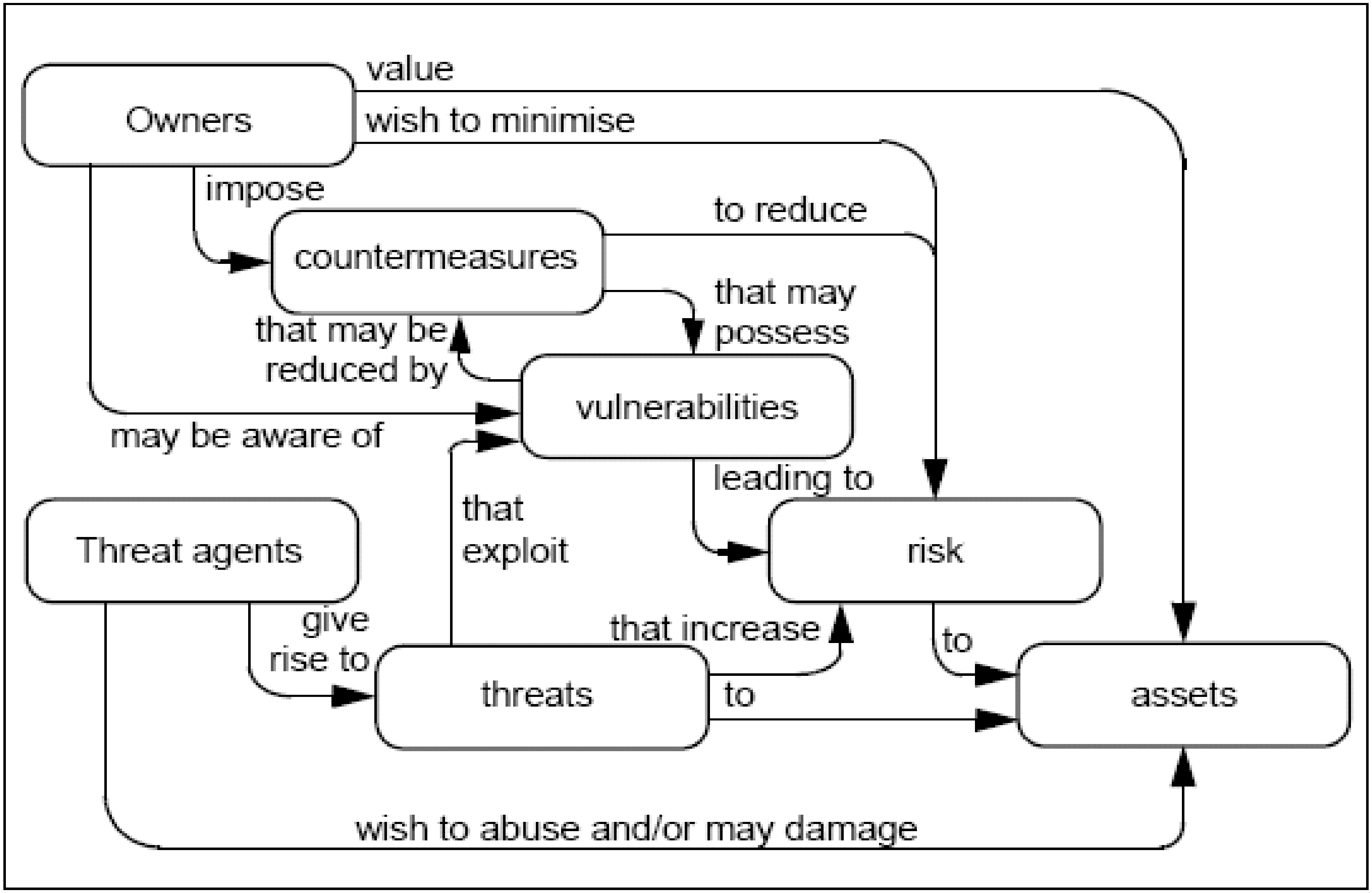


- Confidentiality – computing resources should be accessed only by authorized parties (secrecy)
- Integrity – resources can be modified only by authorized parties in authorized ways
- Availability – resources are accessible to authorized parties whenever necessary (opposite of denial of service)

Methods of Defense

- Reduce security risks
  - Prevent
  - Deter – make the attack harder (not impossible)
  - Deflect – make another target more attractive
  - Detect
  - Recover
- Controls: methods of defense
  - Encryption
  - Software Controls
  - Hardware Controls
  - Policies and Procedures
  - Physical Controls

Security Concepts and Relationships



Attacks -Malicious Code

- Malicious code – written and distributed to make damage
- Excludes all unintentional errors (most faults found in software testing, inspection, and reviews)
  - Virus – Attaches to program and propagates copies to other programs
  - Trojan horse – Contains unexpected, additional functionality
  - Logic bomb – Triggers action when condition occurs
  - Time bomb - Triggers action when specified time occurs
  - Trapdoor – Allows unauthorized access to functionality
  - Worm – Propagates copies through a network
  - Rabbit – Replicates to exhaust resource

Targeted Malicious Code

- Non-Targeted Malicious Code
  - Anonymous code written to affect users and machines indiscriminately
- Targeted Malicious Code
  - Malicious code written for a particular system, for a particular application, and for a particular purpose
    - Trapdoors – an undocumented entry point to a module
    - Rootkits – a later variation on the virus theme
    - Privilege escalation – malicious code to increase the privilege level
    - Keystroke logging
    - Man-in-the-Middle
    - Covert Channels - programs that leak information

Attack Classifications (Webster, 1999)

- An attack changes one privilege level to another privilege level using a method
- Attack classification criteria
  - Privilege levels
  - Attack methods
  - Attack actions

Attack Classification Elements

- Privilege levels
  - Remote network access (R) – the attacker has access via a network to the target system
  - Local network access (L) – the attacker can receive from and send to the same network as the victim system
  - User access (U) – the attacker can run user commands onto the target system
  - Super/root access (S) – the attacker can control any software on the target system
  - Physical access to host (H) – the attacker has complete access to the hardware

Attack Classification Elements

- Attack methods
  - Masquerading (m) - the attacker can access a system by pretending the identity of a victim's trusted person /system
  - An abuse of feature (a) - the attacker can abuse a system by performing an allowed action
  - Implementation bug (b) – the attacker exploits bad programming practices (e.g., buffer overflow)
  - System misconfiguration (c) – exploits unintentional errors in a system's configuration
  - Social engineering (S) - the attacker intimidates or deceives a legitimate user for getting access

Attack Classification Elements – contd.

- Attack actions
  - Probe - an information discovery attack
  - Deny - a denial of service for a short or long time
  - Intercept - an interception of files, keystrokes or some other information
  - Alter - an alteration or deletion of some stored data
  - Use - an action for attacker's own personal enjoyment or preparation for other attacks
- Examples
  - "casesen" attack - a U-b-S attack that elevates the user from a "user" (U) privilege level to a "super root" (S) privilege level via an implementation bug (b)
  - "udpstorm" attack - a R-a-Deny attack because a remote user (R) performs an action that denies (D) access via an abuse of feature (a)

Intrusion Detection Systems (IDS)

- Intrusion – an intentional unauthorized attempt to
  - Access information
  - Manipulate information
  - Make a system unreliable/unusable
- Importance
  - Completely secure system is impossible - a truly secure system may be abused by insiders
  - Detects potential security violations such as unauthorized use or misuse by both external and internal users of a system
- IDSs are usually different from firewall (gatekeeper)
  - Firewalls can also generate alerts in case of some network intrusion

Classification of IDSs

- Two types – based on the target system
  - Host-based - uses information from a host
  - Network-based – use network events
  - Hybrid
- Two Types – based on detection criteria
  - Anomaly detection
  - Misuse detection
  - Hybrid – utilize both approaches

IDS – Major Objectives

- Both for single host or network (cloud?)
- Reduce false positives and negatives
- Detect new and unknown attacks
- Minimize time between actual intrusion occurrence and its detection
- Reduce data collection overhead for detection
- Remove any effect on normal target system operation

Classification of IDSs – Anomaly and Misuse

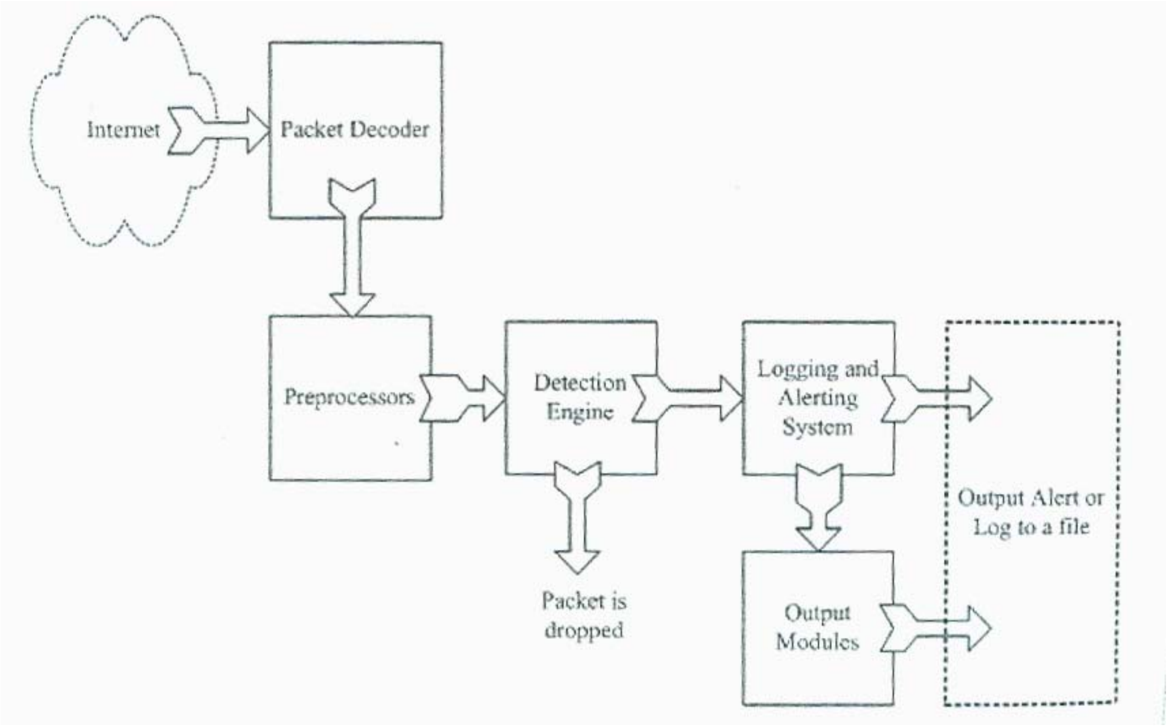
- Anomaly Detection Issues
  - Selection of threshold level and features to be monitored
  - Overhead for managing or updating profiles and the thresholds
  - Not all anomalous activities are intrusions
  - Not all intrusions are anomalous
  - As a result, may report false positive or negative
- Some Examples
  - Statistical, Pattern prediction, Neural networks

Classification of IDSs – Anomaly and Misuse

- Misuse Detection Issues
  - Like virus detection systems – not useful for unknown intrusions
  - Assume that attacks can be represented in signatures compare
  - Some variations of an attack representations may match some legitimate activities
- Some Examples
  - Expert systems, Model (pattern)-based, Software specification-based, Snort

An Open Source IDS – Snort (snort.org)

- Signature-based NIDS - employs a combination of rules
  - The rules allow the creation of signatures to examine packets
  - Packets not matching any rule are dropped
  - Others are logged and can also report and alert



Snort Components

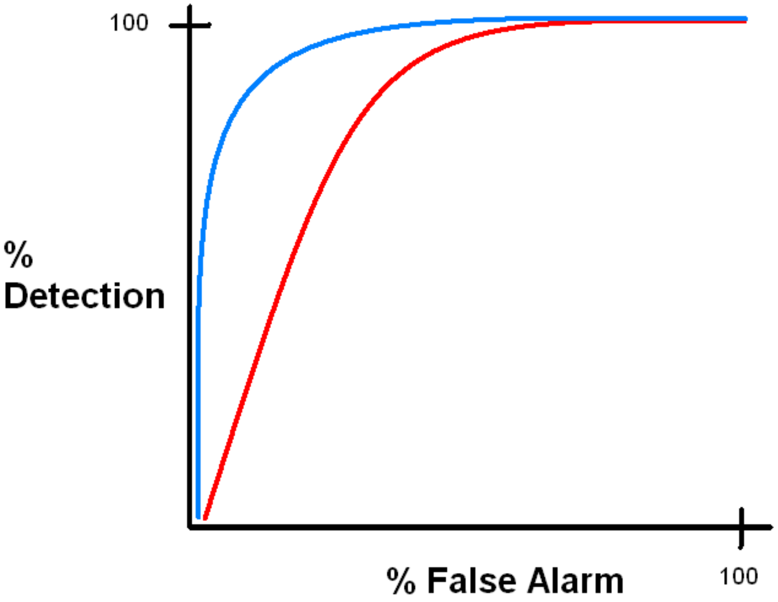
- Packet Decoder
  - Sniffs packets from network interfaces and arrange for processing
- Preprocessors
  - Prepares packets for the detection engine to analyze
- Detection Engine
  - Examines one or more fields of each packet using Snort rules
- Logging and Alerting System
  - Generates alerts and log messages based on detection engine analysis
- Output Modules
  - Process alerts and logs and generate final output based on user choice
- Disadvantages
  - May not pick up all packets due to the speed of the network
  - False positives and negative alerts – like many other IDSs
  - Has become a target of attackers

Quantitatively Measurable IDS Characteristics

- Coverage
  - Signature-based – number of signatures
  - Non-signature-based – attacks out of the set of all known attacks
  - Importance and dimension (consequence) of each attack
- Probability of detection
  - Varies with false positive rate
- Resistance to attacks directed at the IDS
- Ability to handle high bandwidth traffic
  - May drop packets in case of too many packets or signatures

Quantitatively Measurable IDS Characteristics

- Probability of false alarms
  - Alerts caused by normal non-malicious traffic
  - False positive rate may vary with the network environment
  - Receiver operating curve (ROC) – relationship between false positive and detection capability



Quantitatively Measurable IDS Characteristics – contd.

- Ability to correlate events
  - Collect events from other complementary IDSs, firewalls, routers, application logs, etc.
  - Useful to identify staged penetration attacks
  - Important for distributed intrusion detection
- Ability to detect unknown (never before seen) attacks
  - Only used for anomaly based
  - Difficult to measure/interpret
- Ability to identify an attack
  - How well an IDS can label (categorize) each detected attack with a common name or vulnerability name

Quantitatively Measurable IDS Characteristics – contd.

- Ability to determine attack success
  - Some attacks (or probes) may not harm the attacked system
  - Distinguish the failed from the successful attacks
- Capacity verification for NIDS
  - Ability to capture, process, and maintain accuracy given a network load
- Other measurements
  - Ease of use, maintenance, deployment, resource requirements, quality of support, etc.
- Main challenge in IDS Testing
  - Collecting attack scripts and victim software

Outline

- Security Types
  - Target area
  - Hard and soft security
  - Development process
- Computer Attacks and Defenses
  - Attacks - Threat, Vulnerability, and Control
  - Methods of Defense
  - Security Goals, Concepts, and their Relationship
  - Attacks – Malicious code
- Attack Defense - Intrusion detection systems and testing
  - Types of IDS
  - IDS Characteristics
  - IDS Evaluation

Lecture Sources

- C. Pfleeger and S. Pfleeger, Security in Computing, Chapter 1 & 3 Prentice-Hall, 2003
- ISO/JTC1/IEC, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1, Standard ISO/IEC 15408-(1-3):1999
- C. Landwehr et al., "A Taxonomy of Computer Program Security Flaws," ACM Computing Surveys, vol. 26, no. 3, September 1994.
- S. Webster, The development and analysis of intrusion detection algorithms, Master's thesis, MIT, USA, 1998.
- A Sundaram, An introduction to intrusion detection, Crossroads, Volume 2, Issue 4 (April 1996) Special issue on computer security Pages: 3 – 7, ACM Press, USA.
- R. Rehman, Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID, Prentice Hall PTR, 2003.
- R. Anderson, Security Engineering - A Guide to Building Dependable Distributed Systems, Wiley, January 2001
- Northcutt, et al., Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems, Chapter 13, Sams, 2002
- P. Mell, V. Hu, R. Lipmann, J. Haines, and M. Zissman. An overview of issues in testing intrusion detection systems. Technical Report NIST IR 7007, National Institute of Standard and Technology, USA.
- Jay Beale et al., Snort 2.0 Intrusion Detection, Syngress Publishing, 2003.