CS 4910: Intro to Computer Security

Review

Instructor: Xi Tan

Review

- Materials
  - Lectures
  - Homework assignments
  - Labs
- Topics
  - Network Security
  - Malicious Software
  - Software Security
  - Computer ethics

- **Exam time**: 05/11 12:40 PM – 2:00 PM
- **Exam location**: Cyber building A-107

Exam

- Type of questions
  - True/false questions
  - Multiple choice questions
  - Short answer questions
  - Questions regarding the two labs
    - Packet sniffing and spoofing
    - Buffer-overflow attack

- You are allowed to take one letter-size sheet of hand-written notes (front and back)

Network Security

- Network concepts
- DoS attack
- DNS attack
- Firewalls
- IDS

Network Security: Attack Summary

Layers	Data Encapsulation (frame/packet)	Protocols	Attacks
Application	HTTP Header | HTTP Data	DNS	DNS cache poisoning
Transport	TCP Header | HTTP Header | HTTP Data	TCP	TCP flood
Network	IP Header | TCP Header | HTTP Header | HTTP Data	IP, ICMP	IP spoofing, ICMP flood
Data Link	MAC Header | IP Header | TCP Header | HTTP Header | HTTP Data	MAC, ARP	MAC spoofing, ARP spoofing

Network Security: attack

- Students should know the security issues for each protocol
- Students should know how those attacks work for each protocol
- Students should know the methods to ensure the security of the network
  - e.g., firewalls and IDS

Network Security

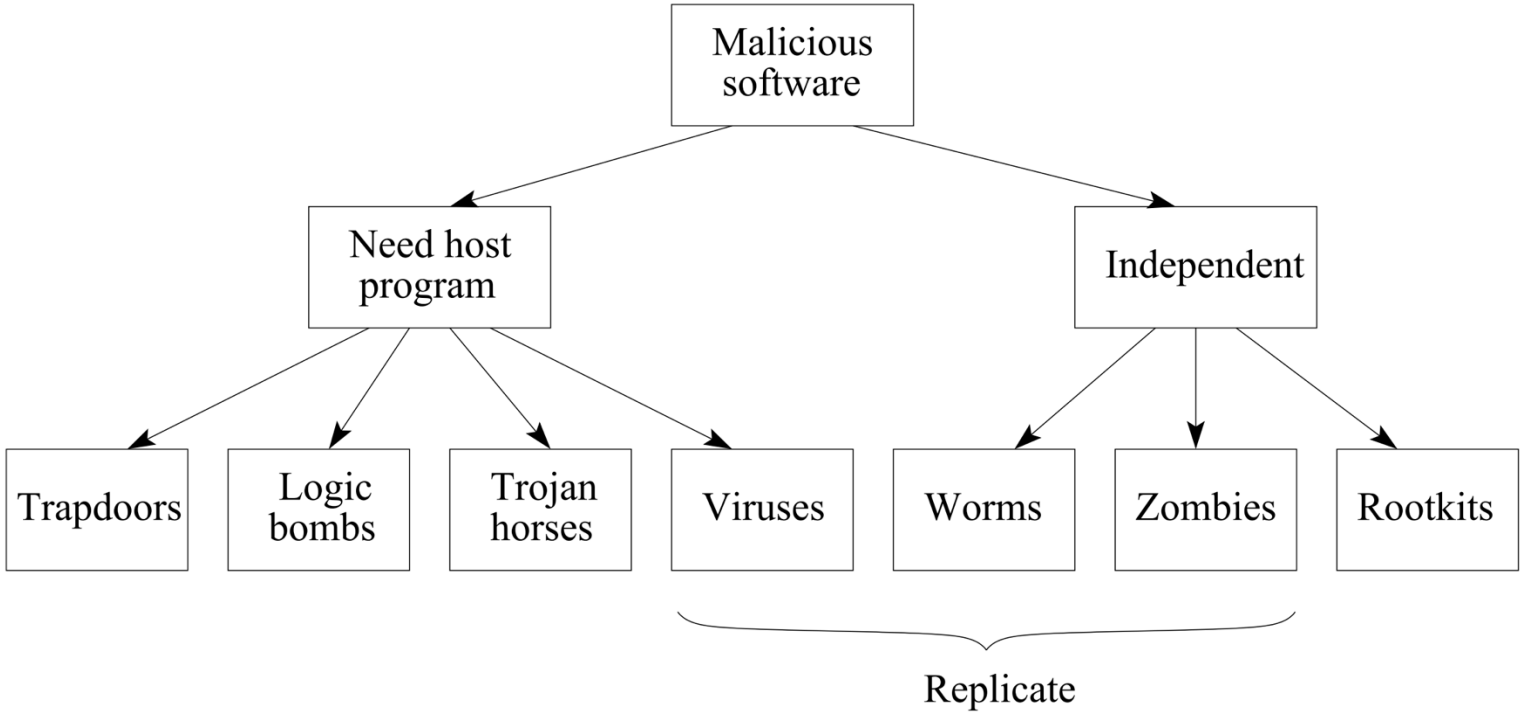
- Firewalls
  - Three types: packet filtering, stateful filters, and application layer
    - Packet filtering polices
- IDS
  - Three types: Host-based IDS, Network-based IDS, Hybrid IDS
  - Detection
    - Signature or heuristic detection
    - Anomaly detection: can detect unknown attacks

Network Security

- Students should know the differences between firewalls and IDS
- Students should understand the simple packet filtering policies for firewalls
- Students should know the differences between host-based IDS and network-based IDS
- Students should know the detection methods used in IDS

Malicious Software

- Taxonomy of malicious software



Malicious Software

- Students should be able to identify the differences between different types of malicious software
- Students should know how malicious software is propagated and hidden from detection

Software Security

- Background knowledge
- Buffer overflow attacks
  - Overwrite local variables
  - Overwrite return address
  - Overwrite return address with parameters
  - Defense
    - Base and bound check
    - Shadow stack
    - Stack canary/cookie
    - Data execution prevention
    - ASLR

Software Security

- Students should be able to identify whether the given piece of code is vulnerable or not
- Students should be able to exploit the vulnerability in theory
- Students should know some basic security mitigation to defend against potential attacks

Computer Ethics

- Students should know how to make a decision and take responsibility for the decision