Chapter 1
Introduction to Computer Security

Reading Chapter 1:

Chuck Easttom, [2016], Computer Security Fundamentals, Third Edition, Pearson Education.

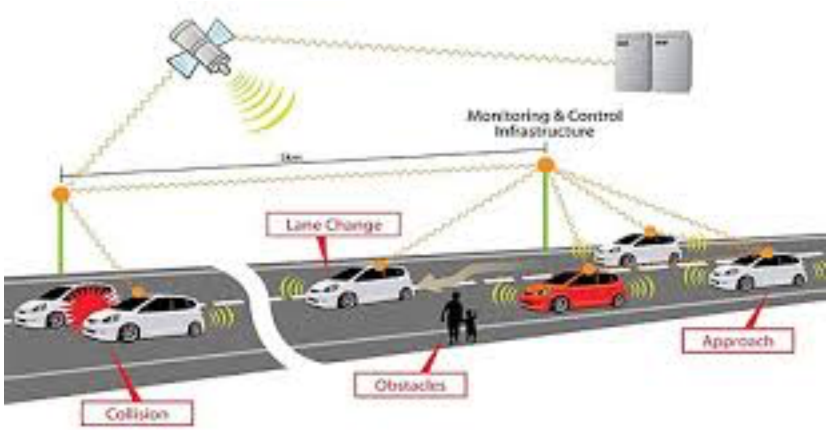
Chapter 1 Objectives

- Identify top threats to a computer network
- Assess the likelihood of an attack
- Define key terms like cracker, sneaker, firewall, and authentication
- Compare and contrast perimeter and layered approaches to network security
- Use online resources

Introduction

- Computer systems and networks are all around us.
  - Online banking
  - Automated supermarket checkouts
  - Online classes
  - Online shopping
  - Online travel resources

Introduction



Introduction (cont.)

- How is personal information safeguarded?
- What are the vulnerabilities?
- What secures these systems?
- Who can access my information?

How Seriously Should You Take Threats to Network Security?

- Which group do you belong to?
  - “No one is coming after my computer.”
  - “The sky is falling!”
  - Middle ground.

Identifying Types of Threats

- **Malware:** **MAL**icious soft**WARE (**virus attacks, worms, adware, Trojan horses, and spyware)
- **Security Breaches:** This group of attacks includes any attempt to gain unauthorized access to your system. This includes cracking passwords, elevating privileges, breaking into a server...all the things you probably associate with the term *hacking*.

Identifying Types of Threats

- **DoS (Denial of Service attacks):** These are designed to prevent legitimate access to your system.
- **Web Attacks:** This is any attack that attempts to breach your website. Two of the most common such attacks are SQL injection and cross-site scripting.
- **Session Hijacking:** These attacks are rather advanced and involve an attacker attempting to take over a session.

Identifying Types of Threats

- **Insider threats:** These are breaches based on someone who has access to your network misusing his access to steal data or compromise security.
- **DNS poisoning:** This type of attack seeks to compromise a DNS server so that users can be redirected to malicious websites, including phishing websites.
- There are other attacks, such as **social engineering**.

Malware

- Software with a malicious purpose
  - Virus
  - Trojan horse
  - Spyware
  - Logic Bomb

Malware (cont.)

Virus

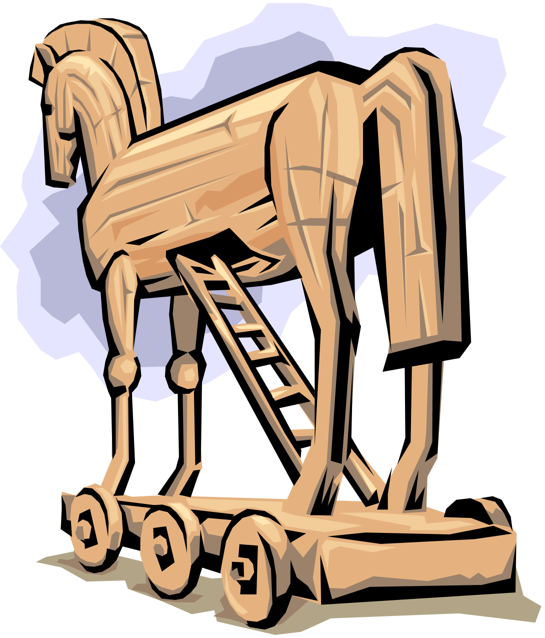
- One of the two most common types
- Usually spreads through e-mail
- Uses system resources, causing slowdown or stoppage

According to Symantec (makers of Norton antivirus and other software products), a *virus* is “**a small program that replicates and hides itself inside other programs, usually without your knowledge**”

Malware (cont.)

Trojan Horse

- The other most common kind of malware
- Named after the wooden horse of ancient history



Malware (cont.)

Spyware

- The most rapidly growing types of malware
  - Cookies
  - Key logger

Malware (cont.)

Logic Bomb

– Lays dormant until some logical condition is met, often a specific date.

Compromising System Security

Intrusions

- Attacks that break through system resources
  - Hackers
  - Crackers
  - Social engineering
  - War-driving

Denial of Service Attacks

- The attacker does not intrude into the system but just blocks access by authorized users.
- Cannon Ion Cannon Low (LOIC).

Web Attacks

- The attacker attempts to breach a web application.
- Common attacks of this type are SQL injection and Cross Site Scripting.

Web Attacks

- SQL injection

```
SELECT * FROM tblUsers WHERE USERNAME = ’ " + txtUsername.Text +' AND PASSWORD = ’ " + txtPassword.Text +” '
```

```
SELECT * FROM tblUsers WHERE USERNAME = ’ ' or '1' = '1' AND PASSWORD = ’ ' or '1' = '1'
```

- Cross-site scripting

```
<script> window.location = "http://www.fakesite.com"; </script>
```

Session Hijacking

- This is a complex attack that involves actually taking over an authenticated session.

Insider Threats

- An insider threat is simply when someone inside your organization either misuses his access to data or accesses data he is not authorized to access.

DNS Poisoning

- This involves altering DNS records on a DNS server to redirect client traffic to malicious websites, usually for identity theft.

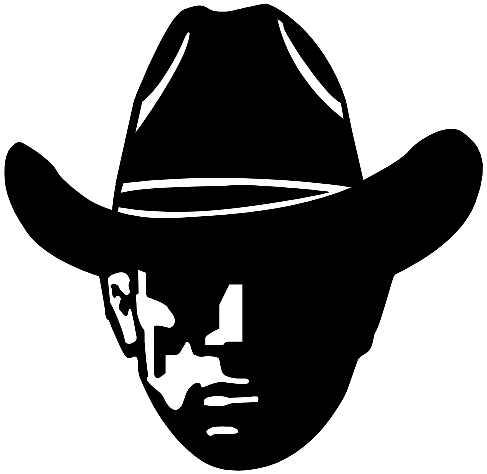
Assessing the Likelihood of an Attack on Your Network

- Viruses
  - Catch up on new and refurbished viruses
- Unauthorized use of systems
  - DoS attacks
  - Intrusions
  - Employee misuse

Basic Security Terminology

People:

- Hackers
  - White hats
  - Black hats
  - Gray hats
- Script kiddies
- Sneakers (*penetration tester = pentester*)
- Ethical hackers



Basic Security Terminology (cont.)

Devices

- Firewall
  - Filters network traffic
- Proxy server
  - Disguises IP address of internal host
- Intrusion Detection System
  - Monitors traffic, looking for attempted attacks

Basic Security Terminology (cont.)

Activities

- Authentication
- Auditing

Network Security Paradigms

- How will you protect your network?
  - CIA Triangle (Confidentiality, Integrity, Availability)
  - Least Privileges
  - Perimeter security approach
  - Layered security approach
  - Proactive versus reactive
  - Hybrid security method

How Do Legal Issues Impact Network Security?

- *The Computer Security Act of 1987*
- *OMB Circular A-130*
- See www.alw.nih.gov/Security/FIRST/papers/legal/statelaw.txt for state computer laws
- Health Insurance Portability and Accountability Act of 1996, HIPAA

Online Security Resources

- CERT
  - www.cert.org
- Microsoft Security Advisor
  - www.microsoft.com/security/default.mspx
- F-Secure
  - www.f-secure.com
- SANS
  - www.sans.org

Summary

- Network security is a constantly changing field.
- You need three levels of knowledge.
  - Take the courses necessary to learn the basic techniques.
  - Learn your enterprise system intimately, with all its strengths and vulnerabilities.
  - Keep current in the ever-changing world of threats and exploits.

Summary

- What is malware?
- What is a penetration tester?
- What is spyware?
- What is a computer virus?
- What is war-driving?
- What is the most common threat on the Internet?
- Hacker Terminology ?