INFO3068 Secure Computing

Course Introduction – Part 2

Press F5 to begin the slideshow

FANSHAWE

Security Overview

Understanding Security

- Physical security (buildings, hardware, devices)
- Network security (connectivity, access, availability, audit)
- **Data security (confidentiality, integrity)**
- **Application security (exploits)**

Goals: protect confidentiality, maintain integrity, assure availability (CIA)

Empirical Attack Data

- How do we know about the techniques that attackers are using?
  - Researchers, both public and private (Universities and Colleges, SANS, CERT, eEye, Ka)
  - Publications and Sites (2600.org, SecuritySpace.com)
  - Conferences (HOPE, Blackhat, DEFCon)
  - Honey Pots, Honey Nets, Honey Monkeys

Attack Trends

- Growing Incident Frequency
- Growing number of vulnerabilities catalogued
  - 8 vulnerabilities in 1998
  - 366 in 2007
  - 16,272 YTD Sept. 19 2020 (source: VulnDB)
- Increased Criticality of vulnerabilities exploited
  - 1 in 5 were considered critical CBSS (Common Vulnerability Scoring System)
- Growing Randomness in Victim Selection
  - In the past, large well-known firms were targeted
  - Now, targeting is increasingly random
  - No more “security through obscurity” for small firms and individuals

Attack Trends

- Growing Malevolence
  - Most early attacks were not malicious, mostly nuisances
  - Malicious attacks are becoming the norm, significant financial loss

Attack Trends

- Growing Attack Automation
  - Attacks are automated through the use of “bots,” rather than human-directed
  - Attack many computers in minutes or hours, then instruct them to attack others
  - Cyberweapons of mass destruction?

Understanding Security

- Security ensures that:
  - Users perform only tasks they are authorized to do
  - Users only information they are authorized to have
  - Users, applications cannot cause damage to data, other applications, or operating environment
  - **Applications cannot perform “arbitrary” or “harmful” instructions**

Threats

- Causes of security threats
  - Technology weaknesses (standards or lack of standards, application exploits)
  - Configuration weaknesses (oversight, defaults)
  - Policy weaknesses
  - Human error

Configuration Weaknesses

- Unsecured accounts
- System accounts with easily guessed passwords (either by humans or by machine)
- Unsecured default settings
- Misconfigured network, firewall equipment/software
- No malware protection (viruses, spyware)

Policy Weaknesses

- Lack of a written security policy
- Politics
- High turnover
- Concise access controls not applied
- Software and hardware installation and changes do not follow policy
- Proper security
- Nonexistent disaster recovery plan

Human Error

- Accident
- Ignorance
- Workload
- Dishonesty
- Impersonation
- Disgruntled employees, political agenda
- Snoop

Security Management

- Security is a Primarily a Management Issue, not a Technology Issue
- Top-to-Bottom Commitment
  - Top-management commitment
  - Operational execution
  - Enforcement
- Security can be a trade off between protection of information and ease of use

Framework for Attackers

- Black Hat, bad intentions without invitation
- White Hat, good intentions with invitation
- Grey Hat, good intentions without invitation
- Virus/Worm Writers and Releasers
- Script Kiddies
- Criminals
- Internal employees, contractors

Social Engineering Examples

- Tricking an employee into giving out passwords, files or other information or taking an action that reduces the security a system
- E-mail attachments or links that appear to be helpful or mandatory
- Phishing e-mail that contains something personalized to you

Social Engineering Defenses

- Training employees
- Enforcement through sanctions? (punishment)
- Defcon Example: https://www.youtube.com/watch?v=lc7scxvKQOo

Security Strategy

- Address both internal and external threats
- Define policies and procedures
- Reduce risk across across perimeter security, the Internet, intranets, and LANs

Security Strategy

- Data CIA is key
- Human factors
- Know your weaknesses
- Limit access
- Achieve security through persistence
  - Develop change management process
- Remember physical security
- Perimeter security
  - Firewalls, control access to critical network applications, data, and services

Recap

- Threats are considerable today
- Threats will be worse tomorrow, so plan for tomorrow’s threat environment
- There are many threats from many attackers
- Technology and training can reduce threats

References

- www.cert.org
- www.us-cert.gov
- www.sans.org
- www.securityspace.com
- www.wikipedia.org

- http://xkcd.com