CS 493
Secure Software Systems
Current And Emerging Threats

Dr. Williams

Central Connecticut State University

OBJECTIVES

- Common organization security threats
- The mentality that allows system compromise
- Impedance mismatch in system development
- Risks associated with personnel
- Risks to the network environment
- Risks to the operating system environment
- Risks to the database environment

Goals

- Identify where security policies need to be established.
- Determine necessary training for personnel.
- Evaluate oversight and cooperation opportunities for your organization.
- Identify likely avenues of attack in the overall organization environment.
- Define weaknesses in the current system in preparation for new development.
- **Recognize all involved must work together to achieve security**

The New Paradigm

- The information age has brought about a remarkable shift in the economy of the world. What was once based on goods and services now competes with the inherent value of information.
- The Russia and Georgia conflicts in August 2008, which lasted only nine days, marked the first time in history that a war was preceded by a massive cyber attack that shut down the Georgian government, including financial institutions and media sites.

The Human Factor

- The second and most dangerous types of attacks we see today are those using a combination of social engineering tactics and technical tools.
- A **social engineering attack** is one in which the attacker uses easily available company information, which a company thinks is innocuous, to disguise him- or herself as someone who is authorized to receive protected information.

The Human Factor

- Modern attacks are so dangerous because users can use social engineering tactics to convince unsuspecting users to install malicious software, creating an opportunistic stealthy environment that can unleash havoc on an organization's data infrastructure.
- It is critical that your organization has a solid **information assurance training program (IATP)**.

The People Problem

- People often break security
  - Both intentionally and unintentionally
  - Here, we consider the unintentional
- For example, suppose you want to buy something online
  - A security textbook from amazon.com

The People Problem cont.

- To buy from amazon.com…
  - Your Web browser uses SSL protocol
  - SSL relies on cryptography
  - Access control issues arise
  - All security mechanisms are in software
- Suppose all of this security stuff works perfectly
  - Then you would be safe, right?

The People Problem

- What could go wrong?
- Trudy tries man-in-the-middle attack
  - SSL is secure, so attack doesn't "work"
  - But, Web browser issues a warning
  - What does the user do?
- If user ignores warning, attack works!
  - None of the security mechanisms failed
  - But user unintentionally broke security
- Lesson- Technology solutions alone have limitations

Social engineering in action

- New employee
- Phishing emails
- Tech support call
- The human factor – build trust
- Security testing of ***information assurance***

The Human Factor

One approach toward the development of an effective security policy is to reference publicly available NIST documents that can facilitate the development of a security framework.

- **SP 800-12:** An Introduction to Computer Security: The NIST Handbook
- **SP 800-14:** Generally Accepted Security Principles and Practices for Securing Information Technology Systems
- **SP 800-18:** Guide for Developing Security Plans for Federal Information Systems
- **SP 800-26:** Security Self-Assessment Guide for Information Technology Systems
- **SP 800-30:** Risk Management Guide for Information Technology Systems
- **SP 800-50:** Building an Information Technology Security Awareness and Training Program

The Network

- The network is an important equation to your overall information systems development strategy.
- Web 2.0 technologies include social networking sites, such as Facebook and Twitter; these have brought about new challenges and threats to the corporate network and personal security.
- Social network sites can also be a haven for malicious code and phishing attacks.

The Operating System Environment

- Defects in operating systems are found on a daily basis, and vendors race to respond with patches depending on the severity of the compromise.
- The Windows operating system has reaped the most significant share of attacks. This does not mean their operating systems (OS) incarnations are the least secure; it just means they have the highest value to attackers

The Operating System Environment

The following list includes a few of the most common websites to visit for security issues and recommended actions:

- http://technet.microsoft.com/en-us/security
- http://www.cert.org
- http://www.owasp.org/index.php/Category:How_To
- http://www.us-cert.gov
- http://www.nist.gov/computer-security-portal.cfm

The Deadly Sins for the OS

- Weak Passwords
- Open network ports
- Old software versions
- Insecure and poorly configured programs
- Insufficient resources and misplaced priorities
- Stale and unnecessary accounts
- Procrastination

Data Management

- The foundations of all of the applications you develop will likely entail a **database management system** (DBMS).
- A relational database management system establishes relationships between tables of data.
- **Data** is simply defined as “raw facts.”
- A **database** is a collection of data that has an established relation.

Data Management

- A database also contains a **data dictionary** known as the **metadata** or “data about data.”
- **Information** is defined as data that has been organized into a format that is useful and actionable.

Data-Centric Threats

- When all is said and done, system security is all about protecting the data, from corporate secrets to your own personal address.
- One of the most common threats to a web application is an SQL injection attack.
- **SQL injection attack** is a serious threat to any application that translates raw user input into database communications.

Summary

- There are a variety of potential vulnerabilities within an organization environment.
- The Operating System
- The Network
- The Database
- The Human Factor
- Business need
- Key concept discussed about these in book it refers to as ***impedance mismatch***