Threats, Vulnerabilities, and Risks

Terminology

- Threat---a potential cause of an incident that may result in harm to a system or organization
- Vulnerability---a **weakness of an asset** (resource) or a group of assets that can be exploited by one or more threats
- Risk---potential for loss, damage, or destruction of an asset as a result of a threat exploiting a vulnerability
- **Example**: In a system that allows weak passwords,
  - Vulnerability---password is vulnerable for dictionary or exhaustive key attacks
  - Threat---An intruder can exploit the password weakness to break into the system
  - Risk---the resources within the system are prone for illegal access/modify/damage by the intruder.
- Threat agent---entities that would knowingly seek to manifest a threat

Who is the enemy? Why do they do it?

- Offenders
  - Crackers---mostly teenagers doing as intellectual challenge
  - Information system's criminals---Espionage and/or Fraud/abuse---for a nation/company to gain a competitive advantage over its rivals
  - Vandals---authorized users and strangers (cracker or a criminal)---motivated by anger directed at an individual/organization/life in general

Motives of Cyber Criminal

- Power assurance---to restore criminal's self-confidence or self-worth through **low-aggression means**;---e.g. cyber stalking
- Power assertive---to restore criminal's self-confidence or self-worth through **moderate- to high-aggression means---** not to harm the victim but to get control of the victim;
- Anger (retaliatory)---rage towards a person, group, institution, or a symbol---the offender may believe that they are correcting some injustice
- Sadistic---derive gratification from the pain/suffering of others
- Profit-oriented---material or personal gain

Risk = Threats x Vulnerabilities

Information Security Risks, Threats and Vulnerabilities

Types of Damage

- Interruption---destroyed/unavailable services/resources
- Interception---unauthorized party snooping or getting access to a resource
- Modification--- unauthorized party modifying a resource
- Fabrication---unauthorized party inserts a fake asset/resource

Components of a Threat

- Components
  - Threat agents---criminals, terrorists, subversive or secret groups, state sponsored, disgruntled employees,, hackers, pressure groups, commercial groups
  - Capability---software, technology, facilities, education and training, methods, books and manuals
  - Threat inhibitors---fear of capture, fear of failure, level of technical difficulty, cost of participation, sensitivity to public perception, law enforcement activity, target vulnerability, target profile, public perception, peer perception
  - Threat amplifiers---peer pressure, fame, access to information, changing high technology, deskilling through scripting, skills and education levels, law enforcement activity, target vulnerability, target profile, public perception, peer perception
  - Threat catalysts---events, technology changes, personal circumstances
  - Threat agent motivators---political, secular, personal gain, religion, power, terrorism, curiosity

Threat Agents

- Types
  - Natural---fire, floods, power failure, earth quakes, etc.
  - Unintentional---insider, outsider---primarily non-hostile
  - Intentional---Insider, outsider---hostile or non-hostile (curious)
    - Foreign agents, industrial espionage, terrorists, organized crime, hackers and crackers, insiders, political dissidents, vendors and suppliers

Top ten Database Security Threats

1. **Excessive Privilege Abuse**---users are granted database access privileges that exceed the requirements of their job function; e.g., a university administrator whose job requires only the ability to change student contact information may take advantage of excessive database update privileges to change grades
2. **Legitimate Privilege Abuse** ---- Users may abuse legitimate database privileges for unauthorized purposes; e.g. a rogue health worker who is willing to trade patient records for money
3. **Privilege Elevation**---Attackers may take advantage of database platform software vulnerabilities to convert access privileges from those of an ordinary user to those of an administrator. Vulnerabilities may be found in stored procedures, built-in functions, protocol implementations, and even SQL statements
4. **Database Platform Vulnerabilities**--- Vulnerabilities in underlying operating systems (Windows 2000, UNIX, etc.) and additional services installed on a database server may lead to unauthorized access, data corruption, or denial of service.
5. **SQL Injection**--- a perpetrator typically inserts (or "injects") unauthorized database statements into a vulnerable SQL data channel. Using SQL injection, attackers may gain unrestricted access to an entire database
6. **Weak Audit Trail**--- Weak database audit policy represents a serious organizational risk on many levels.--- regulatory risk, deterrence, and detection and recovery
7. **Denial of Service (DoS)---** access to network applications or data is denied to intended users
8. **Database Communication Protocol Vulnerabilities---** e.g., Four out of seven security fixes in the two most recent IBM DB2 FixPacks address protocol vulnerabilities; similarly, 11 out of 23 database vulnerabilities fixed in the most recent Oracle quarterly patch relate to protocols
9. **Weak Authentication**--- allowing attackers to assume the identity of legitimate database users by stealing or otherwise obtaining login credentials
10. **Backup Data Exposure**--- Backup database storage media is often completely unprotected from attack. As a result, several high profile security breaches have involved theft of database backup tapes and hard disks.

Ten web threats

1. **Bigger, Subtler DDoS Attacks**---Distributed Denial of Service Attacks
2. **Old Browsers, Vulnerable Plug-Ins**---e.g., browser vulnerabilities and, more frequently, the browser plug-ins that handle Oracle's Java and Adobe's Flash and Reader.
3. **Good Sites Hosting Bad Content**---in VOHO watering hole attack, attackers infected legitimate financial and tech industry websites in Massachusetts and Washington, D.C., commonly accessed by their intended victims
4. **Mobile Apps And The Unsecured Web**--- bring-your-own-device movement has led to a surge in consumer-owned devices inside corporate firewalls
5. **Failing To Clean Up Bad Input**---e.g., Since 2010, SQL injection has held the top spot on the Open Web Application Security Project's list of top 10 security vulnerabilities
6. **The Hazards Of Digital Certificates**--- a series of hacks against certificate authorities gave attackers the tools they needed to issue fraudulent SSL certificates that could disguise a malicious website as a legitimate
7. **The Cross-Site Scripting Problem**--- An attacker going after a banking site with a cross-site scripting vulnerability could run a script for a login box on the bank's page and steal users' credentials.
8. **The Insecure 'Internet Of Things**‘--- Routers and printers, videoconferencing systems, door locks and other devices are now networked via Internet protocols and even have embedded Web servers. In many cases, the software on these devices is an older version of an open source library that's difficult
9. **Getting In The Front Door**--- Automated Web bots scrape from Web pages information that can give a competitor better intelligence on your business.
10. **New Technology, Same Problems**--- People click links all day long -- people are pretty trained to think that clicking a link on the Web is safe.

Major Security Threats on Information Systems

1. Intrusion or Hacking---gaining access to a computer system without the knowledge of its owner---Tools: . Poor Implementation of Shopping Carts, Hidden fields in the html forms, Client-side validation scripts, Direct SQL attack, Session Hijacking, Buffer Overflow Forms, Port Scan
2. Viruses and Worms--- programs that make computer systems not to work properly--- Polymorphic Virus, Stealth Virus, Tunneling Virus, Virus Droppers, Cavity Virus
3. Trojan Horse--- These programs are having two components; one runs as a server and another one runs as a client; data integrity attack, steal private information on the target system, store key strokes and make it viewable for hackers, sending private local as an email attachment.
4. Spoofing---fooling other computer users to think that the source of their information is coming from a legitimate user---IP Spoofing, DNS Spoofing, ARP Spoofing
5. Sniffing---used by hackers for scanning login_ids and passwords over the wires. TCPDUmp and Snoop are better examples for sniffing tools.
6. Denial of Service---The main aim of this attack is to bring down the targeted network and make it to deny the service for legitimate users. In order to do DoS attacks, people do not need to be an expert. They can do this attack with simple ping command

Vulnerabilities

- “Some weakness of a system that could allow security to be allowed.”
- Types of vulnerabilities
  - Physical vulnerabilities
  - Natural vulnerabilities
  - Hardware/software vulnerabilities
  - Media vulnerabilities (e.g., stolen/damaged disk/tapes)
  - Emanation vulnerabilities---due to radiation
  - Communication vulnerabilities
  - Human vulnerabilities

How do the vulnerabilities manifest?

- The different types of vulnerabilities manifest themselves via several misuses:
  - External misuse---visual spying, misrepresenting, physical scavenging
  - Hardware misuse---logical scavenging, eavesdropping, interference, physical attack, physical removal
  - Masquerading---impersonation, piggybacking attack, spoofing attacks, network weaving
  - Pest programs---Trojan horse attacks, logic bombs, malevolent worms, virus attacks
  - Bypasses---Trapdoor attacks, authorization attacks (e.g., password cracking)
  - Active misuse---basic active attack, incremental attack, denial of service
  - Passive misuse---browsing, interference, aggregation, covert channels

Examples of Information Security Vulnerabilities

- Information security vulnerabilities are weaknesses that expose an organization to risk.
- **Through employees**: Social interaction, Customer interaction, Discussing work in public locations, Taking data out of the office (paper, mobile phones, laptops), Emailing documents and data, Mailing and faxing documents, Installing unauthorized software and apps, Removing or disabling security tools, Letting unauthorized persons into the office (tailgating) , Opening spam emails, Connecting personal devices to company networks, Writing down passwords and sensitive data, Losing security devices such as id cards, Lack of information security awareness, Keying data
- Through former employees---Former employees working for competitors, Former employees retaining company data, Former employees discussing company matters
- Though Technology---Social networking, File sharing, Rapid technological changes, Legacy systems, Storing data on mobile devices such as mobile phones, Internet browsers
- Through hardware---. Susceptibility to dust, heat and humidity, Hardware design flaws, Out of date hardware, Misconfiguration of hardware

Examples of Information Security Vulnerabilities (Cont.)

- Through software---Insufficient testing, Lack of audit trail, Software bugs and design faults, Unchecked user input, Software that fails to consider human factors, Software complexity (bloatware), Software as a service (relinquishing control of data), Software vendors that go out of business or change ownership
- Through Network---Unprotected network communications, Open physical connections, IPs and ports, Insecure network architecture, Unused user ids, Excessive privileges, Unnecessary jobs and scripts executing , Wifi networks
- Through IT Management---Insufficient IT capacity , Missed security patches, Insufficient incident and problem management, Configuration errors and missed security notices , System operation errors, Lack of regular audits, Improper waste disposal, Insufficient change management, Business process flaws, Inadequate business rules, Inadequate business controls, Processes that fail to consider human factors, Overconfidence in security audits, Lack of risk analysis, Rapid business change, Inadequate continuity planning Lax recruiting processes
- Partners and suppliers---Disruption of telecom services, Disruption of utility services such as electric, gas, water, Hardware failure, Software failure, Lost mail and courier packages, Supply disruptions, Sharing confidential data with partners and suppliers

Risk and Risk management

- Risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization
- Risk management--- “Process of identifying, controlling and minimizing or eliminating security risks that may affect information systems, for an acceptable cost.” --- assessment of risk and the implementation of procedures and practices designed to control the level of risk
- Risk assessment--- “ assessment of threats to, impact on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.”---identification of the risk, analysis of the risk in terms of performance, cost, and other quality factors; risk prioritization in terms of exposure and leverage

Risk management

- Risk management
  - Risk assessment
    - Risk identification---decision driver analysis, assumption analysis, decomposition
    - Risk analysis---cost models, network analysis, decision analysis, quality factor analysis
    - Risk prioritization---risk leverage, component risk reduction
  - Risk control
    - Risk management planning---risk avoidance, transfer, reduction, element planning, plan integration
    - Risk resolution---Simulations, benchmarks, analysis, staffing
    - Risk monitoring---Top 10 tracking, risk assessment, corrective action

Threat Matrix

- Capabilities of a threat versus type of vulnerabilities
- Similar to risk assessment or risk analysis matrix
- Goel and Chen use examples to illustrate a vulnerability matrix and a threat matrix (*www.albany.edu/~**goel**/publications/**goelchen**2005.pdf*)
- Duggan et al illustrate a threat profile matrix. (Sandia Report, SAND2007-5791)

Risk management

- Process of: assessing risk, taking steps to reduce it to an acceptable level, and maintaining that level of risk
- Five principle:
  - **I. Assess risk and determine needs**
    - Recognize the importance of protecting information resource assets
    - Develop risk assessment procedures that link IA to business needs
    - Hold programs and managers accountable
    - Manage risk on a continuing basis
  - **II. Establish a central management focus**
    - Designate a central group for key activities
    - Provide independent access to senior executives to the group
    - Designate dedicated funding and staff
    - Periodically, enhance staff technical skills
  - III. **Implement appropriate policies and related controls**
    - Link policies to business risks
    - Differentiate policies and guidelines
    - Support polices via the central IA group
  - **IV Promote awareness**
    - Educate user and others on risks and related policies
    - Use attention-getting and user-friendly techniques
  - **V Monitor and evaluate policy and control effectiveness**
    - Monitor factor that affect risk and indicate IA effectiveness
    - Use results to direct future efforts and hold managers accountable
    - Be on the lookout for new monitoring tools and techniques

Summary

- Threat, Vulnerability, and Risk are defined
- The enemies of information systems and their motives are briefly discussed
- Types of damage are classified
- Risk management is discussed
- Different types of threats with examples are discussed
- Different vulnerabilities and threats are described at depth