

Introduction to Information Security

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 2 September 19th, 2005

Vulnerability

- Software, hardware or procedural weakness
- Absence or weakness of a resource that can be exploited
- Examples: buggy service, open port, lax physical security

Threat

- Any potential danger
- Threat agent — that or whom carries out (exploits) threat
- Refers to the potential for exploiting the vulnerability
- Examples: intruder coming in through open port, Hurricane Katrina, employee error

Risk

- Likelihood of a threat agent exploiting a vulnerability
- Loss potential or probability
- More vulnerabilities increase risk

Exposure

- being open to potential losses from a threat agent exploiting a vulnerability
- Possible data stolen through break-in
- Down-time due to facility damage

Safeguard (Countermeasure)

- Software configuration, hardware or procedure that eliminates or reduces risk
- Examples: Strong password management, Anti-virus software, Employee training

The CIA Triad

- Confidentiality
- Integrity
- Availabliltiy

Confidentiality — Definition

- Prevention of unauthorized disclosure
- Data on the internal network
- Transmitted data
- Data at destination

Confidentiality — Vulnerabilities

- Network monitoring
- Shoulder surfing
- Stealing passwords
- Social engineering

Confidentiality — Countermeasures

- Encryption
- Network traffic padding
- Strict access control
- Employee training

Integrity — Definition

- Assurance of accuracy and reliability
- Prevention of unauthorized modification

Integrity — Vulnerabilities

- Virus
- Logic Bomb
- Back door
- Integrity — Techniques
- User error — accidental or malicious

Integrity — Countermeasures

- Strict access control
- Intrusion detection
- Encryption
- Restricted access
- Application checking
- Database rules

Availability — Definition

- Reliable and timely access to data and resources
- Predictable and acceptable level of performance
- Secure and quick recovery from failures

Availability — Vulnerabilities

- Device or software failure
- Environmental issues
- Denial of Service (DoS) attacks

Availability — Countermeasures

- Avoid single points of failure
- Backup and redundancy devices
- Data backups
- Intrusion detection

Organizational Security Model

- Framework for achieving CIA
- Technical and non-technical components
- Analyze risks and develop effective counter-measures

Security Goals

- Operational (daily) goals — productivity and task-oriented activities
- Examples: backup procedures, firewall rules
- Tactical goals — longer term
- Examples: network-based authentication, email-based anti-virus
- Strategic goals - longest term
- Examples: corporate VPN, off-site backup facilities
- One level depends upon the other

- Organizational requirements and risk assessment determine goals and objectives

Organizational requirements

- Function of type of organization
- Function of size
- Private business deals with customer satisfaction and competition
- Non-profit and government - serving the community
- Military and police provide community security
- Security must serve organizational requirements — not the reverse!!!

Risk Management

- Identify
- Assess
- Reduce

Risk Identification — Vulnerabilities

- Physical damage
- Equipment malfunction
- Application error
- Human error
- Misuse of data
- Inside and outside attacks

Risk Identification — Threats

- Malware — virus, auto-rooters, trojan-horse
- Vandals — script kiddies
- Crackers — malicious or for hire
- Users — employees, contractors
- Environment — fire, weather, theft
- Commercial software

Risk Assessment — Definition

- Cost/Benefit analysis
- Probability of exposure
- Dollar value of damage
- Quantitative techniques

Risk Assessment - Major Types of Exposure

- Lost data
- Stolen data
- Data tampering
- Breach of confidentiality
- Downtime

Risk Assessment — Major Cost Types

- Embarrassment — e.g. embarrassing employee emails or vanadalized website
- Productivity losses — e.g. lost data, network downtime
- Lost customers — e.g. website down, go elsewhere
- Competitive risk — e.g. trade secrets revealed
- Business liability — e.g. lawsuit from stolen customer database
- Regulatory liability — e.g. HIPAA
- Countermeasures

Safeguards in the Security Model

- Policies
- Standards
- Guidelines
- Procedures

Policies

- Security program goals
- Assignment of responsibility
- Cost/benefits laid out
- Outlines enforcement
- Strategic

Standards

- Compulsory rules
- Examples: wear company badge, IT facility locked and monitored at all times
- Baseline – minimum level of security required
- Standards are developed to meet the baseline
- Government standards exist as well

Guidelines

- Recommended actions and operational guides
- Addresses grey areas of policies
- Policy: access to confidential data must be audited
- Guideline: audits should contain sufficient information to compare with prior reports

Procedures

- Detailed step-by-step actions to achieve a certain task
- Can apply to users or IT staff
- Spell out how policies, standards and guidelines are actually implemented in the operating environment
- Policy: users who access confidential data must be authenticated
- Procedure: How authentication takes place

Safeguards — Major Types

- Accountability Controls — e.g. audit logs, audit automation
- Physical and environmental controls
- Administration controls — e.g. background checks, supervision
- Access controls — e.g. authentication, biometrics
- Cryptography
- Business continuity planning — e.g. backups, off-site facilities
- Computer operations — e.g. which OS, how configured, securing workstations
- Incident handling — e.g. reporting and correction

Basic Security Tenets

- Minimalism
- Defense in Depth
- Vigilance

Minimalism (KISS)

- Safest way to avoid risk is not to introduce it in first place
- Only install what you need
- Only run what you need
- Do not have users you don't need
- Change control system or journal changes

Defense in Depth

- Multi-layered approach to defense
- Example: external firewall, host firewall, IDS, regular penetration testing

Vigilance

- Bit-rot — situation deteriorates if you do nothing
- System changes and threats change
- Check logs, audit users and groups, monitor files
- Keep patches up-to-date
- Test constantly
- Keep on your reading

Summary

- Security is expensive and time-consuming
- Constantly measure risk vs. reward
- Tools are needed both for testing and safeguarding
- FOSS lowers the costs of tools