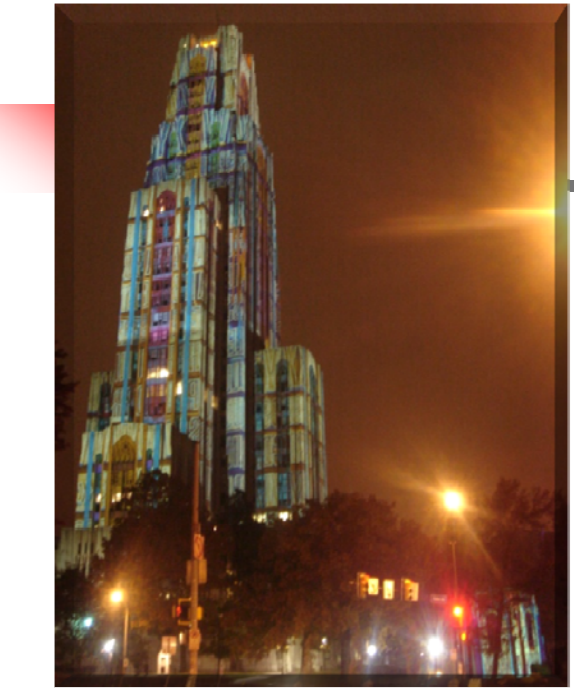
IS 2150 / TEL 2810
Information Security & Privacy



James Joshi
Associate Professor, SIS

Lecture 11
March 31, 2015

Vulnerability Analysis
Risk Management
Legal/Ethical Issues
Physical Security

Objectives

- Understand/explain the issues related to, and utilize the techniques
  - Vulnerability analysis/classification
    - Techniques
    - Taxonomy
  - Security risks management

Vulnerability Analysis

- Vulnerability or security flaw: specific failures of security controls (procedures, technology or management)
  - Errors in code
  - Human violators
  - Mismatch between assumptions
- Exploit: Use of vulnerability to violate policy
- Attacker: Attempts to exploit the vulnerability

Techniques for Detecting Vulnerabilities

- System Verification
  - Determine preconditions, post-conditions
  - Validate that system ensures post-conditions given preconditions

  Can prove the absence of vulnerabilities
- Penetration testing
  - Start with system/environment characteristics
  - Try to find vulnerabilities

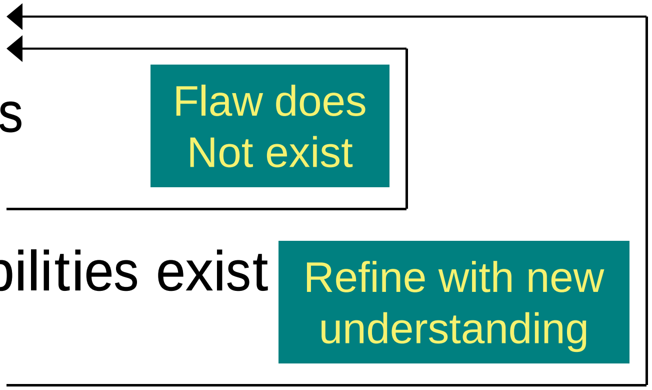
  Can not prove the absence of vulnerabilities

Types/layers of Penetration Testing

- Black Box (External Attacker)
  - External attacker has no knowledge of target system
  - Attacks built on human element – Social Engineering
- System access provided (External Attacker)
  - Red team provided with limited access to system
  - Goal is to gain normal or elevated access
- Internal attacker
  - Red team provided with authorized user access
  - Goal is to elevate privilege / violate policy

Red Team Approach
Flaw Hypothesis Methodology:

- Information gathering
  - Examine design, environment, system functionality
- Flaw hypothesis
  - Predict likely vulnerabilities
- Flaw testing
  - Determine where vulnerabilities exist
- Flaw generalization
  - Attempt to broaden discovered flaws
- Flaw elimination (often not included)
  - Suggest means to eliminate flaw



Flaw does Not exist

Refine with new understanding

Problems with Penetration Testing

- Nonrigorous
  - Dependent on insight (and whim) of testers
  - No good way of evaluating when “complete”
- How do we make it systematic?
  - Try all classes of likely flaws
  - *But what are these?*
- Vulnerability Classification!

Vulnerability Classification

- Goal: describe spectrum of possible flaws
  - Enables design to avoid flaws
  - Improves coverage of penetration testing
  - Helps design/develop intrusion detection
- How do we classify?
  - By how they are exploited?
  - By where they are found?
  - By the nature of the vulnerability?

Example flaw: xterm log

- *xterm* runs as root
  - Generates a log file
  - Appends to log file if file exists
- Problem: ln /etc/passwd log_file
- Solution

```
if (access(“log_file”, W_OK) == 0)
    If ((fd = open(“log_file”, O_WRONLY|O_APPEND)) < 0) {
    -  error handling
    }
```

What can go wrong?

Example: Finger Daemon *(exploited by Morris worm)*

- *finger* sends name to *fingerd*
  - *fingerd* allocates 512 byte buffer on stack
  - Places name in buffer
  - Retrieves information (local finger) and returns
- Problem: If name > 512 bytes, overwrites return address
- Exploit: Put code in “name”, pointer to code in bytes 513+
  - Overwrites return address

RISOS:Research Into Secure Operating Systems (7 Classes)

1. Incomplete parameter validation
   - E.g., buffer overflow –
2. Inconsistent parameter validation
   - Different routines with different formats for same data
3. Implicit sharing of privileged / confidential data
   - OS fails to isolate processes and users
4. Asynchronous validation / inadequate serialization
   - Race conditions and TOCTTOU flaws
5. Inadequate identification /authentication / authorization
   - Trojan horse; accounts without passwords
6. Violable prohibition / limit
   - Improper handling of bounds conditions (e.g., in memory allocation)
7. Exploitable logic error
   - Incorrect error handling, incorrect resource allocations etc.

Protection Analysis Model Classes

- Pattern-directed protection evaluation
  - Methodology for finding vulnerabilities
- Applied to several operating systems
  - Discovered previously unknown vulnerabilities
- Resulted in two-level hierarchy of vulnerability classes
  - Ten classes in all

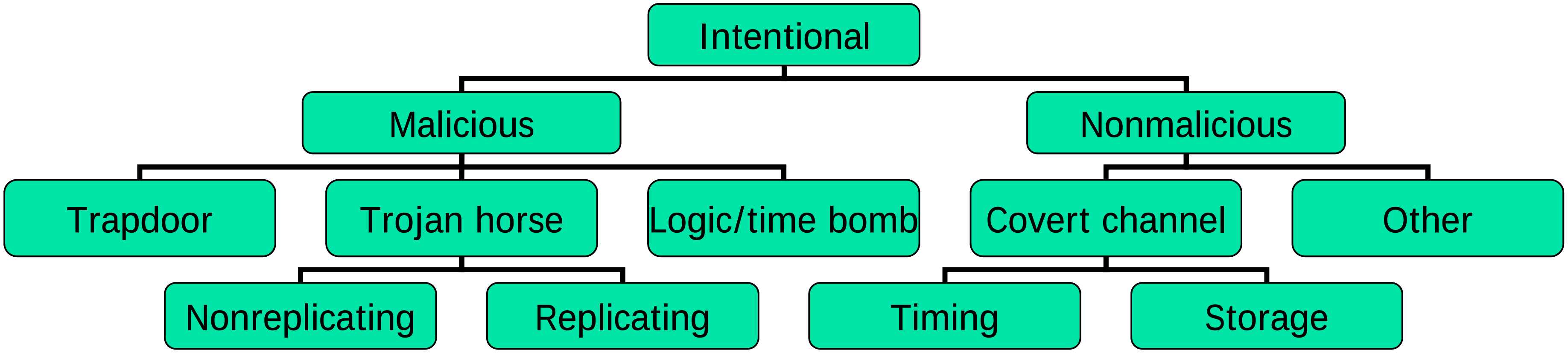
PA flaw classes

1. Improper protection domain initialization and enforcement
   a. *domain*: Improper choice of initial protection domain
   b. *exposed representations*: Improper isolation of implementation detail (Covert channels)
   c. *consistency of data over time*: Improper change
   d. *naming*: Improper naming (two objects with same name)
   e. *residuals*: Improper deallocation or deletion
2. Improper validation *validation of operands, queue management dependencies*:
3. Improper synchronization
   a. *interrupted atomic operations*: Improper indivisibility
   b. *serialization*: Improper sequencing
4. Improper choice of operand or operation *critical operator selection errors*

NRL Taxonomy

- Three classification schemes
  - How did it enter
  - When was it “created”
  - Where is it

Genesis



Intentional

Malicious

Nonmalicious

Trapdoor

Trojan horse

Logic/time bomb

Covert channel

Other

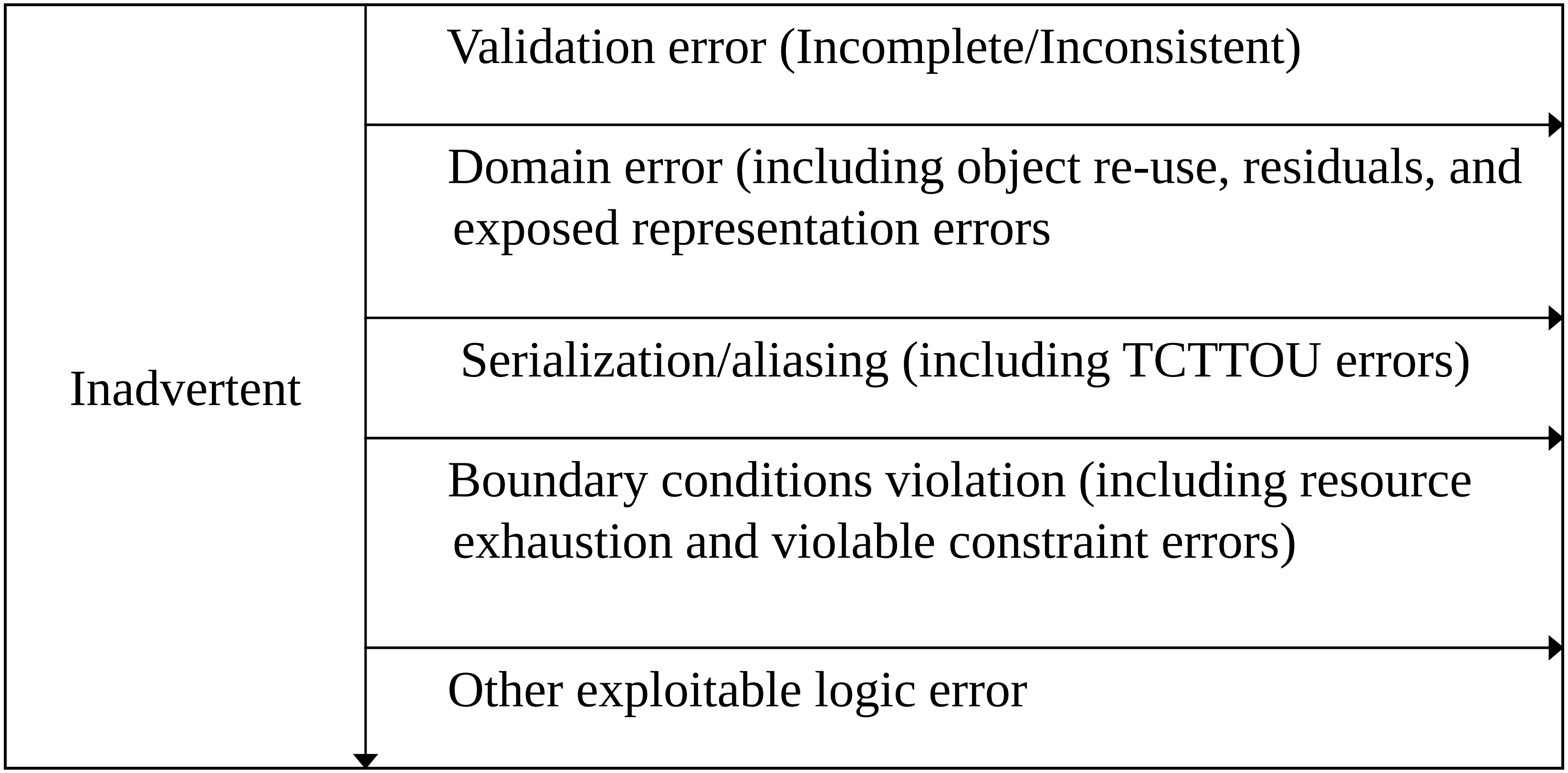
Nonreplicating

Replicating

Timing

Storage

NRL Taxonomy (Genesis)



Inadvertent

Validation error (Incomplete/Inconsistent)

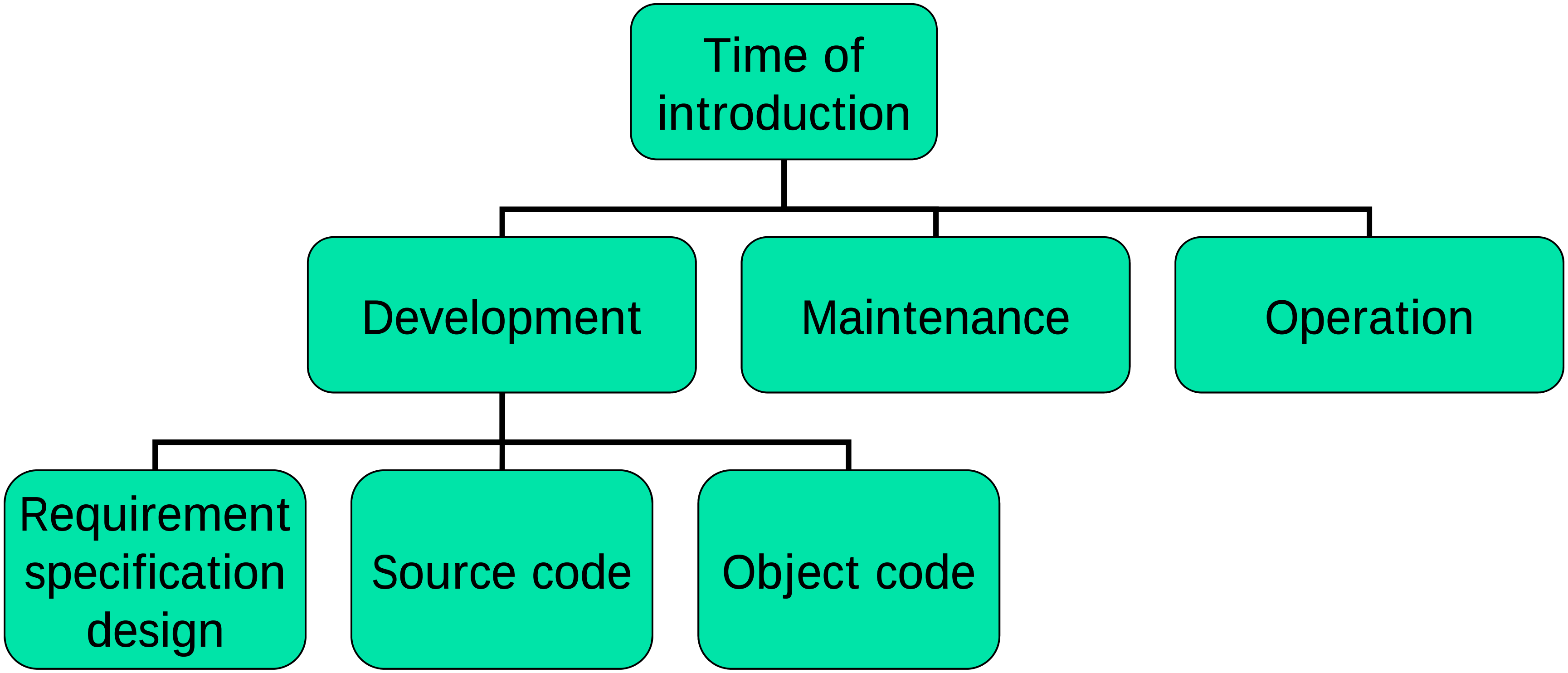
Domain error (including object re-use, residuals, and exposed representation errors

Serialization/aliasing (including TCTTOU errors)

Boundary conditions violation (including resource exhaustion and violable constraint errors)

Other exploitable logic error

NRL Taxonomy: Time



Time of introduction

Development

Maintenance

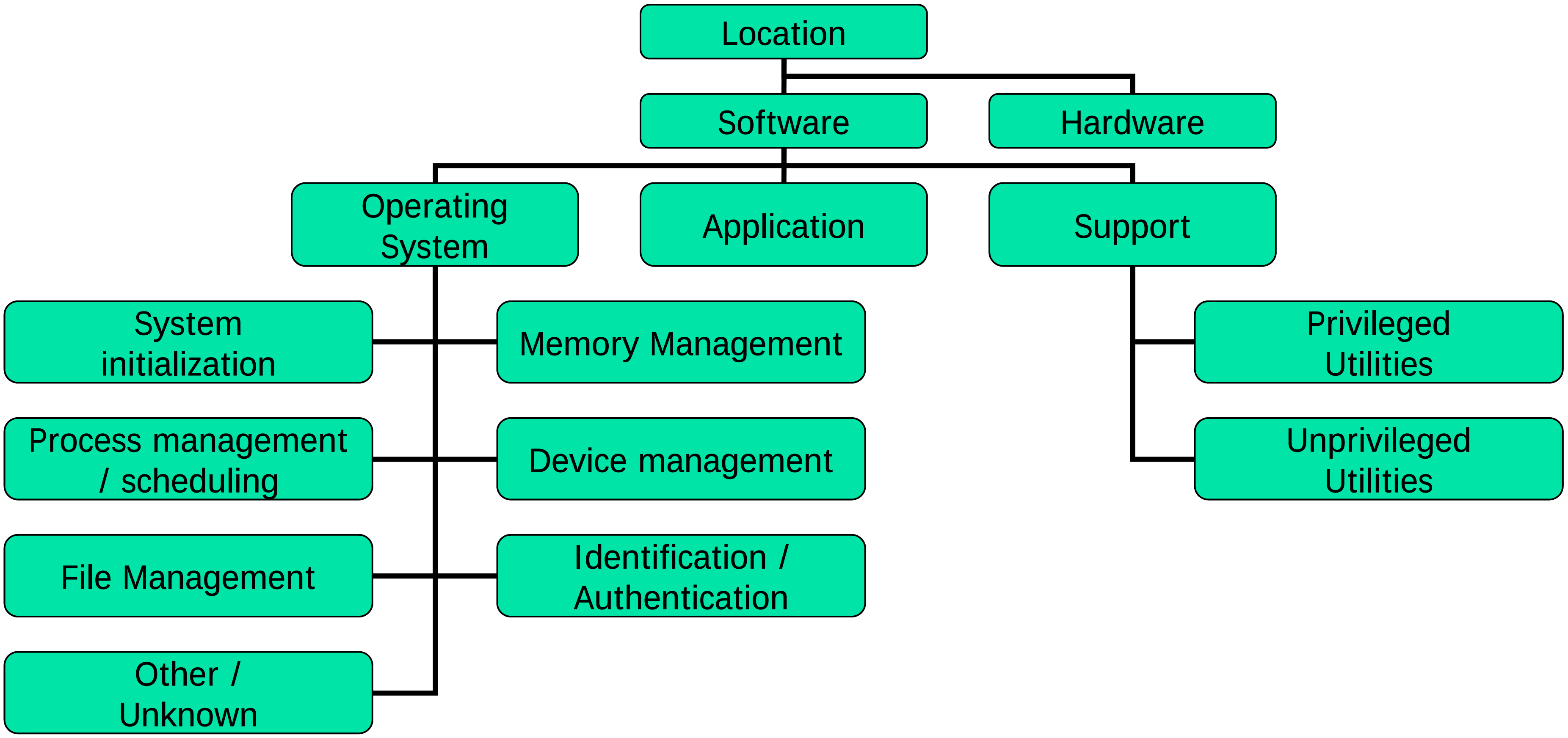
Operation

Requirement specification design

Source code

Object code

NRL Taxonomy: Location



Aslam’s Model

- Attempts to classify faults unambiguously
  - Decision procedure to classify faults
- Coding Faults
  - Synchronization errors
    - Timing window
    - Improper serialization
  - Condition validation errors
    - Bounds not checked
    - Access rights ignored
    - Input not validated
    - Authentication / Identification failure
- Emergent Faults
  - Configuration errors
    - Wrong install location
    - Wrong configuration information
    - Wrong permissions
  - Environment Faults

Common Vulnerabilities and Exposures (cve.mitre.org)

- Captures *specific* vulnerabilities
  - Standard name
  - Cross-reference to CERT, etc.
- Entry has three parts
  - Unique ID
  - Description
  - References

Name	CVE-1999-0965
Description	Race condition in xterm allows local users to modify arbitrary files via the logging option.

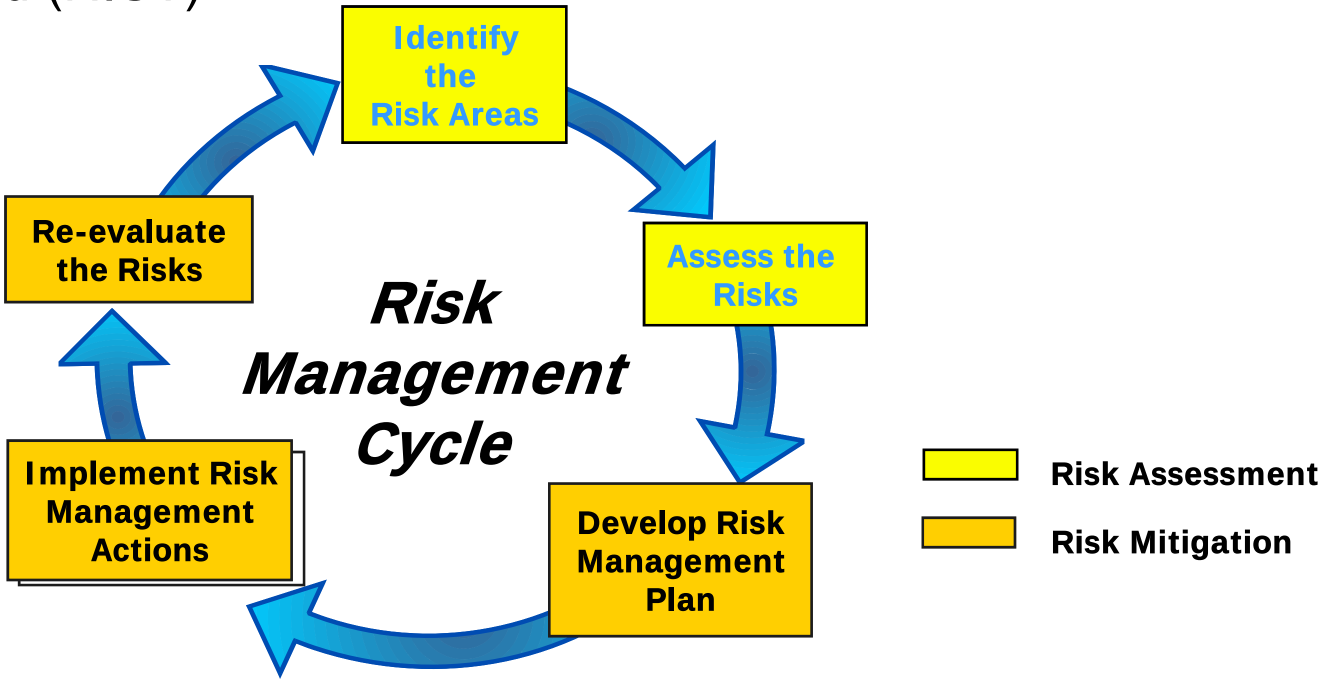
References
•CERT:CA-93.17
•XF:xterm

Risk Analysis

Overview of
Risk, Cost-benefit analysis

Risk Management

- The process concerned with identification, measurement, control and minimization of security risks in information systems to a level commensurate with the value of the assets protected (NIST)



Identify the Risk Areas

Assess the Risks

Develop Risk Management Plan

Implement Risk Management Actions

Re-evaluate the Risks

Risk Management Cycle

🟨 Risk Assessment

🟧 Risk Mitigation

Risk

- The *likelihood* that a particular *threat* using a specific *attack*, will exploit a particular *vulnerability* of a system that results in an undesirable *consequence* (NIST)
  - *Likelihood* of the threat occurring is the estimation of the probability that a threat will succeed in achieving an undesirable event

Risk Assessment/Analysis

- A process of analyzing *threats* to and *vulnerabilities* of an information system and the *potential impact* the loss of information or capabilities of a system would have
  - List the threats and vulnerabilities
  - List possible control and their cost
  - Do cost-benefit analysis
    - Is cost of control more than the expected cost of loss?
- The resulting analysis is used as a basis for identifying appropriate and cost-effective counter-measures
  - Leads to proper security plan

Risk Assessment steps

- Identify assets
  - Hardware, software, data, people, supplies
- Determine vulnerabilities
  - Intentional errors, malicious attacks, natural disasters
- Estimate likelihood of exploitation
  - Considerations include
    - Presence of threats
    - Tenacity/strength of threats
    - Effectiveness of safeguards
  - Delphi approach
    - Raters provide estimates that are distributed and re-estimated

Risk Assessment steps (2)

- Compute expected annual loss
  - Physical assets can be estimated
  - Data protection for legal reasons
- Survey applicable (new) controls
  - If the risks of unauthorized access is too high, access control hardware, software and procedures need to be re-evaluated
- Project annual savings of control

Example 1

- Risks:
  - disclosure of company confidential information,
  - computation based on incorrect data
- Cost to correct data: $1,000,000
  - @10% liklihood per year: $100,000
  - Effectiveness of access control sw:60%: -$60,000
  - Cost of access control software: +$25,000
  - Expected annual costs due to loss and controls:
    - $100,000 - $60,000 + $25,000 = $65,000
  - Savings:
    - $100,000 - $65,000 = $35,000

Example 2

- Risk:
  - Access to unauthorized data and programs
    - 100,000 @ 2% likelihood per year: $2,000
  - Unauthorized use of computing facility
    - 100,000 @ 40% likelihood per year: $4,000
- Expected annual loss:

  $6,000
- Effectiveness of network control: 100%

  -$6,000

Example 2 (2)

Control cost	
Hardware	+$10,000
Software	+$4,000
Support personnel	+$40,000
Annual cost:	+$54,000
Expected annual cost	
(6000-6000+54000)	+$54,000
Savings	
(6000 – 54,000)	-$48,000

Legal & Ethical Issues

Some Arguments against Risk Analysis

- Not precise
  - Likelihood of occurrence
  - Cost per occurrence
- False sense of precision
  - Quantification of cost provides false sense of security
- Immutability
  - Filed and forgotten!
  - Needs annual updates
- No scientific foundation (not true)
  - Probability and statistics

Laws and Security

- Federal and state laws affect privacy and secrecy
  - Rights of individuals to keep information private
- Laws regulate the use, development and ownership of data and programs
  - Patent laws, trade secrets
- Laws affect actions that can be taken to protect secrecy, integrity and availability

Copyrights

  - Designed to protect *expression* of ideas
  - Gives an author exclusive rights to make copies of the *expression* and sell them to public
- Intellectual property (copyright law of 1978)
  - Copyright must apply to an original work
  - It must be done in a tangible medium of expression
- Originality of work
  - Ideas may be public domain
- Copyrighted object is subjected to fair use

Copyright infringement

  - Involves copying
  - Not independent work
    - Two people can have copyright for identically the same thing
- Copyrights for computer programs
  - Copyright law was amended in 1980 to include explicit definition of software
  - Program code is protected not the algorithm
  - Controls rights to copy and distribute

Patent

- Protects innovations
  - Applies to results of science, technology and engineering
  - Protects new innovations
    - Device or process to carry out an idea, not idea itself
  - Excludes newly discovered laws of nature
    - 2+2 = 4

Patent

- Requirements of novelty
    - If two build the same innovations, patent is granted to the first inventor, regardless of who filed first
    - Invention should be truly novel and unique
    - Object patented must be non-obvious
- Patent Office registers patents
    - Even if someone independently invents the same thing, without knowledge of the existing patent
- Patent on computer objects
    - PO has not encouraged patents for software – as they are seen as representation of an algorithm

Trade Secret

- Information must be kept secret
  - If someone discovers the secret independently, then there is no infringement – trade secret rights are gone
  - Reverse-engineering can be used to attack trade secrets
- Computer trade secret
  - Design idea kept secret
  - Executable distributed but program design remain hidden

Comparison

	Copyright	**Patent**	**Trade secret**
Protects	Expression of idea	Invention	Secret information
Object made public	Yes: intention is to promote	Design filed at patent office	No
Requirement to distribute	Yes	No	No
Ease of filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested	No filing
Duration	Life of human originator or 75 years of company	19 years	Indefinite
Legal protection	Sue if copy sold	Sue if invention copied	Sue if secret improperly obtained
Examples	Object code, documentation	Hardware	Source code

Computer crime

- Hard to predict for the following reason
  - Low computer literacy among lawyers, police agents, jurors, etc.
  - Tangible evidence like fingerprints and physical clues may not exist
  - Forms of asset different
    - Is computer time an asset?
  - Juveniles
    - Many involve juveniles

Computer Crime related laws

- Freedom of information act
  - Provides public access to information collected by the executive branch of the federal government
- Privacy act of 1974
  - Personal data collected by government is protected
- Fair credit reporting act
  - Applies to private industries – e.g., credit bureaus
- Cryptography and law
  - France: no encryption allowed (to control terrorism)
  - US, UK, Canada, Germany:
    - Control on export of cryptography; but they are published!

Ethics

- An objectively defined standard of right and wrong
- Often idealistic principles
- In a given situation several ethical issues may be present
- Different from law

Law vs Ethics

Law

- Described by formal written documents
- Interpreted by courts
- Established by legislatures representing all people
- Applicable to everyone
- Priority determined by laws if two laws conflict
- Court is final arbiter for right
- Enforceable by police and courts

Ethics

- Described by unwritten principles
- Interpreted by each individual
- Presented by philosophers, religions, professional groups
- Personal choice
- Priority determined by an individual if two principles conflict
- No external arbiter
- Limited enforcement

Ethics Example

- Privacy of electronic data
  - “gentlemen do not read others’ mail” - but not everyone is a gentleman!
  - Ethical question: when is it justifiable to access data not belonging to you
    - One approach: Protection is user’s responsibility
    - Another: supervisors have access to those supervised
    - Another: justifiably compelling situation

Codes of ethics

- IEEE professional codes of ethic
  - To avoid real or perceived conflict of interest whenever possible, and to disclose them to affected parties when they do exist
  - To be honest and realistic in stating claims or estimates based on available data
- ACM professional codes of ethics
  - Be honest and trustworthy
  - Give proper credit for intellectual property

Physical Security

Physical Security

- Often ignored or considered as of little or no concern
  - If someone working late steals a laptop – the fancy firewall defenses won’t help!
- A NY investment bank spent tens of thousands of dollars on comsec to prevent break-in during the day, only to find that its cleaning staff opened the doors at night!
- A company in SFO had more than $100,000 worth of computers stolen over a holiday; an employee had used his electronic key card to unlock the building and disarm the alarm system

Physical security in security plan

- Organizational security plan should include
  - Description of physical assets to be protected
  - Description of physical areas where the assets are located
  - Description of security perimeter
  - Threats (attacks, accidents, natural disasters)
  - Physical security defense and cost-analysis against the value of information asset being protected

Disaster Recovery

- Natural disasters
    - Flood/Falling water
    - Fire
    - Earthquake
    - Other environmental conditions
        - Dust, explosion (terrorist act), heat/humidity, electrical noise, lighting
- Power loss
    - Uninterruptible power supply
    - Surge protectors
- Accidents: food & drink

Physical security plan

- Should answer (at least) the following
  - Can anybody other than designated personnel physically access the computer resources?
  - What if someone has an outburst and wants to smash the system resources?
  - What if an employee from your competitor were to come to the building unnoticed?
  - What are the consequences in case of fire?
  - How to react in case of some disaster?

Contingency planning

“key to successful recovery is adequate planning”

- Backup/off-site backup
- Cold-site/hot-site
  - Cold site: facility with power/cooling where computing system can be installed to begin immediate operation
  - Hot-site: facility with installed and ready to use computing system.
- Theft prevention
  - Prevent access: guards; locks; cards
  - prevent portability: locks, lockable cabinets
  - detect exit: like in library

Disposal of Sensitive Media

- Shredders
  - Mainly for paper; also used for diskettes, paper ribbons and some tapes
- Sanitizing media before disposal
  - Completely erase data
  - ERASE and DELETE may not be enough
  - Overwrite data several times
- Degaussers
  - Destroys magnetic fields
  - Fast way to neutralize a disk or tape

TEMPEST: Emanations protections

- Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions
  - All electronic and electromechanical info. processing equipment can produce unintentional data-related or intelligence-bearing emanations which, if intercepted and analyzed, disclose the info. transmitted, received, handled or otherwise processed (NSTISSAM 1-00)
  - program certifies an equipment as not emitting detectable signals
- Enclosure
  - Completely cover a tempest device
    - Shielded cable
    - Copper shielding a computer?
- Emanation modification
  - Similar to generating noise

Summary

- Vulnerability Analysis – taxonomy
- Risk Management – cost benefit analysis
- Legal & Ethical Issues
- Physical security