Computer and Network Security

R. E. Newman

Computer & Information Sciences & Engineering
University Of Florida
Gainesville, Florida 32611-6120
nemo@cise.ufl.edu

Introduction to Computer and Network Security

1 Security Goals

1. Confidentiality
2. Integrity
3. Availability

1.1 Confidentiality

only authorized entities may read info
only authorized entities may know communication is taking place at all

1.2 Integrity

more difficult - includes:

1. precision
2. accuracy
3. consistency,
4. only modified in acceptable ways by authorized entities
5. 3 aspects (Welke & Mayfield):
    (a) authorized actions
    (b) separation & protection of resources
    (c) error detection & correction

1.3 Availability

also difficult - data & services -

1. usability
2. capacity to meet needs
3. timely access/results
4. fairness

... sometimes also included...

1.4 Authenticity

know origin of object or modifications

1.5 Non-repudiation

author not able to deny role

2 Terms

2.1 computing system

h/w, s/w, stg media, data, people that do computing tasks

2.2 Exposure

form of loss

2.3 Vulnerability

weakness that may be exploited for loss

2.4 Attack

an attempt to exploit a vulnerability

2.5 Threat

circumstances or agents that could cause loss

2.6 Control

measure to reduce vulnerability

3 Cost of Controls

3.1 financial

3.2 time

1. deployment
2. operational
3. computer/network delays

3.3 convenience, availability

3.4 CPU cycles

3.5 space

1. physical
2. memory
3. disk

Principle of Effectiveness

A control is only effective if you use it properly.
”Use it or lose it”

4 Risk Analysis and Security Planning

1. Risk Assessment
   (a) Inventory and valuate assets
   (b) Evaluate threats
   (c) Gauge vulnerabilities
2. Recommend Controls

4.1 Risk Assessment

4.1.1 Inventory and valuate assets

what is functional importance to mission?
would organization be able to function without this resource?
Note that there are both levels (thresholds) and temporal dependencies....
Note also that information resources, especially software and data, are difficult to value properly - incorrect operation of a $39 program could cause great financial liability; incorrect data in an embedded system could cause loss of life and property

4.1.2 Evaluate threats

Who/what is likely to cause loss/harm?
What valuables could others want to steal or damage?
Who may have political or social agendas that would motivate them to attack us?
What types of loss in the infrastructure are likely?
What forms of natural disasters are likely, ...?

4.1.3 Gauge vulnerabilities

where are the weak points?
Systematic approaches are good, but the system may miss entire vulnerability types...

Principle of Easiest Penetration

An attacker will exploit any vulnerability available, not just the ones of which we are aware, much less those for which we have the strongest controls.
"Weak link in chain"

4.2 Recommend Controls

Provide adequate controls to reduce

- dangerous vulnerabilities (i.e., ones whose exploit would severely impair security of the resource) ... for ...
- critical resources (i.e., ones without which the mission-critical tasks cannot be performed adequately) ... for which there are ...
- significant threats (i.e., the vulnerability is likely to be tested)

Principle of Adequate Protection

Protection should be comensurate with the value of the asset.
”All bikes weigh 50 lbs”

5 Assets

5.1 H/W

CPU, memory, disk space, peripherals

5.2 S/W

applications, OS, utilities

5.3 Data

config files, application input/output

5.4 People

data entry, developers, administrators, ...

6 Threats types

6.1 Interruption

prevent delivery of data, hardware, or services

6.2 Interception

passively observe data, hardware, or service use

6.3 Modification

actively change data, hardware, or code

6.4 Fabrication

actively make up data, hardware, or code

7 Controls by Goal

1. Confidentiality
2. Integrity
3. Availability
4. Authenticity
5. Non-repudiation

7.1 Confidentiality

- Encryption
- Access control (for r)
- Indirection

7.2 Integrity

- Access control (for w)
- Consistency checking
- Integrity checks
- MACs
- Concurrency control

7.3 Availability

- Access control (for x, locks)
- Redundancy
- Fault tolerance
- Monitoring
- Priority mechanisms
- Scheduling

7.4 Authenticity

- Secrets (e.g., passwords, PINs)
- Digital signatures (symmetric or asymmetric)

7.5 Non-repudiation

- Digital signatures (asymmetric)
- Trusted third party

8 Control Mechanisms by Type

1. Access Control
2. Cryptography
3. Monitoring
4. Software Controls
5. Policies

8.1 Access Control

- Requires I & A = identification and authentication plus RM = reference monitor
- Lock & Key
- ACL
- CL
- Change management
- Obscurity

8.2 Cryptography

- Encryption
- MACs
- Digital signatures
- Cryptographic protocols

8.3 Monitoring

- Audit facilities
- Resource pinging
- Network sniffing/protocol analysis
- IDSs
- Anomaly detectors

8.4 Software Controls

- Internal program controls (usually I&A, AC)
- OS controls
  - I&A
  - AC
  - process isolation
  - file protection
  - audit
- Development Controls
  - Standards for quality, process (ISO 9000)
  - Reviews
  - Testing
  - Separation of duty

8.5 Policies

- Establishing policy
- Training
- Enforcement/Monitoring

9 Protection

1. Physical Protection
2. H/W-based protection
3. OS-based protection
4. Application-level protection

9.1 Physical Protection

- Doors
- locks
- shielding
- surge protectors
- UPSs
- climate control, ...

9.2 H/W-based protection

- Mode bits and protected instructions
- write protection
- base & bounds registgers
- VM
- tagged memory
- dongles, ...

9.3 OS-based protection

- I & A
- ACLs
- protection/net groups
- gates/rights amplification, ...

9.4 Application-level protection

- password protection
- crypto, ...

10 Effectiveness of Controls

10.1 Policy

10.2 Awareness

- Need for security/value of resources
- Procedures

10.3 Operational cost/Compliance

10.4 Overlapping controls

Principle of security in depth

There should be more than one control per vulnerabiliity type so that failure of one control does not completely compromise system
"Belt & Suspenders"

10.5 Periodic Review