COMP 424

Lecture 02

Security Goals (Requirements)

- What makes a “secure” system?
  - Financial “Security” requirements
  - Home “security”
  - Homeland “security”
  - Physical “security”
  - Computer “security”
- All these concepts of security have different requirements. We are, of course, interested mostly on computer security; which requires three items:

Thing one:

- Confidentiality:

  Computer related assets are only available to authorized parties. Only those that should have access to something will actually get that access.

  - “Access” isn't limited to reading. But also to viewing, printing or...
  - Simply even knowing that the particular asset exists (steganography)

  – Straight forward concept but very hard to implement.

Thing two:

- Integrity

  Can mean many things: Something has integrity if it is:

  - Precise
  - Accurate
  - Unmodified
  - Consistent
  - Meaningful and usable

Integrity

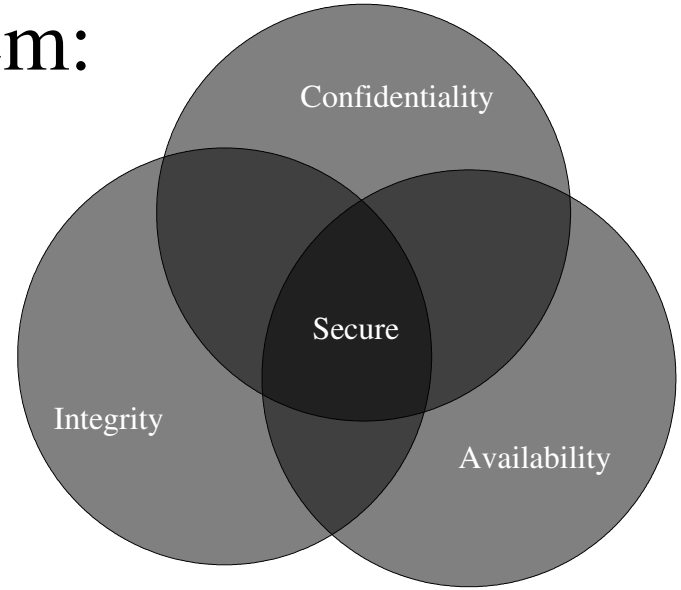
- Three important aspects towards providing computer related integrity:
  - Authorized actions
  - Seperation and protection of resources
  - Error detection and correction.
- Again, rather hard to implement; usually done so through rigorous control of who or what can have access to data and in what ways.

Thing three:

- Availability
  - There is a timely response to our requests
  - There is a fair allocation of resources (no starvation)
  - Reliability (software and hardware failures lead to graceful cessation of services and not an abrupt crash)
  - Service can be used easily and in the manner it was intended to be used.
  - Controlled concurrency, support for simultaneous access with proper deadlock and access

Precense of all three

- The presence of all three things yeilds a secure system:



Vulnerabilities

- When we are tasked with providing security we must know what vulnerabilities exist in order to provide effective controls.
- Hardware vulnerabilities:
  - "Involuntary machine slaughter" (bumps, coffee, smoke)
  - "Machinicide"* hit with hammers, shot, pried open with screwdrivers...
- These attacks primarily limit availability

Software

- Software based attacks can range from obvious to subtle to never detected.
  - Bank interest is a classic case of software vulnerability and exploit.
- Software deletion is common but rather obvious and quickly limits availability.
  - This has plagued Micro$oft for decades since there was no configuration management or permissions in the Windows 3.1,95,95,Me code branch. (Unix has had it from day one)

Version control

- Version control is a sort of deletion operation.
- Can you provide an example of why you wouldn't want to replace version 1.7 with version 1.9 or 2.0?
- How catastrophically bad could such an action be?

Software modification

- More insidious is the concept of “modifying” the software so that it does something other than it was originally intended:
  - Logic bombs (trigger by a set of circumstances)
  - Trojan horse
  - Virus
  - Trapdoor
  - Information leaks

Software theft

- Lastly we can breach security through the theft of software:
  - “Software authors and distributors are entitled to fair compensation for use of their product, as are musicians and book authors.”

Data Vulnerabilities

- Hardware and software can be considered easier to secure because it requires sophisticated technical knowledge.
- Data on the other hand is understed by the general public quite easily so you can no longer rely on lack of technical knowledge to provide any level of security for raw data.

Value of data?

- Almost any piece of hardware is composed of about $17.95 worth of steel, plastic and sand.
- Software is pretty cheap too; at least compared to...
- Data can be hideously valuable. In fact many companies would argue that data (information) is the only important asset they have.
  - (Fail Safe, 1964)

- But the value of data can also be short lived or highly unpredictable.
- Principle of Adequate Protection:

  "Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value."

Data Confidentiality

- Data can be gathered by many means
  - Wire tapping
  - Dumpster diving
  - Survelliance
  - Electromagnetic radiation (tempest project)
  - Inference!!! (John Edwards; yick)
- Confidentiality of data means that only authorized people that should know/see the data can actually know it.

Data Integrity

- The integrity of data needs to be guaranteed as well. This means that data cannot be tampered with , deleted, modified or forged.
  - Salami attack (bank; shave a little meat here and there... press it in a mold and viola! Salami!)
  - Spock in “The Menagerie” [actually he SHOULD have been court martialled!]
  - Replay of transactions

Data availability

- The data should be available to those that are authorized to receive it.

Network problems

- Networks present further problems
- Access
  - Access to computing equipment to perform tasks they weren't intended to.
  - Costs are spread to legitamate users
  - Remote damage, modification or deletion of assets
- Key People
  - Single point of failure
  - Political / ethical problems

Computer Criminals

- Amateurs
  - Commit most of the crime.
  - Ordinary people of recognize and exploit an already present vulnerability.
  - Wide range of motivations
  - Unorganized

- Crackers (NOT Hackers! “Crackers!” and not the Keebler elf kind either.)
  - Sophisticated
  - Set of motivations is smaller and frequently limited to self satisfaction (but don't dismiss this offhandly because it can be one the most powerful motiviations.)
  - Highly organized
  - Less prevelent than amateurs

- Career Criminals
  - Specialized, focused
  - Motivated by profit
  - Used as a resource by other illegal organizations
  - Electronic espionage
  - Probably better funded than amateurs or crackers

Methods of Defense

- Controls
  - Software
    - Internal program controls
    - Operating and network system controls
    - Independent control programs
    - Development controls
    - Scrutiny (I added this)

- Hardware Controls
  - Smart cards
  - Locks, cables, alarms
  - Verification devices (fingerprint, retinal, breath, ...)
  - Firewalls
  - Intrusion detection
  - Dedicated access hardware

- Policies and Procedures.
  - These can be highly unreliable and difficult to establish, enforce or prosecute but are necessary in EVERY situation.

Encryption

- The process of scrambling data so that unauthorized persons cannot obtain the cleartext data.
- Encryption is highly effective, inexpensive and simple to implement and enforce (nearly eliminating the need for prosecution)

Effectiveness of Controls

- Merely having controls is useless if they are ineffective.
  - Awareness of problem: If people are not aware of the need for a particular security measure they will most likely ignore it or refuse to abide by it
  - Likelihood of use: If it is so complicated or difficult to use that nobody will accept to do then it is ineffective and useless.
  - Overlapping controls: Multiple controls that overlap in areas of effective use contribute to the overall effectiveness of the system.

Principle of Effectiveness:

"Controls must be used – and used properly – to be effective. They must be efficient, easy to use, and appropriate"