COMP 424
Computer System Security

Lecture 01
Attacks, Goals and Vulnerabilities

What do we mean by “secure”?

- At one time Bank robbery was common. Now its very rare. What has changed or been implemented to provide this security?
  - Sophisticated alarms
  - Criminal investigation techniques (DNA testing)
  - Change in “assets” (cash was/is inherently insecure)
  - Improvements in communication and transportation
- Risk becomes so high that it is no longer beneficial.

Security is all about protecting valuables

- In our case the “valuables” are computer related assets instead of money
  - Though these days money is so electronic that one can argue that the protection of money is a subset of computer asset security
- Information seems to be the currency of the 21st century.

Money vs. Information

- Size and portability
  - Banks are large and unportable.
  - Storage of information can be very small and extremely portable. (So small that an entire corporations intellectual property can be stored on something the size of a postage stamp.)

- Ability to avoid physical contact
  - Banks: physical interaction with the bank and the loot is unavoidable or impossible to circumvent
  - Computers: require no physical contact to either gain access to, copy or remove data.
- Value of assets:
  - Bank: generally very high (or why would somebody bother to put it in a bank?)
  - Computers: Variable, from very low (useless) to very high.

Side bar 1-1

- Some people (or even groups of people) are just plain idiots... [paraphrasing here ;-)]
  - “[The software is too complicated to be understood by a hacker.] And even if they could [understand it], they wouldn't want to.”
- Compare that to the next quote:
  - “As a software designer, I assume that all digital technologies are fair game for being played with... it takes a special kind of personality to look at a software-enabled device and see the potential for manipulation and change – a hacker personality”
  - (Or an inquisitive 2-year old)

Security is not always about locks, firewalls and hardware

- Public Image often gets in the way of defeats security.
  - Would you deposit your money in a bank that just revealed that it lost fifteen million dollars due to a computer security oversight?
  - Things like this probably happen a lot more often than we care to have nightmares about.

So what does computer security concern itself with?

- The entire system:
  - Hardware
  - Software
  - Storage media
  - Data
  - Memory
  - People
  - Organizations
  - Communications

Principle of Easiest Penetration

- An intruder must be expected to use any available means of penetration. The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.

Attacks

- Vulnerability: A weakness in the security system.
- Threat: a set of circumstances that has the potential to cause loss or harm.
- Attack: A human expoitation of a vulnerability.
- Control: A protective measure. An action, device or measure taken that removes, reduces or neutralizes a vulnerability.

Types of threats

- Interception
  - A perpetrator hijacks or takes control
- Interruption
  - A perpetrator prevents the normal operation.
- Modification
  - Alteration of data or assets to something else
- Fabrication
  - Insertion of network data or transactions.

Method, Opportunity and Motive

- Method: The skills knowledge and tools that enable the attack
- Oppotunity: The time, access and circumstances that allow for the attack
- Motive: The reason why the perpetrator wants to commit the attack

Computer Security

- When we discuss computer security we are talking about three aspects:
- Confidentiality: Ensuring that computer-related assets are only accessible by authorized parties.
  - “Access” means the ability to read, view, print an asset or simply know that the asset exists (steganography)

- Integrity: Assets can only be modified by authorized parties and/or in authorized manners.
  - This ensures that the asset remain valid
  - “Modified” includes writing, changing, changing status, deleting and creating

- Availability: assets are available to authorized parties only at appropriate times.