Lecture 23: Security

- Definition, aspects
- types of threats
- computer assets and typical threats to them
- protection
  - user oriented
  - data oriented
- password protection
- types of intruders and intrusion techniques
- malicious programs (viruses and the like)

Computer security aspects

- A set of procedures and computer tools designed to protect the computer data and equipment and ensure unencumbered operation of computer system
- three aspects:
  - secrecy - information on computer system is only accessible to authorized users
  - integrity - computer system assets can be modified only by authorized parties and only in authorized way
  - availability - computer system assets are available to authorized users

Types of threats

- Types of threats are classified by the way the information is compromised on its way from its storage to consumption
- passive threats - hard to detect, have to prevent
  - interception - unauthorized party gains access to an asset. (attack on part of secrecy - confidentiality)
- active threats
  - interruption - the system asset becomes unavailable or unusable (attack on availability)
  - modification - unauthorized party gains access and modifies the asset (attack on secrecy and integrity)
  - fabrication - unauthorized party inserts counterfeit assets into the system (attack on part of secrecy - authenticity and integrity)

Computer assets wrt security

asset	availability	secrecy	integrity
hardware	stolen and disabled thus denying service		
software	programs deleted or corrupted	unauthorized copy made	modified to cause it to fail during execution or to do unintended task
data	deleted or corrupted	unauthorized read performed, statistical analysis	existing data modified, new data fabricated
network	messages destroyed or deleted, communcication lines made unavailable	messages read, traffic pattern of messages observed	messages modified, reordered, duplicated, false messages inserted

More on Network threats

- Passive attacks
  - release of message contents - message is captured and decoded
  - traffic analysis - attacker has access to messages but cannot decode them; analysis of the size, direction and frequency can reveal the nature of communication
- active attacks
  - masquerading - an unauthorized entity pretends to be authorized entity - usually includes one of the other forms of attack
  - replay - passive replay of captured messages stream
  - modification of messages - modification the contents of the legitimate messages
  - denial of service - prevents or inhibits the normal use of communication facilities

Protection

- User oriented
  - common - before being allowed to access the assets of the computer system the user has to *authenticate* herself - by specifying login and matching password
- data oriented
  - different types of authorized users may have different access privileges
  - generic model - *access matrix*

	item 1	…	item m
subject 1	privileges		privileges
…		…	
subject n	privileges		privileges

  - users and data items in access matrix can be grouped
  - access matrix can be stored
    - by row - capability token
    - by column - access control lists

Password protection

- Problems
  - with improvement of computer equipment brute force attacks become feasible
  - untrained users tend to select easy to guess passwords
    - study: out of 7000 accounts 3% of passwords had 3 characters or fewer in length
    - pick their names or common words
  - users tend to be lax about keeping passwords secret or changing them regularly
- password selection strategies
  - user education
  - computer generated passwords
  - reactive password checking
  - proactive password checking

Types of intruders

- Masquerader - not authorized to use computer system, penetrates system protection by way of legitimate user account - usually an outsider
- misfeasor - legitimate user who accesses assets that she is not authorized to, or who is authorized but misuses her privileges - usually somebody on the inside
- clandestine user - user who gains supervisory access to the system - can be either insider or outsider

Intrusion techniques

- frequently to gain unauthorized privileges the intruders need to find out the password that protects these privileges
- common password learning techniques
  - check default passwords
  - find out passwords by exhaustive search
  - try words from dictionaries
  - guess password on the basis of personal user information - full name, names of relatives, birth dates, etc. license plate
  - use Trojan horse (described later)
  - eavesdrop the unencrypted password

Intrusion detection

- No intrusion protection system is able to withstand a determined attack indefinitely
- objective – detect intrusion in a timely manner
- principle – behavior of intruder differs from that of legitimate user
- how to detect
  - statistically
    - threshold - determine thresholds for the number of certain event occurrences that are typical of normal usage patters
    - profile - compile a profile of activity of each user
  - rule-based - define a set of rules that signify the behavior of intruder
- audit record - tool for intrusion detection
  - native (OS)
  - detection specific - only for intrusion detection

Malicious programs

- Independent
  - bacteria - consumes resources by replicating itself
  - worm - replicates and sends its copies to other computers over the network
- needs host program
  - virus - code embedded within a program that causes a copy of itself to be inserted in other program
  - trapdoor - secret undocumented entry point into a program, used to grant access without normal methods of access authentication
  - logic bomb - logic embedded in a computer program that checks for certain set of conditions and executes some unauthorized action when these conditions are met
  - Trojan horse - secret undocumented routine embedded within useful program. Execution of program results in the execution of the routine

Viruses

- Virus is a piece of code that inserts itself in a useful program. When this program is executed the virus code takes over the control
- virus features:
  - parasitic - attaches to executables programs, replicates by finding other executables to infect
  - memory resident - lodges in main memory as resident part and infects every program that is executed
  - boot sector - infects the boot record or boot sector
  - stealth - hides from being detected - may use compression so that the length of infected program is the same as uninfected, intercepts disk I/O commands to give an impression that the executable is not infected
  - polymorphic - replicates by creating copies that are functionally equivalent but have different patterns

Anti-virus approaches

- Ideal solution - prevention. Do not allow virus to get into system
- otherwise:
  - detection - check if the virus is present
  - identification - recognize what virus it is
  - removal - delete the virus
- how to detect
  - scan for virus “signature”
  - scan for features that look like probable virus infection
  - attach checksums to all executables and check if the program was tampered with
  - memory resident program that identifies virus by its actions