Unit 3
Threats and attacks on security

Shantha Fernando

Department of Computer Science and Engineering

University of Moratuwa

E-mail: shantha@cse.mrt.ac.lk

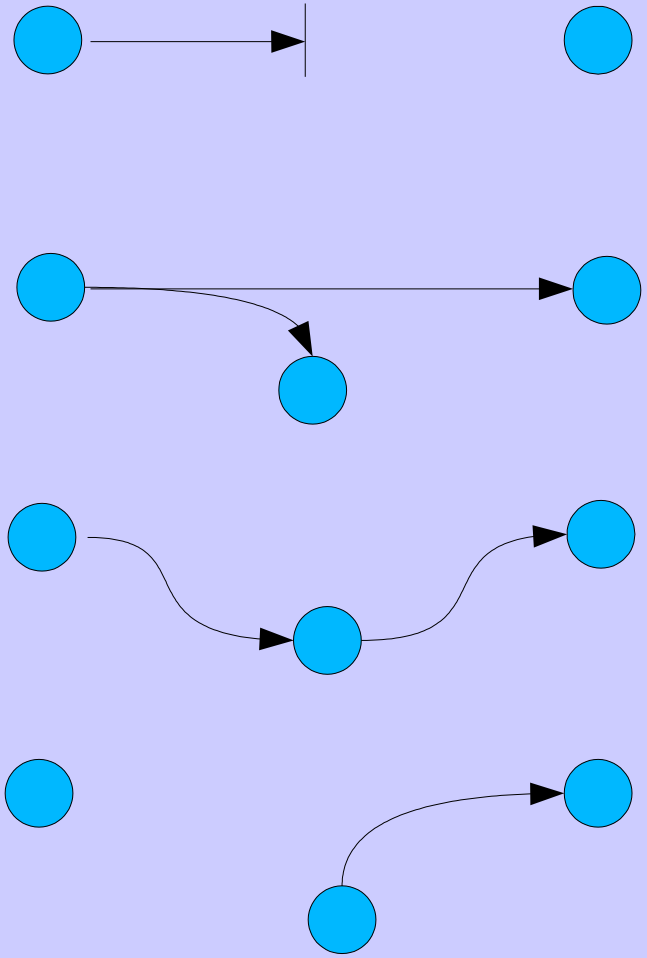
Department of Computer Science and Engineering
University of Moratuwa

Contents

- Concepts
  - Interruption
  - Interception
  - Modification
  - Fabrication
- Virus and worm attacks
- System compromisation

Threats & attacks on security

- Concepts
  - Interruption
  - Interception
  - Modification
  - Fabrication



Interruption (1/2)

- Communication is interrupted
  - Effect: recipient does not get information
- Attacker does not allow the information to reach the destination
- Usually detected by both the sender and the receiver
  - In some cases one of them may not detect
- Interruption mechanisms
  - Causing communication link failures
    - Physical damage – sabotage
    - Disabling interfaces of networking devices
    - Induction of fields or noise to the links

Interruption (2/2)

- Interruption mechanisms cont..
  - Removal of routing
    - Alteration of routing tables
  - Denial of service
    - Packet flooding
    - Disabling services
      - Web, mail, DNS, etc
- Class exercise (at the end of lecture):
  - Discussion on DOS attacks
    - Refer the research paper

Interception (1/2)

- Attacker receives information
  - But the legitimate recipient also receives information
  - Effect: confidentiality at stake
- Difficult to detect
- Mechanisms
  - Eavesdropping
  - Link monitoring
  - Packet capturing
  - System compromisation (can be detected)
    - Utilities planted to send information to attackers

Interception (2/2)

- Inherent catalysts
  - Nature of wireless transmissions
  - Packet broadcast or multicast requirements of applications and protocols
  - Promiscuous mode network operations
  - Store-and-forward nature of many protocols
    - Even real-time protocols go through intermediate buffering processes
      - Not everything is worm-hole routing
- Class exercise (at the end of lecture):
  - Discussion on eavesdropping
    - Refer the research paper

Modification (1/2)

- The attacker
  - blocks the transmission
  - receives information
  - modifies it
  - and then transmits to the receiver
- Detection before using is possible if encryption, signing, or validity checks are used
  - Manual detection may work for static information, but probably after using
    - e.g. Web content observed by the content developer himself
    - How about dynamic content? (e.g. Search results)

Modification (2/2)

- Modification mechanisms
  - Transmission with IP spoofing
    - Recipient believes the content is from the legitimate sender
  - System compromisation
    - Modified while information is with the sender
  - Intermediate store-and-forward provides good opportunities for modification
  - Difficult in a broadcast environment
    - Original information also will be received, hence they can be compared
- Effect
  - confidentiality compromised, recipient misled

Fabrication

- Sending generated information, pretending to come from a legitimate sender, but that sender has not sent them
- Motivation/effect
  - To get the recipient to disclose confidential information
- Can take place in push technologies
  - Advertisements – e-mail or web
  - Pop-up clients, agents

Virus and worm attacks (1/4)

- Viruses can cause
  - Interruption, interception, modification, fabrication
- Worms usually do fabrication
  - But may interrupt
- Viruses are malicious codes
  - May change an existing code to have malicious code
- Worms get an existing application to do some task
  - No modification of existing code

Virus and worm attacks (2/4)

- Viruses mainly affect windows platform
  - But cannot say it will not be there for other platforms
- Remedies are released usually after a damage
  - Difficult to develop virus scanners for future viruses
    - Though some say they have
- Continuous updating required for
  - Virus definitions
  - Virus detection engine

Virus and worm attacks (3/4)

- Virus spreading mechanisms
  - Sometimes exploits the features/loopholes open for application development
  - File system insecurity exploitation
  - OS and application bugs
  - Communication stack bugs
    - e.g. Use of NetBIOS protocols to inject viruses
- To control virus effects good IT policies and user training is a must

Virus and worm attacks (4/4)

- Worms affect network based services
  - Any platform
    - Even UNIX
  - Exploitation of bugs in server application software
  - Usually a multiplication/generation of messages
  - Networks can be flooded
  - Servers may run out of resources
- Remedies
  - Proper patches for server software
  - Proper configuration
    - e.g. Some worms were due to poor configuration of sendmail
    - Precautionary limitations

System compromisation

- There will be a separate unit on client and server security
- Focus of this lecture
  - System compromisation causes
    - Interruption
      - No service availability due to compromise
    - Interception
      - Outsiders can monitor the information passing through a system
    - Modification
      - File data is in the custody of the system
    - Fabrication
      - Attacker uses the system to generate tempting information

Conclusion

- We looked at
  - The security threat concepts such as interruption, interception, modification & fabrication
  - The effects of those security threats
  - Causes for those security threats
  - Possible remedies
  - How viruses and worms cause them
  - How system compromisation cause them