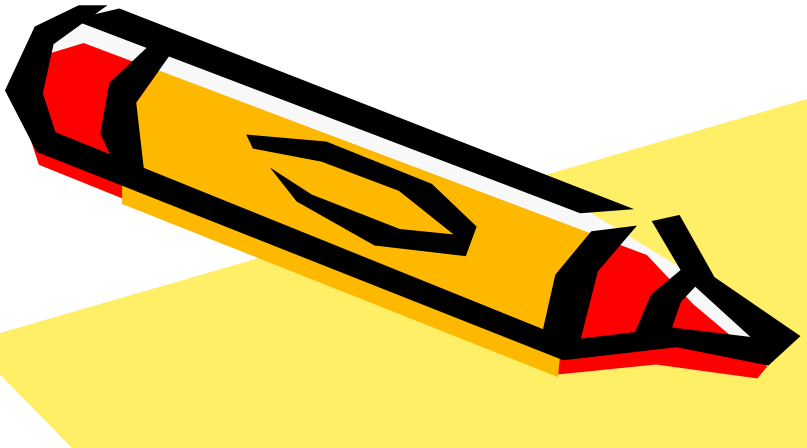


CHAPTER THEE: INFORMATION SYSTEMS SECURITY MANAGEMENT

Objectives INFORMATION SYSTEMS SECURITY MANAGEMENT

Objectives

- Describe:
  - *Basic Steps/Stages for Risk Assessment*
  - *Gaining Access to Systems and Data: Summary*

1. Basic Steps/Stages for Risk Assessment

Definition: Risk Assessment

- *The concept of risk assessment is crucial to developing proportionate defenses.*
- To perform a risk analysis, organizations need to understand possible *threats and vulnerabilities.*
- *Risk* is the probability that a vulnerability will be exploited.
  - The *basic steps/stages for risk assessment* are listed as follows:

    i. Identifying and prioritizing assets;

    ii. Identifying vulnerabilities;

    iii. Identifying threats and their probabilities;

    iv. Identifying countermeasures;

    v. Developing a cost benefit analysis;

    vi. Developing security policies and procedures.

Activity:

Perform the basic steps for the risk assessment for Dekut Case Study.

1. Basic Steps/Stages for Risk Assessment

Activity:

- *Perform the basic steps for the risk assessment for Dekut Case Study/or any other company.*

To identify and prioritize information assets and to develop a cost benefit analysis, it is helpful to ask a few simple questions such as the following.

-Why Do You Want To Safeguard It?

-What Is Its Value?

-What Are The Threats?

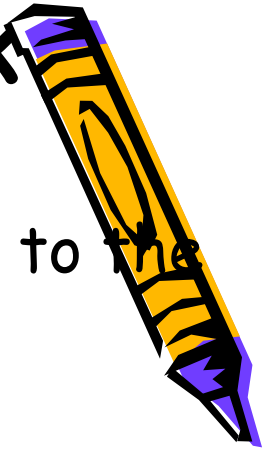
-What Are The Risks?

-What Are The Consequences of its Loss?

-What Are The Various Scenarios?

-What Will The Loss Of The Information Or System **Cost?**

3.0 Basic Steps/Stages for Risk Assessment



Prioritize assets and systems by assigning a Ksh value to the asset.

- The Ksh. value can be;
  - the replacement cost,
  - the cost to not have the asset available or the cost to the organization to have the asset,
    - such as proprietary information,
  - obtained by a competitor.
- It is also necessary to include more obscure costs, such as loss of customer confidence.
- Weed out the *probable* threats from the *possible*.

  Determine what threats are *most likely*, and develop measures to protect against those threats.

3.1 Security models and architecture

Introduction

- Computer and information security covers many areas within an enterprise.
  - Each area has security vulnerabilities and,
  - some corresponding countermeasures
    - that raise the security level and provide better protection.
      - *the different areas and security levels of:-*
        - *network devices*
        - *operating systems,*
        - *hardware,*
        - *protocols, and*
        - *Applications*
    - *can cause security vulnerabilities that can affect the environment as a whole.*

Security models and architecture

- Two fundamental concepts in computer and information security are:-

a) *A security policy*

- Outlines
  - how data is accessed,
  - what level of security is required, and
  - what actions should be taken when these requirements are not met.
- The policy outlines the expectations of a computer system or device..

b) Security Model,

- Which outlines how security is to be implemented—in other words,
  - providing a "blueprint" and the architecture of a computer system,
    - »which fulfills this blue print.

Introduction Security models and architecture

Security Model,

- If a security policy
  - i. dictates that all users must be:-
    - identified,
    - authenticated, and
    - Authorized
  - before accessing network resources,
  - the security model might lay out an access control matrix:-
    - *that should be constructed so that it fulfills the requirements of the security policy.*
  - ii. states that:-
    - no one from a lower security level should be able to view or modify information at a higher security level,
      - *the supporting security model will outline the necessary logic and rules that:-*
      - *need to be implemented to ensure that under no circumstances can a lower-level subject access a higher-level object in an unauthorized manner.*
- A security model provides a deeper explanation of how a computer operating system should be developed to properly support a specific security policy.

Security Models

There are three basic approaches used to develop a security model e.g.

- network security,
  - organizations employ some combination of the three approaches to achieve security.

The three approaches are:

- *Security by obscurity,*
- *Perimeter defense model, and*
- *Defense in depth model.*

3.2.1 Security Through/By Obscurity(STO):-

- Is the belief that a system of any sort can be secure so long as nobody outside of its implementation group is allowed to find out anything about its internal mechanisms
- The concept behind this model is that if no one knows that a network or system is there, then it won't be subject to attack.
  - The basic hope is that hiding a network or at least not advertising its existence will serve as sufficient security.
- The problem with this approach is that it never works in the long term, and once detected, a network is completely vulnerable.

3.2 Security Models Cont…

3.2.2 The Perimeter Defense

- The perimeter defense model is analogous to a castle surrounded by a moat.
- *When using this model in network security, organizations harden or strengthen perimeter systems and border routers, or an organization might "hide" its network behind a firewall that separates the protected network from an untrusted network.*
  - *Not much is done to secure the other systems on the network. The assumption is that perimeter defenses are sufficient to stop any intruders so that the internal systems will be secure.*
- Challenges/flaws Perimeter Defense:

  1), this model does nothing to protect internal systems from an inside attack.
  - the majority of attacks on company networks are launched from someone internal to the organization.

  2) Second, the perimeter defense almost always fails eventually.
  - Once it does, the internal systems are left wide open to attack.

3.2 Security Models Cont…

3.2.3 The Defense in Depth/layered approach

- This is the most robust approach to use is the defense in depth model.
- *The defense in depth approach strives for security by hardening and monitoring each system; each system is an island that defends itself.*
  - *Extra measures are still taken on the perimeter systems,*
    - *but the security of the internal network does not rest solely on the perimeter systems.*
- This approach is more difficult to achieve and requires that all systems and network administrators do their part.
- With this model, however,
  - the internal network is much less likely to be compromised if a system administrator on the network makes a mistake like putting an unsecured modem on the system

3.2 Security Models/strategy Cont

3.2.3 The Defense in Depth cont……..

Layered security, as in the previous example, is known as defense in depth.

- This security is implemented in overlapping layers that provide the three elements needed to secure assets: prevention, detection, and response.
- Defense in depth also seeks to offset the weaknesses of one security layer by the strengths of two or more layers.
  - *A bank would never leave its assets inside an unguarded safe alone. Typically, access to the safe requires passing through layers of protection that might include human guards and locked doors with special access controls.*
  - *Furthermore, the room where the safe resides could be monitored by closed-circuit television, motion sensors, and alarm systems that can quickly detect unusual activity. The sound of an alarm might trigger the doors to automatically lock, the police to be notified, or the room to fill with tear gas.*

3.2 Security Models/strategy Cont.

3.2.3 The Defense in Depth cont……..

- In the information security world,
  - Defense in depth requires layering security devices in a series that protects, detects, and responds to attacks on systems.
  - For example,
  - a typical Internet-attached network designed with security in mind includes routers, firewalls, and intrusion detection systems (IDS) to protect the network from would-be intruders;
  - employs traffic analyzers and real-time human monitors who watch for anomalies as the network is being used to detect any breach in the layers of protection; and relies on automated mechanisms to turn off access or remove the system from the network in response to the detection of an intruder.

Finally, the security of each of these mechanisms must be thoroughly tested before deployment to ensure that the integrated system is suitable for normal operations. After all, a chain is only as good as its weakest link.

3.3. Gaining Access to Systems and Data

- Scanning
  - refers to the process of running a series of automated tools against IP addresses or IP ranges to target and identify known and potential vulnerabilities and/or unpatched or misconfigured systems.

- During the scanning phase, the attacker is able to put together the following important information, which can then be used to compromise systems:
  - *Phone numbers with modems;*
  - *Addresses of live hosts;*
  - *Network topology;*
  - *Open ports;*
  - *Firewall rule sets (rules determining what packets the firewall allows or refuses to pass through it)*

3.3. Gaining Access to Systems and Data

- Based on the above information, the attacker can compromise systems through the following attacks:

a) Application and Operating System Attacks

- Buffer overflow attacks;
  - Passive sniffing works with hubs, but if switches are involved, active sniffing is required
- Password attacks;
- Web application attacks

b) Network-based attacks

1. Sniffing attack;
   - Is theft or interception of data by capturing the network traffic using a packet sniffer(can be hardware or software installed on the system).
     - When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer
2. IP address Spoofing;
   - **is the process in which an intruder introduces fake traffic and pretends to be someone else (legal source or the legitimate entity)**. Spoofing is done by sending packets with incorrect source address over the network.
3. Session Hijacking

- **a technique used by hackers to gain access to a target's computer or online accounts**. In a session hijacking attack, a hacker takes control of a user's browsing session to gain access to their personal information and passwords

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

(a). Application and Operating System Attacks

i). Buffer Overflow Attacks

- Buffers represent temporary holding area in a computer's memory;
- *buffer overflow occurs when some function is carried out with more data than the function knows how to handle*. In that case, some of the data overflows into the adjoining area of memory. If an attacker forces a program to fill one of its local variables (a buffer) with data that is longer than the space allocated, it is possible for the attacker to overwrite the local variables with machine code (executable code). The processor can then start executing the instructions (machine code) that the attacker has put into the buffer.

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

(a). Application and Operating System Attacks

i). Buffer Overflow Attacks CONT…

- ***Systems administrator:***
  - *Ensure that publicly available systems like ;Internet Mail, DNS, Web, FTP servers, etc have configurations with a* ***minimum of unnecessary services and software extras*** *– because these serve as doorways to inserting the data for overflow attacks.*
  - *Keep your systems patched(update or resolve functionality issues)– vendors are always trying to create fixes for newly discovered vulnerabilities in the developed software.*
  - *Configure your systems with non-executable stack – so that it refuses to execute instructions.*
  - Software developers can, on the other hand, avoid programming mistakes involving the allocation of memory space and check the size of all user-input as it flows through applications (better programming and testing practices).

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

a). Application and Operating System Attacks cont…

ii) ***Password Attacks***

- Passwords are the commonly used computer security tool in the world, protecting all sorts of information people have on their computers. Often, users have easy to guess passwords – or too many passwords used for gaining access into various applications. Users often choose these passwords.
- Password attacks may involve guessing default password or active password cracking.
- In guessing default passwords,
  - » the attacker may use a database of various default passwords for various platforms (security.nerdnet.com); the attacker can then use *password guess scripts running on his/her machine to repeatedly try to login to the target system across the network*.

- *Such scripts can be found at* ***Packetstorm.securify.com/Crackers/***

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

a) Application and Operating System Attacks cont….

ii) Password Attacks cont….

- Generally, password determination using default password guessing has the following limitations (hence the need for automated password cracking, especially where default passwords have been changed):
  - ***i. A slow process;***
  - ***ii. Login attempts can be detected;***
  - ***iii. Account lock-out feature.***
- *In automated password cracking,*
  - *the automated tool guesses a password, encrypts the password, then compares the values of the encrypted guess with an encrypted value found from a stolen password hash file.*
- *If there is a match, the password is found; if not, the loop repeats.*

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

Password attack defenses include:

i. A strong password policy;

ii. Better user awareness;

iii. Use of password filtering software that will help enforce organizational password policy (that is, the software will determine whether a password is appropriate, etc);

iv. Use of authentication tools other than passwords;

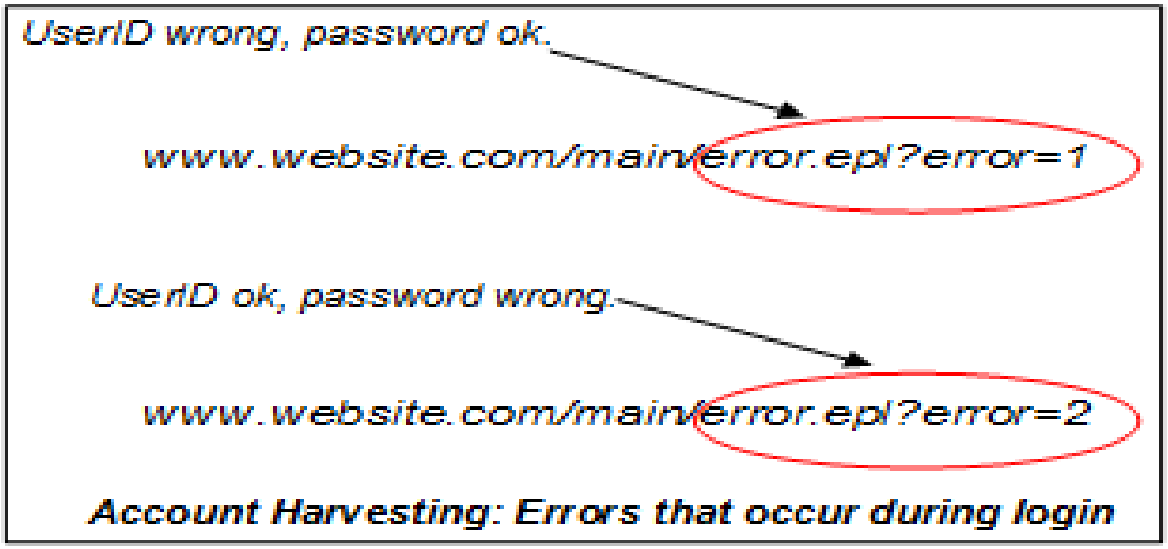
v. Protection of password hash files;

vi. Company can conduct its own password cracking exercises to see how exposed it is.

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

iii) *Web Application Attacks Cont…*

- ***Account Harvesting***
  - Consider the diagram:



Account Harvesting: Errors that occur during login

❑See the steps …. Next slide

3.3. Gaining Access to Systems and Data Cont…. APPS&OS attacks

iii) *Web Application Attacks Cont…*

- ***Account Harvesting***

- Thus, account harvesting is a technique that allows an attacker to determine account numbers based on different error messages returned by an application;
  - often, an attacker can write a script that interacts with the Web application across the network, guessing all possible userIDs and a wrong password.
- Valid userIDs can be harvested from a target application. Next, the attacker can try to harvest passwords (if the application doesn't lock out user accounts due to a given number of invalid password attempts). If the application locks out accounts, the attacker in effect is performing a denial of service (DoS) attack, since users will be locked out.
- Account harvesting can be prevented if there is a consistent message that is returned when wrong authentication data is transmitted to the application, a message that will not give hints to the attacker on whether the User ID or Password is wrong.

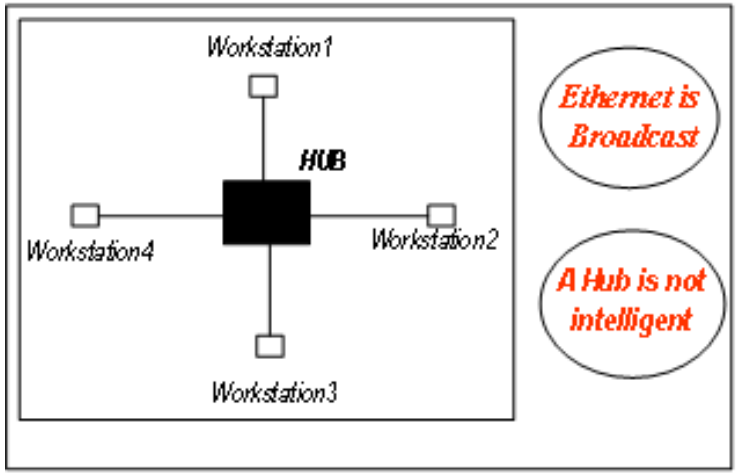
3.3. Gaining Access to Systems and Data Cont…. Network attacks

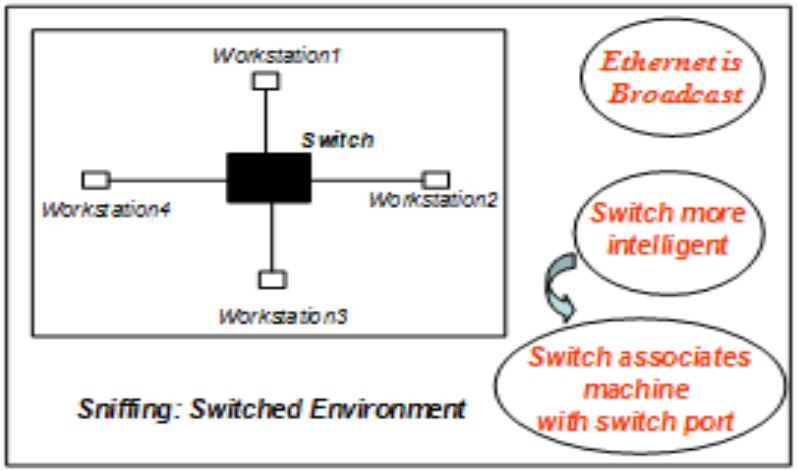
b) Network-based attacks

Key techniques are: Sniffing, IP Address spoofing, and Session Hijacking.

i) Sniffing

- A sniffer is a program used to capture traffic from the network; the program is often used to gather sensitive information such as userIDs, passwords, DNS queries and responses, sensitive email messages, etc. Often, it has the capability to decode the messages.
- Consider the two Ethernet environments below:





3.3. Gaining Access to Systems and Data Cont…. Network attacks

i) Sniffing Cont….

- **Active type of sniffering.**

a) A passive sniffer (e.g., Snort and Sniffit)

- passively waits for traffic/data to be sent to it; it will silently gather data on the LAN. On the other hand, an active sniffer (e.g., Dsniff) will actively inject traffic in the LAN. This will help to sniff all the data in a switched Ethernet network. Such injected traffic could be bogus MAC address (MAC flooding) or spoofed ARP messages.

b) Spoofed ARP Messages

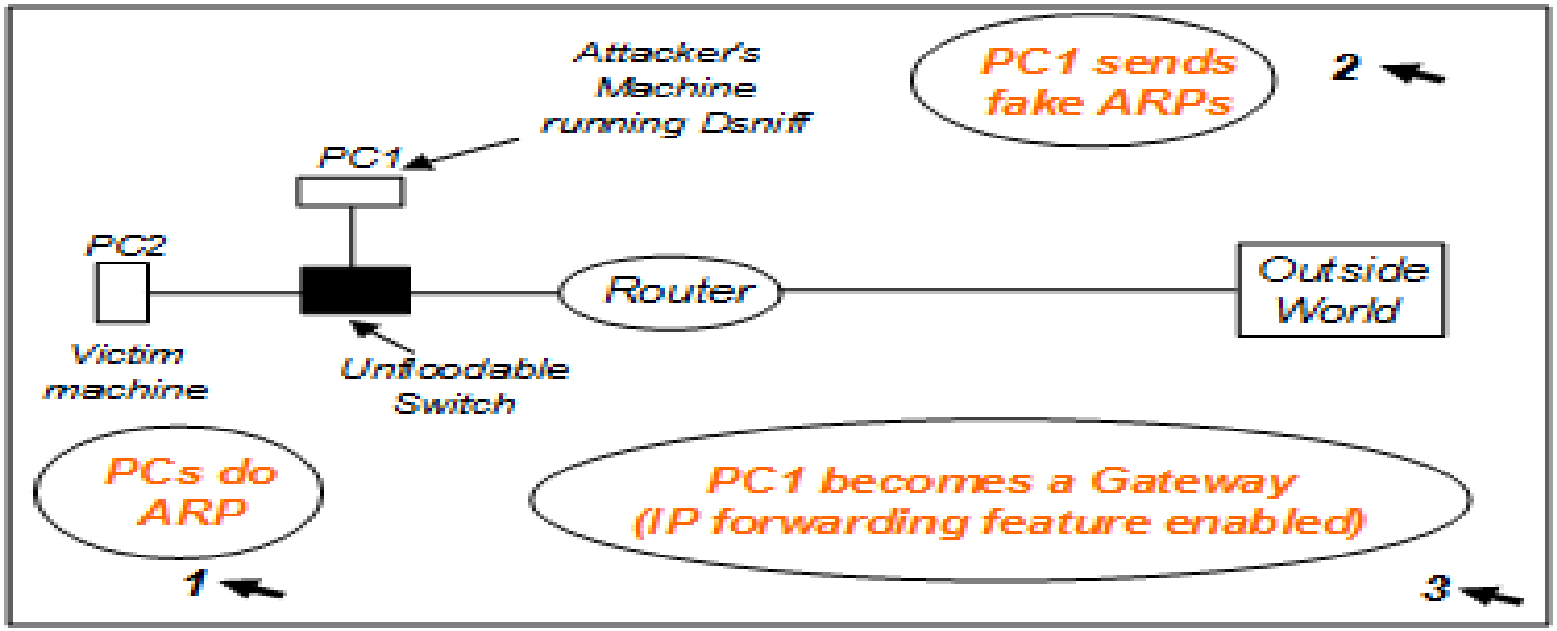
This is also a form of active sniffing, in which the attacker sends fake ARP replies to victim's machine; the victim's ARP table changed.

3.3. Gaining Access to Systems and Data Cont…. Network attacks

i) Sniffing Cont….

Spoofed ARP Messages

- *Consider the scenario below, with PC1 the attacker's machine running Dsniff, an active filter that contains an arp spoof module. In the scenario, the router is the true gateway to the actual world; all PCs on the network will have to find the MAC address of the router – through ARP broadcasts.*



3.3. Gaining Access to Systems and Data Cont…. Network attacks

i) *Spoofed ARP Messages*

- If PC1 can send fake ARP replies, then other PCs on the network will consider PC1 to be the gateway to the outside world. In this way, all communications by others will pass through PC1. The arpspoof program, therefore, provides the following features:
- Arpspoof program redirects traffic so that it bounces through the attacker's machine on its way to outside world; this allows sniffing in a switched environment
- IP forwarding set up is crucial (on the attacker's machine), so that it (the attacker's machine) forwards the traffic to the true gateway (the router)
- The result of arpspoof is to manipulate the IP_to_MAC addresses mapping on the victims' machines.

3.3. Gaining Access to Systems and Data Cont…. Network attacks

i) Spoofed ARP Messages

NB.

- The possible defenses against sniffing are indicated below:
  1. Encrypt data that gets transmitted across the network;
  2. Consider replacement of hubs – use switches;
  3. Enable port-level security on switches: configure each switch with a specific MAC address of the machine using that port.

3.3. Gaining Access to Systems and Data Cont…. Network attacks

b) Network-based attacks Cont….

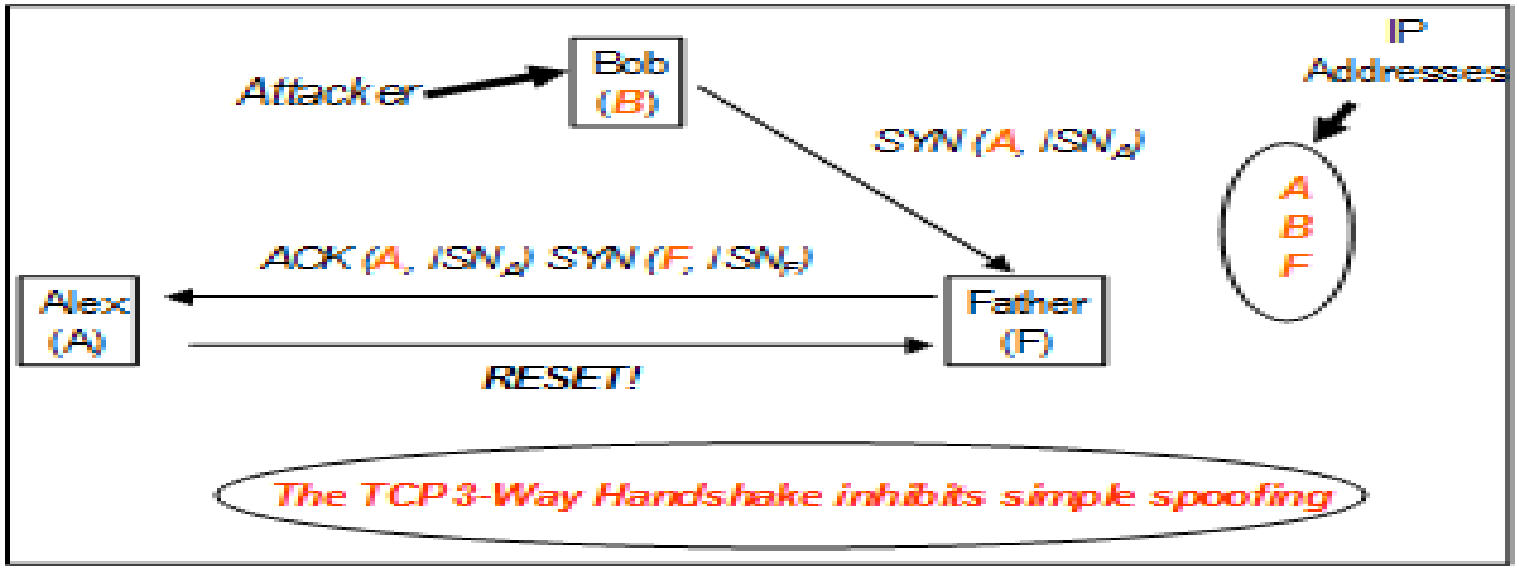
ii) IP Address spoofing ***panic***

- This kind of attack involves changing/disguising the source IP address of a system, and it is helpful for attackers who do not want their actions traced back (for example, the source of a packet flood may never be known if the true source is disguised);
  - Disguising the source IP address also helps attackers undermine applications that rely on IP addresses for authentication or filtering, since the address may not be the right address.
- Note that in this kind of attack (simply disguising the source IP address), the attacker will not be able to have interactive sessions with the target system, since responses will go to the source IP address indicated in the packets, which in this case is not the actual machine sending the packets.

3.3. Gaining Access to Systems and Data Cont…. Network attacks

ii) IP Address spoofing *panic cont……*

- Also, with simple disguising of source IP address, the TCP 3-way handshake process will never complete, as shown. Bob [IP address B] sends packets to Father using Alex's address [IP address A], responses go to Alex's address and TCP handshake process can not complete.



3.3. Gaining Access to Systems and Data Cont…. Network attacks

ii) IP Address spoofing *panic cont……*

- Another form of IP address spoofing involves what is known as spoofing with source routing. In source routing, the source machine sending a packet specifies the path the packet will take on the network. Source routing is often divided into:
  - i. Loose source routing:
    - the attacker to specify just some of the hops (handoff points) that must be taken as the packet traverses the network.
  - ii. Strict source routing:
    - the entire route is included in the packet header
- Basically, source routing:
  - *Allows a packet to carry information that tells a router the correct or better way for it to get back to where it came from (by a packet carrying information about path to the destination, it is also carrying information about the path backwards)*
  - *The router's own prescribed routing rules for the packet can be overridden.*
  - *This could allow an attacker to guide traffic wherever they want.*

3.3. Gaining Access to Systems and Data Cont…. Network attacks

ii) IP Address spoofing *panic cont……*

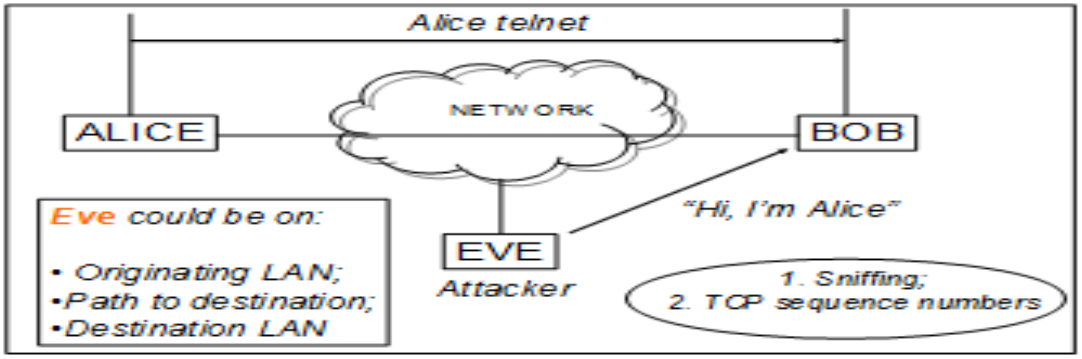
- Source-routing attacks are rare across the Internet. Most organizations block them at their Internet gateways.
  - However, many organizations allow source-routed packets on their internal networks and an insider can launch spoofing attacks using this technique.
- Several techniques combined will help with ip spoofing attacks:
  - Apply the latest security patches from your OS vendor;
    - this ensures that the initial sequence numbers are difficult to predict.
  - Avoid applications that use IP addresses for authentication purposes.
  - Do not allow source-routed packets ("no ip sourceroute").
  - Implement anti-spoof packet filters at border routers.

3.3. Gaining Access to Systems and Data Cont…. Network-based attacks

b) Network-based attacks

iii) Session Hijacking.

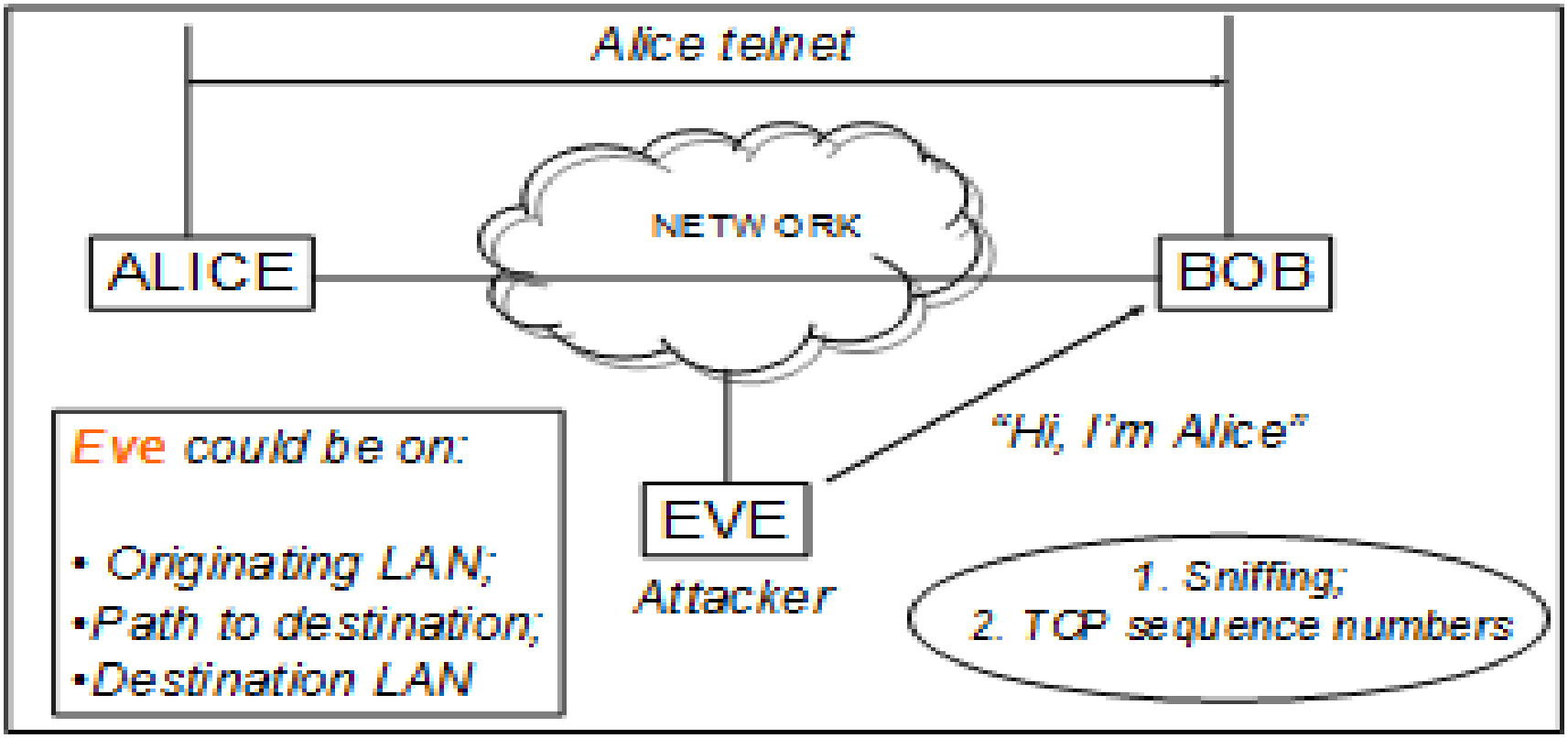
- Sniffing allows an attacker to observe traffic on a network; packet sniffer
- spoofing supports an attacker in pretending to be another machine.
- In session hijacking,
  - an attacker steals an existing session established between a source and a destination, using both sniffing and spoofing techniques.
  - In the diagram below, explain how Eve can still Alice's session with Bob using sniffing and spoofing techniques. Session hijacking can be defended through encrypted sessions, especially if the sessions traverse the Internet.



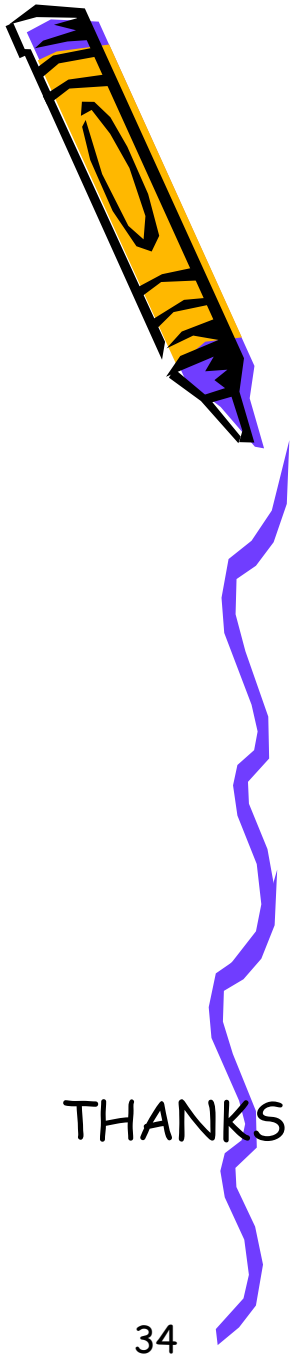
Network-based attacks

b) Network-based attacks

iii) Session Hijacking.



The End



Question

&

Answers

THANKS