ISM 414:
COMPUTER SECURITY

[WEEK ELEVEN]

PHILIP OKPOSO

SCHOOL OF
MEDIA AND
COMMUNICATION

PAN-ATLANTIC UNIVERSITY

NETWORK SECURITY

- Internet vulnerabilities **(done)**
- Port scanning **(done)**
- Spoofs **(done)**
- Spam **(done)**
- Denial of Service
- Firewall Basics

DENIAL OF SERVICE

- Many Internet attacks try to obtain private data or to damage data. In contrast, a denial-of-service attack aims to shut down an entire network, a single server, or a particular Web site.
- The attack tries to prevent legitimate users of a service from using that service.
- This can be done by one of the following methods:
  - Flood a network with traffic. This makes it hard or impossible for legitimate users to send or receive data.

DENIAL OF SERVICE

- Disrupt connections between two computers. This prevents remote access to the machines.
- Attempt to prevent a particular user from accessing a service.
- Disrupt or prevent network access to a particular computer or network. A hacker may open an account at an ftp site, then store data and retrieve it repeatedly, thereby consuming disk space and monopolizing network services at the site.

- A denial-of-service may be part of a bigger attack, but it disables a useful resource such as a computer or a network.

Denial of Service

- If the resource is private, its owner may be inconvenienced.
- If the resource is public, its users may suffer loss of service.
- If the resource is commercial, its owner suffers monetary losses.
- A denial-of-service is considered an easy type of attack.
- Even a single hacker, using an old, slow computer and a slow modem may be able to disable (or at least slow down) faster servers or even whole networks.

Types of Denial of Service

- There are three types of denial-of-service:
  - ✓consumption of scarce or nonrenewable resources,
  - ✓destruction or alteration of network information, and
  - ✓physical destruction or alteration of network components.

CONSUMPTION OF SCARCE OR NONRENEWABLE RESOURCES

- This type, relies on the fact that the computers and networks need resources such as electrical power, CPU time, memory space, disk space, and network connections.
- The easiest resource for a hacker to consume is network connectivity. It is possible to tie up the network connections of a computer, such that it waits for some data that never arrives, so it remains hung up.
- All that the hacker has to do is start opening a connection to a network server but never complete this process.
- The victim server has reserved a port and a data structure for the connection, but the port remains half open.
- The hacker (or a group of coordinated attackers) can very quickly tie up all the available ports of a server. In the meantime, other users, legitimate or not, who try to establish connections are denied access.

DESTRUCTION OR ALTERATION OF NETWORK INFORMATION

- The second type of DoS threat involves destruction or alteration of network information.
- An attacker may be able;
  - to change the IP number of a victim’s personal computer,
  - change the registration of the operating system, or
  - change prerecorded telephone numbers used by the modem to call outside servers.

PHYSICAL DESTRUCTION OR ALTERATION OF NETWORK COMPONENTS.

- The third type of DoS threat involves physical destruction or alteration of network components.
- This can be done by an intruder physically appearing in a computer center and
  - disabling,
  - breaking, or
  - disconnecting cables and other hardware devices.
- A hacker may also climb a utility pole and disconnect telephone lines or television cables, thereby disrupting service to users in the neighbourhood.

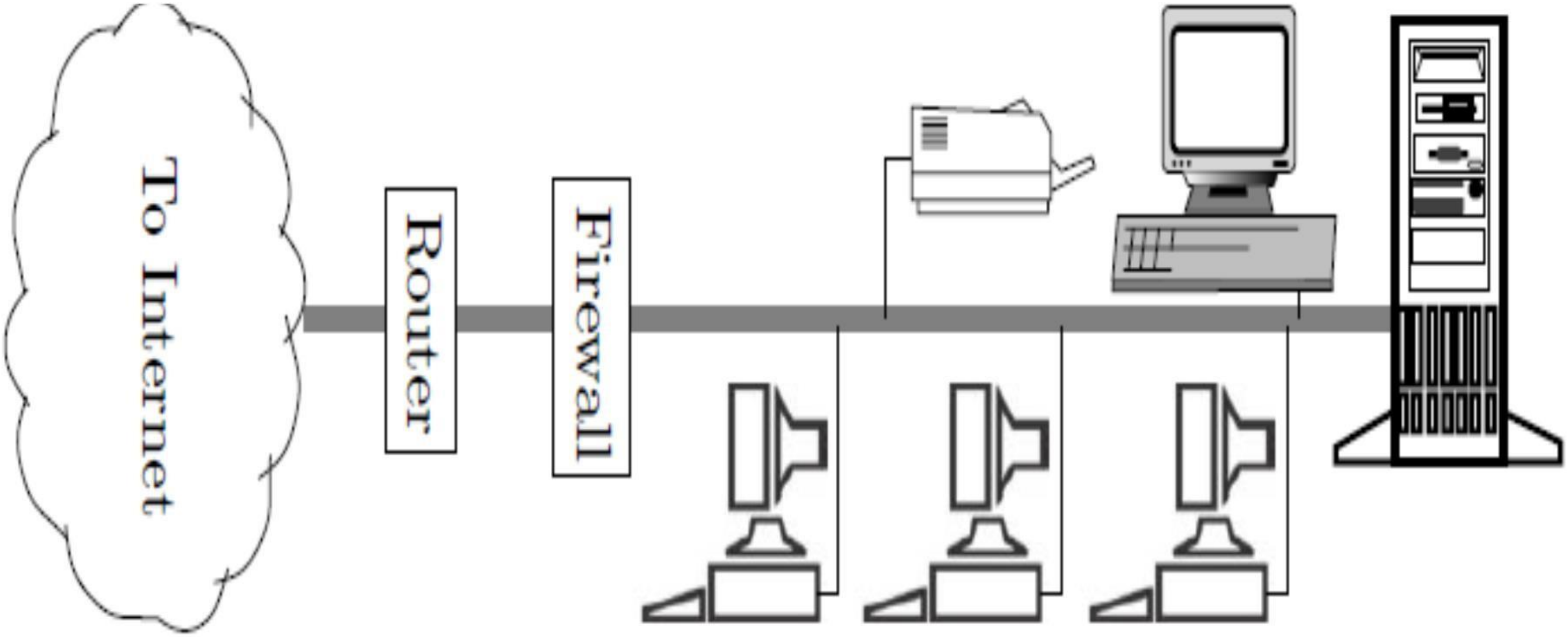
MITIGATING DoS Attacks

- Resource throttling: Implement mechanisms to limit the number of connections from a single IP address or identify and block suspicious connection patterns.
- Scaling resources: If possible, consider temporarily scaling up server resources (e.g., CPU, memory) to handle the increased load until the attack subsides.
- Physical Security Enhancements: Consider methods of either increasing man-power or investing in technological devices such as an alarm signal when an attack is observed or sensed.

FIREWALL BASICS

- A firewall is a combination of software and hardware that decides what kinds of requests and what specific data packets can pass to and from a computer or a local network.
- A firewall for a personal computer is normally fully implemented by software, whereas a small network of computers often found in a home (typically consisting of 2–3 computers and a printer) may use a hardware firewall that's built into the network's router.
- An effective firewall must be easy to adapt to the needs of any user.
- Such a firewall should be able to check any property of a data packet, should be able to take various actions depending on what it finds, and should do all this fast, so as not to slow down the flow of data to and from its host computer or network.

A firewall in a LAN



FUNCTIONS OF A FIREWALL

- A typical firewall performs the following tasks:

- limit incoming data, so that data coming from certain senders (or that has certain properties) will be blocked,
- limit outgoing data, so a program will not be able to send data outside (to call home) without the owner's knowledge,
- generate and save a log of all its activities, especially on data packets it has blocked, and
- do all this fast and be transparent to the user.

COMPONENTS OF A FIREWALL

- The two main components of a firewall are the gate and the choke (there can be several such pairs in a large firewall).
- The gate transfers or blocks the data and
- the choke is the filter that decides which data to block.
- Those familiar with firewalls like to compare the gate to a security checkpoint and the choke to a security guard.

ADVANCED TASKS OF FIREWALLS

- A modern firewall may also include rules for checking the data of a data packet.
- This useful feature is referred to as *content filtering*.
- The user may instruct the firewall to block all incoming (and perhaps all outgoing) data packets that contain a certain string of characters.
- This can block common viruses and worms that have already been detected and analyzed.
- An advanced firewall should also be able to recognize ethernet hardware addresses (the so-called MAC addresses), so that the rules would be able to distinguish between outside traffic and local traffic.

ADVANCED TASKS OF FIREWALLS

- Another advanced task is to limit the amount of data (the bandwidth) allocated to certain users or to certain applications.
- This way, a firewall can help in *bandwidth management*.
- Consider an ISP that offers cable Internet access to private users.
- A private user normally has one or two computers and generates a small amount of traffic, perhaps browsing, sending email, and transferring files.
- Also, most of this traffic should be incoming.
- As long as each user conforms to this pattern, the ISP can support many users with one cable and can remain competitive.
- If one user suddenly starts consuming large amounts of bandwidth (perhaps because the user generates spam or has other commercial activities), other users may notice low speeds and may start complaining.
- The ISP may decide to limit the amount of data each user can send, and this task (bandwidth management) should best be performed by the ISP’s firewall.

ADVANCED TASKS OF FIREWALLS

- *Bandwidth accounting* is another important task performed by modern firewalls.
- The owner/operator of a local network needs to know how the network is used over time.
- Network usage varies between day and night, weekdays and weekends, and from month to month.
- A firewall can provide information about the amount of traffic flowing to and from (and the amount being blocked at) each computer on the network.
- When such information is presented graphically, it can tell an important story.
- It can tell the network manager that certain computers are active on weekends, and that the total network bandwidth is insufficient, say, right before lunch time on Fridays.

ADVANCED TASKS OF FIREWALLS

- Another important picture that a good firewall can paint is the pattern of *connection logging*.
- The firewall can keep a record of every connection opened between a computer in the network and an outside address.
- The date, time, and amount of data transferred in each direction can also be logged.
- Such information can provide an audit trail which may be invaluable when something out of the ordinary, such as an attack, occurs.
- Connection logging provides a bird’s eye view of the usage of an entire local network, and may suggest ways to improve its behavior.

AUTHENTICATION

- The term *authentication* signifies the process of verifying someone’s identity.
- Our discussion concentrates on local authentication, authentication by biometric means, and password authentication.
- Local authentication is verification done when the person is located nearby and is available for questioning and scrutiny.
- Local authentication of a person is achieved by something that the person has, knows, or is.

AUTHENTICATION

- A key is something a person *has*, so it is a means of authentication.
- A key authenticates a person to a lock.
- A password is something that a person *knows*, and it authenticates the person to a computer or an ATM machine in a bank.
- A fingerprint or a DNA is part of a person.
- It is something a person *is*, and it also serves as (biometric) authentication.

LOCAL AUTHENTICATION

- Thus, local identification, where a person tries to use a local computer, is easy and reliable.
- It may use attributes such as;
  - a key (to open the door to a protected facility),
  - personal knowledge (a guard at the door may personally know the user),
  - paper or plastic identification (examined by a guard),
  - fingerprints (verified by touching a special pad),
  - voice prints (verified by talking to a special circuit), or
  - facial identification (currently not very reliable).

REMOTE AUTHENTICATION

- Remote authentication is more complex and is never absolutely secure.

- You can send your picture remotely to authenticate yourself to a person who knows you, but this requires a person who knows you, and it isn’t completely secure, because a determined perpetrator pretending to be you can get hold of your picture, or wear a latex mask resembling you and attempt to fool someone watching him on a remote screen.

- You can place your finger in a device that reads your fingerprints and sends them to a remote location for authentication, but such a device can be fooled by a glove with your fingerprints or by an eavesdropper who intercepts the fingerprint data on its way and modifies it.

- Currently, remote authentication is normally done by passwords which is why fraudsters are always after passwords.

CONCLUSION

NEXT:

- Biometric Techniques
- Passwords