ISM 414:
COMPUTER SECURITY

[WEEK TEN]

PHILIP OKPOSO

SCHOOL OF MEDIA AND COMMUNICATION
PAN-ATLANTIC UNIVERSITY

NETWORK SECURITY

- Internet vulnerabilities
- Port scanning
- Spoofs
- Spam
- Denial of Service
- Firewall Basics

NETWORK VULNERABILITIES

- A network vulnerability is an inherent weakness in the design, implementation, or use of hardware component or a software routine.
- A vulnerability invites attacks and makes the network susceptible to threats.
- A threat is anything that can disrupt the operation of the network.
- A threat can even be accidental or an act of nature, but threats are mostly intentional.
- A threat can damage the network, slow it down, or make it unavailable. Any type of rogue software represents a threat.

Internet vulnerabilities

- An attack is a specific approach employed to exploit a known vulnerability.
- A passive attack is designed to monitor and record network activity in an attempt to collect information to be used later in an active attack.
- Examples of passive attacks are packet sniffing and traffic analysis (Wireshark, CAPSA).
- Passive attacks are difficult to detect.
- An active attack tries to damage a network or its operation.
- Such attacks are easier to detect, but are also more damaging.

PORT SCANNING

- When two programs on different computers exchange data, all the data packets sent between the programs have (among other specifications) the same port number.
- Accessing a network opens a port and is similar to opening a door.
- This makes ports especially important for network security.
- When data packets arrive at a computer from different sources, each stream of packets uses a port number.
- Port numbers are 16-bit unsigned integers, meaning they can range from 0 to 65535.

Classes of Ports

- There are three classes of ports, **well known** (0 through 1023), **registered** (1024 through 49151), and **dynamic/privat**e (49152 through 65535).
- The *well-know*n ports are assigned by [IANA port 04] and are normally used by operating system processes.
- IANA stands for the Internet Assigned Numbers Authority, a key organization that plays a vital role in the smooth functioning of the internet by managing critical resources like IP address, DNS.
- Some examples are FTP (port 21), TELNET (port 23), SMTP (port 25), and HTTP (port 80).
- *Registered* ports are typically used by user applications (as opposed to operating system processes) when they have to contact a server, but such ports can also identify named services that have been registered by a third party. Examples is port 5222, commonly used for XMPP (Extensible Messaging and Presence Protocol) communication.

Classes of Ports

- *Dynamic/private* ports are used by user applications.
- Unlike well-known and registered ports, these aren't pre-assigned for specific services. Instead, your operating system dynamically assigns them on the fly when applications need to establish temporary connections.
- Dynamic ports might be used for:

✓ Downloading files with a web browser.

✓ Streaming online music or videos.

✓ Online gaming communication.

✓ Video conferencing applications.

Port scanner

- A port scanner is a program that listens to data arriving at and departing from certain ports on a computer.
- Port scanning has legitimate uses in managing networks, but is also used heavily by hackers to gather information that identifies open doors to the computer.
- Information collected by port scanners is used to identify operating system utilities installed in the computer, and exploit known vulnerabilities in those utilities in order to break into the computer.
- Port scanners are implemented by sophisticated hackers who make them available on the Internet.

Port scanner

- In many cases, it is easy to detect the activity of a port scanner simply by checking the log files that are continuously updated by the operating system.
- Once a port scanner is detected, its transmissions can be traced back to their origin and sometimes stopped.
- However, the mere activity of port scanning is not illegal.

Types of port scanners

- **Vanilla:** The scanner attempts to connect to all I/O ports.
- **Strobe:** A specialized scan looking only for certain services to exploit.
- **Fragmented packets:** The scanner sends fragments of packets. Such fragments can sometimes get through certain packet filters in a firewall.
- **UDP:** The scanner looks for open UDP ports.
- **Sweep:** The scanner connects to the same port on several (even many) computers.
- **FTP bounce:** The scanner goes through an FTP server (to appear legitimate).
- **Stealth scan:** The scanner partly disables the log service of the operating system, so it can no longer record the scanner's activities.

SPOOFS

- The term spoof means to pretend to be someone else, to falsify one's identity, or to cover tracks.

- It is no wonder that various spoofing methods are used by hackers to gain access or to obtain information.

IP Spoofing

- A computer may be protected from attack by restricting the IP addresses that may send it data.
- A router may have a list of IP numbers and it allows only data from these numbers to enter the computer.
- A hacker who has this list may spoof the router by sending data that appears to have come from a legitimate IP address.
- Someone who doesn't have the list may discover an allowed IP number by sending the computer data packets with consecutive IP numbers until a packet gains entry to the computer.

Defence against Spoofing

- Defending against spoofing is never perfect, because it involves built-in weaknesses in the TCP protocol.
- However, a full understanding of the problem, combined with a few simple precautions, can reduce this threat.
- The defense involves two main techniques as follows:

SPOOFING:- Filtering

- Implementing spoofing filters on routers and firewalls is crucial. This helps identify and block traffic with spoofed IP addresses.

SPOOFING:- Encryption and Authentication

- There are Internet protocols that specify the details of data encryption and how to authenticate messages.

- While imperfect, such protocols may help to eliminate simple IP spoofing attacks.

SPOOFING: Sequence number spoofing

- Sequence number spoofing is the case where a hacker can compute or guess the next set of sequence numbers in a data transmission.

A TCP sequence prediction attack is an attempt to predict the sequence number used to identify the packets in a TCP connection which can be used to counterfeit packets.

- The hacker can, in such a case, send false packets of data and they will be received with full trust by the client program in the receiving computer.
- Good defense against this kind of attack is to encrypt the data.
- If the hacker doesn't know the encryption key, any false data inserted will not decrypt properly and will therefore be useless to the owner (who can request a retransmission) as well as to the hacker (who can try to corrupt the next transmission).

CASE STUDY: Sequence Number Spoofing

Perhaps the most famous case is that of Kevin Mitnick.

On a particular day in December 1994, a hacker first probed a set of computers owned by Tsutomu Shimomura, a scientist and computer security professional in the San Diego area.

Once vulnerability was discovered, an attack was launched employing IP spoofing. The hacker managed to break into the computers and steal files. True to being a security expert, Shimomura kept detailed logs on the use of his computers in his absence.

Once back from his vacation, the logs told him of the attack. The stolen files were tracked by the FBI to toad.com, to computers in Marin county, north of San Francisco, to Denver, San Jose, and finally to Kevin Mitnick, a hacker in Raleigh, North Carolina.

After spending five years in jail, Mitnick was released on January 21, 2000.

SPOOFING: Session hijacking

- This type of attack occurs when a hacker gains privileged access to a network device, such as a router, that serves as a gateway between the server and client.
- The hacker can, in such a case, use IP spoofing to take over the entire session of data transmission and send any information, rogue programs, and corrupt data to the client's computer.
- Most authentication in the TCP/IP protocol takes place at the time the connection is established, and this can be exploited by a hacker to gain access to a machine by, for example, using source-routed IP packets.

Session Hijacking

- This allows a hacker at node *A on the* network to participate in a data exchange between *B and C by placing himself in the* middle and routing the IP packets to pass through his machine.
- An alternative is to use “blind” hijacking, where the hacker guesses the responses of the computers at *B and C.*
- *The hacker can, in such a case, send a command and* cannot see the response, but can guess the response to many commands.
- A typical command is to set a password allowing access to *B and C from somewhere else on the* network.

CLASS ACTIVITIES …….a

- Give a real life scenario that simulates an IP address spoofing.
- Have you or someone else you know, encountered any of such spoofing incidents?
- Give a good difference between an ACTIVE attack and a PASSIVE attack
- What is a Port Scanner?

DNS

- A domain name server (DNS) is a computer used specifically for networking.
- It has a dictionary with IP addresses and the corresponding URLs.
- When a computer wants to send data, it has to prepare packets with the IP address of the receiving computer.
- The human user normally knows the URL (a meaningful string), so the sending application has to connect to the DNS first, send it the URL, and receive the corresponding IP address.
- Only then can the application send data with the proper IP and TCP headers.

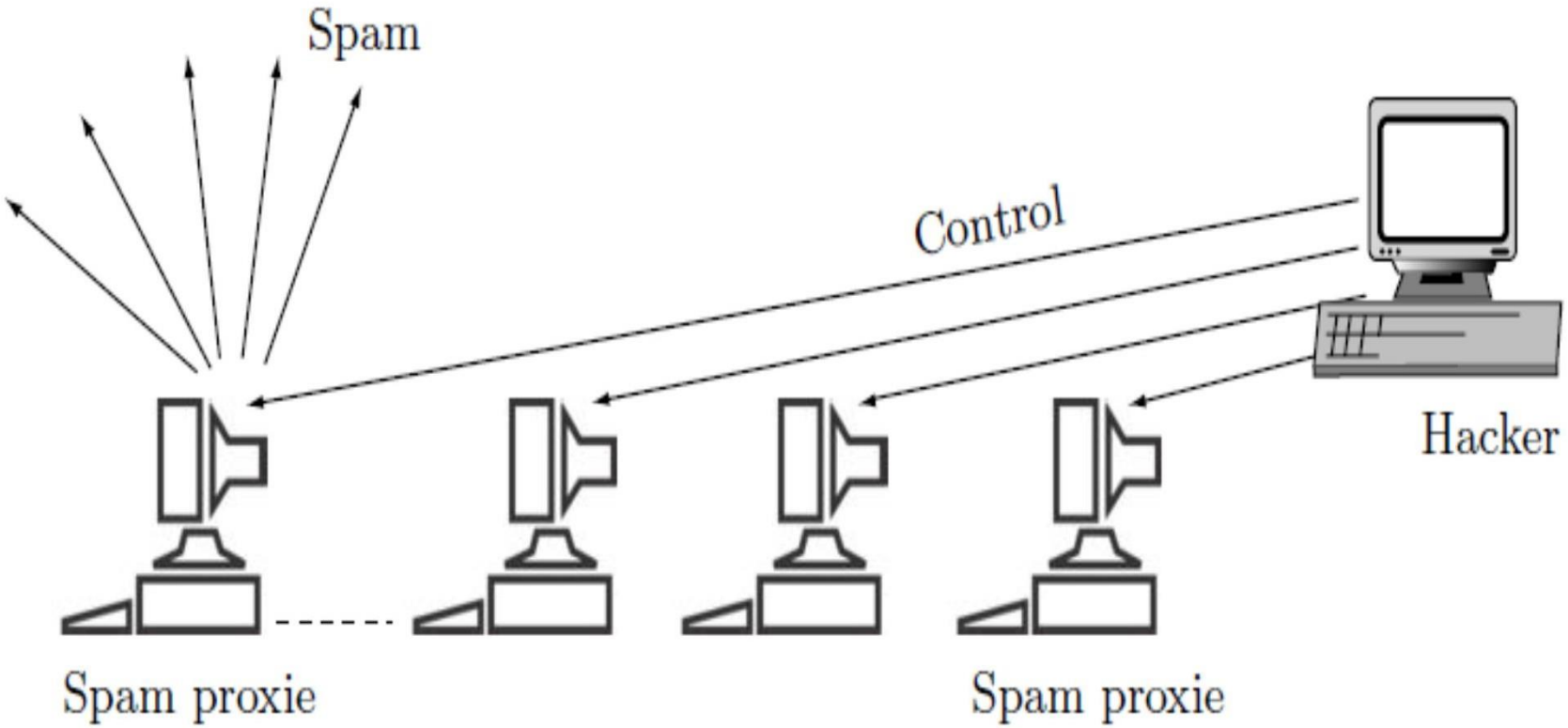
SPAM

- Spam is unwanted, unsolicited email sent in bulk to many unwilling recipients.
- Most of it is commercial advertising for dubious products, get-rich-quick schemes, or quasi-legal or health services.
- Current spam levels (in early 2019) are estimated at 72% of all email and are growing.
- By itself, spam is nuisance, not a security concern, but it can be exploited for a DoS attack.
- A central computer dedicated to sending and receiving email for a large organization can be attacked by sending its many users massive quantities of identical email messages.
- This consumes valuable network bandwidth, it overloads the CPU, eats up disk space on the email server, and can cause it to crash (by overflowing some data structure) or freeze (by keeping the CPU permanently occupied with receiving, logging, sending, and forwarding the spam messages).

SPAM

- It may come as a surprise to many that most spam messages are sent from computers (mostly private personal computers on high-speed cable) that have been infected by special strains of viruses.
- Such a virus hijacks the infected computer and turns it into a *spam proxie* (a special case of zombie).
- A major spammer may at any time control thousands of spam proxies that serve him obediently and send millions of spam messages anonymously

SPAM



An Army of Spam Proxies

SPAMS

- The sobig virus (technically a worm) was the first specimen of malicious software designed to create spam proxies, but similar viruses (mostly variants of the original sobig) are implemented and released and manage to infect tens of thousands of computers worldwide every week.
- The virus installs special software known as spamware that takes over the computer (essentially hijacking it) and handles the distribution of spam.
- Once a hacker has released such a virus and has obtained a fresh army of spam proxies, he may try to sell them to spammers through special online forums that are often closed to the general public.
- Much of the spamware currently in use is written by the Russian programmers and spammers

Why SPAM is bad

- The four main reasons why spam is so bad are as follows:
- **It is easy to send.** All that a spammer needs is spam software and a fast Internet connection. Such a connection may send a flood of millions of identical messages a day, while costing only about $100 a day. On the other hand, if any of the millions of receivers spends just 10 seconds on deleting a spam message, the total effort may add up to thousands of hours wasted each day by the receivers. In addition, spam sent as email to cell telephones may cost its receiver money, not just time.
- Many spam messages ask the user to click on a link to be removed from the mailing list. As many of us have found, clicking to be removed from such a list at best verifies to the spammer that the email address exists and at worst may result in a virus infection. There is also the ethical question of why I should have to get off a mailing list I never asked to be placed on.

Why SPAM is Bad

- Spammers tend to use computing resources illegally or even to steal them outright. A spammer may employ an Internet attack to get hold of a PC, then use that PC to forward its spam messages. The receivers see messages coming from the PC, and complain to its owner, often a clueless individual who has no idea of the many security pitfalls lurking in the Internet.
- Spam is trash. We have all seen messages advertising worthless merchandise and deceptive or fraudulent services.

How to avoid spam

- Use anti-spam software, update and run it regularly. This software can significantly reduce unwanted email, especially if it is programmed to receive feedback from the user/reader and employ it to learn (from the subject line or sender's address) which messages are spam.
- Never buy anything advertised by unsolicited email because this only encourages future spam. Once your email address becomes known to the seller, it will be added to the huge address lists that are sold to other spammers, with the result that you'll receive even more junk email. Worse still, responding to spam advertises you as a sucker and opens you to further fraud and identity theft attempts.
- If the sender's name sounds unfamiliar, delete the email without any hesitation.
- Most spam is just a nuisance, but often it includes viruses and other nasty software.

How to Avoid SPAM

- Never respond to spam messages or click on any links in them. Replying to spam—even to unsubscribe from it—confirms to the spammer that your email address is a valid one, thereby encouraging more spam.
- Opt out of any further information or free or attractive offers. When you fill out forms on the Web, uncheck any checkboxes that offer further information or offers.
- Don’t use the preview mode in your email viewer. Spammers can verify that a message has been previewed, even if it hasn’t been opened, because the preview effectively opens the email.) Knowing that you have read their messages encourages the spammers.
- Try to decide whether an email message is spam based only on the subject line and sender’s name and address. Use the bcc field if you email many people at once. The bcc (blind carbon copy) field hides the list of recipients from any individual recipient. If you include the addresses in the To field, spammers may harvest them and add them to mailing lists.

How to Avoid SPAM

- Restrict the use of your email address on the internet. Don't publish it on Web sites, newsgroup lists or other online public forums. Spammers have software that crawls the internet to find addresses in such places, harvest them, and add them to mailing lists.
- Give your main address only to those you trust (and even then be ready for your address to be discovered and abused by spammers).
- Always have several secondary email addresses ready. (Those are easy to open at sites such as Yahoo, Hotmail, and emailaddresses.com) When you fill out Web registration forms or surveys on sites with which you don't want further contact, use a secondary email address. If the secondary address is flooded by spam, simply close it. This protects your main address from spam.