COSC130

Fundamentals of Cybersecurity and Privacy

LECTURE 8: COMPUTER NETWORKS

How to Protect Yourself from Network Threats

1. Overview of Computer Networks and Cryptography
2. HTTP vs HTTPS
3. Firewalls
4. Virtual Private Networks

Much of this lecture is based on

1. Week 4 Networking and Communications
   Week 6, Network Security Section 1 Firewall Basics; Section 2 VPN Basics
   OpenLearn. *Introduction to Cyber Security, 2016*.
2. Section 2.4.4 Case Study: HTTP
   Section 2.7.1 Case Study: Reconnaissance
   Section 2.7.2 Case Study: Perimeter Security vis Firewalls
   Section 2.7.3 Case Study: Denial of Service Attacks
   Section 2.7.4 Case Study: Network Intrusion Detection Systems
   Markuset al. (Eds.), The ethics of cybersecurity (Vol. 21). Champaign, IL: Springer.

In-text references to this source are typically omitted for readability.

What is a Computer Network?

A computer network is a structure that connects two or more computers (or, more generally, devices) and allows them to communicate and exchange information.

In its simplest form, communication involves a sender, a receiver, and a transmission medium.

A transmission medium is the physical communication channel:

1. Copper wires
2. Fiber optic cables
3. Wireless - electromagnetic waves

What is a Computer Network?

Some types of networks:

1. PAN – Personal Area Network – spanning the personal space of an individual and connecting personal devices and peripherals (e.g., a laptop and a headset)

2. LAN – Local Area Network – spanning a small area, usually a single building or a few adjacent buildings – school, company, hospital, home

3. MAN – Metropolitan Area Network – spanning an entire city and consisting of multiple interconnected LANs

4. WAN – Wide Area Network – spanning large areas across different cities or countries; consists of multiple interconnected LANs and/or MANs

5. Internet – World Wide Area Network

What is the Internet?

The Internet is a network of networks spanning the whole world.

It consists of thousands of separate LANs and WANs, organised hierarchically, and owned by different owners: governments, companies, various organisations, individual users, etc.

The Internet is based on two key design principles:

1) There should be no single device controlling the Internet.

2) Even if some of the internet devices fail, any two devices should still be able to communicate via alternative routes.

Network Components

1. Device - (computers, tablets, smartphones, etc.)
2. Switch – connects devices within a Local Area Network (LAN) to each other thus allowing transfer of data within LAN; it only has LAN ports
3. Router – connects devices within a Local Area Network and also connects LAN to the Internet; has both WAN and LAN ports
4. Firewall - protects LAN and can be installed on the router
5. Transmission medium – the way information is transmitted (e.g., through cable or wireless)

IP Addresses

Each device on the internet has a unique IP address, consisting of 4 bytes, for example, 35.222.0.93.

A bit is a unit of information and can hold only two distinct values, 0 or 1.

A byte consists of 8 bits and can hold numbers between 0 and 255.

Therefore, an IP number consists of 4 numbers separated by dots, where each number can be any integer between 0 and 255.

There are altogether 256*256*256*256 = 4,294,967,296 distinct IP addresses. While this looked like a really big number when the IP addresses were first created, it is not enough today – some estimates show that in 2023, around 15 billion devices connected to the internet.

Network Address Translation (NAT)

A temporary solution, known as NAT (Network Address Translation) was first proposed in RFC1631 document.

NAT turned out to be a very effective solution, which also contributed to the network security by hiding the identity of the devices in the local network.

Some of the IP addresses are designated as private addresses, which can only be used for devices in a private network. They are:

10.0.0.0 – 10.255.255.255 (starts with 10 and has a fixed 8-bit prefix)

172.16.0.0 – 172.31.255.255 (starts with 172.16 and has a fixed 12-bit prefix)

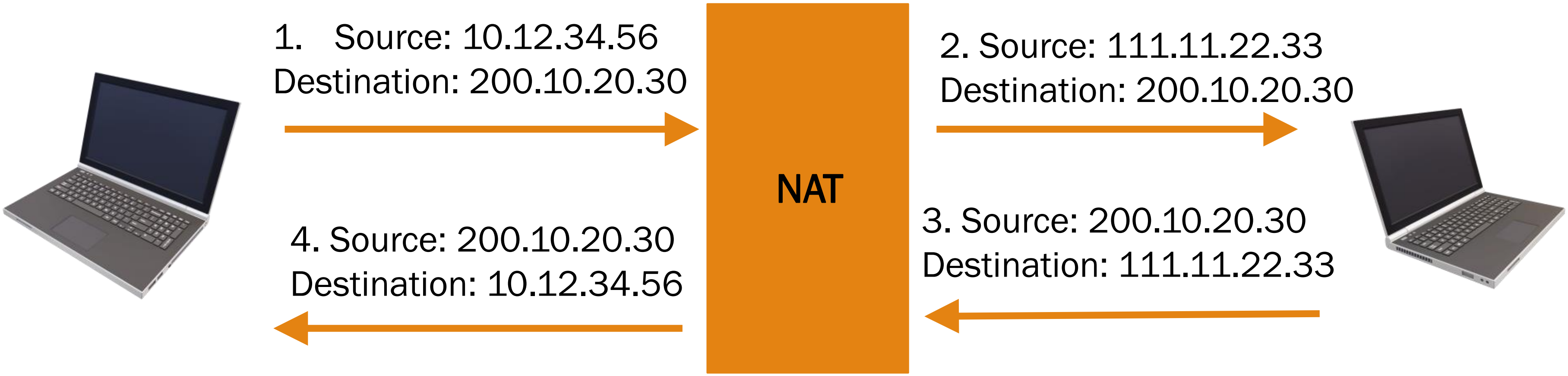
192.168.0.0 – 192.168.255.255 (starts with 192.168 and has a fixed 16-bit prefix)

The remaining IP addresses are public.

Network Address Translation (NAT)

Using NET, a single public IP address can be used for the whole private network that can have a large number of devices. Public IP addresses are assigned by the Internet Service Provider (ISP) and are expensive.

When a device with a private IP address tries to connect to the internet, its private IP address is replaced by the network's public IP address.



1. Source: 10.12.34.56
Destination: 200.10.20.30

2. Source: 111.11.22.33
Destination: 200.10.20.30

NAT

3. Source: 200.10.20.30
Destination: 111.11.22.33

4. Source: 200.10.20.30
Destination: 10.12.34.56

When communication arrives from the outside network in step 3., how does the NAT know which internal IP address it is intended for? It knows because it allocated an unused port number above 1023 and is keeping the mapping between these port numbers and internal IP addresses/port numbers during the communication. This is referred to as Port Address Translation (PAT).

How do computers and other devices communicate via the Internet?

A question: How can all the different devices and networks using different technologies exchange information?

The answer: By using communication protocols.

A communication protocol is a set of rules and procedures for transmitting data between network devices.

A useful analogy here is to think of a group of people trying to communicate, but each one of them speaks a different language. If they all speak a common language, say English, then each pair of people can communicate. Here ‘English’ has the role of a network protocol.

IP (Internet Protocol) and TCP (Transport Later Protocol) work together to allow data to move around the Internet, and they are commonly referred to as the TCP/IP protocol suite.

How does TCP/IP work?

TCP breaks a document* to be transmitted over the internet into “packets”, also called “datagrams”. Each datagram contains a header with the IP address of the sender/receiver and some other information, such as time stamp and error correcting code, and the payload (the content of the datagram).

IP is responsible for sending datagrams across the internet.

At the destination, TCP combines the packets to reconstruct the original documents and requests re-transmission if some packets have been lost or corrupted.

* Here ‘document’ refers to any data we send over the internet, including an email, a web page, an image, a video, a file, and so on.

How do datagrams move across the internet?

From a sender's computer, datagrams are passed to the local router. The local router has a table with a known IP address, and it looks for the recipient IP address in that table.

- If it finds it, it send the datagram directly to the destination IP address.
- If it does not find it, it sends the datagram to a higher-level router.

This process continues until it reaches the router that has the destination IP address in its list, which then sends the datagram to the lower-level router.

Eventually, the datagram reaches the recipient's local router, which then sends it to the recipient's IP address.

Two datagrams belonging to the same document may or may not take the same route through the internet, as the route is chosen in such a way as to avoid congested parts of the internet and unavailable routers. This is possible as routers communicate with each other and let each other know what their status is and how busy they are.

Wireless Networks

Wireless networks are computer networks that use electromagnetic (radio) waves as their transmission medium.

Wireless Local Area Networks (WLAN) are very common nowadays.

Wi-Fi refers to WLANS that comply with IEEE 802.11 standard family.

WLANs are identified by the Service Set Identifier (SSID), there the 'service set' is the collection of devices connected to the WLAN.

One has to be careful when connecting to free, unsecured Wi-Fi networks, as they may be set up by attackers; the name of such a network may be intentionally chosen to resemble the legitimate provided, for example, "Airport Wi-FI".

Attacks on Networks

1. Packet sniffing

2. Men-in-the-middle-attack, where an attacker places themselves between the sender and the receiver and modifies or deletes the message

3. Denial of service – an attacker transmits a large amount of data on the network frequency in order to overwhelm the network and prevent legitimate users from transmitting the data.

Packet Sniffing

We saw that data packets (datagrams) can take different routes, depending on internet traffic conditions and the availability of routers. Therefore, it is not possible to know upfront which routers the packet will go through.

A packet sniffer is a program or a hardware device that captures and logs internet traffic. It can record the packet header or the entire content of the packet including the payload.

Packet sniffing is used for various purposes including analysing network traffic and identifying problems, detecting intrusion attempts, and fulfilling legal obligations, but it can also be used to breach confidentiality and, for example, read login details of network users.

Packet Sniffing

We saw that data packets (datagrams) can take different routes, depending on internet traffic conditions and the availability of routers. Therefore, it is not possible to know upfront which routers the packet will go through.

A packet sniffer is a program or a hardware device that captures and logs internet traffic. It can record the packet header or the entire content of the packet including the payload.

Packet sniffing is used for various purposes including analysing network traffic and identifying problems, detecting intrusion attempts, and fulfilling legal obligations, but it can also be used to breach confidentiality and, for example, read login details of network users.

Denial of Service Attack

We said that in the Denial of Service (DOS) attack, an intruder attempts to consume as much as possible of the victim's resources such as communications lines of computational power, in order to deny these resources to legitimate users.

In a Distributed Denial of Service (DDOS), an intruder employs a botnet, that is, an army of infected 'zombie' computers to launch an attack.

In an amplification attack, the attacker sends a small request that requires a large response to a third party and also spoofs the sender's address – instead of being the attacker's address, it is set the victim's address. Then the third party will send a large response to the victim for each small request by the attacker (thus the name 'amplification' attack). This is possible because the Internet Service providers are not incentivized to check for spoofing attacks.

Some zombie malware, such as Mirai, makes use of security weaknesses of the devices on the Internet of Things. The IoT owners are not incentivized to provide security to IoT devices.

Denial of Service attacks are difficult to protect against and are costing online companies a lot. The best way to protect against this type of attack is to provide a very large amount of resources (which is also costly!) and to filter internet traffic to try to identify traffic potentially belonging to a Denial of Service attack.

Security Mechanisms: Encryption

Encryption is the process of converting the plaintext message into a cyphertext, by using the encryption key.

The most widely used type of encryption is the so-called “symmetric” encryption. The sender Alice and the receiver Bob share a secret key only known to them. Alice encrypts the message using the shared key and sends it to Bob.

Bob uses the same key to decrypt the message.

As discussed before, Alice knows that Bob is the only one who can decrypt and read the message; similarly, Bob knows that Alice is the only one who could have encrypted the message. Therefore, symmetric encryption supports the following security services:

1. Confidentiality
2. Integrity – if the ciphertext decrypts to a meaningful plaintext, Bob knows that it has not been modified
3. Authenticity

Wi-Fi Encryption

On wireless networks, encryption was/is provided by the following standards:

1. Wired Equivalent Privacy (WEP)
2. WiFi Protected Access (WPA) was developed by WiFi Allience and become available in 2002; subsequently, new versions were released:
   - WPA2 in 20024
   - WPA3 in 2018

.

Firewalls

A firewall is a wall designed to prevent fire from spreading or at least to slow the spread.The role of a firewall in computer networks is to protect a LAN, a part of LAN, or a single computer from malicious traffic. All communication with the LAN/computer should come through the firewall, so it is often convenient to place the firewall at the router.

A firewall can be

- a dedicated network device;
- a part of a router or operating system.

The basic roles of a firewall are:

1. Packet filtering
2. Stateful packet filtering
3. Application-level gateways

Packet Filtering

A firewall inspects the data packet header and checks

- the source and destination IP address and port
- protocol
- some other information

and compares it against the given set of rules. If it matches a rule it is accepted, otherwise it is dropped or the connection is terminated.

Advantages:

1) It is simple.
2) It is widely available.

Disadvantages:

1) Rules are hard to define.
2) Once defined, it is hard to do security tests.
3) Since packet filtering is stateless, it is vulnerable to spoofing and other attacks.

Stateful Packet Filtering

A firewall keeps track of the state of connection for all packets, both inbound and outbound.

Then the firewall only permits the data packets belonging to an established connection.

Advantages:

1) Instead of writing a comprehensive set of rules for all data packets, the administrator only needs to provide rules for the first packet when the connection is opened.
2) More efficient

Application Level Gateways (Application Proxies)

A firewall inspects the data packet in depth to identify the application (HTTPS, SNMP, etc) and can block certain applications, for example, if they require extensive bandwidth.

Advantages:

1. More secure as proxies replace direct connections between trusted internal and untrusted external hosts

Disadvantages:

1. It is slower and requires more CPU processing time/power
2. Each new application requires a new proxy

Personal Firewalls

A personal firewall is a firewall installed on an individual computer as a part of its operating system.

Its role is to protect the computer and the attached devices, and it should not replace the network firewall protecting the LAN from outside of the network.

A personal firewall is especially useful for people who regularly connect to different networks.

.

Virtual Private Networks (VPNs)

The best way to provide secure communication across networks is to have one's own communication lines, not shared with anyone else. However, this would be a very costly solution.

Virtual Private Networks use untrusted networks (internet) to provide secure communication. This is achieved by creating a secure 'tunnel' between *VPN clients* and the *VPN server*. The communication via tunnel is typically encrypted to provide confidentiality and integrity of transmitted data.

VPN client software is installed on all computers using the VPN.

VPN server is installed on a dedicated device and authenticates users and routes the traffic. This may slow down the access to resources.

VPN servers can be located

1) at the perimeter of the company's network to protect its traffic
2) on a remote server anywhere in the world allowing paying clients to connect – from the outside it appears that a VPN client is located where the VPN server is
3) on a home computer that was left on running so the owner can connect to it from elsewhere – from the outside it appears that the owner is connecting from home

Virtual Private Networks (VPNs)

VPNs use cryptography to ensure confidentiality, integrity, authenticity and non-repudiation.

1) Encryption
2) Hashes
3) Digital Signatures
4) Message Authentication Codes (MACs)

Virtual Private Networks (VPNs)

VPN protocols:

1) PPTP (Point to Point Tunnelling Protocol)

Designed by Microsoft as an inbuilt component of Windows NT 4 and a free add-on to Windows 95 and Windows 98.

User authentication and encryption were not standardized leading to incompatibility. This led to its replacement by L2T2 in 2000.

2) L2TP (Layer 2 Tunnelling Protocol)

l2TP was designed by PPTP Forum, Cisco and the Internet Engineering Task Force (IETF). It was built upon PPTP and L2F that was designed by Cisco to compete with PPTP.

3) *IPSec (Internet Protocol Security)*

- Originally designed by the *Internet Engineering Task Force* (IETF)) in 1992.
- Widely adopted (Intel, IBM, HP/Compaq, Microsoft, etc.)
- Made use of existing, well-tested and trusted cryptographic technologies

Security Risks Introduced by VPNs

1) Security of remote machines

VPNs allow employees to work on their own computers running their own software, or they can even share their computers with other users.

Since remote computers are now incorporated in VPNs they must also be secured.

2) Security of the VPN implementation

While the protocols used by VPNs may be secure, their implementation may introduce new vulnerabilities. For Example, Microsoft's implementation of PPTP introduced vulnerabilities later exploited by hackers.

3) Security of interoperation

New vulnerabilities may be introduced as a result of mixing technologies supplied by different vendors – it is safer to go with the same vendor.

4) Security of network availability

VPNs depend on the internet's reliability for the delivery of information.

References

[**OpenLern, 2016**] OpenLearn. *Introduction to Cyber Security*, *2016*.

[**Markus et al., 2020**] Markus, C., Gordijn, B., & Loi, M. (2020). C. Markus, B. Gordijn, & M. Loi (Eds.), The ethics of cybersecurity (Vol. 21). Champaign, IL: Springer.

[**Nayak et al, 2014**] **U.** Nayak and U.H. Rao. (2014) The InfoSec Handbook: An Introduction to Information Security (p. 505). Apress. Kindle Edition.