The Internet and Cybersecurity

A system of interconnected networks

Alwin Tareen

What is the Internet?

- In general, the Internet is a system of interconnected networks based on open standards and protocols.
- It is a network of global exchanges, which include private, public, business, academic, and government networks.
- The connection links can consist of wired, wireless, or fibre optic networking technologies.
- The Internet carries a vast range of information resources and applications of the World Wide Web.

Protocols and Systems

Internet Protocol(IP)

- The IP protocol is used to designate identifying addresses to the devices that are connected to the Internet.
- IP addresses are 32 bits in length. They can be expressed in decimal form by: `#.#.#.#`
- Each # in the above address is a number from 0 to 255, inclusive.

The Internet Engineering Task Force(IETF)

- All Internet standards are developed and maintained by this Task Force.
- It is the standards organization whose mission is to improve the usability and interoperability of the Internet.

Protocols and Systems

Access Point

- In order for a device to connect to the Internet, it must go through an access point. Usually, this takes the form of a home router.
- The home router is then connected to a switch, then to a commercial router, then to the Internet.

Dynamic Host Configuration Protocol(DHCP)

- The DHCP protocol is responsible for assigning IP addresses to connected devices. This process occurs automatically.

Protocols and Systems

Domain Name System(DNS)

- These are the servers which take human-readable Uniform Resource Locators(URLs), and translate them to numerical IP addresses.

Transmission Control Protocol(TCP)

- This is responsible for guaranteeing the delivery of all data packets that are submitted via the Internet.
- It also indicates the intended service of these data packets(web browsing, email, etc.).

The Internet Protocol(IP)

- The Internet Protocol is a set of rules that helps define how information on the Internet is transmitted.
- Each device on the Internet is assigned an identifying number called an IP address.
- The current version is IPv4. However, it is in the process of being upgraded to IPv6.

IPv4 Addresses

Machine-readable form:

- An IP address is 32 bits in width, when expressed in binary.

```
11010011 10111001 10110110 11011011
```

Human-readable form:

- Each IP address is composed of four decimal numbers, separated by decimal points.
- Each number is a decimal number in the range 0 to 255, inclusive.

```
140.247.16.31
```

IPv4 Addresses

- There can be at most 2^{32} unique addresses under IPv4, which is about 4.3 billion.
- However, this amount is no longer sufficient to handle all of the connected devices currently in use, so the IPv6 standard was developed.
- IPv6 addresses are 128 bits wide, which means that there are 2^{128} unique addresses available under this scheme.

IPv6 Addresses

Machine-readable form:

- An IP address is 128 bits in width, when expressed in binary.

```
1101..............................1011
```

Human-readable form:

- Each IP address is composed of eight hexadecimal numbers, separated by colons.
- Each number is a hexadecimal number in the range 0000 to ffff, inclusive.

```
28aa:0018:a5b2:d793:e383:43ab:8ca1:b95d
```

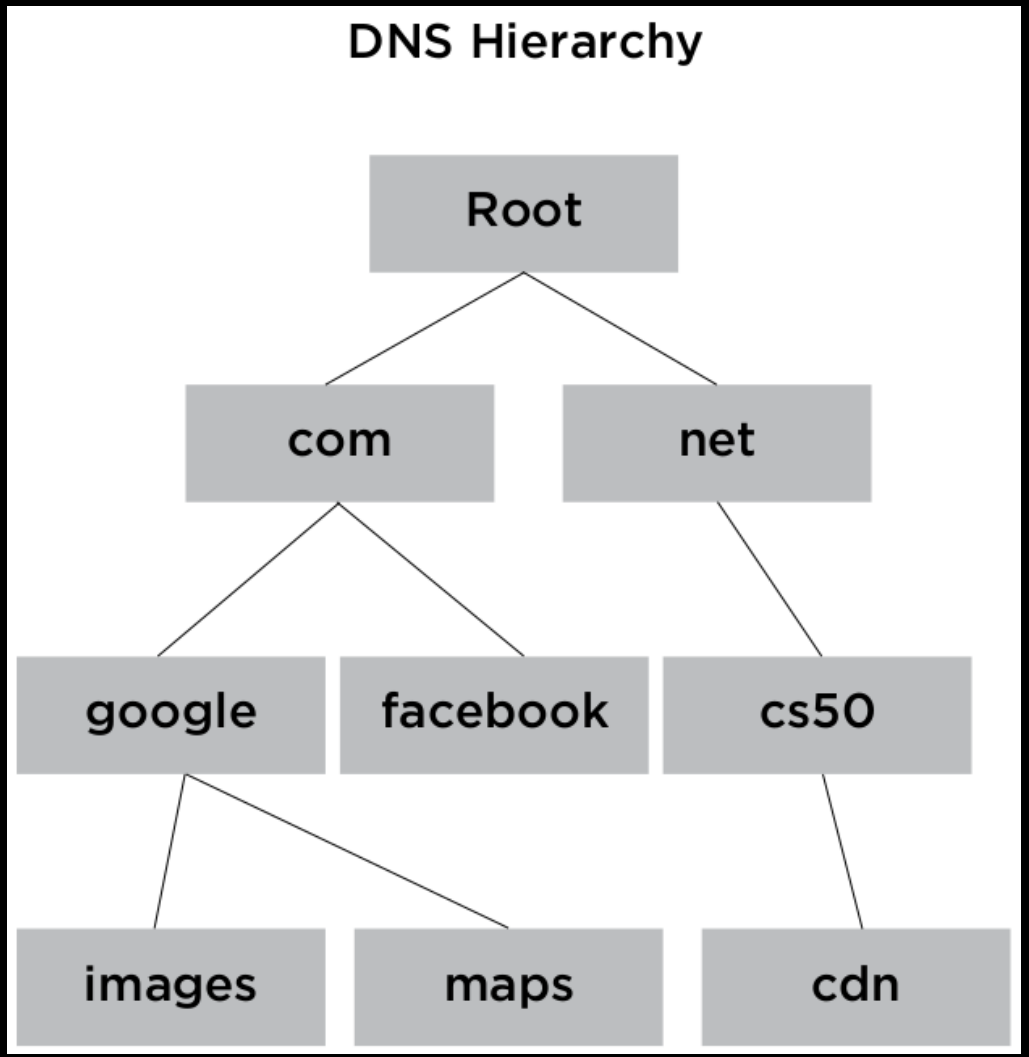
Domain Name System(DNS)

- When you want to access a web page, you must type in a human-readable Uniform Resource Locator(URL) into your web browser.
- However, the Internet Protocol still requires the computer to know which IP address it is trying to access.
- DNS is the system which is responsible for taking the domain, which is just an identifier like `baidu.com` and translating it into its respective IP address.

Domain Name System(DNS)

- When a user types in a URL into a web browser, the computer contacts a DNS server, which stores information about which domain names map to which IP addresses.
- Then, the corresponding IP address gets sent back to the browser.
- Domains in the DNS are organized in a tree-like hierarchy. There are a set of basic top-level domains(TLDs), which are: `com`, `net`, `org`, `edu`, etc.
- Website URLs must branch off from one of these top-level domains.

DNS Hierarchy



Dynamic Host Configuration Protocol(DHCP)

- Computers need a mechanism of being assigned IP addresses.
- At one point in the Internet's history, a human network administrator was responsible for assigning IP addresses to computers.
- Now, the DHCP protocol is able to take care of this process automatically.

Dynamic Host Configuration Protocol(DHCP)

- When computers connect to a network, they will connect to a DHCP server.
- The DHCP server is able to access a pool of available IP addresses, and the server is responsible for assigning each computer on the network a unique IP address.
- Using DNS and DHCP, devices on the Internet are able to receive their own IP, and determine which IP address corresponds to the website that a user is trying to visit.

Transmission Control Protocol

- Instead of sending all of the data in a transmission in one big packet, information on the Internet is sent in smaller data packets.
- TCP is responsible for breaking up the data into ordered packets.
- There's no guarantee that the packets will arrive at their destination at the same time, or even in the correct order.
- Therefore, TCP labels each packet with the order in which it should be assembled.
- This way, the receiving computer can re-assemble the packets together in the correct order.

Transmission Control Protocol

- In addition to assigning a packet number, TCP also assigns the data a **port** number, to indicate what type of Internet service the data should be used for.
- For instance, SMTP(email) uses port 25, while HTTP(web browsing) uses port 80.

Transmission Control Protocol

The steps in transmitting data across the Internet:

- The data is first broken up into smaller packets.
- TCP labels each packet with a port number, and a packet number.
- IP tells the packet its destination.
- The data is transmitted via routers, which eventually direct the packet to its destination.

Routing

- Routing between two points on the Internet is redundant, since there is more than one way for data to move from one point to another.

Bandwidth

Calculating bandwidth(bits/second)

- The flow of data on the Internet is typically measured by bandwidth, which is calculated as follows:
- The size of the information being sent at any time is measured in bits.
- Latency is the duration of time that is incurred from when a data packet is sent, to when it is received.
- Bandwidth is the quantity of bits being transmitted, over a fixed amount of time.

$$\text{bandwidth} = \frac{\text{quantity of bits}}{\text{latency}}$$

- The units are bits/second.

Cybersecurity

- Cybersecurity refers to systems and practices that websites and users can employ in order to better protect themselves against cyber threats.
- Users can help to protect themselves against cyber threats through a variety of means, including choosing more secure passwords, and being mindful of spam email.

Examples of Cyber Threats

Phishing

- This is where a hacker sends an email to a user, pretending to be from a legitimate source. In the body of the email, the user is asked to click on links that may request passwords, or other sensitive information.
- Hackers may also convince users to send email replies to them directly, containing their personal and sensitive information.

Viruses

These are pieces of malicious software that replicate quickly, and are designed to harm and destroy a computer system.

Examples of Cyber Threats

Distributed Denial of Service(DDoS) attacks

This involves flooding a website with false or irroneous requests, so that the site becomes overwhelmed, and cannot handle legitimate requests.

Man-in-the-middle attacks

A malicious piece of equipment(like a router) is inserted between a user and a web server. The result is that an adversary can return web pages to a user that seem legitimate, but are actually fake.

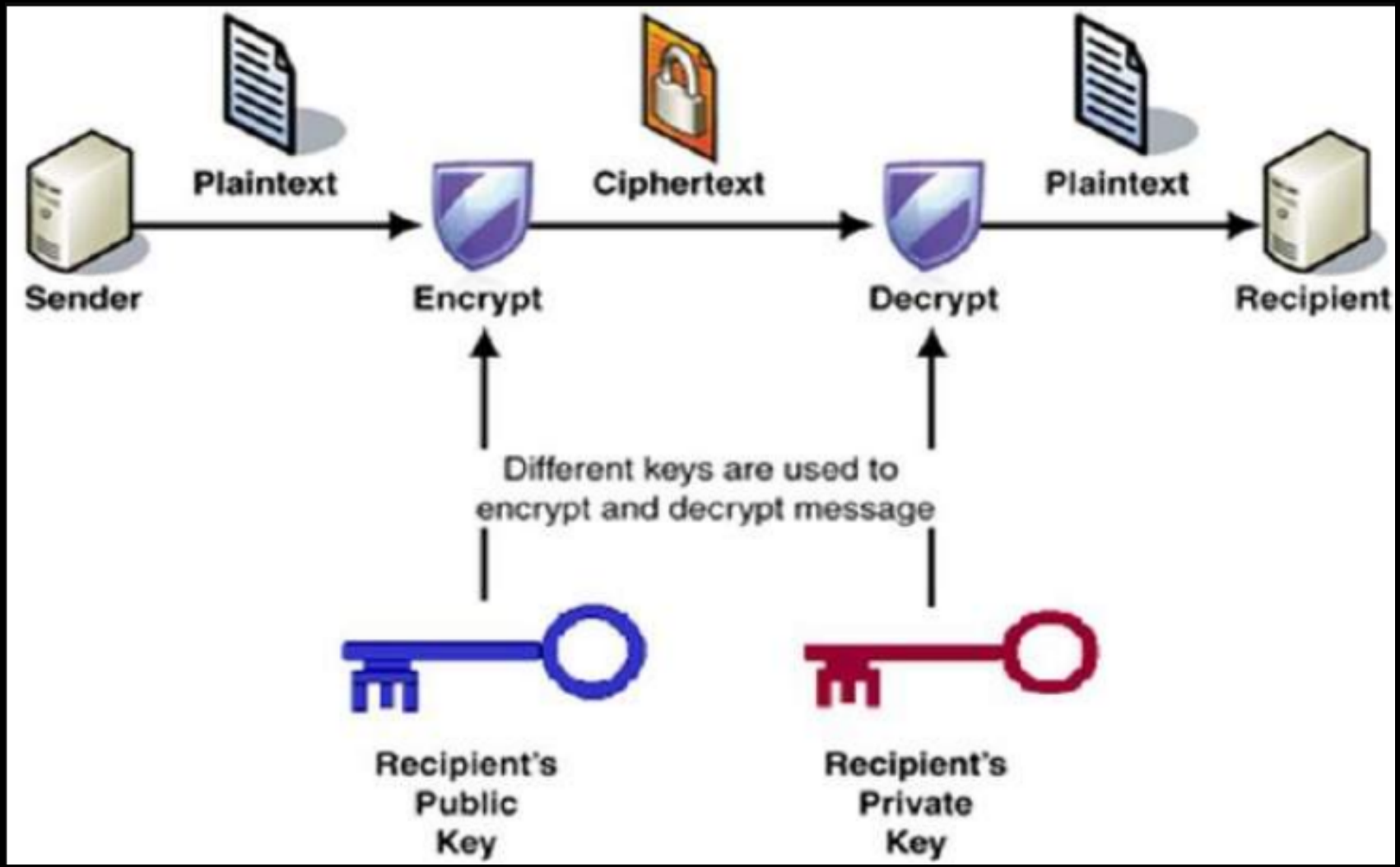
Public-Key Encryption

- Let's consider a case where Alice wants to send an encrypted message to Bob.
- First, Bob must generate his authentication credentials. They consist of a public key and a private key, also known as a **matched pair**.
- Then, Bob publishes his public key openly.
- Alice acquires Bob's public key, and encrypts her message with it.
- Alice then transmits this encrypted message to Bob, through the Internet.

Public-Key Encryption

- Since the Internet is an open transmission medium, an adversary can observe Alice's encrypted message, but they cannot decode it.
- Bob receives the encrypted message from Alice.
- Bob then uses his private key to decrypt the message, and view its contents.
- Public-key encryption is also known as **asymmetric key encryption**.
- One of the most popular schemes in use today is **RSA** encryption.

Public-Key Encryption



Symmetric Key Encryption

- Under this scheme, Alice and Bob must share a single authentication credential, which is a **secret key**.
- Let's say that Alice wishes to send a message to Bob.
- Alice uses the shared secret key to encrypt the message.
- Alice then sends the encrypted message to Bob through the Internet.
- Bob receives the encrypted message, and uses the shared secret key to decrypt the message.

Symmetric Key Encryption

- Note that the same shared secret key is responsible for encryption and decryption.
- If an adversary were to discover the secret key, then they could reveal all transmissions between the two parties.
- Alice and Bob must meet beforehand, and decide upon a shared secret key, prior to sending messages. If they are geographically far apart, then performing this action is problematic.
- Public-key encryption is not affected by this problem.

The Routing Model

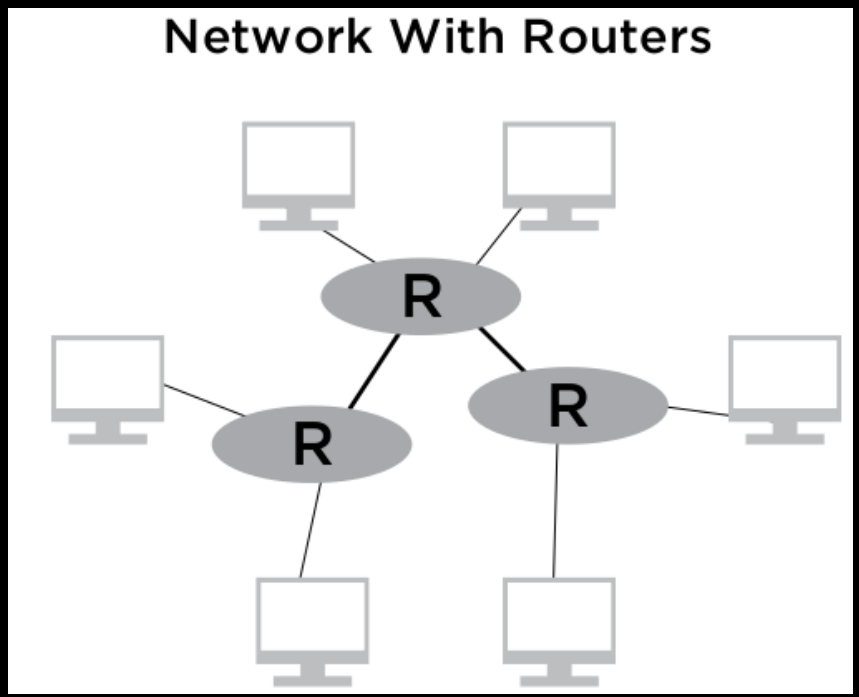
- Routers are the components of the Internet that direct packets of data across the various networks.
- Every Internet-connected device must be able to communicate with every other Internet-connected device.
- One possible scheme would be to directly connect every device to every other device.
- However, this would require too many connections, and would be utterly impractical.

The Routing Model

- Instead, the Internet makes use of routers.
- Every device is connnected to a router, and each router is connected to other routers.
- In this manner, information can be transmitted by passing through one or more routers.
- Each router sends the data packet along to another router, which is closer to the final destination.
- Eventually, the data packet will arrive at a router which is connected to the destination computer.

The Routing Model

- In addition, there is often more than one route that a data packet can take, to get from one location to another.
- Routers will frequently move packets of data across different routes, even if they are intended for the same location.
- This allows data transmissions to be redundant.



The Internet and Cybersecurity: End of Notes