Data Security
Ch 1: Introduction

I. What is the internet

↳ What is inside the internet

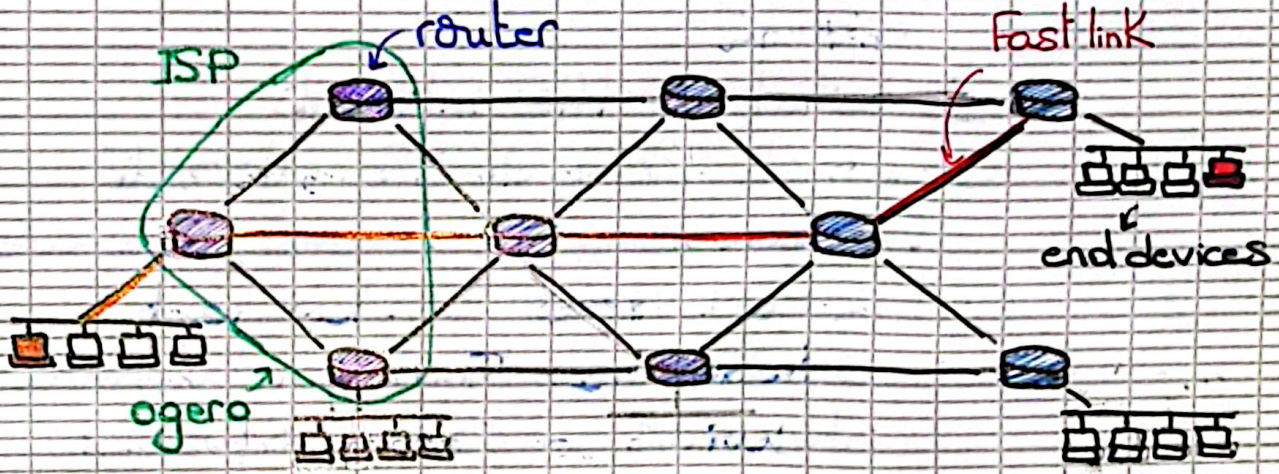
- When using the internet, we are on the network layer
- On the network layer, the data is divided into small pieces called packets
- A packet is a small unit of data that is transmitted over a network, it contain binary data : 0 and 1.
- Each packet has unique IP source and IP destination

↳ Ethernet vs Internet

Ethernet: Refers to a wired network technology used to connect devices within a local area network (LAN). It enables computers, printers and other devices to communicate directly with each other in a confined space (home, office) through physical cables.

Internet: This is a global network that connects millions of computers and networks around the world. It relies on various technologies (like WiFi, Satlelite) to to transfer data.

↳ Network Topology



1) Routers:
- These devices are responsible for managing network traffic by directing data packets between devices and networks
- In the diagram, there are multiple routers connected in a mesh-like pattern, allowing data to flow between them through various paths.

2) Links (Lines connecting routers)
- Links represents connections between routers used for data packets transmission

3) End devices
- The devices connected at the edges (like computers, servers, or switches) are endpoints that utilize the network for communication
- These devices access network resources through the routers.

4) Internet Server Provider (ISP):

Organizations that provide access to the internet

What's the internet: "nuts and bolts" view

1) Devices

- PC, server, wireless laptop, cellular handheld → These are example of end devices, or "hosts", that connect to the internet. Hosts are responsible for running network applications such as web browsers or email ...

- Access points and wired links: Devices connect to the network either wirelessly through access point or with physical connections (wired links)

- Router: direct data packets across the network, helping them reach their destination by choosing efficient path

2) Communication Links

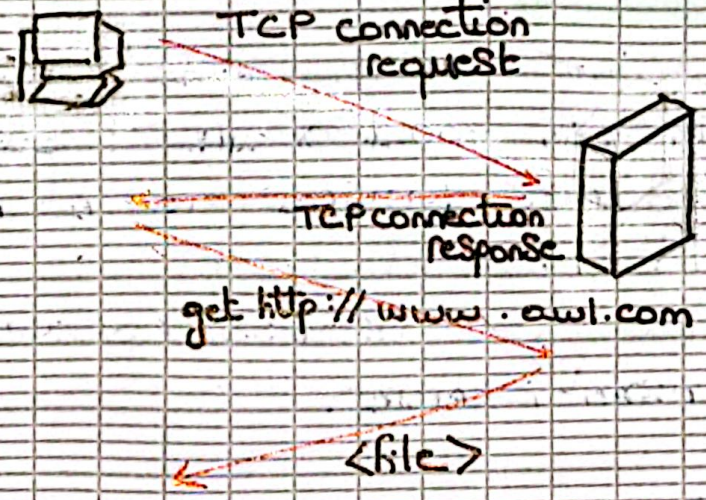
- Fiber, copper, radio, satellite: These are types of communication links that carry data

Quantity of internet by second →

- Transmission rate = bandwidth: the rate at which data is transmitted accross a link, known as bandwidth, determines how fast data moves between devices.

3) Protocols:

- Rules and conventions that control how data is sent and received over the Internet
- Examples: TCP, IP, HTTP, Skype, Ethernet



↳ What's the Internet: a Service View

- The internet, from a service perspective, acts as a communication infrastructure enabling various applications like Web, VoIP, email, games, e-commerce and file sharing

- To enable the functionality of distributed apps, the internet provides 2 main communication services that apps rely on to transmit data

  ↳ Reliable data delivery (TCP):
  ensures data is delivered accurately and in order suitable for app that requires accuracy.

  ↳ Best-Effor (Unreliable) data delivery (UDP):
  delivers data quicly without guarantees suitable for real-time apps (streaming, online games)

II. Network Edge

. The network edge refers to end systems (or hosts) that run applications, such as web browsers and email client, located at the "edge" of the network

↳ **Client / Server Model:**
In this model, a client requests and receives services from an always-on server.
e.g. web browser / server, email client / server.

2 edges on the same level

↳ **Peer - Peer Model**
In P2P, there's minimal or no use of dedicated servers, instead, hosts (peer) directly connect to each other for sharing resources.
e.g. Whatsapp, Skype, BitTorrent.

. At the network edge, data transfer services use 2 main protocols : TCP and UDP

1) **TCP (Transmission Control Protocol)**
. Provides a reliable, in-order data transfer by setting up a connection (handshaking) between host and data transfer

- Reliability: Uses acknowledgments and retransmissions to prevent data loss.
- Flow Control: Prevents the sender from overwhelming the receiver.
- Congestion Control: Slows down data transmission if the network is congested (مزدحم)
- Used by: Applications like HTTP (web), FTP (file transfer), Telnet (remote login), SMTP (email)

2) UDP (User Diagram Protocol)
- Connectionless and unreliable; does not ensure data order, reliability, flow control, or congestion control
- Faster than TCP, prioritize speed over accurancy
- Used by: Streaming media, teleconferencing, DNS, and Internet telephony

III. Network Core - Packet-Switched networks

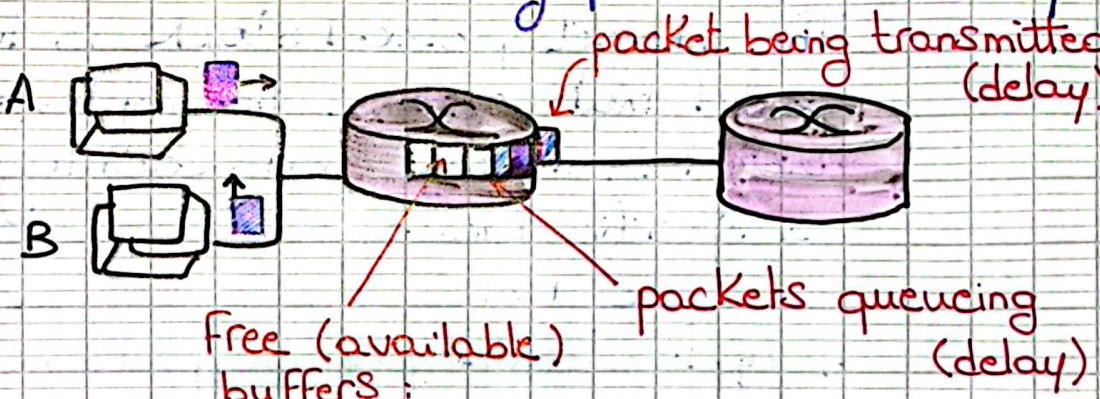
↳ How do loss and delay occur ?

1) Packets Queue in Router Buffer (Delay)

. When the rate of incoming packets (data) exceeds the capacity of the router's output link, packets cannot be transmitted immediately

. These packets are temporarily stored in the router's buffer (temporary storage area) and queue up, waiting for their turn to be send.

This waiting period causes delay



2) Packet Loss

If the buffer is full (no free space) any new packets that arrive will be dropped (lost) because they cannot be stored in the buffer.

- Handling Lost Packets:
  - Lost packets can sometimes be retransmitted by the previous node (the last device that sent it) or by the source end system (the original sender)
  - In other cases, the packet may not be retransmitted at all, depending on the protocol in use (e.g. TCP retransmits, but UDP does not)

IV. Protocol Layers

- Internet protocol stack

The internet protocol stack is layered model that organizes how data is transmitted over the internet, with each layer serving a specific function:

1) Application Layer: Supports network application by providing end-user services (e.g. FTP, SMTP, HTTP)

2) Transport layer: Manages data transfer between processes (apps) on different devices. (e.g. TCP, UDP)

3) Network Layer: Handles routing of datagrams (data packets) from the source to the destination across different networks. (e.g. IP, Routing protocols)

4) Link Layer: Manages data Transfer between neighboring devices on the same network Segment (e.g. PPP(point-to-point protocol), Ethernet). It convert from machine to user language

5) Physical Layer: Transmits raw bits over the physical medium (e.g. cables, fiber optics). It convert data into signals to be sent "on the wire" or through wireless channels

↳ ISO/OSI Reference Model

This model include additional layers not present in the internet protocol stack namely the presentation and Session layers.

1) Presentation Layer:

- Ensures the data is present in a format that apps can understand.
- This layer is responsible for data encryption, compression and translating data between different machine-specific formats
- In Internet Stack: This layer is absent. If needed apps most implement these functions themselve, such as handling encryption within the app.

2) Session Layer

- Manage Synchronization, checkpointing, and recovery of data exchange. It helps maintain sessions in long-running data transfers by managing connections and re-establishing them if they are disrupted
- In Internet stack: This layer is missing. Apps requiring session managment (e.g. real-time collaboration tools) have to handle this themselves, often using protocols within the application layer

These 2 Layers are added for data security purpose

- Difference Between Internet Protocol Stack and ISO reference model

- They have 5 layers in common (Application, Transport, Network, Link, Physical)
- 2 extra layer are added to the ISO model between the Application and Transport layers, wich are (presentation and session)
- These 2 added layers are security

↳ Summary

. Application Layer: Initiates a request or accepts a request
. Presentation Layer: Adds formatting, display and encryption information to the packet
. Session Layer: Adds traffic flow information to determine when the packet gets sent
. Transport Layer: Adds error-handling informationerver
. Network Layer: Sequencing and address info and is added to the packet
. Data-link Layer: Adds error-checking information and prepares data for going on to the physical connection
. Physical Layer: Packet sent as a bit stream

↳ Information formats in layers.

. Frame: information unit at the data link layer
. Packet: information unit at the network layer
. Datagram: information at the transport layer that use connectionless network service
. Segment: information unit at the transport layer
. Message: information unit at the application layer
. Cell / bit: information unit of a fix size at the data link layer. Cells are used in swilched environments.

V- Network Security

Types of Attacks on Internet Infrastructure

1) Infecting / Attacking Hosts

- Methods:
  - Malware (malicious software)
  - Spyware (software that secretly gathers user information)
  - Worms (self-replicating malicious programs)
- Goals:
  - Steal Data
  - Access user accounts without permission

2) Denial of Service (DoS)

- Objective: Prevent access to resources
- Targets: Servers, Link bandwidth (network connections)

Challenges in Internet security

- Original Internet Design
  - Build with limited security in mind
  - Assumed a network of trusted users in a transparent system
- Modern Reality
  - Internet Protocol developers now addressing security issues as they arise ("playing catch-up")

Security Across Layers

↳ Security measures must be integrated at all levels of the network stack

↳ What Can Attackers Do with Malware?

1) Spyware

- Dowloading a webpage containing spyware
  - ↳ Records sensitive data, like keystores and visited websites
  - ↳ Sends collected information to a remote server

2) Worm

- Passively receives an object that automatically executes itself
  - ↳ Propagates to other hosts and users without user interaction

3) Virus

- Receiving and opening an infected object (e.g. email attachment)
  - ↳ Actively executed by the user
  - ↳ Spreads to other hosts and users

↳ Denial of Service (DoS) Attacks

. Goal: Make resources (e.g. servers, bandwidth) unavailable to legitimate (legal) users by overwhelming them with fake (bogus) traffic.

. Steps in DoS Attack:

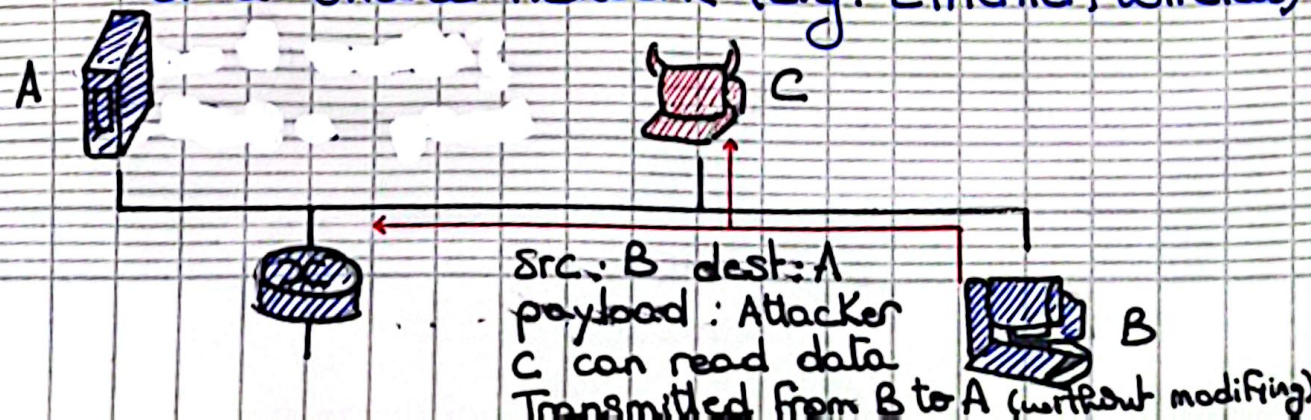
1) Select Target: Identify the resource to disrupt
2) Compromise Hosts: Use malware (like viruses, worms, or spyware) to break into multiple devices across the network and gain control
3) Launch Attack: Use the compromised devices (now part of a botnet) to send a large volume of packets to the target, overwhelming its resources and denying access to legitimate traffic

↳ Network Attacks: Sniffing, Modifying, Deleting Packets

1) Packet Sniffing

. What it does?

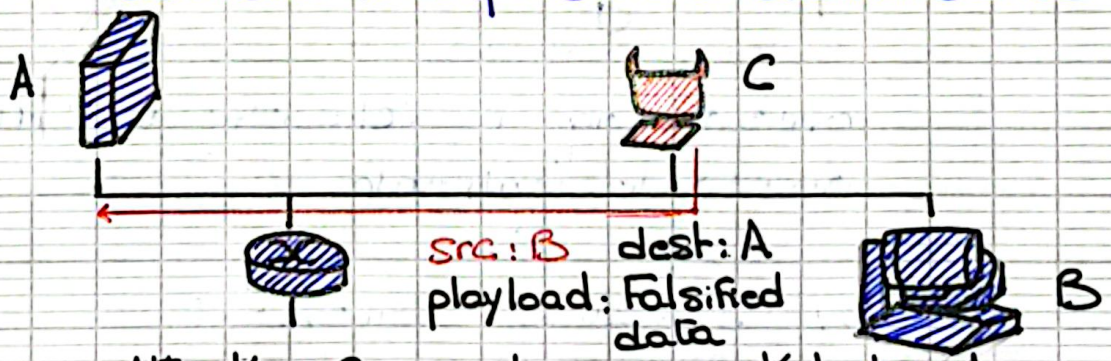
↳ Captures and reads all data packets on a shared network (e.g. Ethernet, wireless)



. How It Works?
  ↳ Uses a promiscuous network interface to read packets not intended for the attacker.
  ↳ Can capture sensitive data like passwords

. Example Tool:
  ↳ Ethereal/Wireshark: A free packet-sniffing software

2) IP Spoofing (Masquerading as a User)
. What it does?
  Sends packets with a false source address to impersonate another device

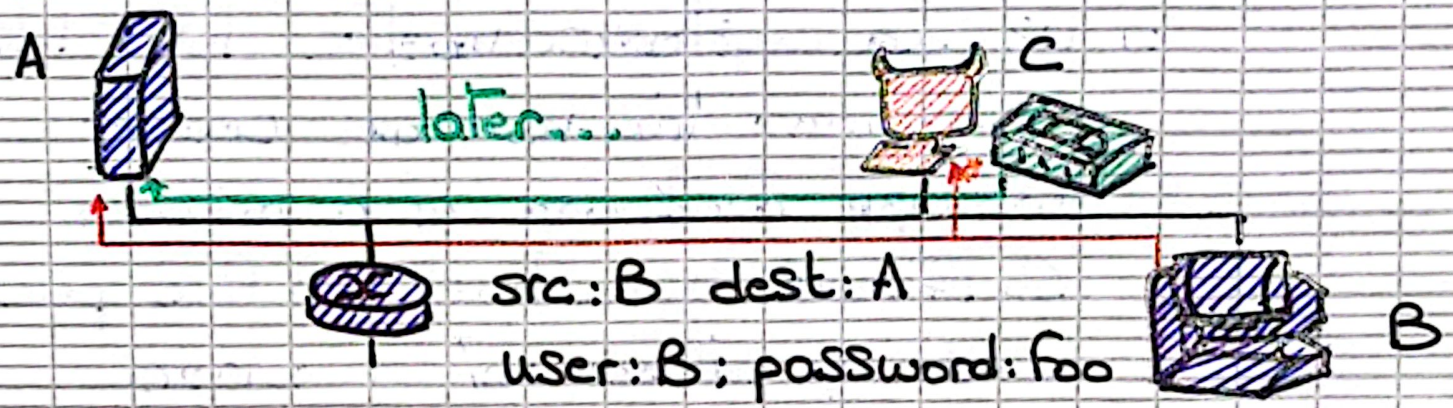


  ↳ Attacker C sends a packet to A prendending to be from B

3) Record-and-Replay (Replay Allack)
. What It does?
  ↳ Captures sensitive information (e.g. usernames and passwords) using packet sniffing.
  ↳ Reuses the data later to impersonate the legitimate user.

. System Behaviour :

The system authenlicates the attacker as the original user because it sees valid credentials



- Attacker C captures a packet from B to A with password and user
  Later, C reuse these credenlial to access A predenling to be B