CS Revision Lecture 1, 2

- ## Lecture 1 - Introduction
  - ### Goal of the course
    - Identify **security, privacy and trust issues** in various aspect of computing, such as
      - programs
      - Operating Systems
      - Networks
      - Distributed systems
      - Internet applications
    - The ability to **critically read and digest the key elements** of research papers in the field
    - The awareness of how **security, privacy and trust** can be achieved in practice
  - ### Who is We?
    - Ordinary Citizen
    - Whistle blower
    - Corporate worker
    - Dissident activist
    - Secret agent
  - ### What is Security?
    - The main general properties are:
      - **Confidentiality**
        - Information access to only **authorized(authenticity)** entities
      - **Integrity**
        - The data is **untampered** and **uncorrupted**

- **Availability**
  - Both the data and the system that provides **access** to it are there **when you need** them

- What is Privacy?
  - Concerns **individuals** and their **expectations** on how their data, behaviour and interactions are recorded, utilized and spread.
  - A useful definition: "**Information self-determination**"
    - A **person** gets **control** information about **themselves**.
    - Controls can include:
      - **Who** gets to **see** it
      - **Who** gets to **use** it
      - **What** they can **use** it for
      - **Who** they can **give** it to

- What is Trust?
  - We trust when we have:
    - **Assurance**
      - The **means to know** that the system is secure
    - **Reliability/Resilience**
      - To **operate intact** in the face of natural disasters and human-launched attacks
    - **Accountability**
      - The **means to verify** that the system is operating as designed (i.e. securely)
    - NB: There is a difference between trustworthy and trusted

- Who are Adversaries?
  - All systems are vulnerable to all matter of threats

- Adversary types:
  - Nature
  - Script Kiddies
  - Crackers/Hackers
  - Organised Crime
  - Governments
  - Terrorists

- Thread Modeling
  - **Who** is the adversary (the system may protect against many types)?
  - **What** are they allowed to do? Or, what can't we prevent them from doing?
    - The adversary need not be malicious, he/she could be merely curious
  - **What** do we want to prevent the adversary from doing or learning?
    - What is the adversary's aim? Or, what does he/she win?
  - The set of threats we want to protect against given this(set of) adversaries
    - What do we win?
    - What does the adversary win?
  - Terminology
    - **Assets**: **Things we want to protect**, like:
      - Hardware
      - Software
      - Information
    - **Vulnerabilities: Weaknesses in a system that may be exploited**

- Example: Public facing email server without spam protection
- **Threats**:
  - **Loss or damage to the system, its users or operators**
    - E.g. Proprietary source code being stolen and sold
  - The six major categories of threats:
    - Interception
    - Interruption
    - Modification
    - Fabrication
    - Repudiation
    - Epistemic
- **Attack: An action that exploits a vulnerability to carry out a threat**
  - E.g. Hacking the company public facing email server to read emails to steal company trade-secrets
- **Controls:**
  - **Mitigating or removing a vulnerability**
  - The control mitigates a vulnerability to prevent an attack and that defends against a threat
  - No system is perfect: Control vulnerabilities when discovered
- Security Principles
  - Economy of mechanism: easy to understand, verify and maintain
  - Fail-safe defaults: conservative permission and functionality
  - Complete mediation: every access should be checked (again)
  - Open design: no security by obscurity

- Separation of privilege: cooperation required to act, no single point of failure
- Least privilege: programs and users on bare minimum of access
- Least common mechanism: minimize shared means of access to resources
- Psychological acceptability: well designed UI that are intuitive and clear
- Work factor: compare effort for the value of the resource
- Compromise recording: record failures and breaches

- Common defence methods
  - There are 5 common defence patterns:
    - Prevent
    - Deter
    - Deflect
    - Detect
    - Recover
    - NB: Not all attacks can be prevented!
  - Best practice to employ some form of all to get "defence in depth"
- Trade-offs
  - Can we have secure, privacy-friendly and trustworthy (SecPrivTru) systems? **NO!**
    - Privacy means potentially hiding information; The system can not assure to be safe when it does not know all the data?
  - SecPrivTru vs. Cost
    - There is a cost to operate more secure systems
    - Are the assets worth the effort?
    - Non-technical solutions (e.g. insurance)

- SecPrivTru vs. Performance
  - There is an overhead to gain SecPrivTru properties
  - How much performance degradation can we tolerate?
  - What properties do we really need?
- How secure, private, trusted should it be?
  - Weakest link
    - An adversary will attack the most vulnerable part of the system, not the one that is the easiest for you to defend
    - Requires thinking like an attacker
    - Attack trees and threat modeling can be useful tools
  - Cost-benefit analysis
    - Economic incentives
    - Do not spend more on protecting an asset than it is worth
      - What about users privacy?
- Defence tools of the trade
  - Protect assets that can be
    - Hardware, software, data (PII, social graph, confidential information, etc.)
  - Many form of control
    - **Cryptography**
      - Protects the data, making it unreadable by anyone without keys
      - Authenticating users with digital signatures
      - Authenticating transactions with cryptographic protocols
      - Ensures the integrity of data against unauthorized modification
    - **Software controls**
      - Passwords

        - Sandboxes
        - Virus scanners
        - Source code versioning systems
        - Software Firewalls
        - Privacy enhancing technologies (PETs)
    - **Hardware controls**
        - Fingerprint readers
        - Smart tokens
        - Firewalls
        - Intrusion detection systems
    - **Physical controls**
        - Protecting against unauthorized physical access to hardware
        - Locks
        - Guards
        - Off-site backups
        - Not placing critical systems in natural disaster zones
    - **Policies and procedures**
        - Non-technical means to protect against some type of attacks
        - Disallow personal hotspot within work place
        - Password rules
        - Security training against social engineering attacks
- Recap
    - What is our goal in this course?
        - Identify security and privacy issues

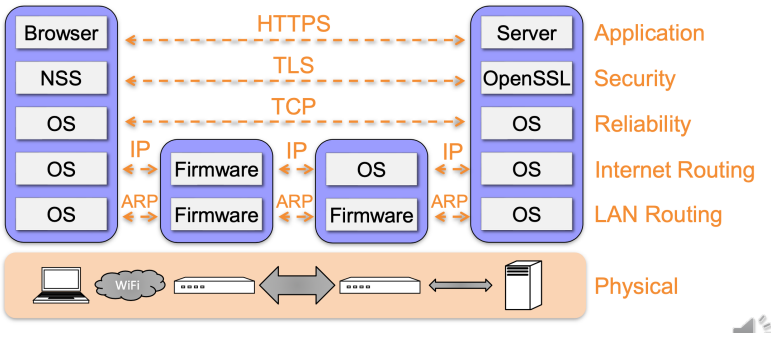
- Design systems that are more protective of security and privacy
- What is Security?
  - Confidentiality, Integrity, Availability, Authenticity
- What is Privacy?
  - Informational self-determination
- What is Trust?
  - Assurance, Reliability/Resilience, Accountability
- Who are the adversaries?
  - Threat modeling
  - Learn to think like an attacker
- Trade-offs
  - Security, Privacy, Performance, Cost
- Assets, vulnerabilities, threats, attacks and controls
  - You control a vulnerability to prevent an attack and block a threat
- Methods of defence
  - Cryptography, software controls, hardware controls, physical controls, policies and procedures

Lecture 2 - Network security: Networking Principles

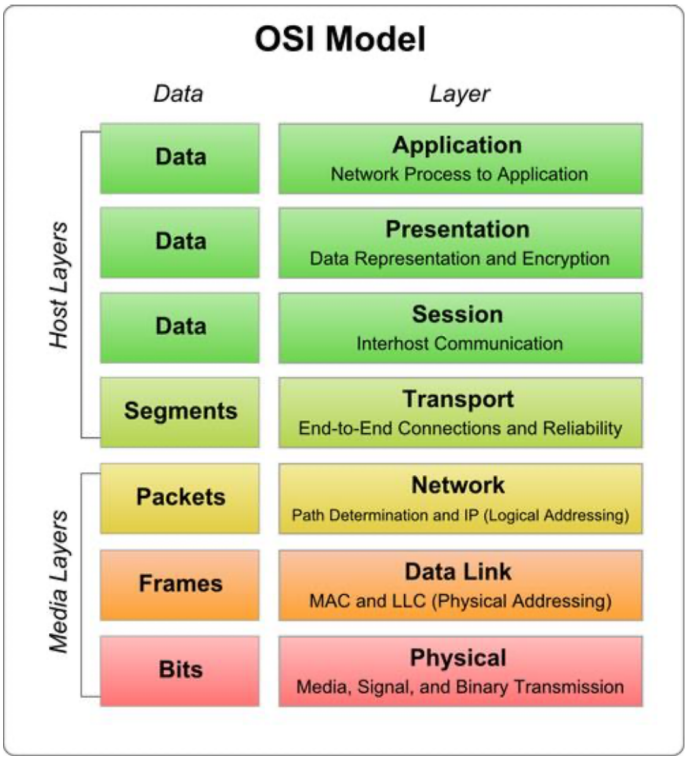
Network Communication

- Communication in modern networks is characterised by the following fundamental principles
  - Packet switching
    - Data splits into **packets**
    - Each packet is
      - Transported **independently** through network
      - Handled on a **best efforts** basis by each device

- Packets may
  - Follow different routes between the same endpoints
  - Be dropped by an intermediate device and never delivered
- Stack of layers
  - Network communication models use a stack of layers
    - Higher layers use services of lower layers
    - Physical channel at the bottommost layer
  - A network device implements several layers
  - A communication channel between two devices is established for each layer
    - Actual channel at the bottom layer
    - Virtual channel at the higher layers
  - Internet Stack (simplified)

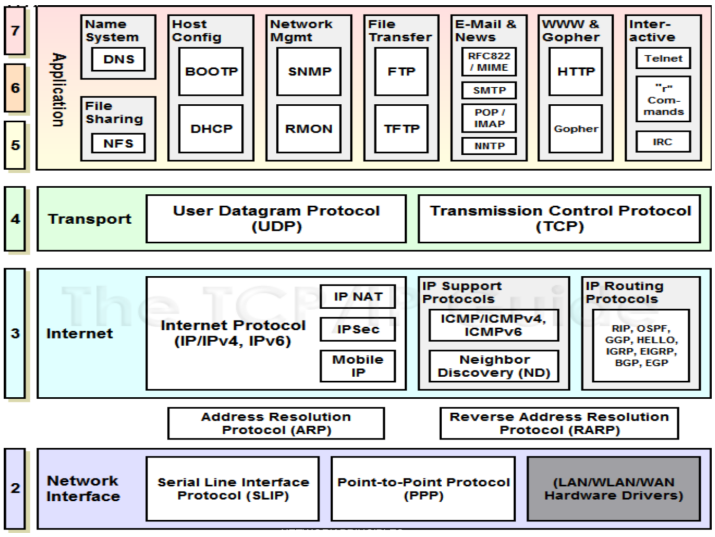


  - The OSI model



- The **OSI** (Open System Interconnect) ReferenceModel is a network model consisting of **seven** layers
- Created in 1983, OSI is promoted by theInternational StandardOrganization (ISO)

- TCP/IP Model Mapped onto OSI

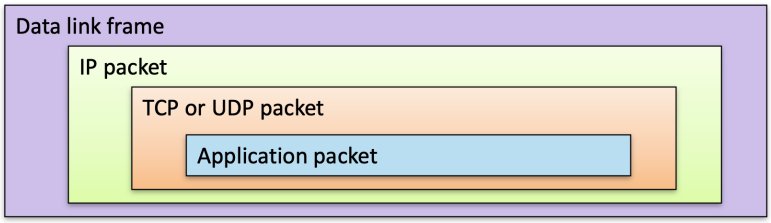


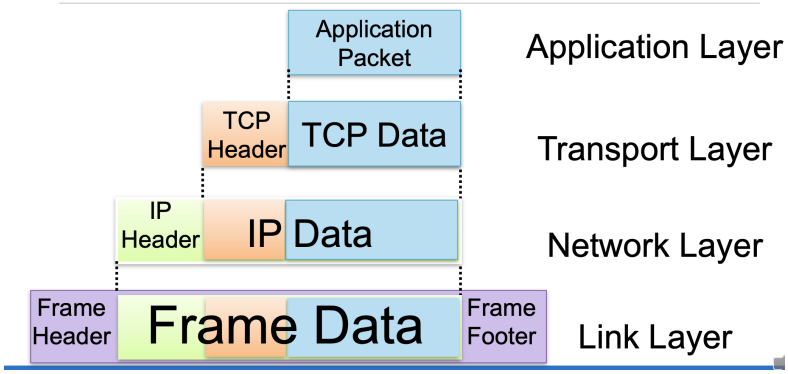
- Encapsulation

- A packet typically consists of
  - Control information: **header** and **footer**
  - Data: **payload**

- A protocol P uses the services of another protocol Q through **encapsulation**

  - A packet p of P is encapsulated into a packet q of Q
  - The payload of q is p
  - The control information of q is derived from that of p
- Internet Packet Encapsulation



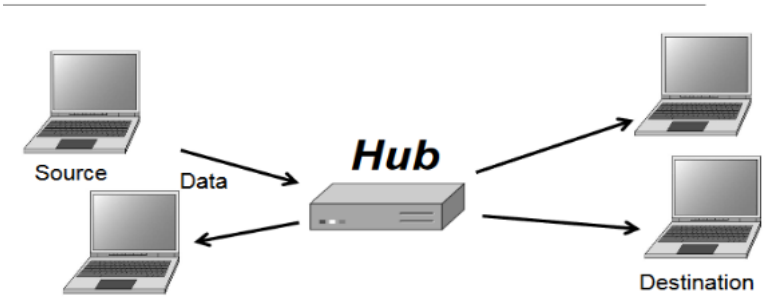


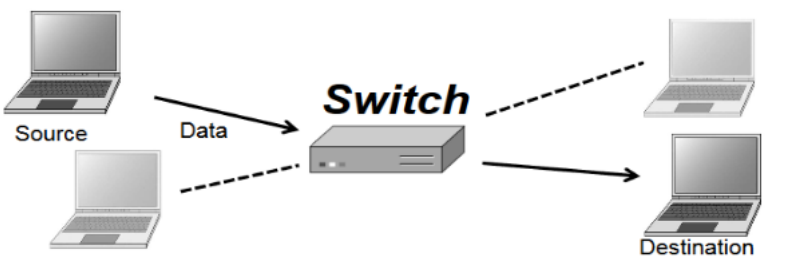
  - Application Layer >> Transport Layer >> Network Layer >> Link Layer

- Network Interfaces
  - device connecting a device to a network
    - Ethernet card
    - Wifi adapter
    - DSL modem
  - A computer may have multiple network interfaces
  - Packets transmitted between network interfaces

- Most local area networks, (including Ethernet and WiFi) broadcast frames

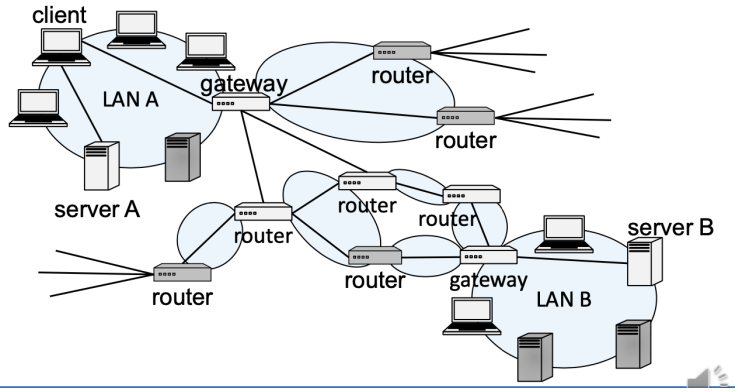
- Media Access Control (MAC) Addresses
  - Most network interfaces come with a predefined MAC address
  - A MAC address is a 48-bit number usually represented in hex
    - E.g., 00-1A-92-D4-BF-86
  - The first three octets of any MAC address are IEEE-assigned Organizationally Unique Identifiers
  - The next three can be assigned by organizations as they please, with uniqueness being the only constraint
- Switch
  - A switch perform **routing** in a **local area network**
    - Operates at the link layer
    - Has multiple interfaces, each connected to a computer/segment
  - Operation of a switch



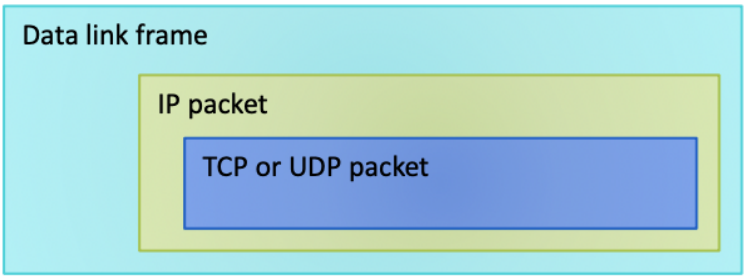


- Learn the MAC address of each computer connected to it
- Forward frames only to the destination computer

- Hub
  - Forward frames to all computer
- Combining Switches
  - Switches can be arranged into a **tree**
  - Each forwards frames for the MAC addresses of the machines in the segments (subtrees) connected to it\
  - Frames to unknown MAC addresses are **broadcast**
  - Frames to MAC addresses in the **same segment** as the sender are **ignored**
- The internet



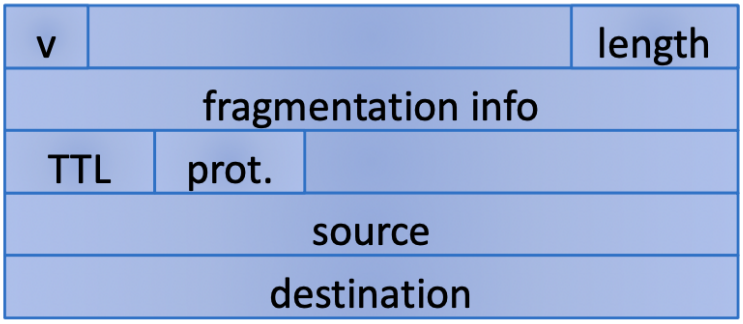
- Internet Protocols(IP) Functions



- **Addressing**:
  - In order to delivery data, IP needs to be aware of where to deliver data to, and hence includes addressing systems

- **Routing**:
  - IP might be required to communicate across networks, and communicate with networks not directly connected to the current network
- **Fragmentation and Reassembly**:
  - IP packets are carried across networks which may have **different maximum packet length**

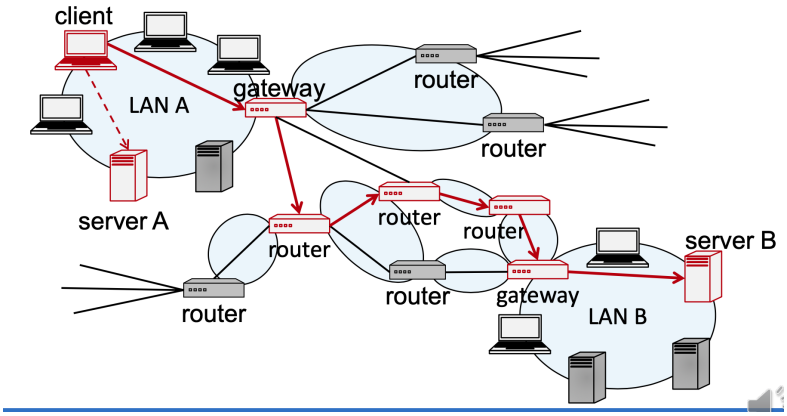
- IP Addresses and Packets
  - IP Addresses
    - IPV4: 32bit 4 * 8
    - IPV6: 128bit 8 * 16
  - Address subdivided into network, subnet, and host
    - E.g., 128.148.32.110
  - Broadcast addresses
    - E.g., 128.148.32.255
  - Private networks
    - not routed outside of a LAN
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
  - IP header includes



    - Source address
    - Destination address

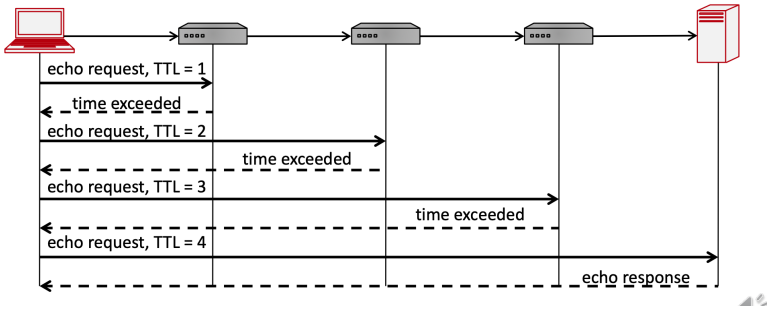
- Packet length (up to 64KB)
- Time to live (up to 255)
- IP protocol version
- Fragmentation information
- Transport layer protocol information (e.g., TCP)

- IP Routing
  - A router bridges two or more networks
    - Operates at the network layer
    - Maintains tables to forward packets to the appropriate network
    - Forwarding decisions based solely on the destination address
  - Routing table
    - Maps ranges of addresses to LANs or other gateway routers
  - Routing Example

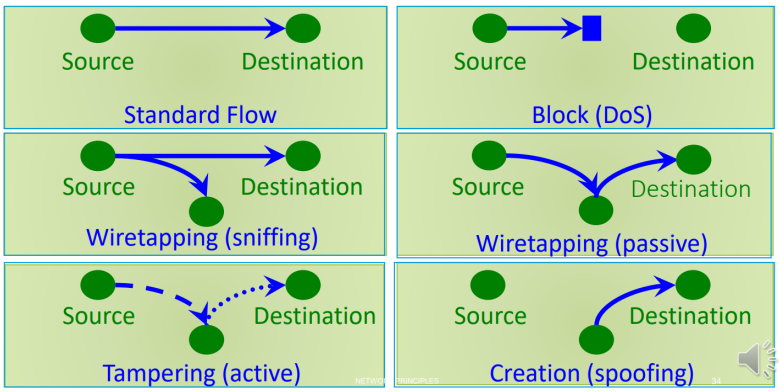


- Exploring Internet Routes
  - Internet Control Message Protocol (ICMP)
    - Used for network testing and debugging
    - Simple messages encapsulated in single IP packets
    - Considered a network layer protocol
  - Tools based on ICMP

- **Ping**: sends series of echo request messages and provides statistics on roundtrip times and packet loss
- **Traceroute**: sends series ICMP packets with increasing TTL value to discover routes



- Network Attack



- Wireshark
  - Packet sniffer and protocol analyzer
  - Captures and displays network packets for analysis
  - Supports plugins
  - Usually requires administrator privileges because of security risks associated with the program
  - When run in promiscuous mode, captures traffic across the network
- What we have learned
  - Networking principles
    - Packet switching
    - Stack of layers
    - Encapsulation

- Network interfaces, MAC Addresses and Switches
- Internet Protocol (IP) Routing, autonomous systems
- Types of network attacks
- Traceroute and Wireshark tool

以上内容整理于 幕布文档