COMP 3704 Computer Security

Christian Grothoff
christian@grothoff.org

http://grothoff.org/christian/

TCP/IP Layers

1. Physical Network (Ethernet, PPP, ...)
2. Internet (ARP, IP, ICMP, ...)
3. Transport (UDP, TCP)
4. Application (DNS, HTTP, SMTP, SSH, ...)

Internet Security

- Original design neglected security
- Some security features are in TCP
- Most security on application level
- Many crucial applications are still lacking (SMTP, DNS)

Ethernet

- Best-effort delivery (unreliable)
- Each machine identified using "unique" 48-bit MAC address
- ARP protocol used to discover mapping of MAC address to IP
- Some hardware can lie about MAC addresses
- ARP can lie about mapping of MAC to IP addresses

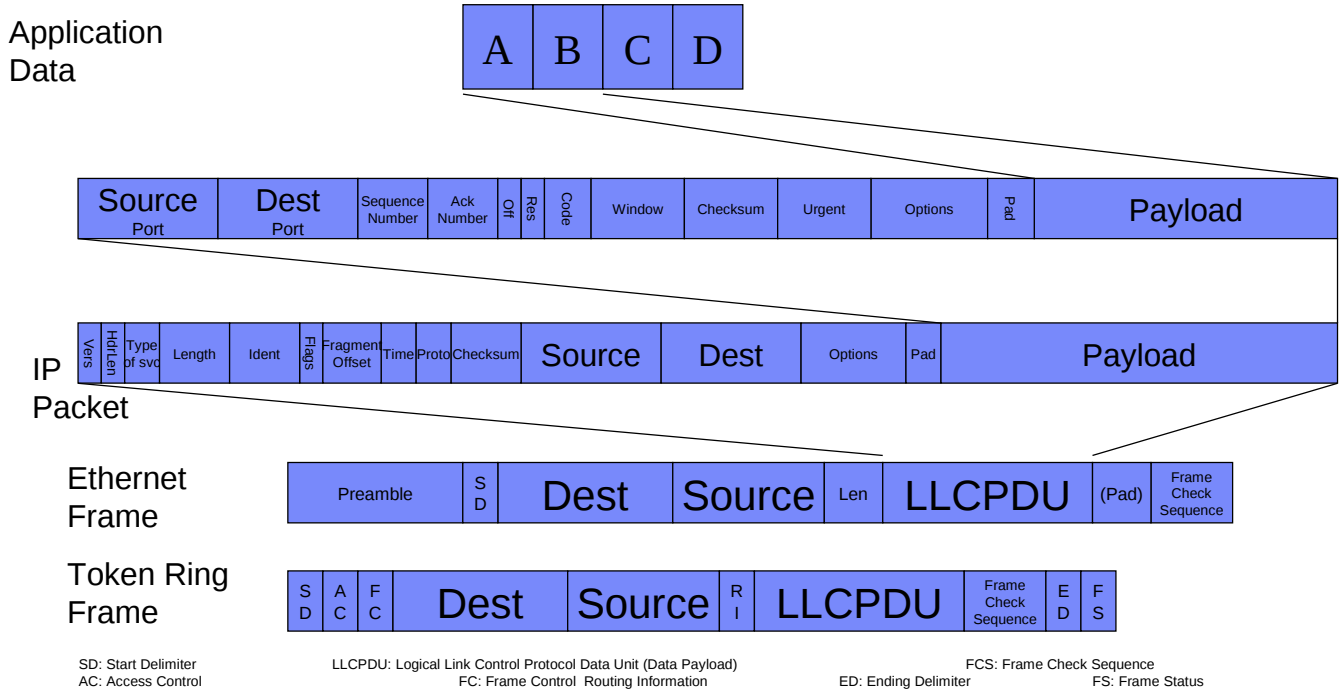
Packet Sniffing

- Many physical transports allow listening in (Ethernet, WiFi)
- Hardware in **promiscuous mode** captures all traffic, not only traffic destined for the device
- Eve is hard to detect...

IP – the Internet Protocol

<table>
<tr><td>Version</td><td>HDL</td><td>ToS</td><td colspan="2">Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>T. Protocol</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Options (optional)</td></tr>
<tr><td colspan="5">Data (Length–HDL bytes)</td></tr>
</table>

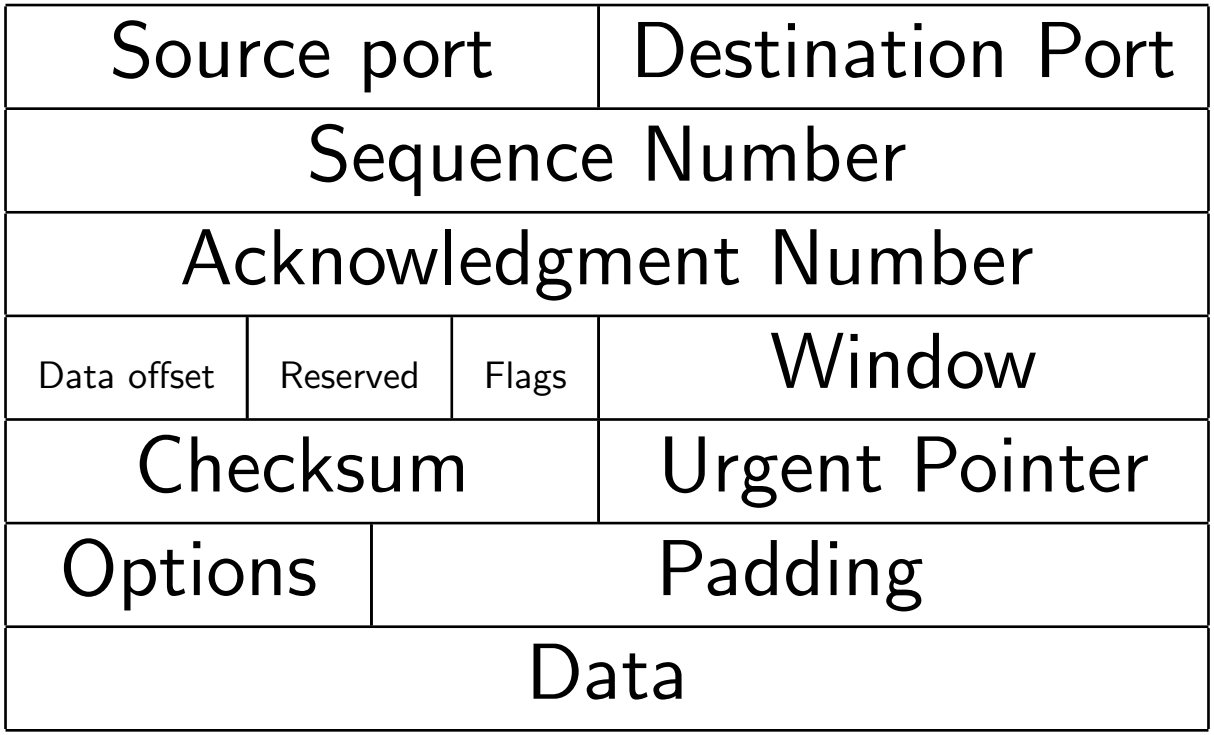
Encapsulation



Ports

- Used to identify desired application-level service
- There are 65535, lowest 1024 reserved for `root`
- Ports > 32000 are usually used by the clients
- Only used for TCP and UDP transports
- `/etc/services` lists well-known ports

TCP – the Transmission Control Protocol



Firewalls

- Filters network traffic (drop)
- Some firewalls integrate logging, prioritizing and on-the-fly traffic modifications
- Firewall administrator specifies rules (`ipchains`)
- Rules can be positive (`accept`) or negative (`drop`)
- Default (no rule matches) should be `drop`

Stateless Firewalls

- High-performance, scalable, easy to implement
- Granularity of rules is determined by physical layer (frames)
- IP-level frames include IPs and TCP/UDP ports of sender and receiver
- Stateless firewalls are *application agnostic*

Stateful Firewalls

- Slow, complex, not scalable, difficult to configure
- Integrate knowledge about application-level protocols
- Possibilities include knowledge of TCP sequence numbers and connection handshakes to inspection of FTP connection management and HTTP cookie values
- Security depending on stateful inspection is most likely flawed

Network Address Translation (NAT)

- Initially designed to share IPs between multiple computers
- NAT replaces source IP with NAT IP address
- NAT can also map ports
- Inbound traffic is mapped back to LAN IP based on port (and possibly context)
- Traffic to unmapped ports is dropped $\Rightarrow$ stateful firewall!
- Many design variants, some cause problems with legitimate traffic

TCP Wrappers

- Wrapper listens on port, not the real application
- Wrapper performs security checks (source IP)
- Wrapper spawns actual application and hands of connection
- Rarely used today, replaced by firewalls and checks integrated into application
- Still useful if application uses lots of memory and is rarely needed

Restricted `bind`

- `bind` allows application to restrict IP range
- Most common restriction is `localhost`
- Can only specify simple address or address family

$\Rightarrow$ Firewalls are more flexible

- Can apply additional checks upon `accept`

ICMP

- Used to establish if machine is reachable (`ping`) and to signal network problems
- Can be used to establish network distance (`traceroute`)
- ICMP messages contain arbitrary data that is echoed back
- Some ICMP messages can be used to change network configurations

$\Rightarrow$ Firewalls usually filter those, modern OSes rarely support those ICMP messages

DNS

- Uses TCP or UDP
- Can lookup IP for hostname, hostname for IP or specific services for a particular domain (MX)
- Local DNS servers delegate requests to parent DNS servers
- Still not encrypted, signed or verified (DNSSEC replacement should help)
- Traditionally ASCII only, UNICODE extensions are risky!

IPsec

- Encryption (asymmetric + symmetric) of TCP/IP traffic
- Performed at the level of the operating system
- IPsec configuration specifies key for each IP address
- Usually used for secure Intranet routed via global Internet
- PKI issues limit it to individual organizations

SSH Tunneling

- SSH allows confidential and encrypted communication
- `ssh -L` and `ssh -R` options allow tunneling of **any** TCP-traffic through `ssh`
- Must be enabled by administrator
- Poses little security risk – user needs to already local access!

SMTP

- DNS MX record determines mail server
- Backup mail servers can be specified (MX priority)
- Mail servers relay mail down MX-specified chain
- Sender is not validated, anyone can use any username
- No authorization required for inbound e-mail
- Mail servers confirm receipt, no mail gets lost...

POP3/IMAP/IMAPS

- Used to retrieve e-mail from server
- Independent of SMTP
- Authentication generally required
- Password often transmitted in cleartext

TELNET

- Traditionally used for remote login
- Everything in plaintext $\Rightarrow$ security risk!
- Can be used to establish TCP connection to any port
- Useful for network diagnosis and as a replacement for HTTP/SMTP/POP3 clients...

NTP

- Used to synchronize time
- Important to use to avoid time-based attacks
- NTP does **not** use cryptography

NETBIOS

- Microsoft protocol
- Allows users to share printers
- ... and all of their other data
- ... often without them knowing it is enabled

Peer-to-Peer Networking

- The Internet is a peer-to-peer system (on the IP level)
- Evil because the lack of centralization means it is hard to control
- Most Peer-to-Peer systems have a default port
- ... but they can easily use any port!
- NAT is a major problem since NAT often blocks all inbound traffic

Essential Tools

- traceroute
- nmap
- wireshark
- tcpdump
- iptraf

Questions

?

Problem

You're working for LMCO. Your company does not allow any inbound traffic, but you are allowed to surf the web (outbound http only). How can you allow your friend in China to freely access the LMCO Intranet (say to download the war "plans")?

Assume that your job keeps you too busy to hunt for the data yourself, your friend needs to be able to interactively browse (after all, he is paying well).

Problem

Is spam a social or a technical problem?

Who can solve the problem? How?