Computer Security (COM-301)

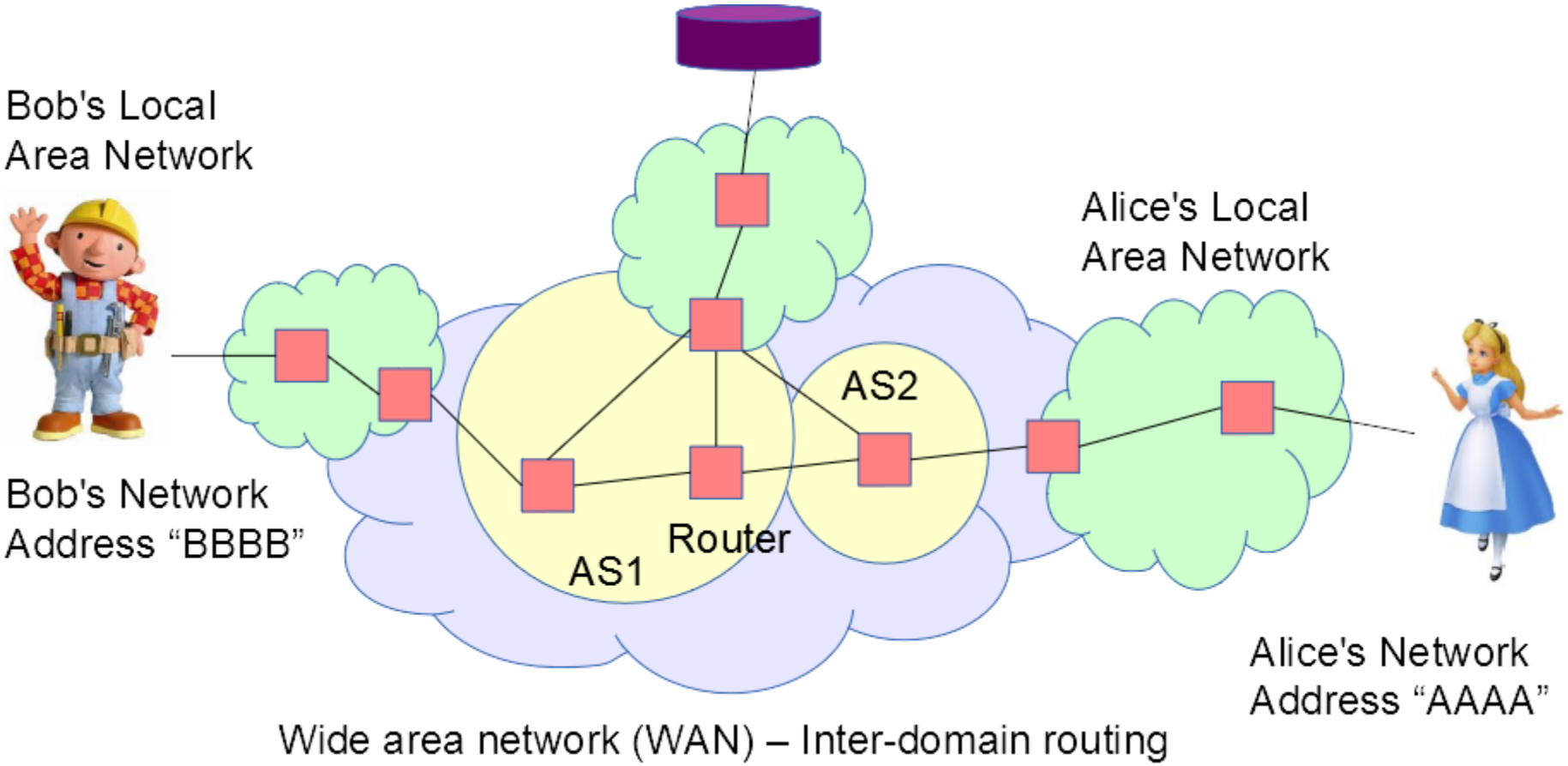
Network security

Slides from Carmela Troncoso
Some slides/ideas adapted from: George Danezis

Up to here: attacks on hosts
What about the network?

Up to here: attacks on hosts
What about the network?

The network is not a tube!!!



Desired properties

Confidentiality, Integrity, Availability, Authentication, Authorization?

Naming security: The association between lower level names (eg. network addresses) and higher level names (e.g. Alice / Bob) must not be influenced by the adversary
Routing security: The route over the network and the eventual delivery of messages must not be influenced by the adversary
Session security: Messages within the same session, cannot be modified (keep ordering and no adding/removing messages)
Content security: The content of the messages must not be readable or influenced by adversaries

Desired properties

Confidentiality, Integrity, Availability, Authentication, Authorization?

Naming security: The association between lower level names (eg. network addresses) and higher level names (e.g. Alice / Bob) must not be influenced by the adversary	**Integrity** **Authentication** **Availability (naming service)**
Routing security: The route over the network and the eventual delivery of messages must not be influenced by the adversary	**Integrity** **Authentication** **Availability** **Authorization**
Session security: Messages within the same session, cannot be modified (keep ordering and no adding/removing messages)	**Integrity** **Authentication**
Content security: The content of the messages must not be readable or influenced by adversaries	**Confidentiality** **Integrity**

Network security in COM-301

- Do deployed network protocols provide the desired properties?
  - Naming security
  - Routing security
  - Session security
  - Content security
- What are the existing solutions to improve network security?

Where are the problems?

In this lecture security issues on…

We will not see UDP, similar concepts, but differences in the implementation

Application	Web, Bittorrent, SMTP/POP/IMAP, XMPP/IRC, VoIP
Presentation	
Session	(SSL, TLS)
Transport	Transmission Control Protocol (TCP) UDP
Network	Internet Protocol (IP) (Naming and routing: DNS, BGP)
Datalink	IEEE802.3 (Ethernet) (Naming & routing ARP)
Physical	Modulation & coding …

Open Systems Interconnection (OSI) Model '94

Computer Security (COM-301)

Network security

ARP Spoofing

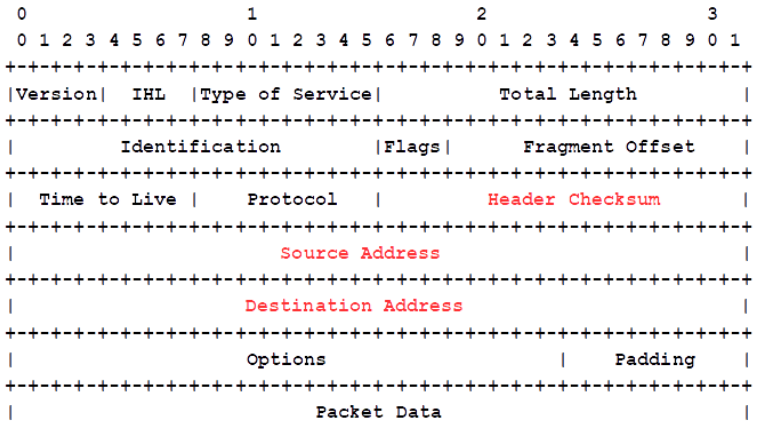
Slides: Carmela Troncoso
Some slides/ideas adapted from: George Danezis

Routing: routing IP on an Ethernet LAN

Refresher

- **Ethernet:**
  - Local area network (LAN) technology
  - Machines have a “unique” 48 bit MAC address (Medium Access Code)

- **Internet Protocol (IP)** on the LAN
  - Hosts communicate using the IP protocol
  - Each machine has an IP address (4 bytes in IPv4).
    - Part of the address denotes the network and part the host



Example Internet Datagram Header

RFC791 “INTERNET PROTOCOL” http://www.ietf.org/rfc/rfc791.txt

Routing: routing IP on an Ethernet LAN

Refresher

How does IP routing work?

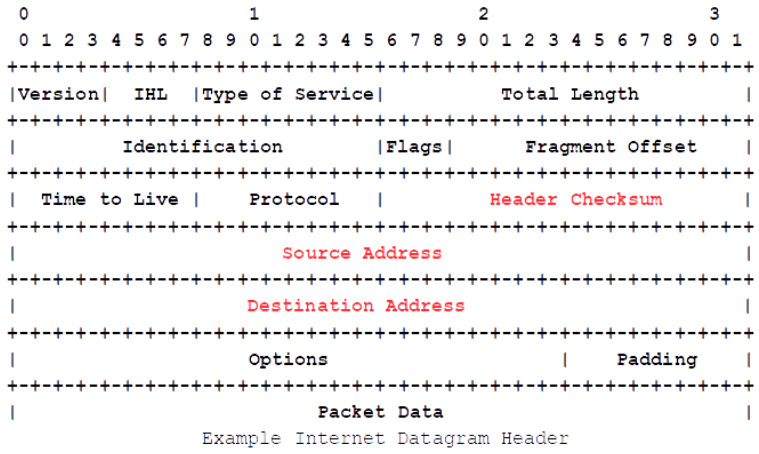
- Alice needs:
  - Her own IP address (eg. 192.128.5.130)
  - Bob's IP address (eg. 192.128.5.125)
  - Her “subnet mask” (eg. 255.255.255.0)
  - Her “gateway” (eg. 192.128.5.1)

- Option 1: Alice and Bob are on the same subnet
  - Address Alice AND mask = Address Bob AND mask
  - Route through the LAN

- Option 2: they are on different subnets
  - Send to gateway
  - Route through the WAN (Wide Area Network)

Alice

Send this packet from address 192.128.5.130 to 192.128.5.125



Example Internet Datagram Header

Routing: routing IP on an Ethernet LAN

Refresher

How does IP routing work?

and inside the LAN?

- Alice does not (want to) know network details
- Alice does not know Bob's MAC address

Alice

Send this packet from address 192.128.5.130 to 192.128.5.125

How can she learn about Bob's MAC?

ARP: "translation" between IP address and MAC address

- Each host maintains a cached table of IP ↔ MAC mappings
- If not available: broadcast an ARP request to query for target IP
- An ARP reply responds with the MAC address for that IP

```
*-----------------------*
| HTYPE (2 bytes)       |
| PTYPE (2 bytes)       |
| HLEN (1)    | PLEN (1)|
| OPERATION (2)         |
| Sender HA (HLEN)      |
| Sender PA (PLEN)      |
| Target HA (HLEN)      |
| Target PA (PLEN)      |
*-----------------------*
```

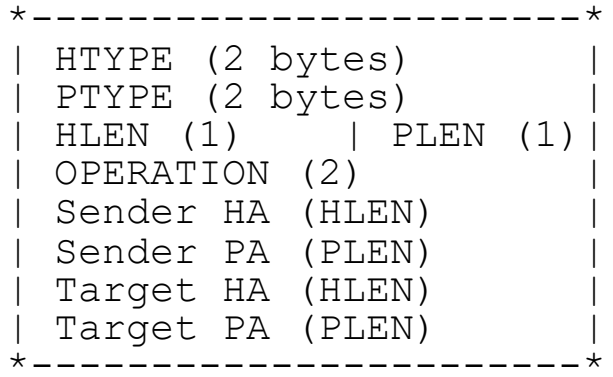
Routing: routing IP on an Ethernet LAN

Naming security: The association between lower level names (eg. network addresses) and higher level names (e.g. Alice / Bob) must not be influenced by the adversary

Integrity
Authentication

Does ARP provide naming security?

ARP: “translation” between IP address and MAC address
- Each host maintains a cached table of IP ↔ MAC mappings
- If not available: broadcast an ARP request to query for target IP
- An ARP reply responds with the MAC address for that IP



No Integrity check, nor Authentication

ARP spoofing

If nobody checks…

You can impersonate! (provide the identity of others)

What can you achieve?

- Just impersonation is bad

- Man in the middle: provide two hosts (sender/receiver) with your MAC address

- Monitor communication or tamper with it

- **Abuse resource allocation**

- **Denial of Service**: avoid that packets arrive to one host

Also bad for

Routing security: The route over the network and the eventual delivery of messages must not be influenced by the adversary	**Integrity** **Authentication** **Availability** **Authorization**

ARP spoofing

If nobody checks…

You ca

What can you a

- Just in

- Man i

address

- **Abuse resource allocation**

- **Denial of Service**: avoid that packets arrive to one host

The same happens in DNS, IP, Ethernet,…
No network protocol was (initially) designed with security in mind!

BECAUSE OF A VERY NAÏVE THREAT MODEL:
outsiders are bad, insiders behave, trust them!

Also bad for

Routing security: The route over the network and the eventual delivery of messages must not be influenced by the adversary	**Integrity** **Authentication** **Availability** **Authorization**

ARP spoofing - Defenses

- Use of static, read-only entries for critical services in the ARP cache of a host

- Use ARP spoofing detection and prevention software
    - check if one IP has more than one MAC or one MAC reported by multiple IPs
    - certify requests by cross-checking
    - sends email if IP-MAC association change

Separation of privilege: force the adversary to gain control of more entities

Computer Security (COM-301)

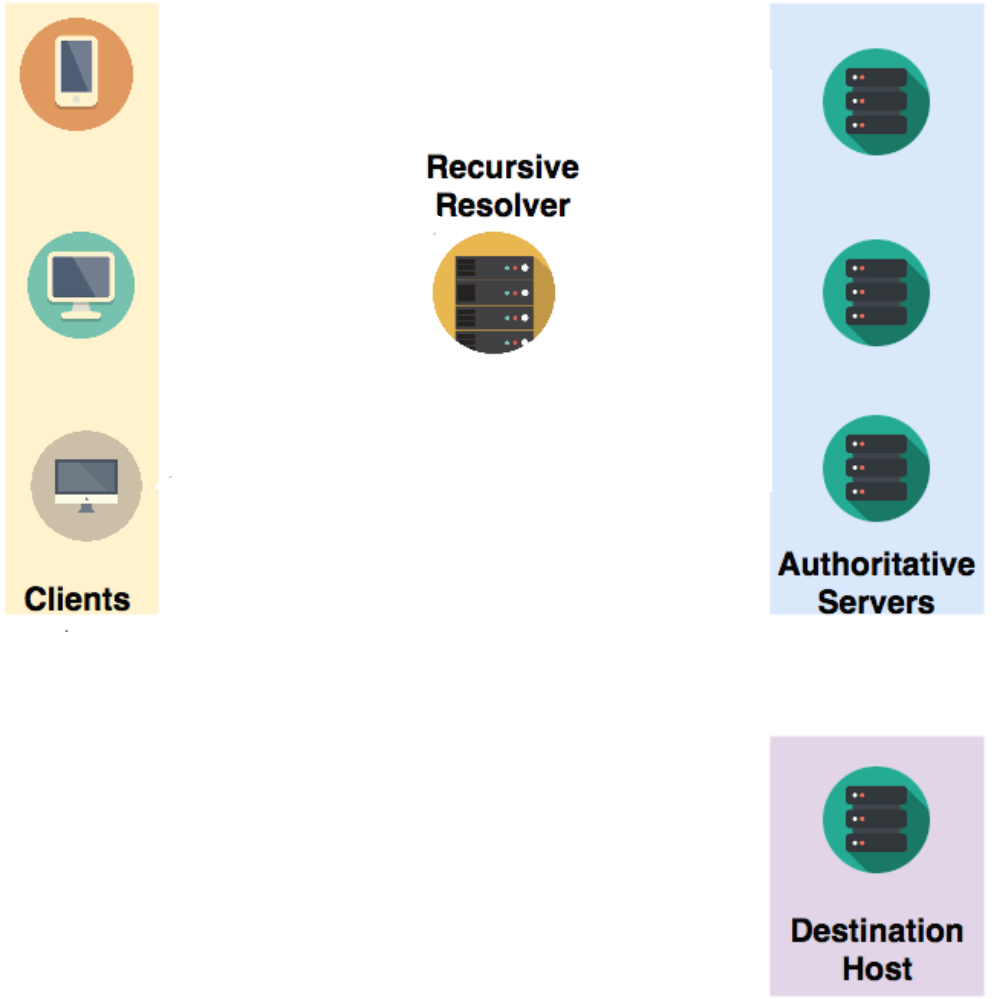
Network security

DNS Spoofing

Slides from Carmela Troncoso
Some slides/ideas adapted from: George Danezis

Domain Name Service (DNS)

Refresher



DNS spoofing – Attacks

Cache poisoning: corrupt the DNS resolver with fake pairs (IP,domain)

DNS Hijacking: corrupt the DNS responses (man in the middle) with fake pairs

https://www.cloudflare.com/learning/dns/dns-cache-poisoning/

DNS spoofing – Attacks

DNS Spoofing

Cache poisoning: corrupt the DNS resolver with fake pairs (IP,domain)

DNS Hijacking: corrupt the DNS responses with fake pairs

What can you achieve?

- **Denial of Service**: avoid that packets arrive to one host→ censorship

- **Redirection**: reroute clients to malicious host
  - Malicious host attacks client (e.g., serving malware…)
  - Malicious host act as man in the middle (e.g., monitoring)

DNS spoofing – Defenses

Domain Name System Security Extensions (DNSSEC)

- Extensions to DNS that provide **origin authentication**
    - DNS responses are **digitally signed by authoritative name server** – prevents poisoning!
    - DNSSEC responses are not encrypted – **does not provide confidentiality**!

- 1st attempt (RFC 2535) 99-01: impractical, non-scalable, complex key management
- Nowadays (*DNSSEC-bis* RFC 4033): simplified messages and key management

DNS-over-HTTPS (DoH) (RFC8484)

- Since 2019 – DNS queries over HTTPS connection (confidentiality & integrity)

- Deployed by Cloudflare (integrated in Firefox), Google, others

Others: DNS-over-TLS, DNSCrypt, DNSCurve

Computer Security (COM-301)

Network security

BGP Spoofing

Slides by Carmela Troncoso
Some slides/ideas adapted from: George Danezis

If we fix DNS, do we solve the routing problem?

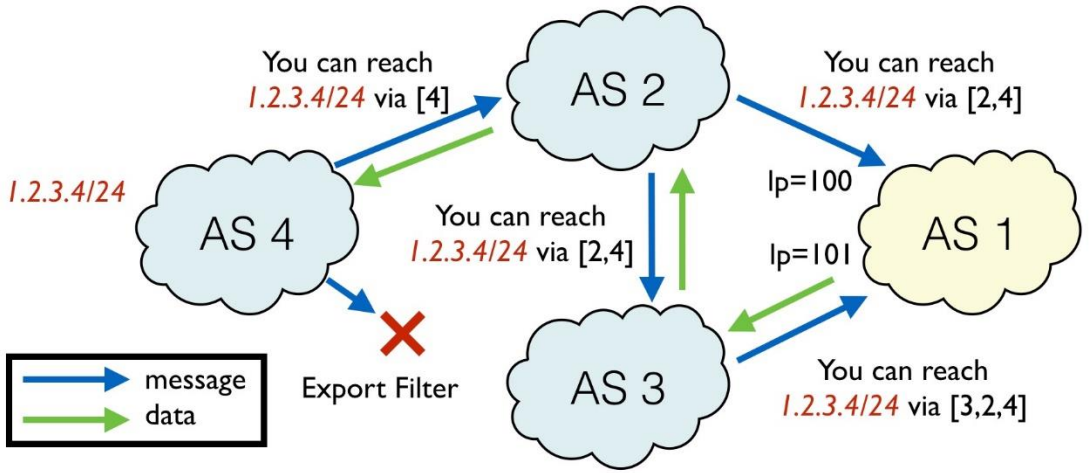
Routing security: The route over the network and the eventual delivery of messages must not be influenced by the adversary

Integrity
Authentication
Availability
Authorization

If we fix DNS, do we solve the routing problem? BGP (Border Gateway Protocol) (RFC 4271)

Refresher

- BGP **constructs the routing tables** between AS - Autonomous Systems with independent routing domains
  - Routers maintain tables of (IP subnet → Router IP, cost)
  - Routes change (faults, new contracts, new cables) - BGP updates constantly
  - Cost is **crucial**: BGP chooses the routes with lowest cost (real money!)



BGP Security

Weak authentication mechanism between routers (RFC 2385):

- Aimed at preventing DoS
- Short shared secret (up to 80 bytes of ASCII)
- Ad-hoc message authentication code based on the weak algorithm MD5

Does this guarantee the integrity of the advertised routes?

NO!! BGP Hijacking!

- An adversary controls or compromises a BGP router *somewhere* on the Internet
- Injects false low-cost routes to redirect portions of traffic to themselves
- The routing information propagates to routing tables until it expires

What can you achieve?

- **Redirection**: surveillance, injection, modification, or censorship.

Example 1: Belarus hijacks internet (2013)

- Global traffic redirected to Belarusian ISP GlobalOneBel.
  - Daily basis throughout February 2013
  - Changing set of victims: major financial institutions, governments, and network service providers.
  - Affected countries included the US, South Korea, Germany, the Czech Republic, Lithuania, Libya, and Iran

https://dyn.com/blog/mitm-internet-hijacking/

Example 2: BGP hijacking as censorship

- 2000: Pakistan tries to censor YouTube (and accidentally shuts it down…)
  - https://www.wired.com/2008/02/pakistans-accid/

- 2014: Turkey bans Twitter by hijacking DNS provider routes (after direct DNS hijacking stopped working)

https://www.bgpmon.net/turkey-hijacking-ip-addresses-for-popular-global-dns-providers/

- 2017: Iran censors a number of webpages (mostly porn)
  - https://bishopfox.com/blog/bgp-hijacking-technical-post-mortem

- 2021: Myanmar tries to censor Twitter
  - https://www.manrs.org/2021/02/did-someone-try-to-hijack-twitter-yes/

BGP Spoofing - Defenses

Filtering help alleviating
(some routes should really not come from some routers).

But… there is no authority to guarantee the correctness of routes (all contractual).

Fundamental flaw (again): Design did not consider insiders as adversaries!

BGPsec

Each AS is given a certificate that links its verification key to its IP blocks.
Updates are only accepted if they are signed by the authority for the AS/IP Block.
Delegation is possible
Effort started in 2003 (RFC8205) -- weakly deployed

Spoofing: lesson to be learned

1. The network is hostile!

Routing security attacks, facilitated through **poor association of high level and low level names & addresses** (IP to Ethernet MAC / Route to router).

- **Threat model**: assumes network "insiders" are trusted to provide authoritative information.
- Also **no** integrity or confidentiality.

2. The solution is intimately linked to cryptography

Why? There is **no centralized authority** to act as either (a) originator of policy or (b) provide a trusted computing base

- Cryptography allows mutually distrustful actors to achieve some collective security properties
- Asymmetric cryptography (certificates and signatures) particularly useful for all to verify name and route associations!

But also… Who has authority?

Not a cryptographic question! related to name resolution & security policy

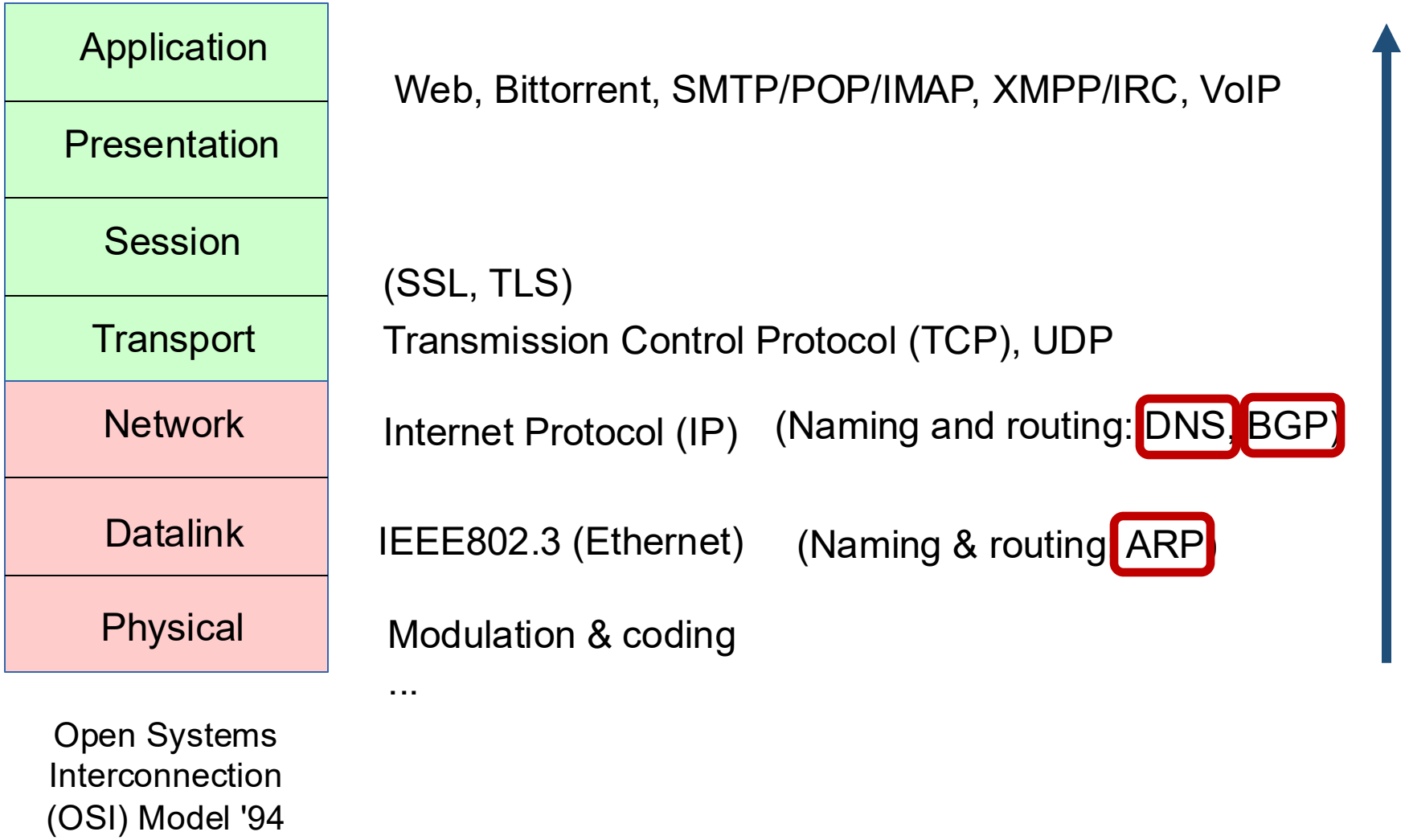
Computer Security (COM-301)

Network security

IP

Slides by Carmela Troncoso
Some slides/ideas adapted from: George Danezis

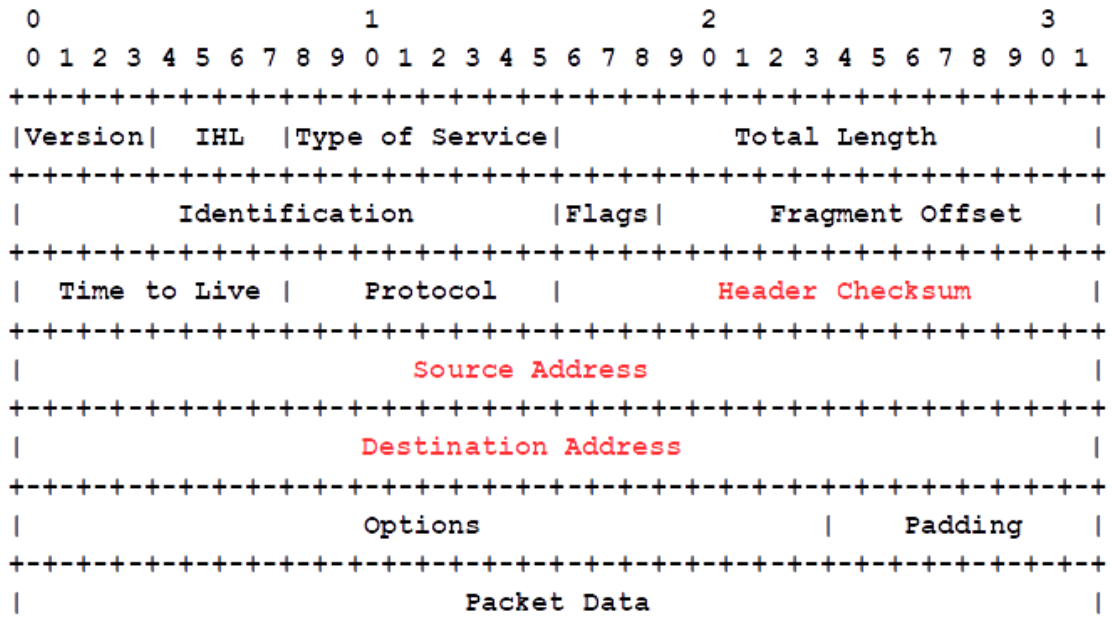
Where are the problems?



Open Systems Interconnection (OSI) Model '94

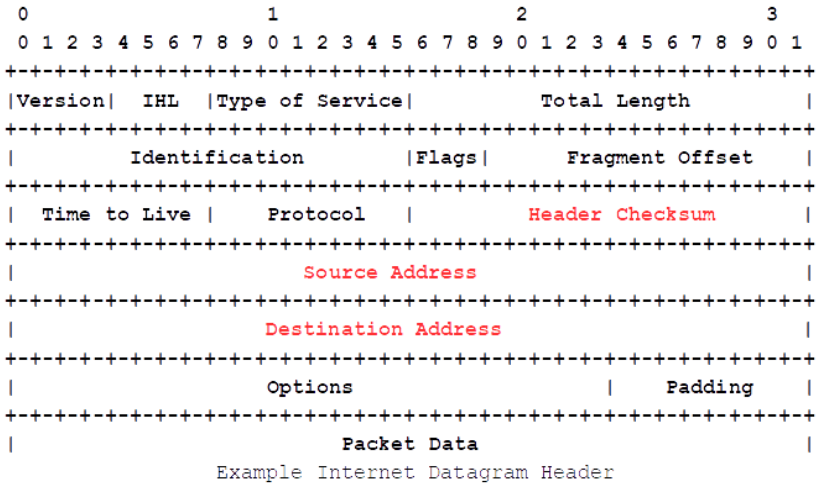
So what about IP?

Refresher



Example Internet Datagram Header

IP spoofing



Example Internet Datagram Header

No integrity or authentication mechanism for `Source Address`

What can we do?

- **Impersonation:** for instance to steal resources
- **Man in the middle:** monitor, intervention, deny service
- **Denial of Service:** fake source IP so that others send packets to a target victim with that IP

IPSec - Internet Protocol Security

- Cryptographic security properties at the IP level
  - Key exchange based on public key cryptography or shared symmetric keys
  - **Authentication Header (AH)**: authentication & integrity (HMAC), protection from replay attacks (sequence number)
  - **Encapsulating Security Payload (ESP)**: can add confidentiality on top of auth

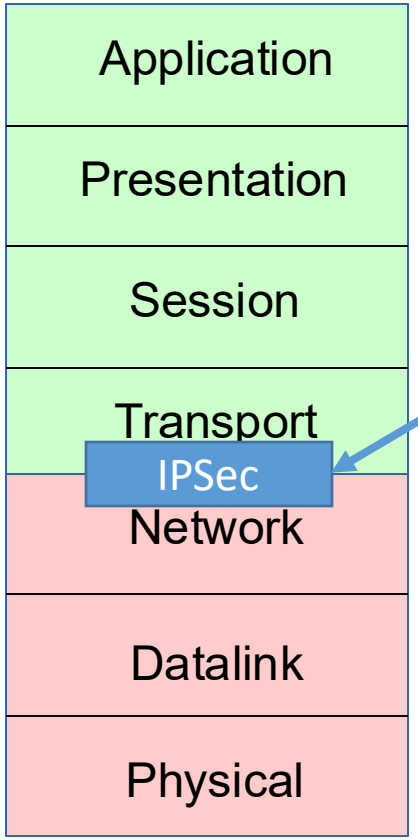
- Two modes:
  - **Transport**:

    protects IP packet payload using AH/ESP

    sent with the **original IP headers**
  - **Tunnel**:

    protects the whole packet (Headers + Payload) is protected and placed inside another packet

Where does IPSec in Transport Mode happen?

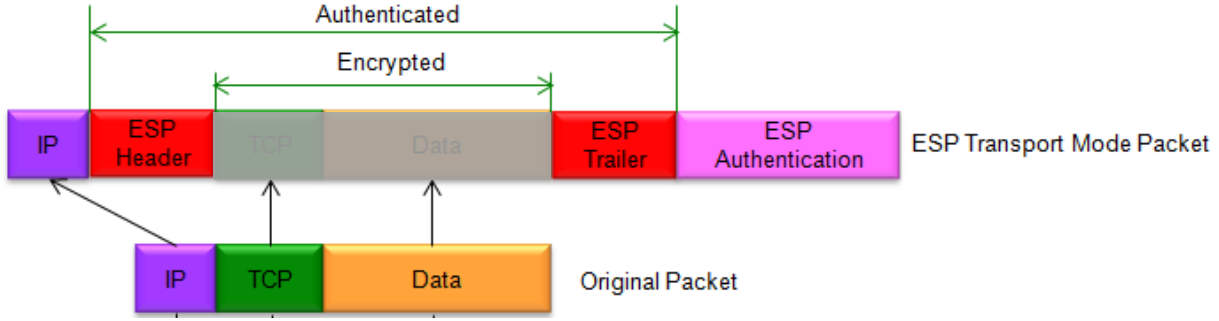


Open Systems Interconnection (OSI) Model '94

IPSec in **TRANSPORT MODE**, **<u>protects the payload</u>** but keeps the headers.

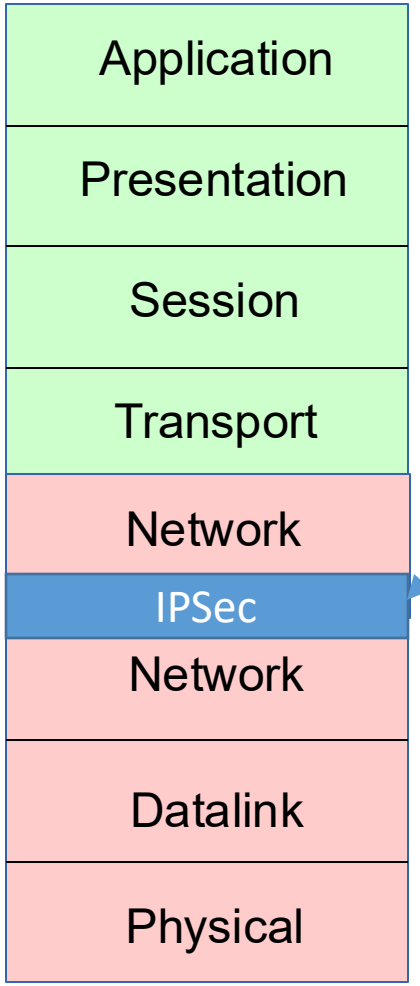
Transmission Control Protocol (TCP), UDP

Internet Protocol (IP)



http://www.sharetechnote.com/html/IP_Network_IPSec_ESP.html

Where does IPSec in Tunnel Mode happen?

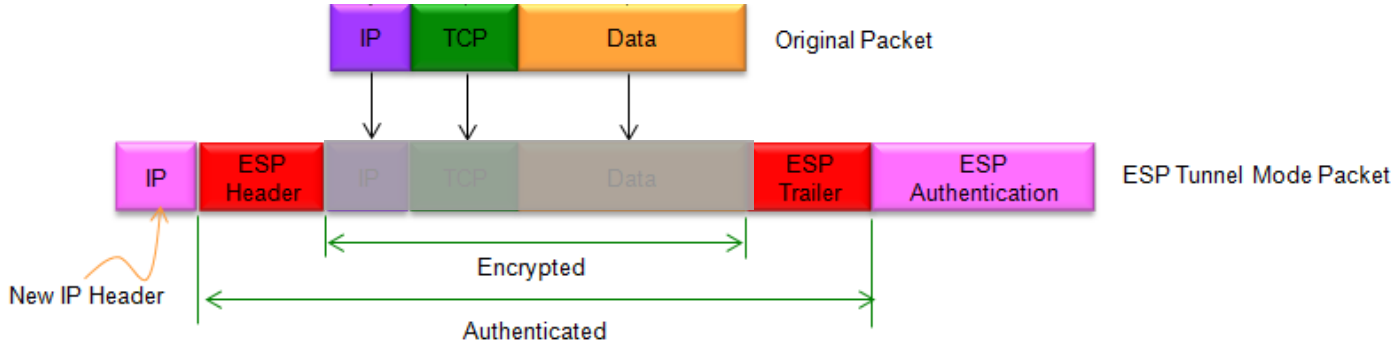


Open Systems Initiative (OSI) Model '94

IPSec in **TUNNEL MODE**, **<u>encrypts payload</u>** and **<u>the headers</u>**.

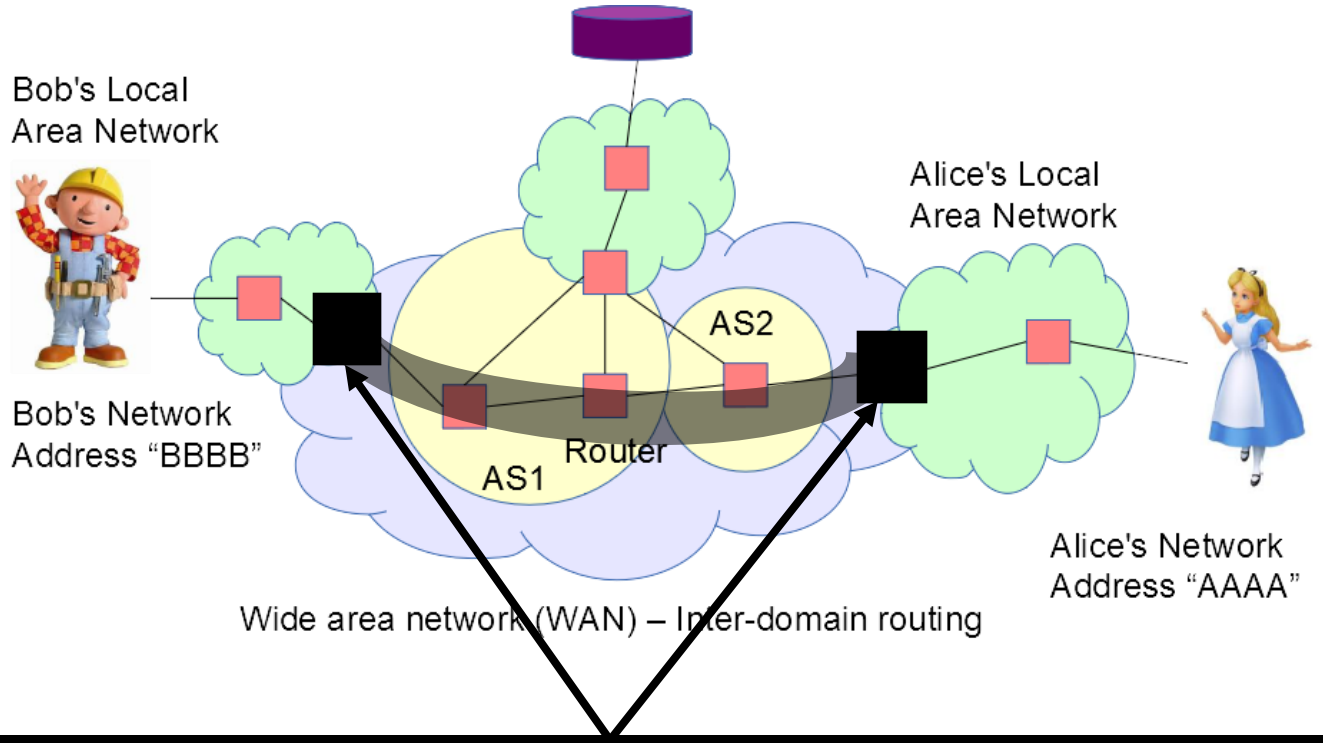
Transmission Control Protocol (TCP), UDP

Internet Protocol (IP)



http://www.sharetechnote.com/html/IP_Network_IPSec_ESP.html

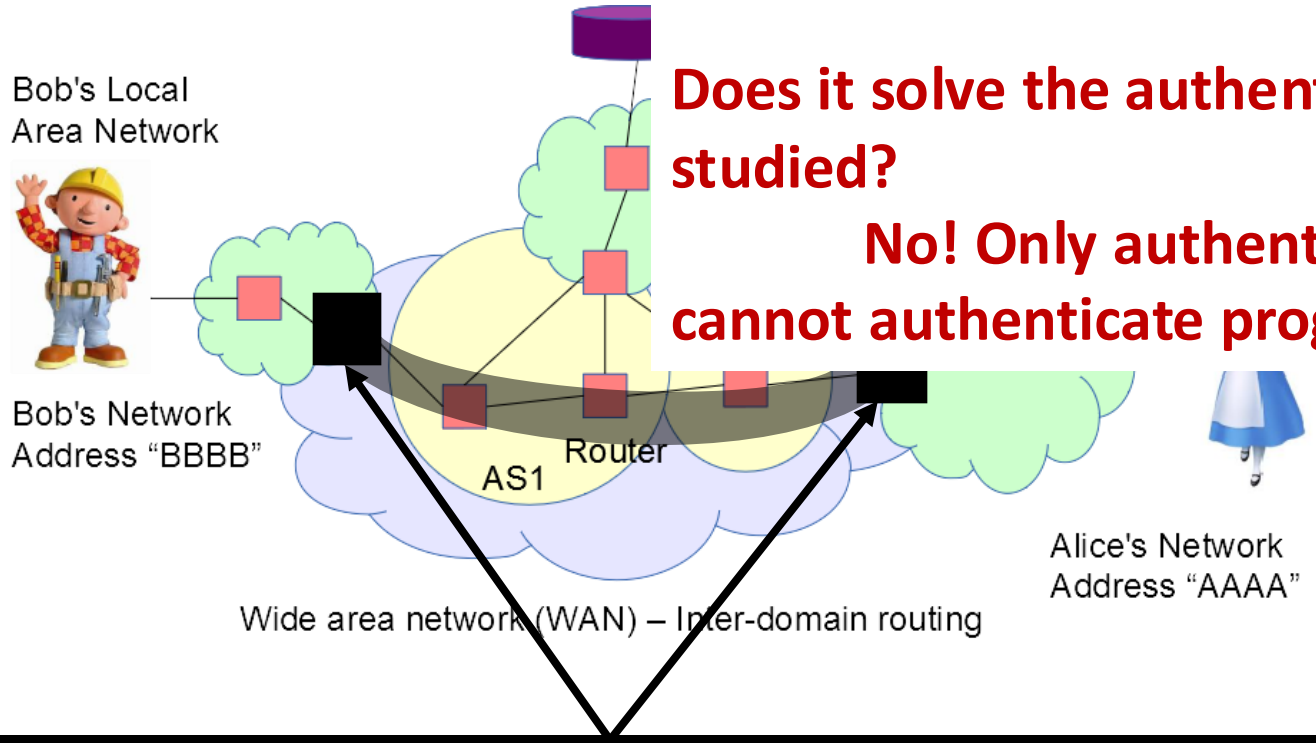
Use of IPSec: Virtual Private Network



- IPSec in tunnel mode. The VPN
  - Looks like one single network
  - Routing internally
  - Inside VPN "tunnel" fully protected packets: confidentiality, authentication, integrity, reply

Use of IPSec: Virtual Priv

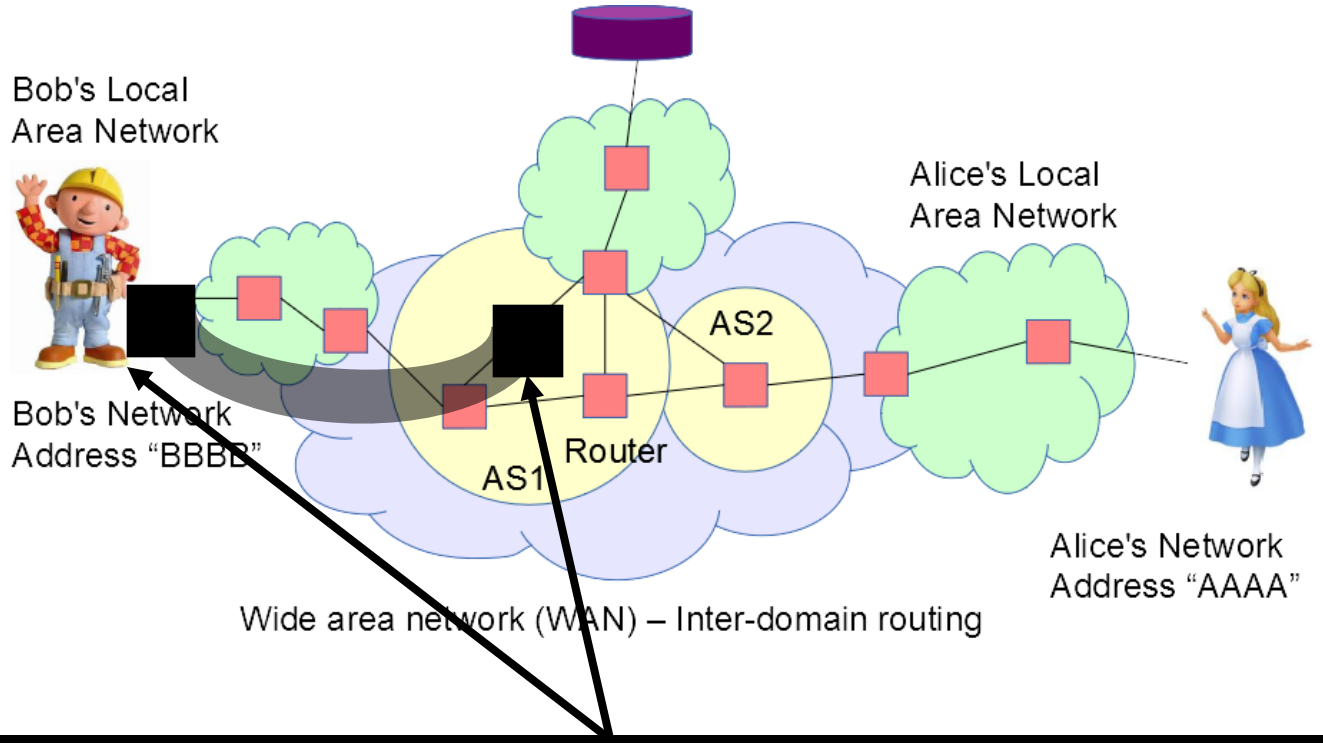
Does it protect against Denial of Service?
No! Your IP still exists



Does it solve the authentication problem we have studied?
No! Only authentication at network level. It cannot authenticate programs or applications

- IPSec in tunnel mode. The VPN
  - Looks like one single network
  - Routing internally
  - Inside VPN "tunnel" fully protected packets: confidentiality, authentication, integrity, reply

Virtual Private Network - other common configuration

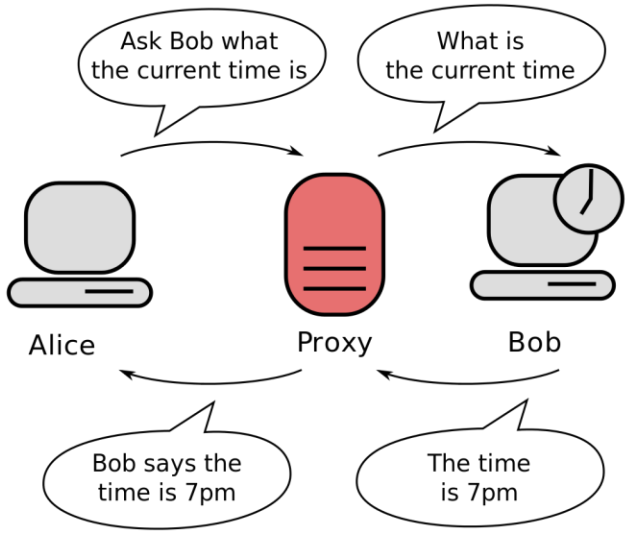


VPN out of Bob's LAN (VPN as a Service)

AS1 can see the connection from the VPN to the server (if that connection is in the clear, it can spy)

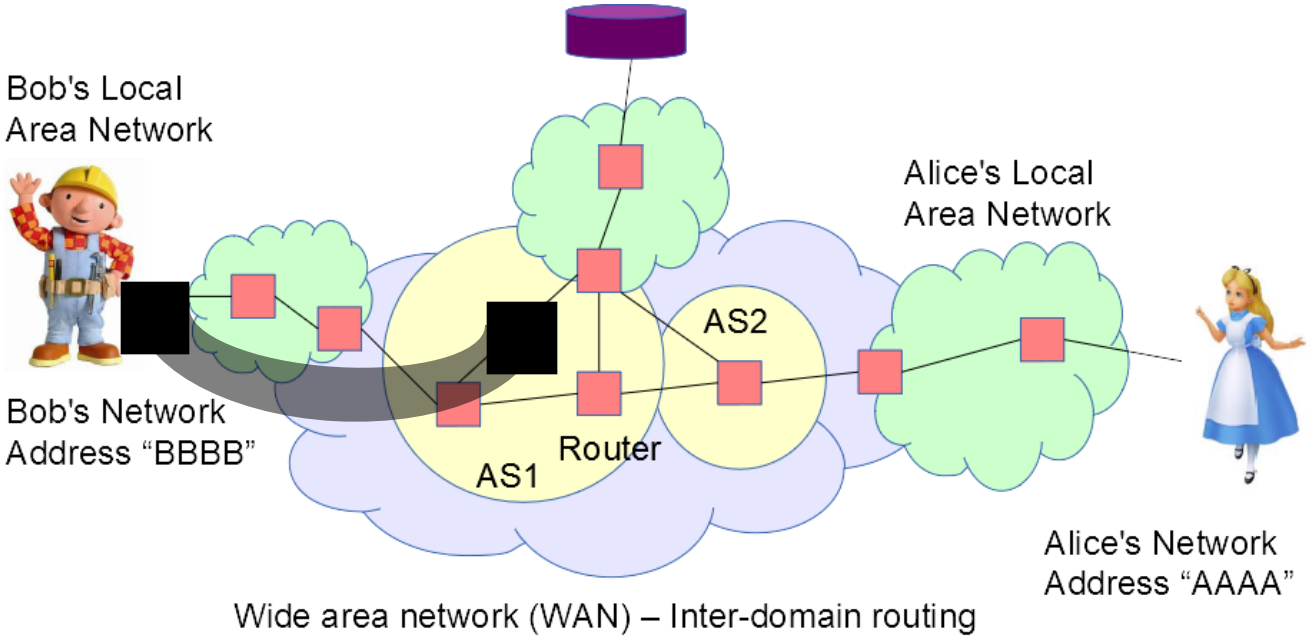
Is a VPN the same as a proxy?

No! They both hide the IP from the receiver but they offer very different properties!



Encrypted traffic end-to-proxy

Proxy separates two networks



Encrypted traffic end to end

Acts as one network

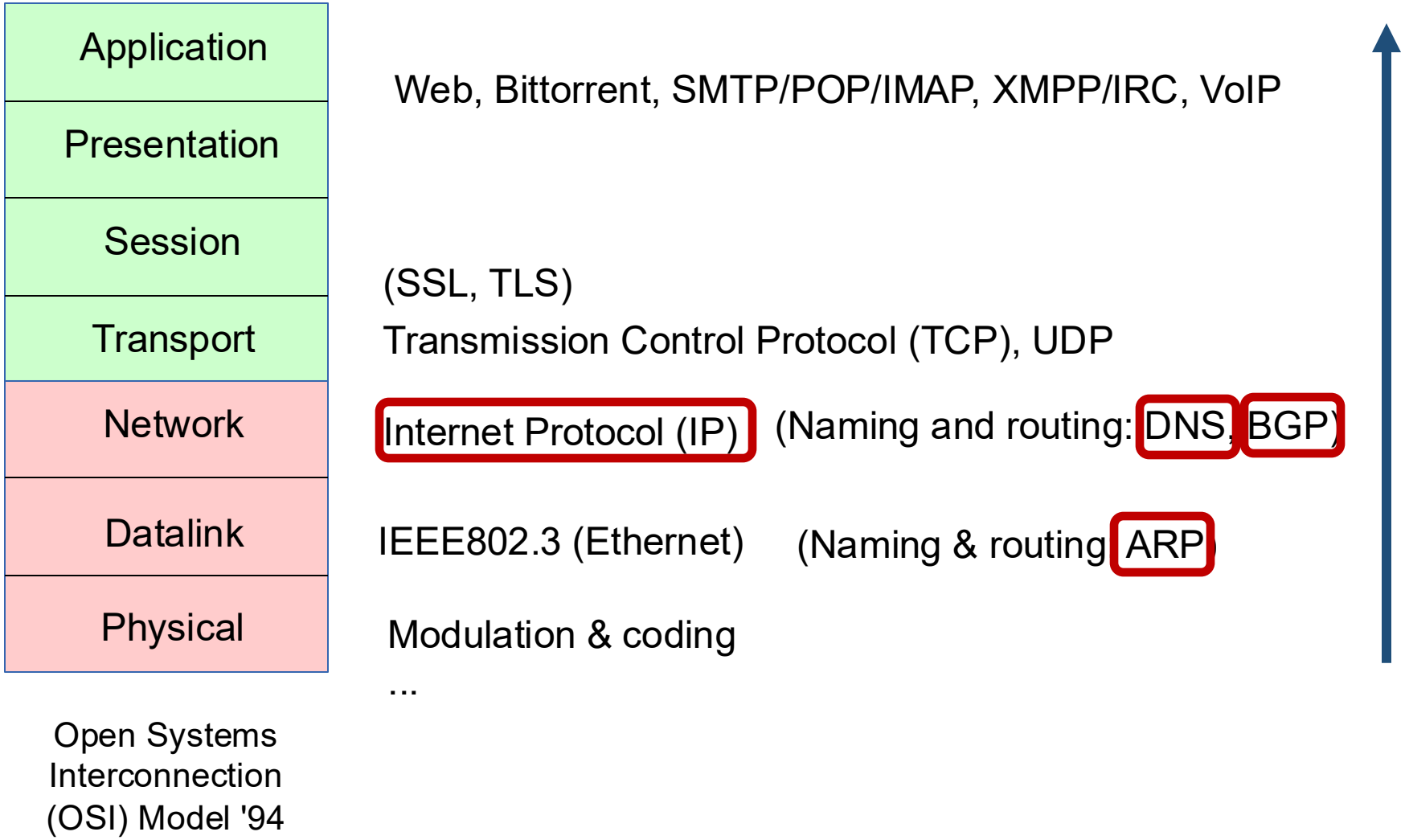
Computer Security (COM-301)

Network security

TCP

Slides by Carmela Troncoso
Some slides/ideas adapted from: George Danezis

Where are the problems?



IP limitations

Refresher

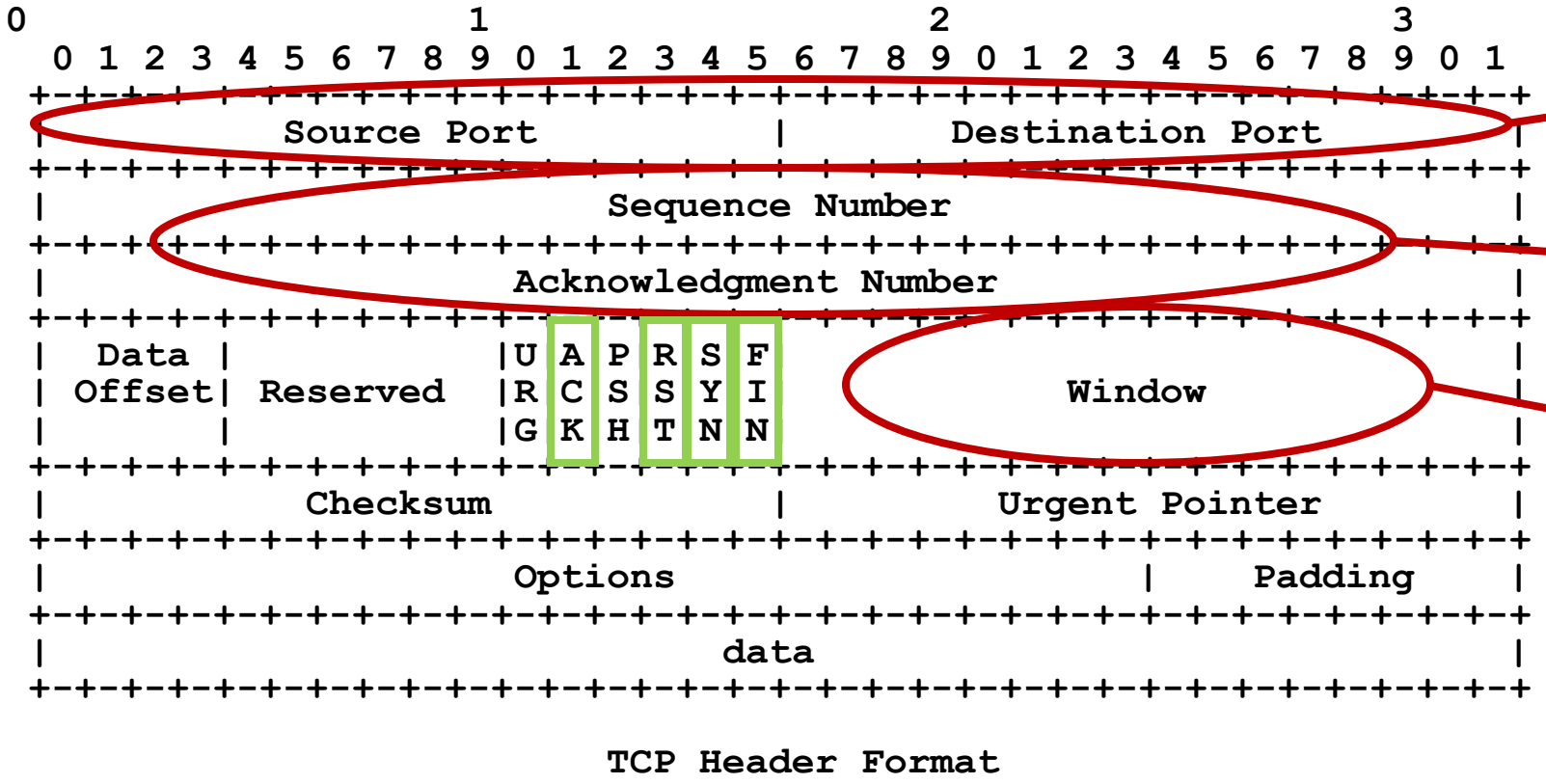
- **No reliability**: messages can get dropped, there is no mechanism to ensure a message was received
- **No congestion/flow control**: no mechanism to avoid congestion either in the network or the end hosts
- **No sessions**: no way to associate messages together (and in both directions) into one logical “session”
- **No multiplexing**: no way to associate messages to a network address to specific applications / users on host.

The Transmission Control Protocol (TCP)

- Protocol run “inside/above” the IP protocol
- Addresses the issues above

TCP header

Refresher



TCP Header Format

Multiplexing

Reliability
Congestion control

Flow Control

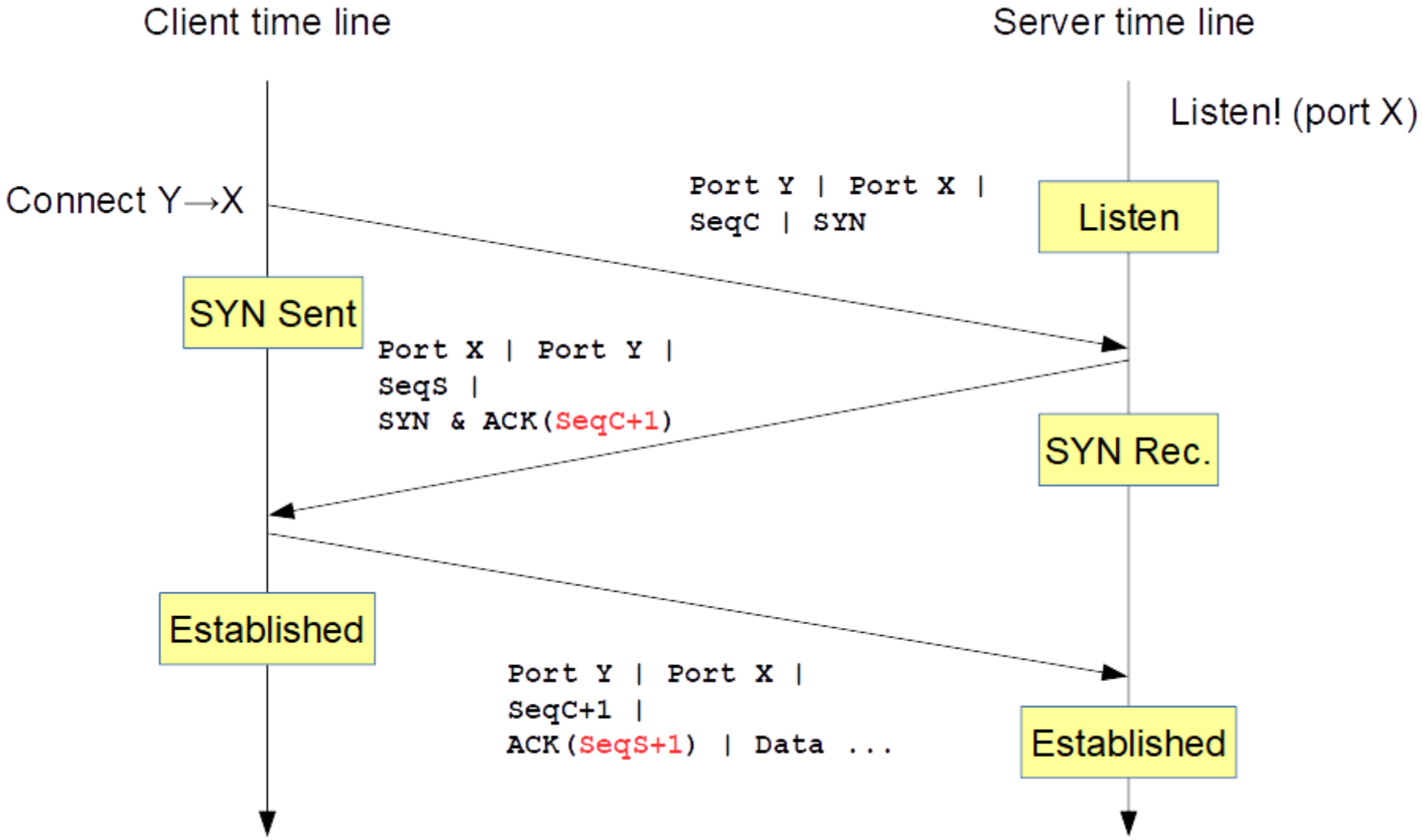
Well known Ports:

20-21 – FTP
22 – SSH
25 – SMTP
53 – DNS
80 – HTTP
110 – POP3
143 – IMAP
443 – HTTPS

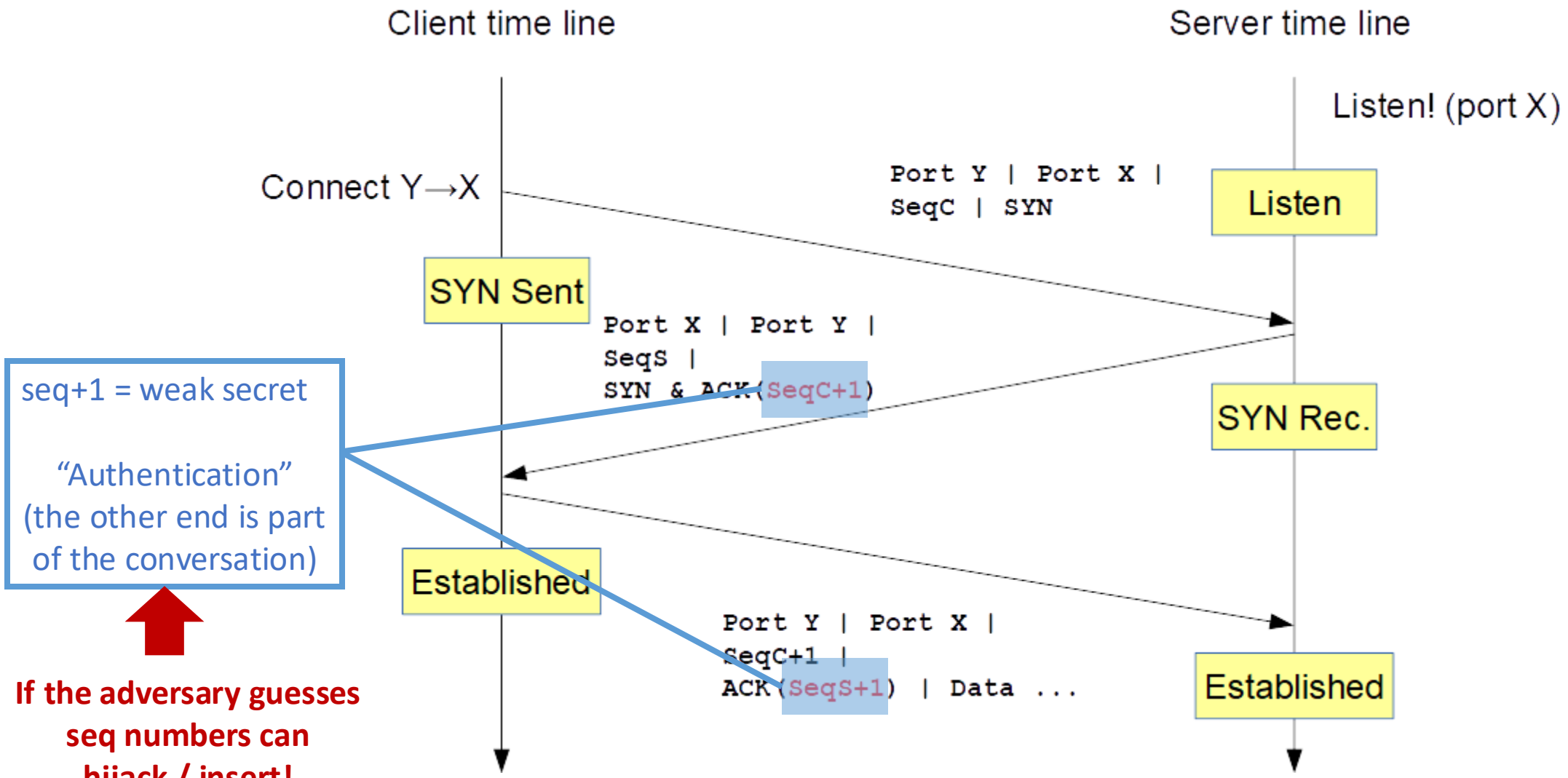
RFC793 (1981) http://www.ietf.org/rfc/rfc793.txt

TCP 3-way handshake

Refresher



TCP 3-way handshake – Security considerations



TCP 3-way handshake – Security considerations

Can the adversary guess???

- Weak random numbers generation
- Observation (if connection in the clear)

Example attack

- The (historical) “rsh” UNIX utility that provides a remote shell implemented authentication and authorization on the basis of remote IP address only! (**Bad idea**)
- The Robert Morris Attack:
  1) Send a SYN packet **spoofed** as if it was from authorized host.
  2) Guess server SeqS and send an ACK with SeqS+1 and some data.
  3) The data is interpreted as a shell command and executed!

https://www.techrepublic.com/article/tcp-hijacking/