CAL POLY

CSC 321: Introduction to Computer Security

Module 7: Network Security

Bret Hartman

Department of Computer Science and Software Engineering

California Polytechnic State University

E-mail: bahartma@calpoly.edu

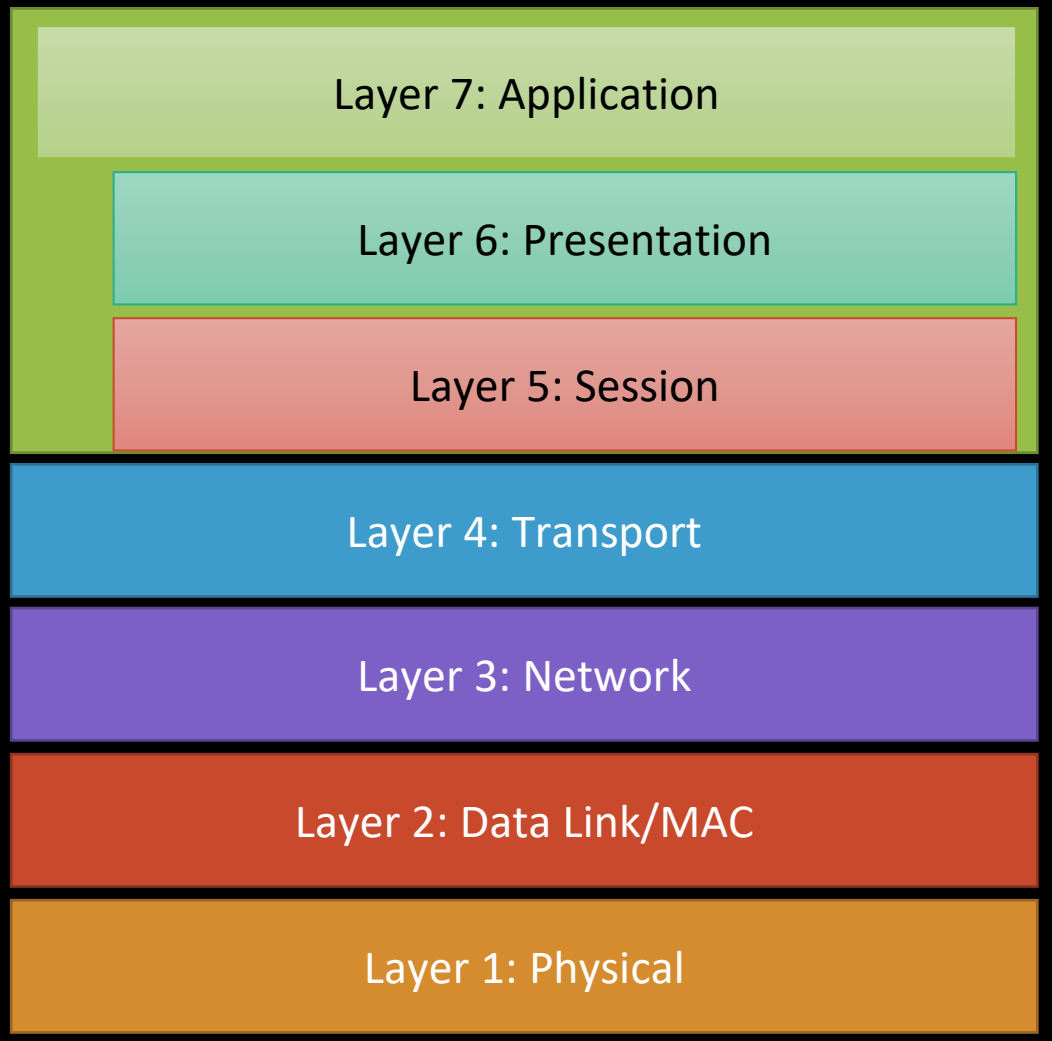
A special thanks to Dr. Bruce DeBruhl and Dr. Phoenix (Dongfeng) Fang, the authors of most of this material

Quiz 6 available
6a Lab Leviathan,6b Lab Microcorruption due

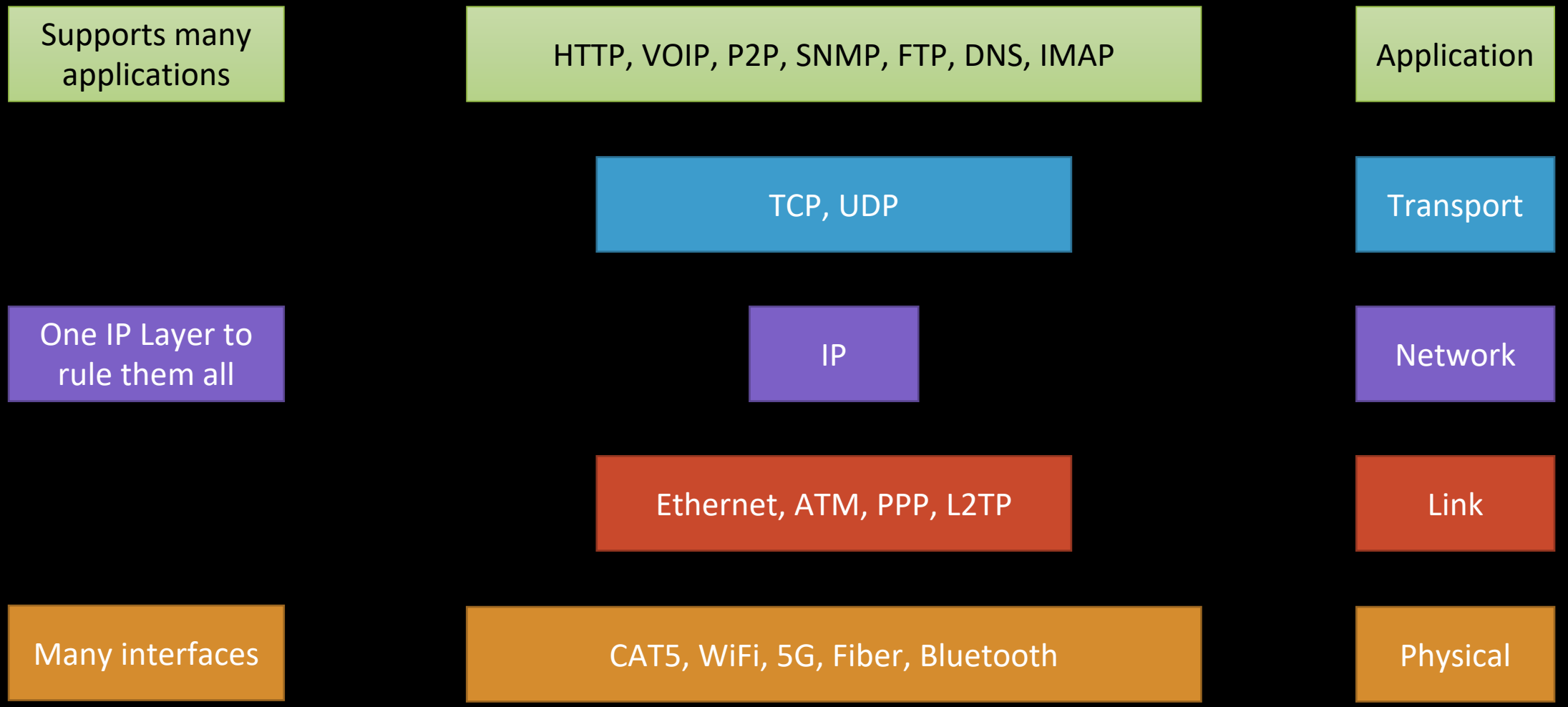
Network model – OSI stack

Open systems interconnection (OSI) model

- Standardized network connections across layers
- Each layer provides well-defined set of functionality
- Allows communication between any layer
- Transmission Control Protocol (TCP) / Internet Protocol (IP) developed in 1970s for availability
- Not confidentiality or integrity!

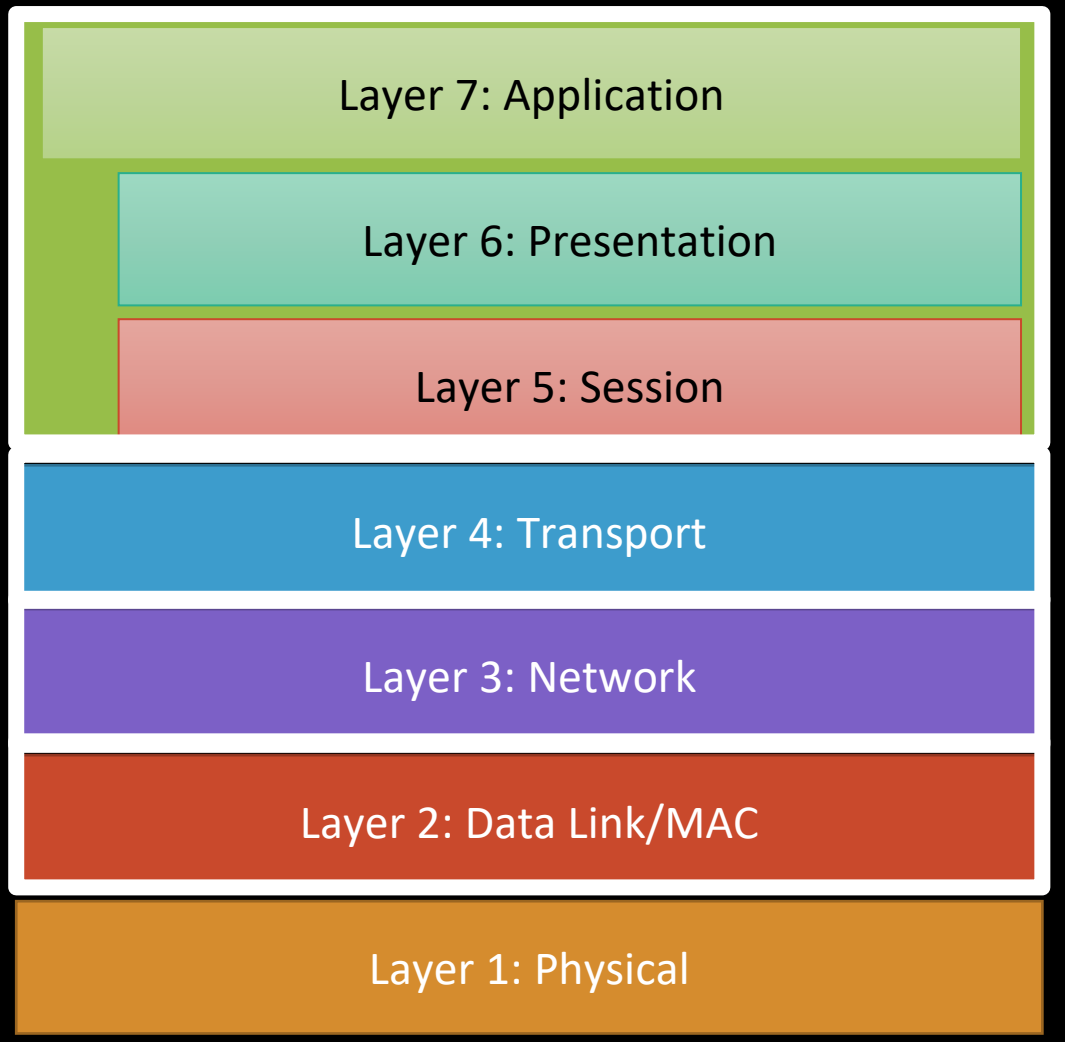


IP hourglass



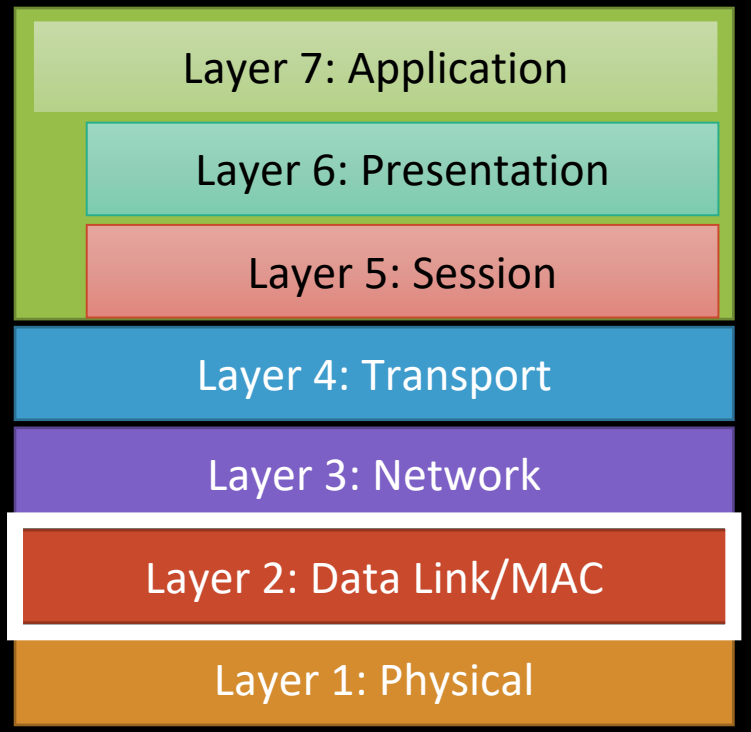
Network security topics

- Layer 2: Data Link / MAC
- Layer 3: IP, ICMP, Tor
- Layer 4: TCP
- Firewalls: IP, DMZ, IDS / IPS, NGFW
- VPNs: IPsec
- TLS
- DNS
- Bots



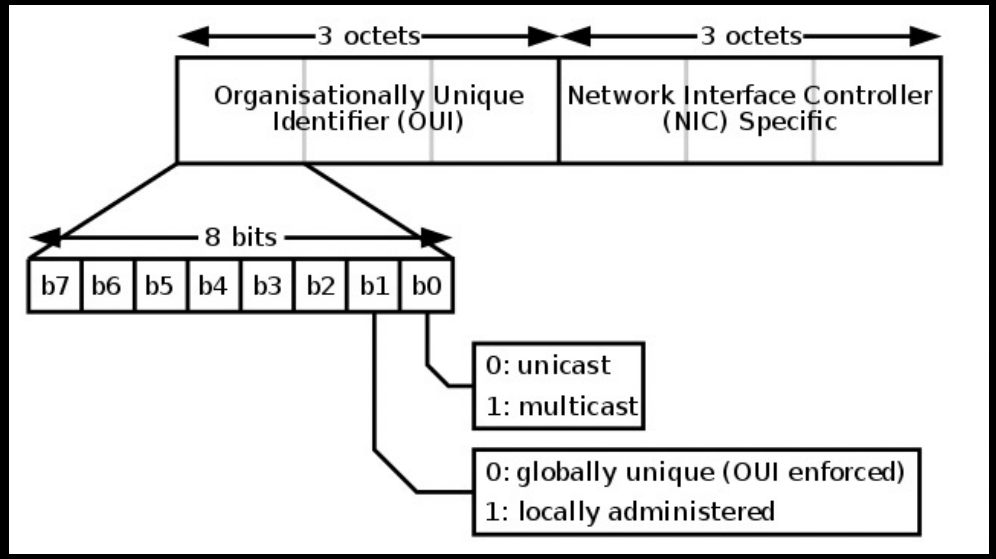
Layer 2 what goes wrong

- Spoofing
  - Media Access Control (MAC) addresses theoretically unique
  - Change MAC address via software tools
- Address Poisoning
  - Pretend to be another IP address
- Degradation/denial of service/load attacks
- Privacy leakage
  - Exposure of metadata



MAC address attacks

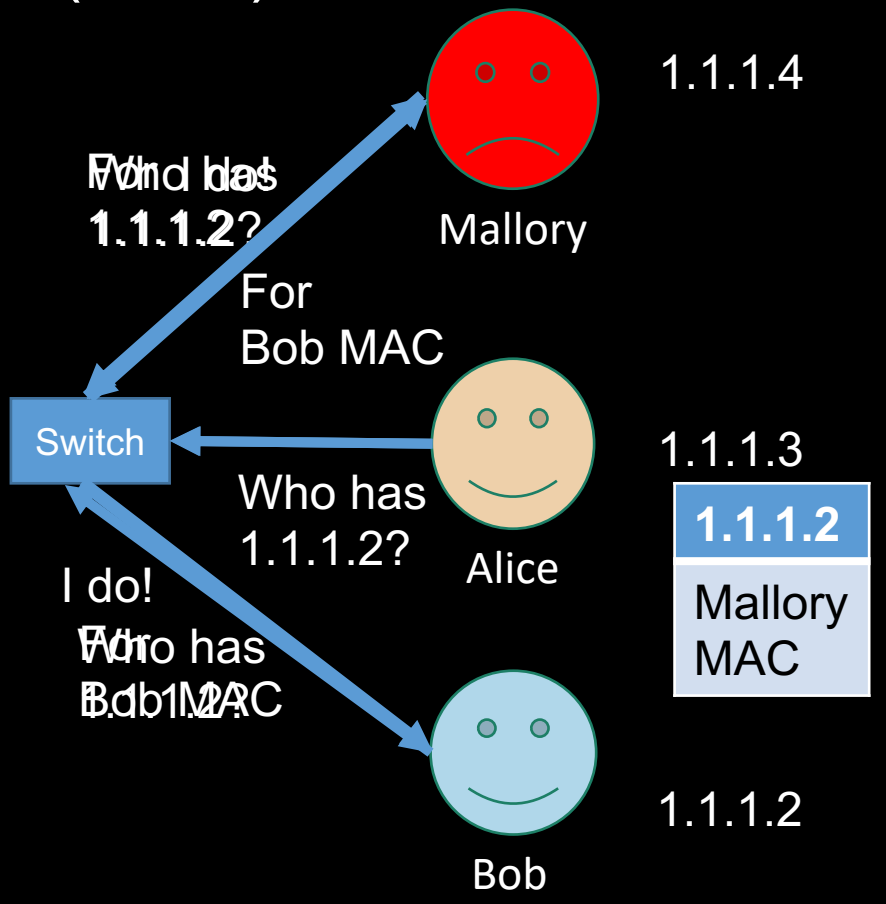
- OUI: First three bytes represent an organizationally unique ID
  - Useful during penetration testing to identify device
  - If it is Cisco, it could be a router, switch, firewall, IPphone, …
- Impersonation attacks
  - Set OUI/MAC address to look like a particular device
- Load Attacks
  - Broadcast increase packet load




```
50E549  GIGA-BYTE TECHNOLOGY CO.,LTD.
50E666  Shenzhen Techtion Electronics Co., Ltd.
50EAD6  Apple, Inc.
50EB1A  Brocade Communications Systems, Inc.
50ED78  Changzhou Yongse Infotech Co.,Ltd
50ED94  EGATEL SL
50F003  Open Stack, Inc.
50F0D3  Samsung Electronics Co.,Ltd
50F14A  Texas Instruments
```

Address Resolution Protocol (ARP)

- Protocol maps IP address to physical layer (MAC)
  - ARP request: who has xxx.xxx.xxx.xxx?
  - ARP response: Me!
- Allows for proper switch forwarding
- ARP Poisoning
  - Allows MitM attack



ffs Hak5 WiFi Pineapple Mark VII + Field Guide Book

Brand: ffs

7 ratings

$199.99

& FREE Returns

Get a $100 Amazon Gift Card instantly upon approval for the Amazon Prime Rewards Visa Card. No annual fee.

- The industry standard pentest platform has evolved. Equip your red team with the WiFi Pineapple Mark VII. Newly refined. Enterprise ready.
- Automate WiFi auditing with all new campaigns and get actionable results from vulnerability assessment reports.
- Command the airspace with a new interactive recon dashboard, and stay on-target and in-scope with the leading rogue access point suite for advanced man-in-the-middle attacks.
- Next-gen network processors combine with multiple role-based radios and the Hak5 patented PineAP suite to deliver impressive results. Hardened and stress tested for the most challenging environments.
- The new WiFi Pineapple Mark VII features incredible performance from a simple web interface with an expansive ecosystem of apps, automated pentest campaigns, and Cloud C2 for remote access from anywhere.

MOTHERBOARD
TECH BY VICE

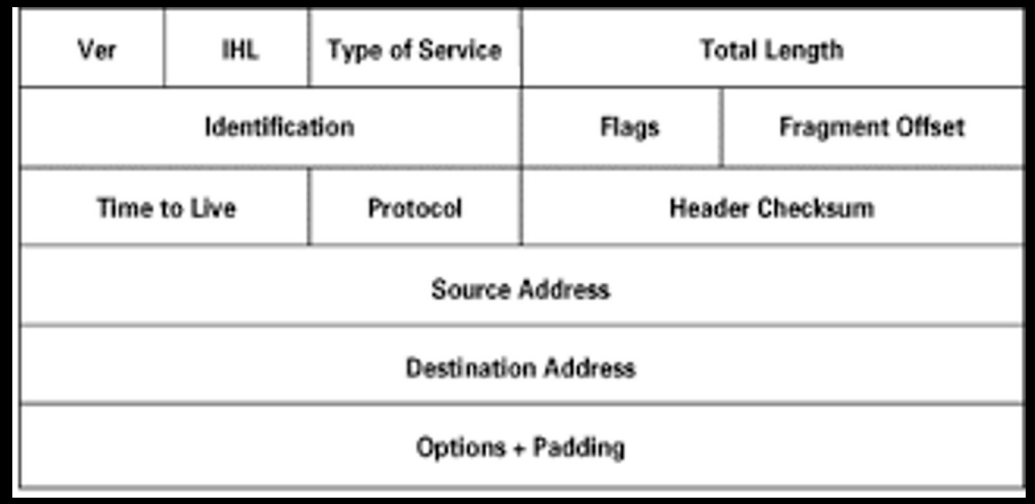
How a Wi-Fi Pineapple Can Steal Your Data (And How to Protect Yourself From It)

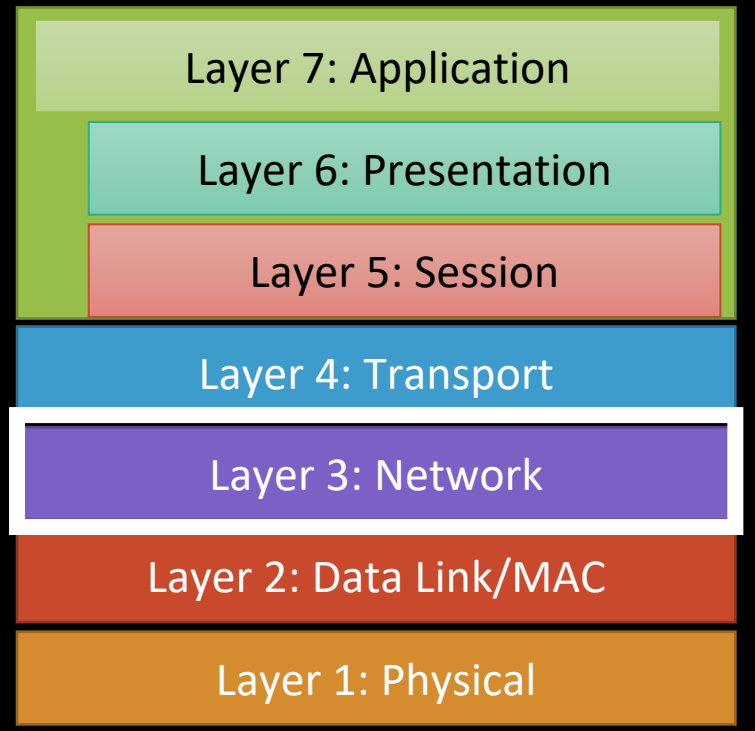
The Wi-Fi Pineapple enables anyone to steal data on public Wi-Fi networks. Here's how it facilitates two sophisticated network attacks and how to protect yourself against them.

- Evil twin
- Man-in-the-Middle
- Spoofed website
- Countermeasures?

Layer 3: IP attacks

- IP addresses are not private
  - TLS doesn't help
- IP hijacking
  - Claim IP address
  - Route/path attraction attack for eavesdropping
- Replay attacks
  - Authentication, Industrial control system (Stuxnet)
- Packet storm denial of service (DoS) attacks
- Fragmentation DoS attacks
  - Teardrop: Fragment offset in Windows
  - Nestea: Linux version





Internet Control Message Protocol (ICMP) Attacks

- Smurf Attack
  - ICMP with a response
    - Source = victim
    - Dest = broadcast (everyone replies)
  - Defenses: Don’t respond to or forward ping broadcasts
  - Fraggle - similar but uses UDP on port 7 (echo port)
- Ping Scans
- Ping of death
- Unreachable attacks
  - Send an ICMP unreachable packet to reset TCP connection

Tor: The onion router

Home > Security > Privacy

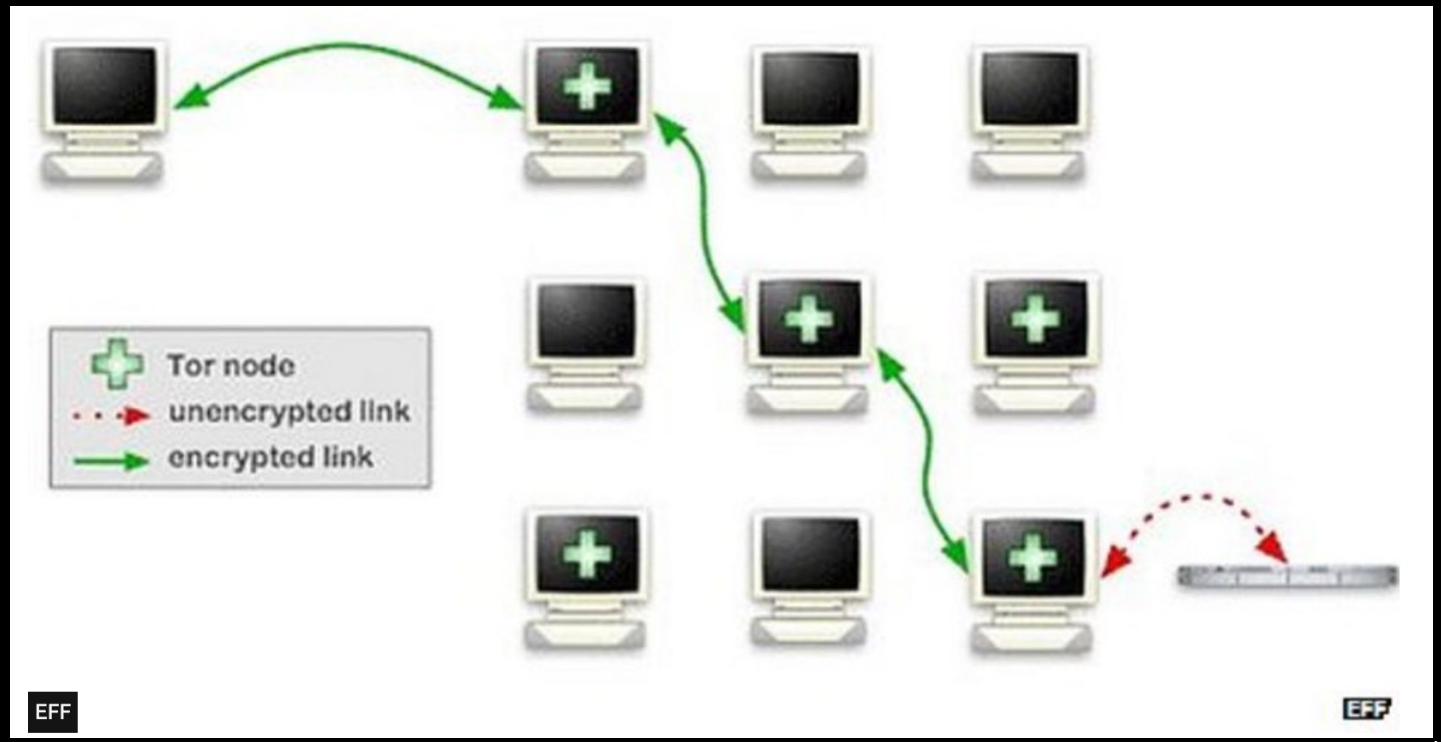
FEATURE

What is the Tor Browser? And how it can help protect your identity

Tor Browser offers the best anonymous web browsing available today, and researchers are hard at work improving Tor's anonymity properties.

By J.M. Porup

Senior Writer, CSO | OCT 15, 2019 3:00 AM PDT



Web-based onion services in February 2016[20][21]

Category	% of total	% of active
Violence	0.3	0.6
Arms	0.8	1.5
Illicit Social	1.2	2.4
Hacking	1.8	3.5
Illicit links	2.3	4.3
Illicit pornography	2.3	4.5
Extremism	2.7	5.1
Illicit Other	3.8	7.3
Illicit Finance	6.3	12
Illicit Drugs	8.1	15.5
Non-illicit+Unknown	22.6	43.2
Illicit total	29.7	56.8
Inactive	47.7	
Active	52.3	

Feds Arrest Alleged ‘Silk Road 2’ Admin, Seize Servers

November 6, 2014 65 Comments

Federal prosecutors in New York today announced the arrest and charging of a San Francisco man they say ran the online drug bazaar and black market known as **Silk Road 2.0**. In conjunction with the arrest, U.S. and European authorities have jointly seized control over the servers that hosted Silk Road 2.0 marketplace.

According to federal prosecutors, since about December 2013, Benthall has secretly owned and operated Silk Road 2.0, which the government describes as “one of the most extensive, sophisticated, and widely used criminal marketplaces on the Internet today.” Like its predecessor, Silk Road 2.0 operated on the “Tor” network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the network’s users.

New Mirai botnet lurks in the Tor network to stay under the radar

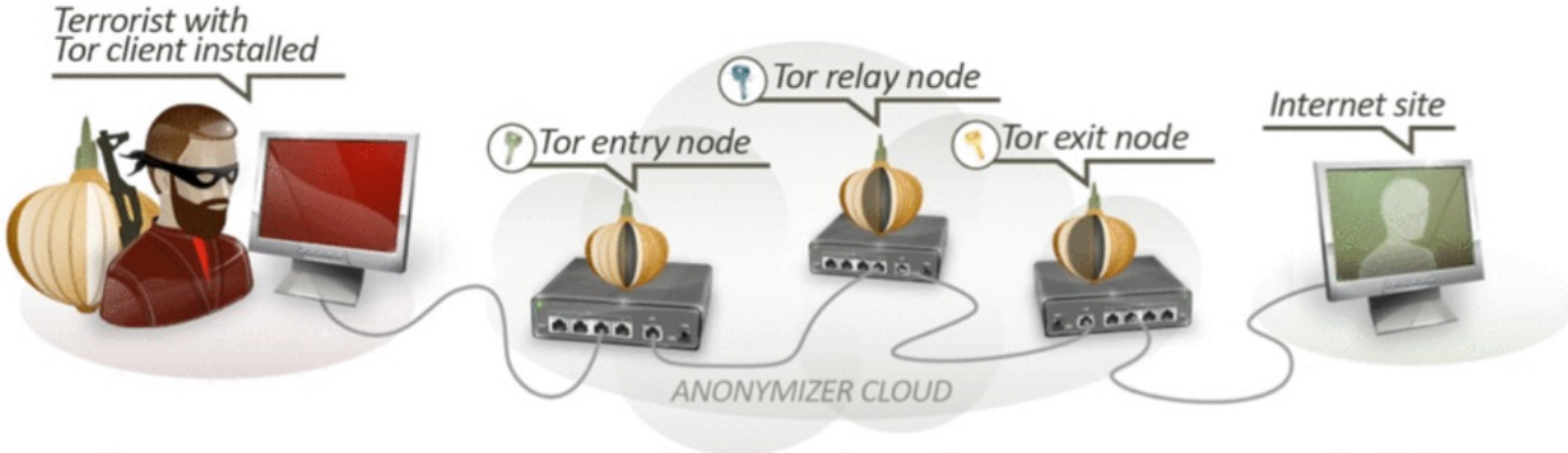
The malware’s command center is hidden to make takedowns a more complicated process.

Tor Stinks… (U)

- We will n
  users all t
- With mar
  very sma
  success d
  TOPI requ

TOP SECRET//COMINT// REL FVEY

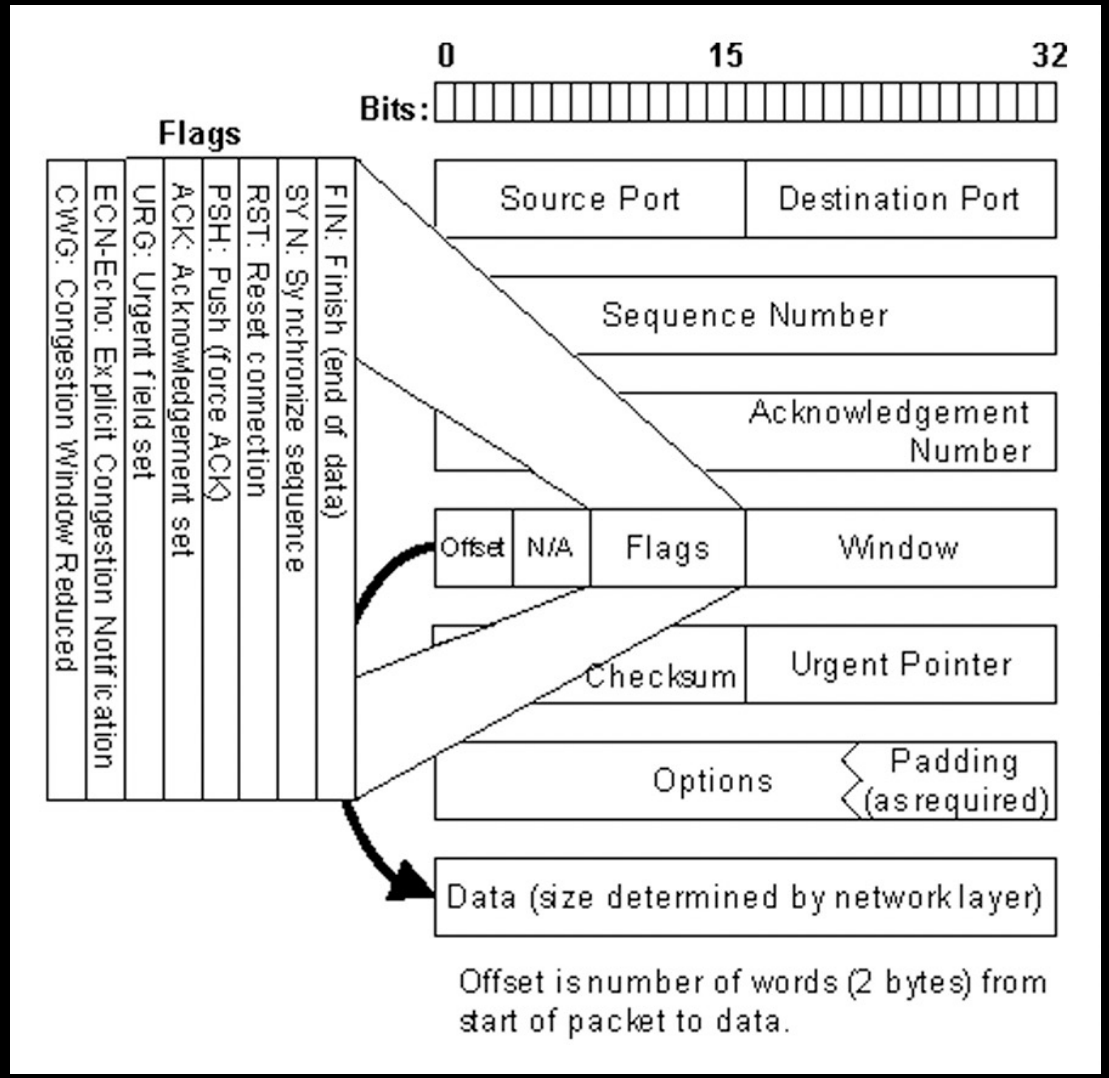
Analytics: Circuit Reconstruction (S//SI)



- Current: access to **very** few nodes. Success rate negligible because all three Tor nodes in the circuit have to be in the set of nodes we have access to.
  - Difficult to combine meaningfully with passive SIGINT.

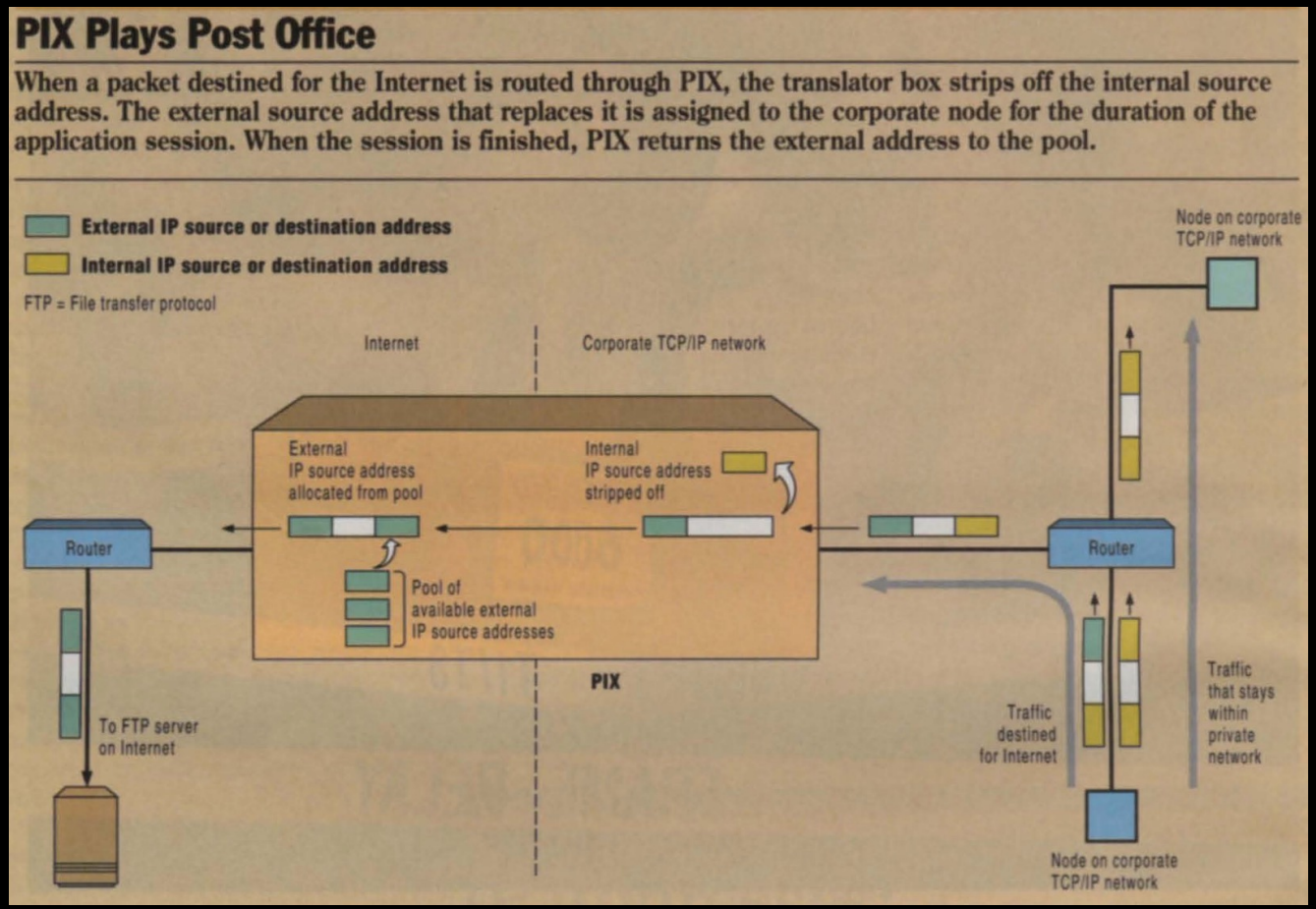
Layer 4: Transmission Control Protocol (TCP) vulnerabilities

- TCP connection: ordered stream of IP packets
  - You will see lots of these in lab!
- Sequence number attacks
  - Reordering
  - Hijacking
- Denial or degradation of service
- Eavesdropping
  - Unencrypted protocols
  - Metadata



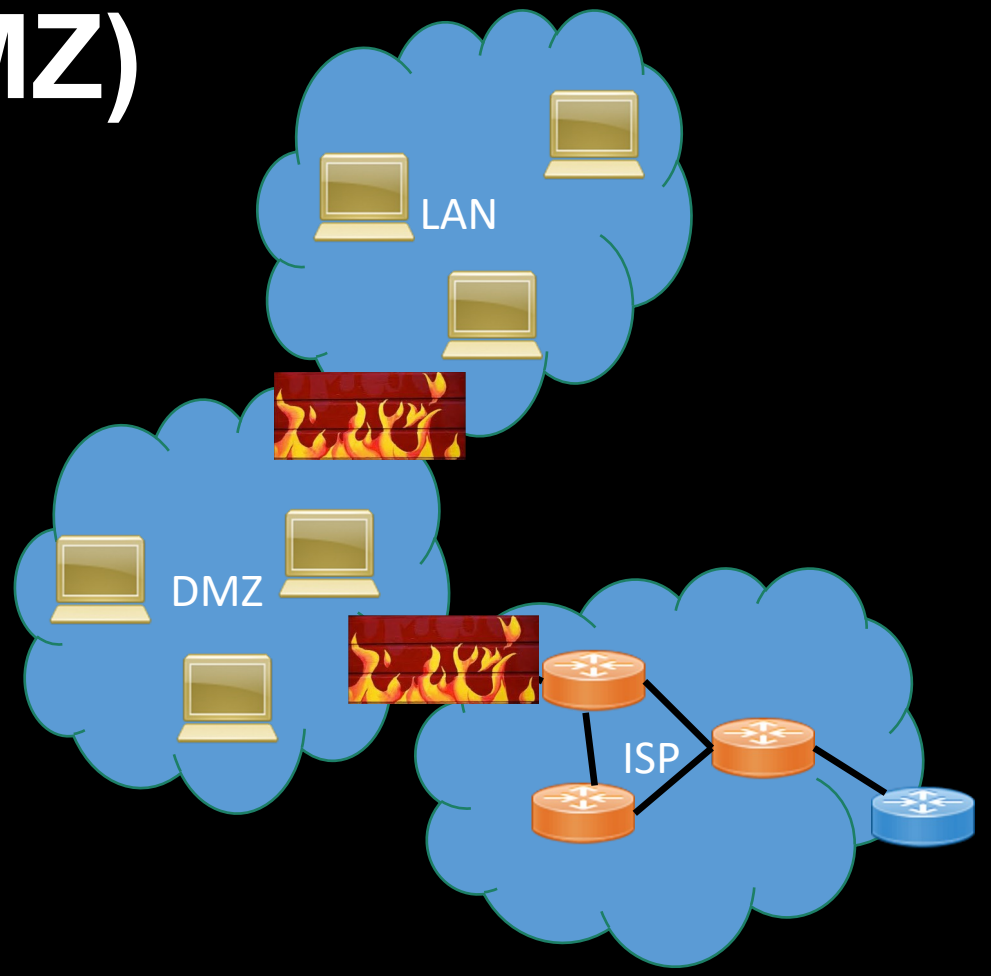
1990: Internet – Traditional IP firewalls

- Securing IP traffic
  - IP address / port packet filters
  - Network Address Translation (NAT)
  - Stateful inspection
- Implementations
  - Trusted Information Systems / McAfee Gauntlet
  - Cisco PIX
  - iptables / netfilter



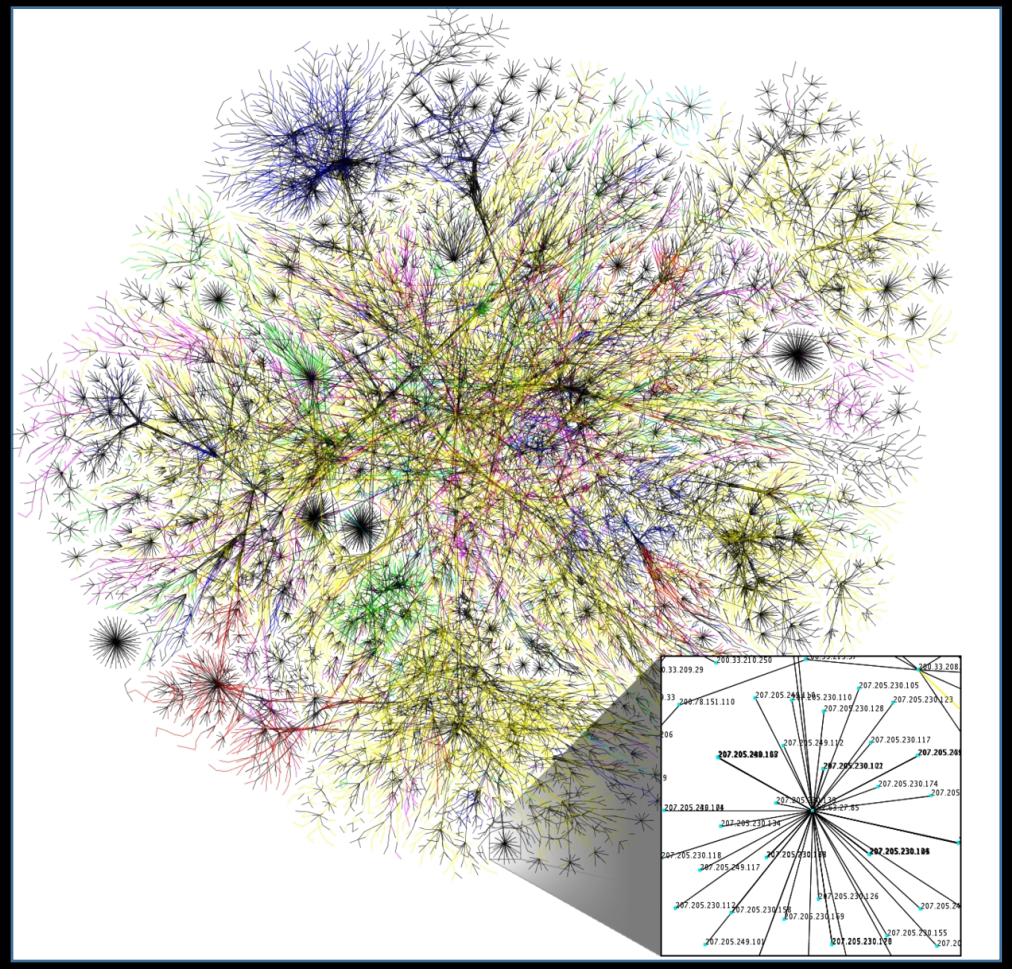
Demilitarized Zone (DMZ)

- Safe zone between
  - Local Area Network (LAN) and Internet Service Provider (ISP)
  - Protects web servers in DMZ
- LAN is behind a second firewall
- Network segmentation is an important countermeasure to prevent attacks from spreading (Target, NotPetya)



2000: Internet explosion – Host-Based / DPI / IDS

- Traditional IP firewalls became less effective
  - Why?
- Host-based firewalls
  - Windows Firewall
  - Mac OSX – application firewall
- Deep packet inspection
  - Web application firewalls
  - Reverse proxies
- Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)



Intrusion detection system (IDS)

- Misuse detection – recognize known bad
- Anomaly detection – distinguish from normal known good
- Does attack detection alarm always indicate something bad?
  - Alarm could be something normal that is confused with an attack (false positive)
  - Silence could indicate that all of your data is being stolen (false negative)
- Detection rate vs false positive rate
  - False positive rate must be extremely low
  - 1% false positive rate on 100,000 daily detections is unusable

Signature detection

- Create a signature (intrusion pattern)
  - Compare to known database
  - Works well for known attacks
- But what about zero-day attack?
  - Let's use machine learning!
- A few requirements
  - Training
  - Detecting
  - Guided by threat intelligence team

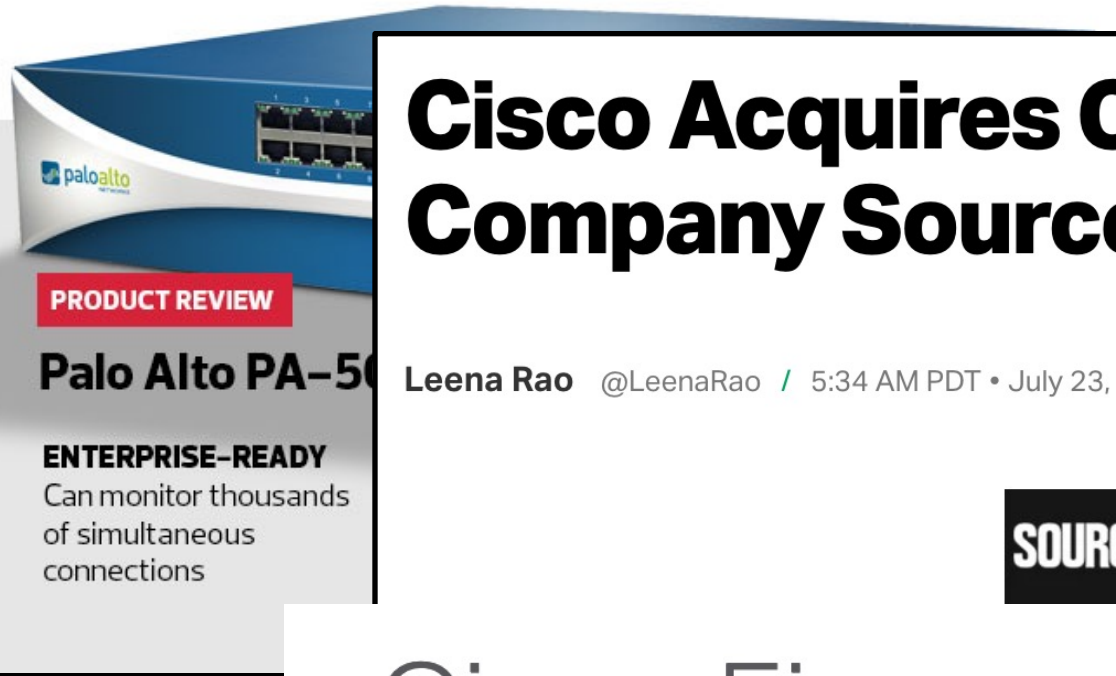
Table 16-1. Cisco Signature Classification Categories

Signature Series	Description
1000	Signatures on IP header rules, which include IP options, IP fragments, and bad or invalid IP packets
2000	Signatures on ICMP packets, which include ICMP attacks, ping sweeps, and ICMP traffic records
3000	Signatures on attacks using TCP, including TCP host sweeps, TCP SYN floods, TCP port scans, TCP session hijacking, TCP traffic records, TCP applications, e-mail attacks, NetBIOS attacks, and legacy web attacks
4000	Signatures on attacks using UDP, including UDP port scans, UDP applications, and UDP traffic records
5000	Signatures on web server and browser attacks using HTTP
6000	Signatures on cross-protocol (multiple-protocol) attacks, including distributed DoS (DDoS) attacks, DNS attacks, Loki attacks, authentication attacks, and RPC attacks
8000	Signatures that look for string matches in TCP sessions/applications
10,000	Signatures that trigger on an ACL violation on a Cisco router (match on a deny statement)

2010: Internet maturity – NGFW

- Next Generation Firewall
  - Converges many of the technologies we discussed
  - Wider range of inspection at the application layer
- Deep packet inspection functionality includes:
  - Web filtering
  - Intrusion prevention systems
  - User identity management
  - Web application firewall

Cisco vs Palo Alto Networks: Top NGFWs Compared



Cisco Acquires Cybersecurity Company Sourcefire For $2.7B

Leena Rao @LeenaRao / 5:34 AM PDT • July 23, 2013

Comment

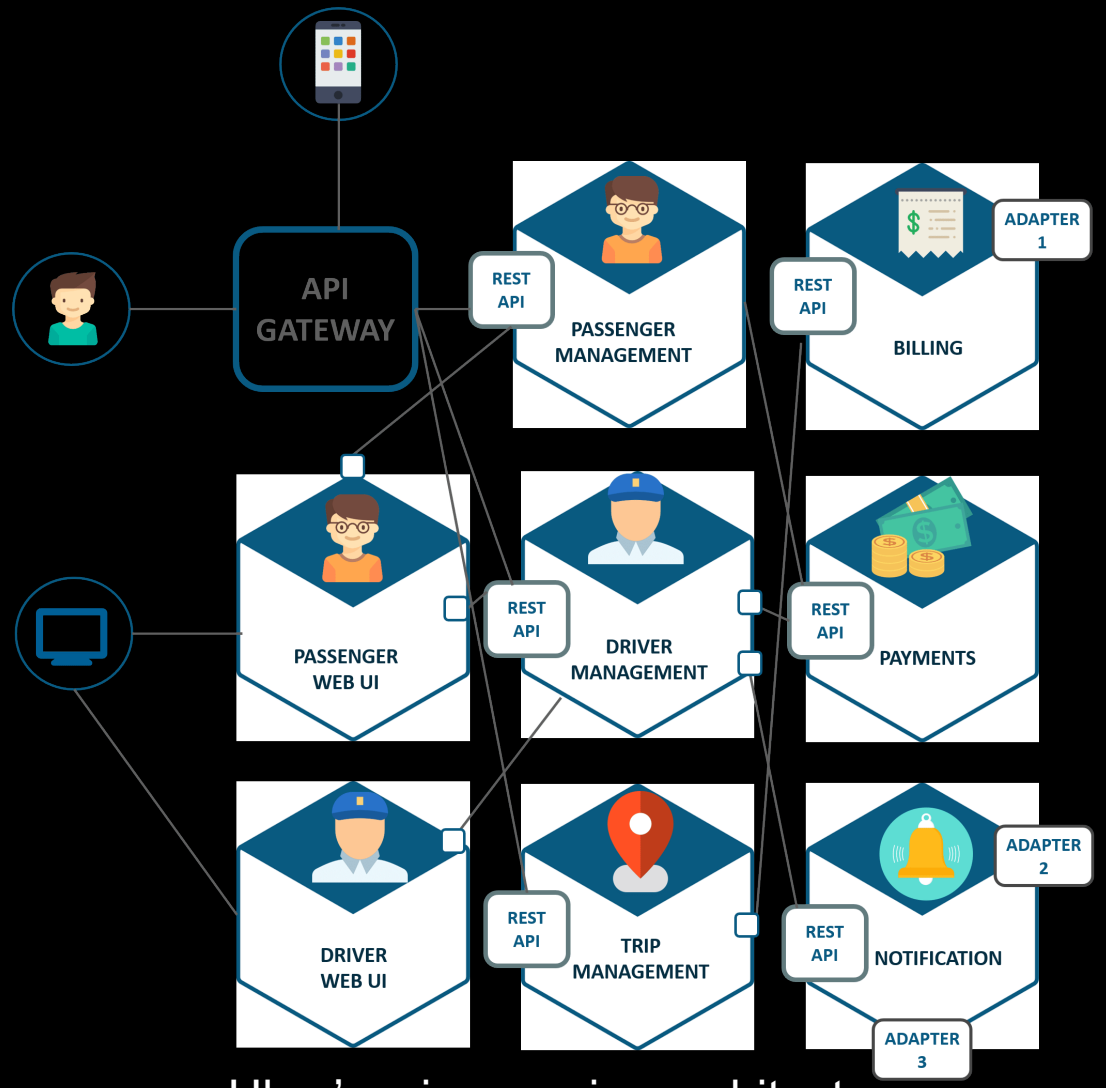
Linkedin Email Print

SOURCEfire

Cisco Firepower 4100 Series

2020: Cloud and workloads – FWaaS

- Disappearance of the perimeter
  - Where does the firewall go?
- Expansion of cloud-deployed firewalls -- firewalls as a service
  - Use of hardware firewalls is rapidly declining
- DevSecOps
  - Moving this functionality into the container workload
  - Full circle – security is moving from network back into the application!



Uber's microservice architecture

What we discussed

- OSI stack and IP hourglass
- Layer 2
  - MAC impersonation
  - ARP poisoning
- Layer 3
  - IP hijacking
  - Replay
  - ICMP
  - Tor
- Layer 4
  - TCP
- Firewalls
  - IP filtering
  - DMZ
  - DPI / IDS / IPS
  - NGFW
  - FWaaS

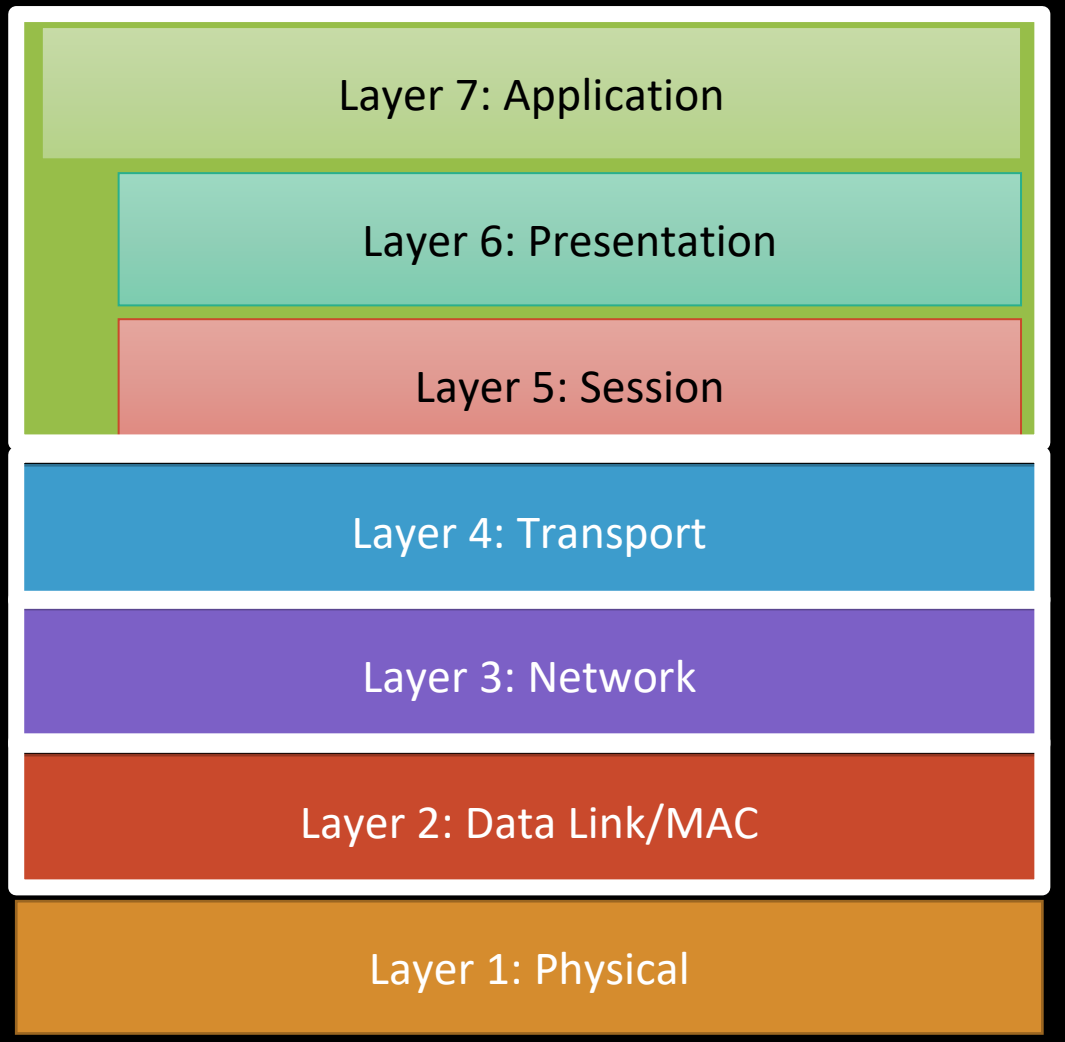
What's next

- Module 7 Network Security – continued
- Readings
  - Anderson Chapter 21 on Network Attack and Defence (especially 21.2 Network protocols and service denial; 21.4 Defense against network attack; 21.5 Cryptography: the ragged boundary)
- You should be working on 7 Lab Network Security due next Tuesday
- #breach-of-the-week – participate on slack!
- Office hours Thurs 11:00am-12:00pm in 192-333 or M/W/F on zoom

Breach of the Week!

Network security topics

- Layer 2: Data Link / MAC
- Layer 3: IP, ICMP, Tor
- Layer 4: TCP
- Firewalls: IP, DMZ, IDS / IPS, NGFW
- VPNs: IPsec
- TLS
- DNS
- Bots

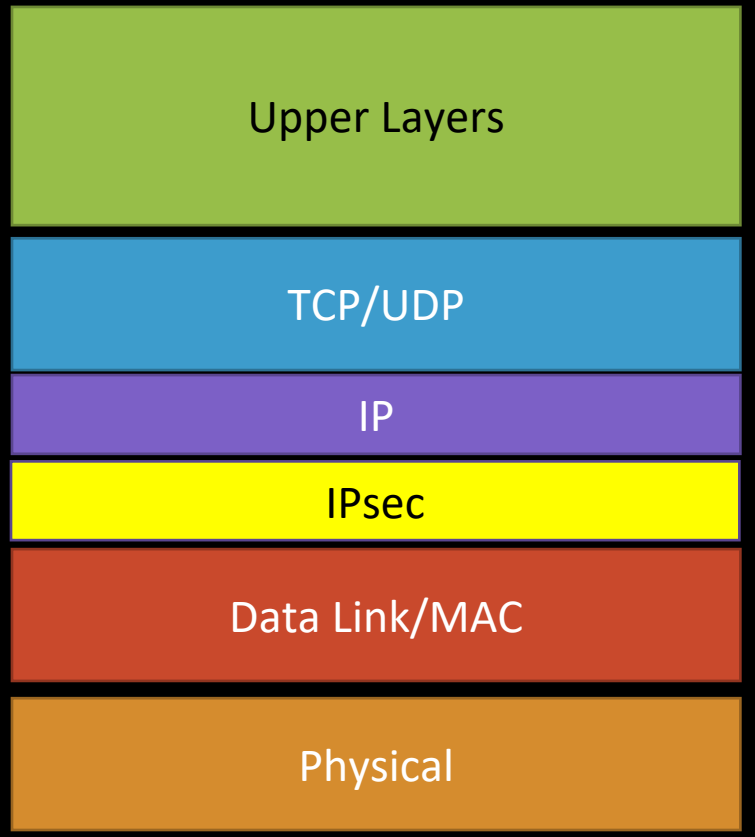


Virtual Private Networks (VPNs)

- VPNs provide distributed hosts a common logical network over an unsecure network
  - Enable employee telecommute into the LAN
  - Connect multiple locations
  - Secure user access out to the internet
- VPN service requirements
  - User authentication (mutual authentication) – why?
  - Address management across VPN connections
  - Data encryption for tunneling – data and addresses
  - Integrity
  - Key management
  - Multiprotocol support
  - Many firewalls have VPN capabilities built-in

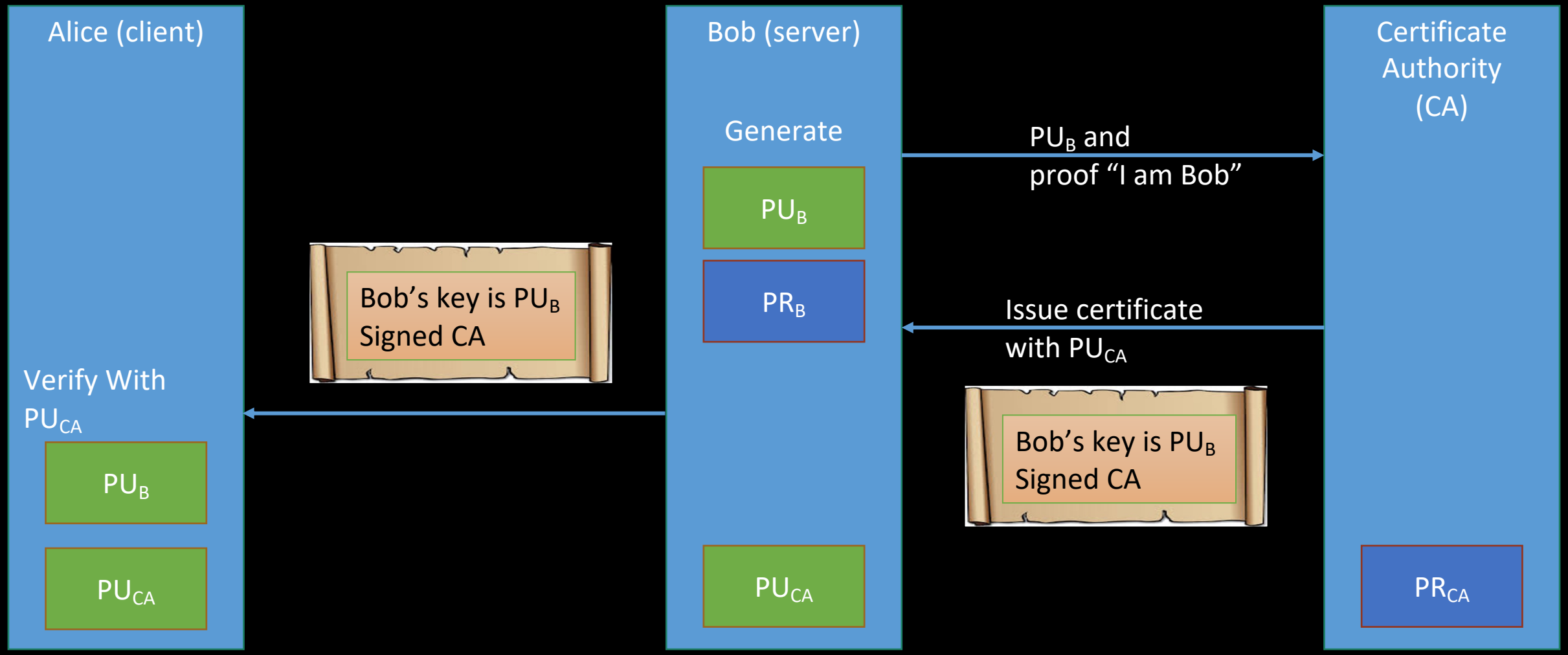
VPN – Internet Protocol Security (IPsec)

- IPsec is a common protocol for VPNs
  - Provides confidentiality and authenticity on IP packets
- Hosts can share an address space, even when geographically separate
- Sits below transport layer, transparent to applications over a lossy network
  - Supports UDP, TCP, DNS, HTTP, FTP, SNMP,…



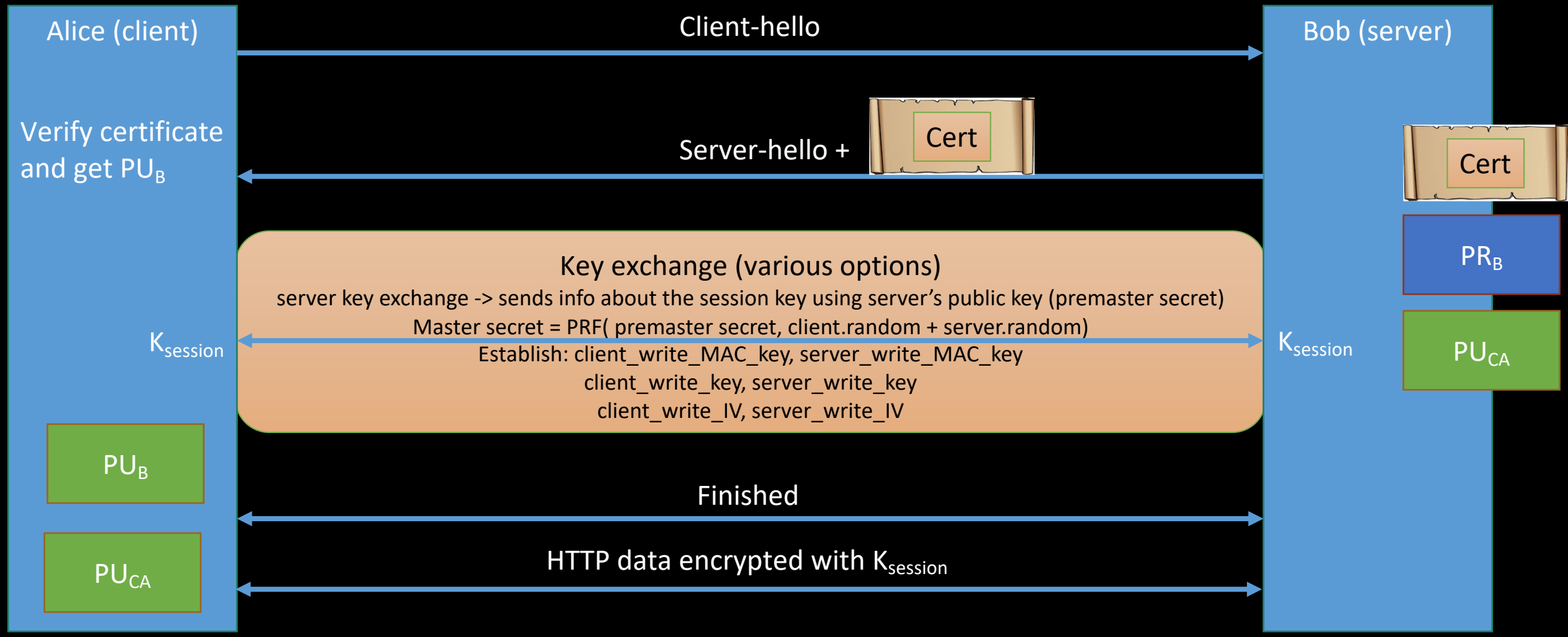
Public-key certificates

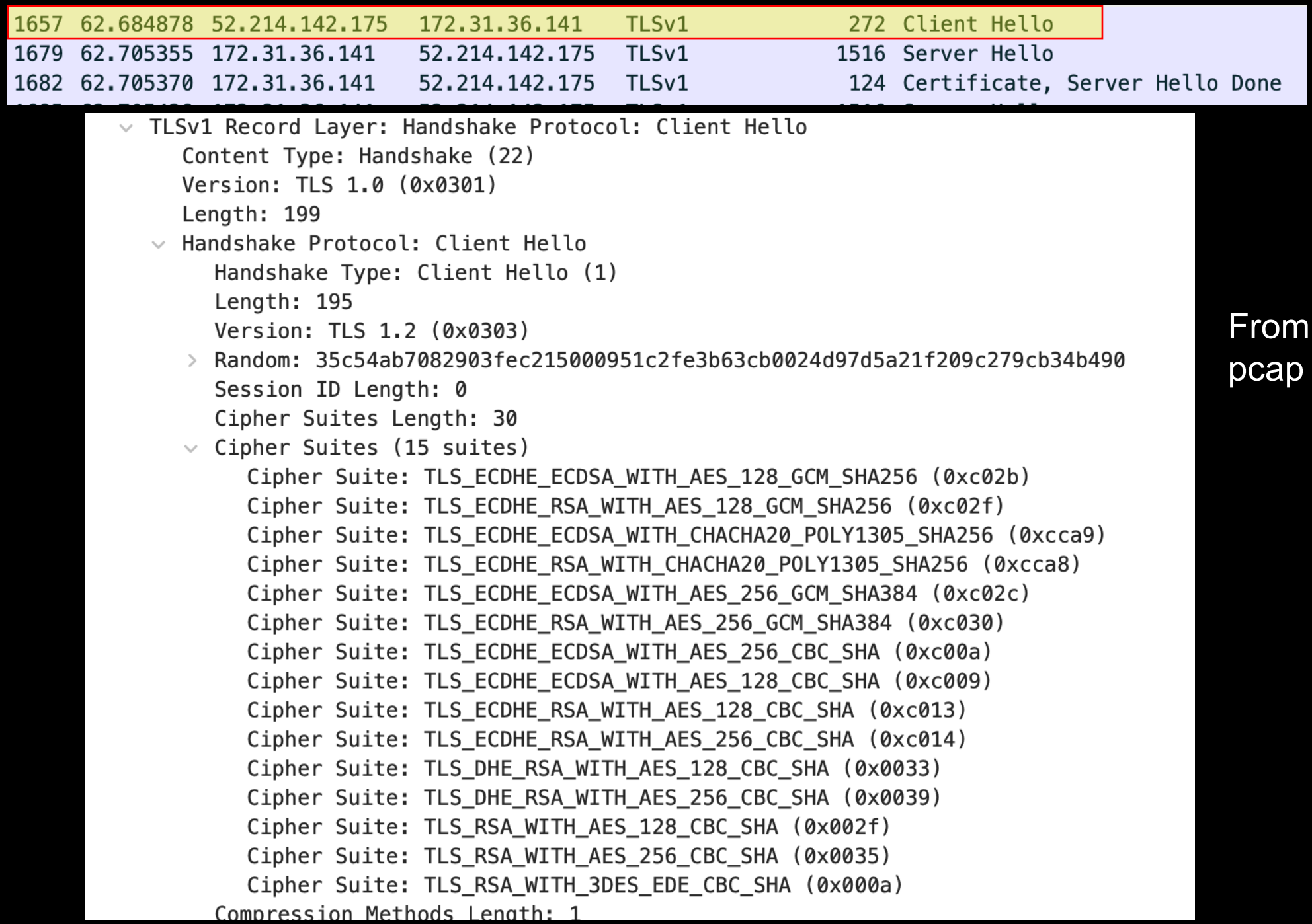
Bob's certificate is used for a long time (a year) to prove he owns PU_B



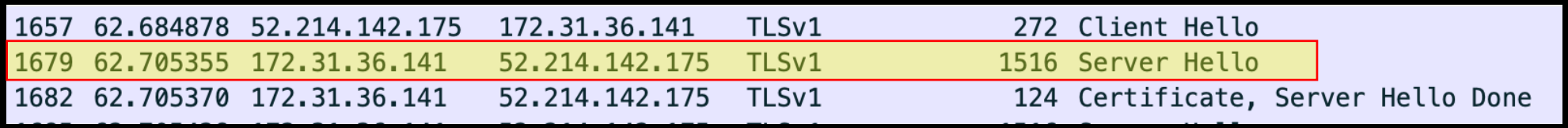
Transport Layer Security (TLS/SSL)

Enables tunnel between server and client to avoid network attacks

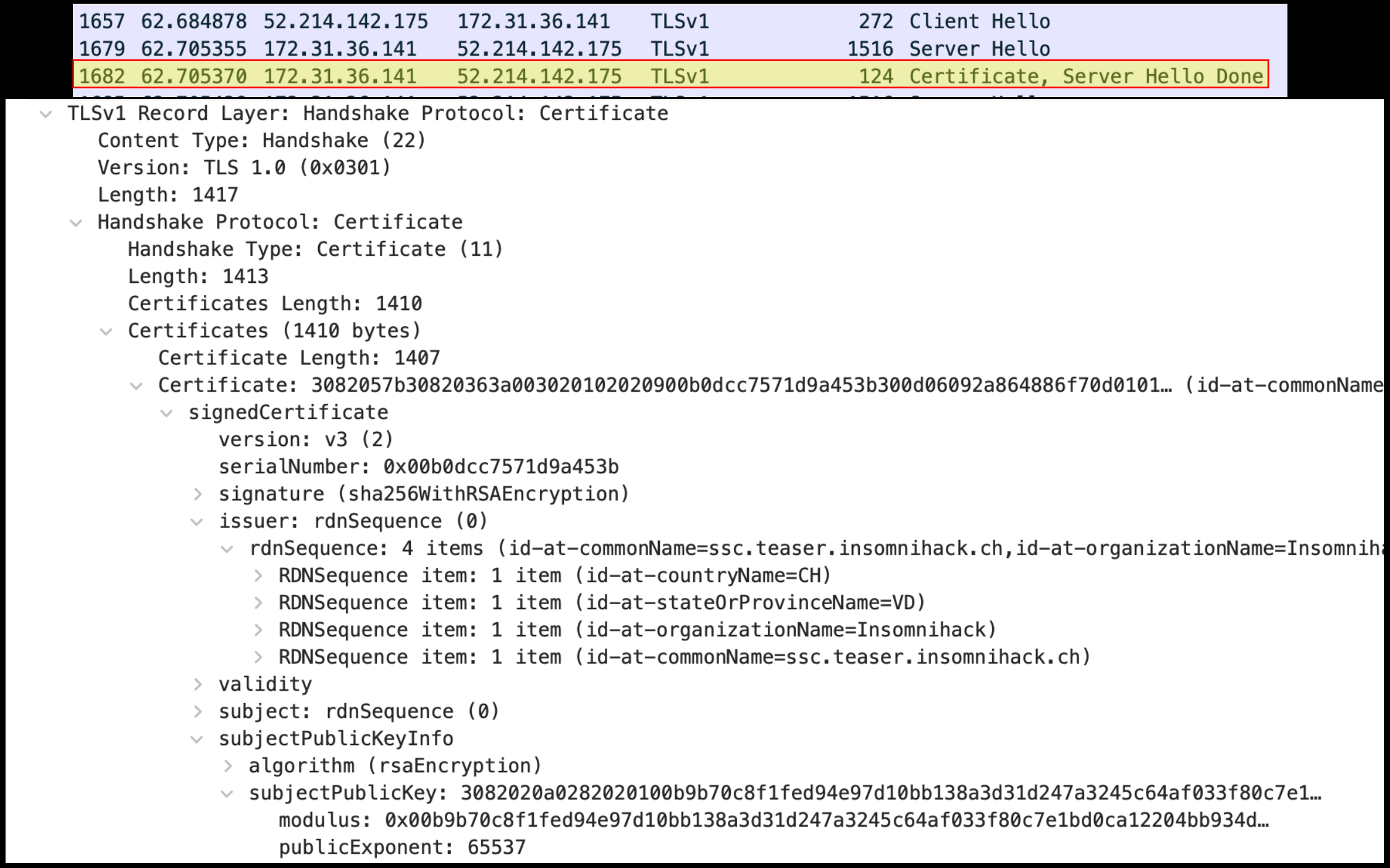




From medium-1 pcap


1657 62.684878 52.214.142.175 172.31.36.141 TLSv1 272 Client Hello
1679 62.705355 172.31.36.141 52.214.142.175 TLSv1 1516 Server Hello
1682 62.705370 172.31.36.141 52.214.142.175 TLSv1 124 Certificate, Server Hello Done


TLSv1 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 96
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 92
Version: TLS 1.0 (0x0301)
Random: c6c2ecff443adf2dddeba3cae3992fbc9cf02ba29a01409aec019946305b74e4
Session ID Length: 32
Session ID: 7240e005d984c74bc7d5213fed945bb91f39e49c413123ab17fd3bc927fb0dcd
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
Compression Method: null (0)


1657 62.684878 52.214.142.175 172.31.36.141 TLSv1 272 Client Hello
1679 62.705355 172.31.36.141 52.214.142.175 TLSv1 1516 Server Hello
1682 62.705370 172.31.36.141 52.214.142.175 TLSv1 124 Certificate, Server Hello Done
TLSv1 Record Layer: Handshake Protocol: Certificate
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 1417
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 1413
Certificates Length: 1410
Certificates (1410 bytes)
Certificate Length: 1407
Certificate: 3082057b30820363a003020102020900b0dcc7571d9a453b300d06092a864886f70d0101… (id-at-commonName
signedCertificate
version: v3 (2)
serialNumber: 0x00b0dcc7571d9a453b
signature (sha256WithRSAEncryption)
issuer: rdnSequence (0)
rdnSequence: 4 items (id-at-commonName=ssc.teaser.insomnihack.ch,id-at-organizationName=Insomnih
RDNSequence item: 1 item (id-at-countryName=CH)
RDNSequence item: 1 item (id-at-stateOrProvinceName=VD)
RDNSequence item: 1 item (id-at-organizationName=Insomnihack)
RDNSequence item: 1 item (id-at-commonName=ssc.teaser.insomnihack.ch)
validity
subject: rdnSequence (0)
subjectPublicKeyInfo
algorithm (rsaEncryption)
subjectPublicKey: 3082020a0282020100b9b70c8f1fed94e97d10bb138a3d31d247a3245c64af033f80c7e1…
modulus: 0x00b9b70c8f1fed94e97d10bb138a3d31d247a3245c64af033f80c7e1bd0ca12204bb934d…
publicExponent: 65537

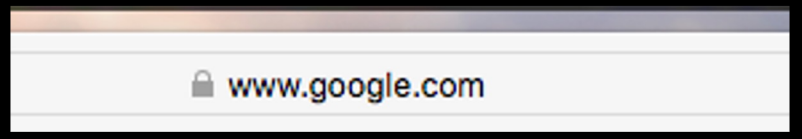
Why don’t we always use HTTPS?

- Slows down web server
- Breaks internet caching
  - What is caching?
  - ISPs can’t cache https traffic
  - Results in increased web traffic
- Breaks virtual hosting (in older browsers)

- There aren’t any good reasons!

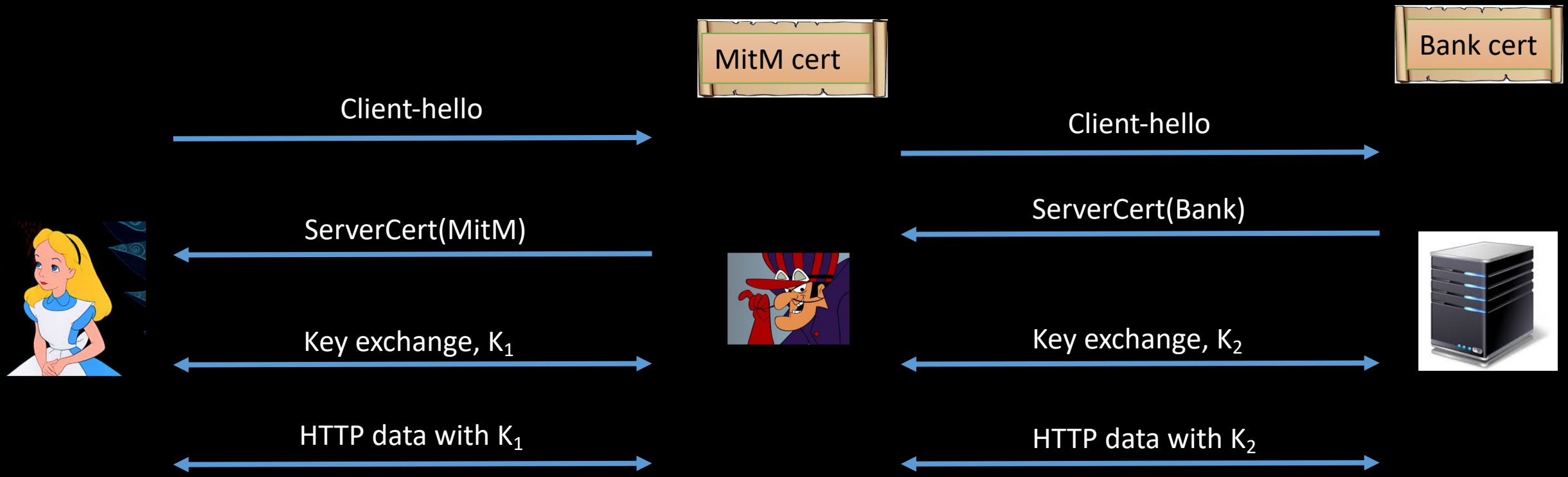
Are you using https?

- How do you know?
  - Lock icon
  - HTTPS instead of HTTP (if shown)
- Lock icon goal
  - Alert user of page origin
  - Indicate lack of network attacker
- Reality?
  - Lots of problems
  - Are you on the right website?
  - Typosquatting – gooogle.com



Man-in-the-Middle (MitM) – For good or evil

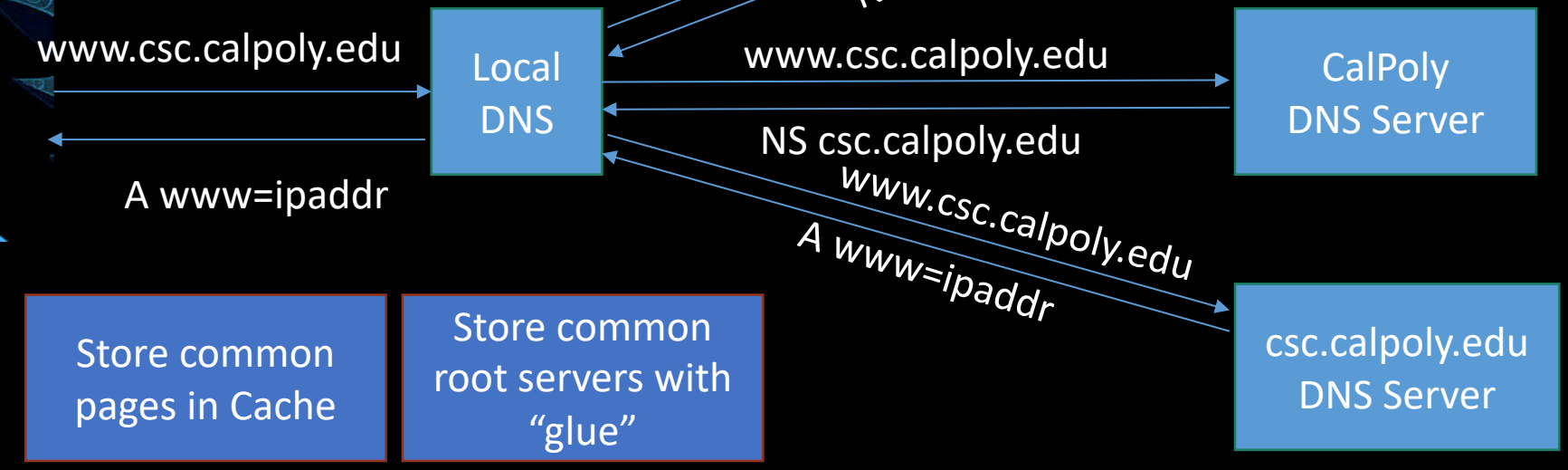
- Attacker proxies data and observes everything
- Could be a trusted proxy or an evil impersonator using invalid cert (expired, wrong domain, unknown CA)



Domain Name System (DNS)

- Goal: map between host name (csc.calpoly.edu) and IP address (129.65.180.125)
  - Why can't you use IP addresses?
- Strategy – recursively map between servers
- Local DNS assigned with DHCP

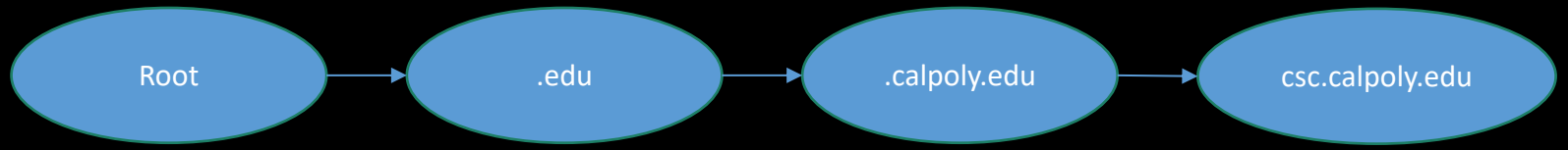
DHCP: Dynamic Host Configuration Protocol
NS: Name server
A: Address record
ICANN manages top level domains



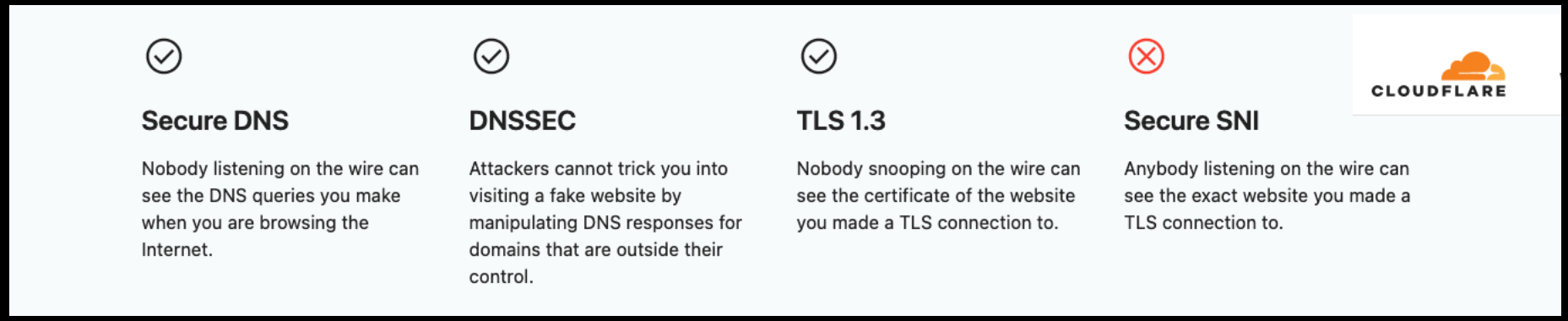
DNS attacks

- No authentication
  - Spoofing is possible
  - All hope is lost!
- Cache is critical
  - can be poisoned
  - Slow flushing
- Bypass browser same origin policy (SOP) – port / protocol / *hostname*
- DNS allows for “mapping” the network
  - Opens vulnerabilities to DoS

DNS security



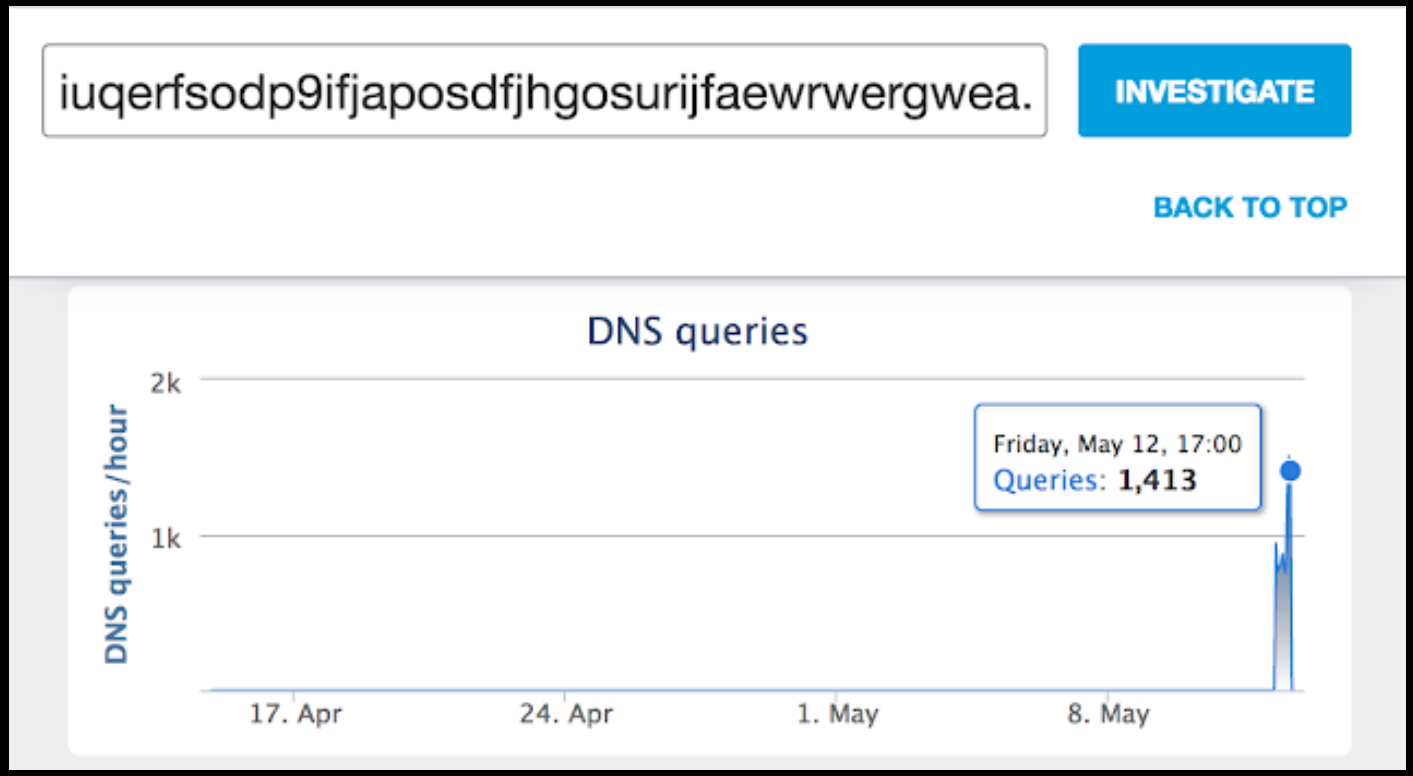
- DNS Security Extensions (DNSSec)
  - Public-key based solution to verifying integrity and authenticity
- DNS over TLS (DoT)
  - DNS - TLS - UDP (Port 853)
- DNS over HTTPS (DoH)
  - DNS - HTTP - TLS - TCP (Port 443)
  - Default in many browsers



SNI – Server Name Indication

Securing DNS vs DNS for security

- We've talked about how to make DNS secure
- But there is a deeper story:
  - DNS plays an important role in securing organizations
- Critical policy enforcement point
  - Stop typosquatting
- Visibility and intelligence



https://blog.talosintelligence.com/2017/05/wannacry.html

Free and Public DNS Servers

Updated list of the best publicly available and free DNS servers

By Tim Fisher · Updated on May 3, 2022 · Reviewed by Chris Selph

Best Free & Public DNS Servers		
Provider	**Primary DNS**	**Secondary DNS**
Google	8.8.8.8	8.8.4.4
Quad9	9.9.9.9	149.112.112.112
OpenDNS Home	208.67.222.222	208.67.220.220
Cloudflare	1.1.1.1	1.0.0.1
CleanBrowsing	185.228.168.9	185.228.169.9
Alternate DNS	76.76.19.19	76.223.122.150
AdGuard DNS	94.140.14.14	94.140.15.15

Press Release

Cisco Announces Intent to Acquire OpenDNS

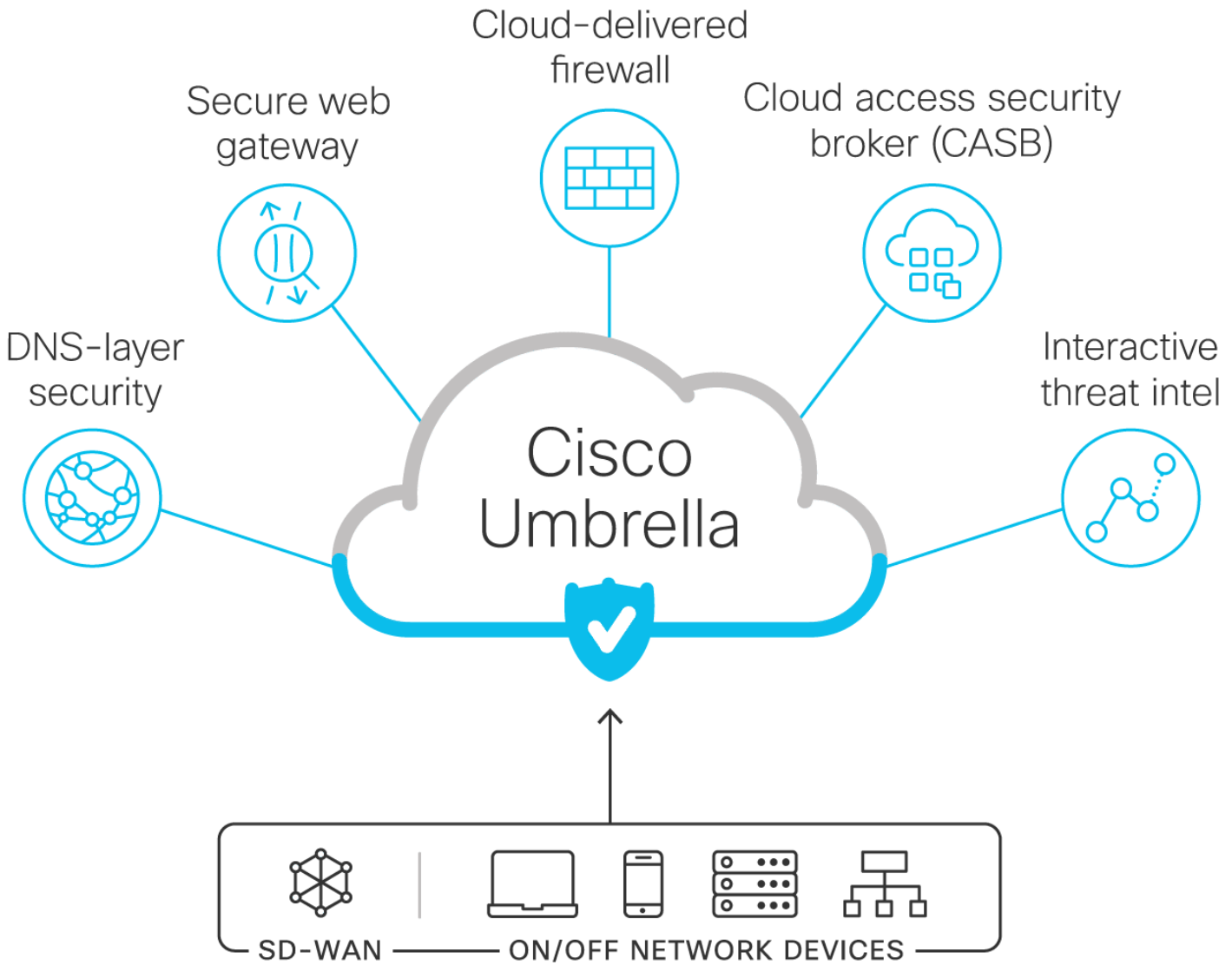
Cisco To Buy Cloud Security Company OpenDNS for $635M In Cash

Ron Miller @ron_miller / 5:51 AM PDT • June 30, 2015

Comment

Secure Access Service Edge (SASE)

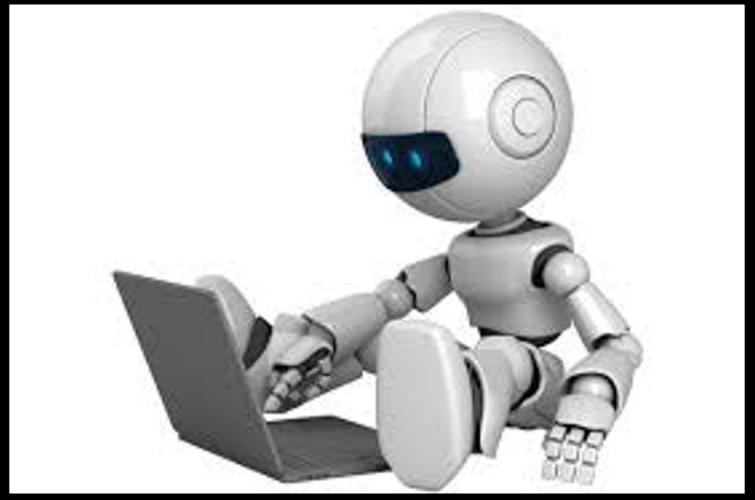
Multiple security functions in a single cloud security service



Moving security from on-premise hardware to the cloud

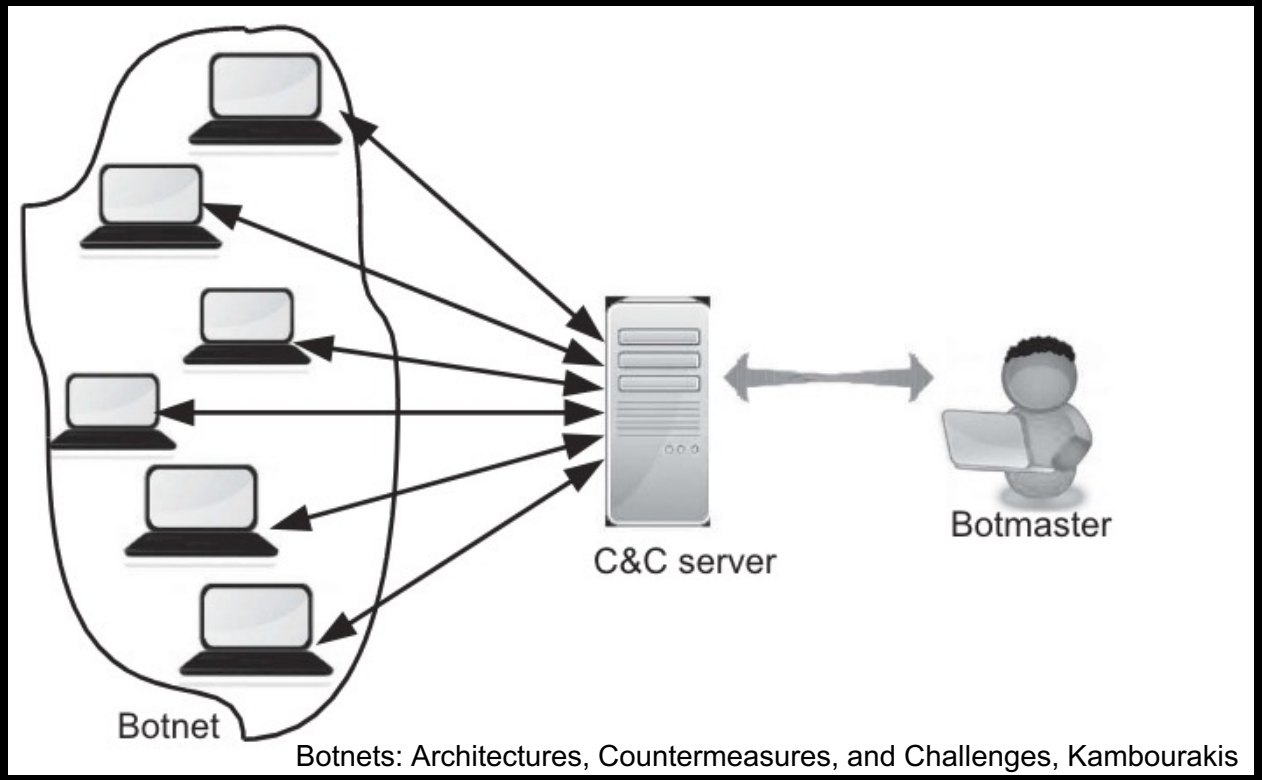
Zombies and bots

- Zombie as botnet node
- Infected machines wait for commands
- Commands can have various effects
  - Can be rented out as a service



Command and Control (C&C)

- Historically low security
- Now using better security, including encryption
- Why would botmaster use proxy?
- Generally polling
  - Why?



Botnets: Architectures, Countermeasures, and Challenges, Kambourakis

Bot tasks

- Fraudulent applications for financial aid!
- Ransomware
- Information Stealing
- Phishing and Spam Proxying
  - Avoids detection by coming from multiple IP address
- Pirated Hosting
- Distributed denial-of-service (DDoS) attack services
- Mining Bitcoin
  - How would you detect?
  - How would avoid detection?
- Recruiting – getting more bots

Example bots since 2010

2010 (around)		TDL4	4,500,000[66]
		Zeus	3,600,000 (US only)[67]
2010	(Several: 2011, 2012)	Kelihos	300,000+
2011 or earlier	2015-02	Ramnit	3,000,000[68]
2012 (Around)		Chameleon	120,000[69]
2016 (August)		Mirai	380,000
2014		Necurs	6,000,000

Wikipedia

Mirai

- Mirai and Minecraft
- Looks for default userid/pw in Linux-based Internet of Things (IoT) devices: webcams, home routers
- Mostly for DDoS
  - 1 Tbit/sec volumetric attack!!
- Extended for other uses
  - Bitcoin mining

GARRETT M. GRAFF BACKCHANNEL DEC 13, 2017 3:55 PM

How a Dorm Room *Minecraft* Scam Brought Down the Internet

A DDoS attack that crippled the internet wasn't the work of a nation-state. It was three college kids working an online gaming hustle.

What makes bot defense hard?

- Scale
- Anonymity – Tor
- International
- How do you stop a DDoS attack?
- How do you handle infected nodes?
  - Humans are awful at patching

What we discussed

- VPNs
  - IPsec
- TLS
  - https
  - MitM
- DNS
  - DNSSec
  - DoT / DoH
  - Evolution of security to SASE
- Zombies and bots

What's next

- Module 8 Web Security
- Readings
  - Sessions and cookies
  - Cross-Site Scripting (XSS)
  - Cross-Site Request Forgery (CSRF)
  - CSRF defenses
  - Server side request forgery (SSRF)
  - Structured Query Language (SQL) Injection
  - SQL injection defenses
- Quiz 7, 7 Lab Network Security due on Tuesday
- #breach-of-the-week – participate on slack!
- Office hours Thurs 11:00am-12:00pm in 192-333 or M/W/F on zoom