PRACTICAL NETWORK SECURITY PART 2

Kunwadee Sripanidkulchai, Ph.D.

kunwadee (AT) cp.eng.chula.ac.th

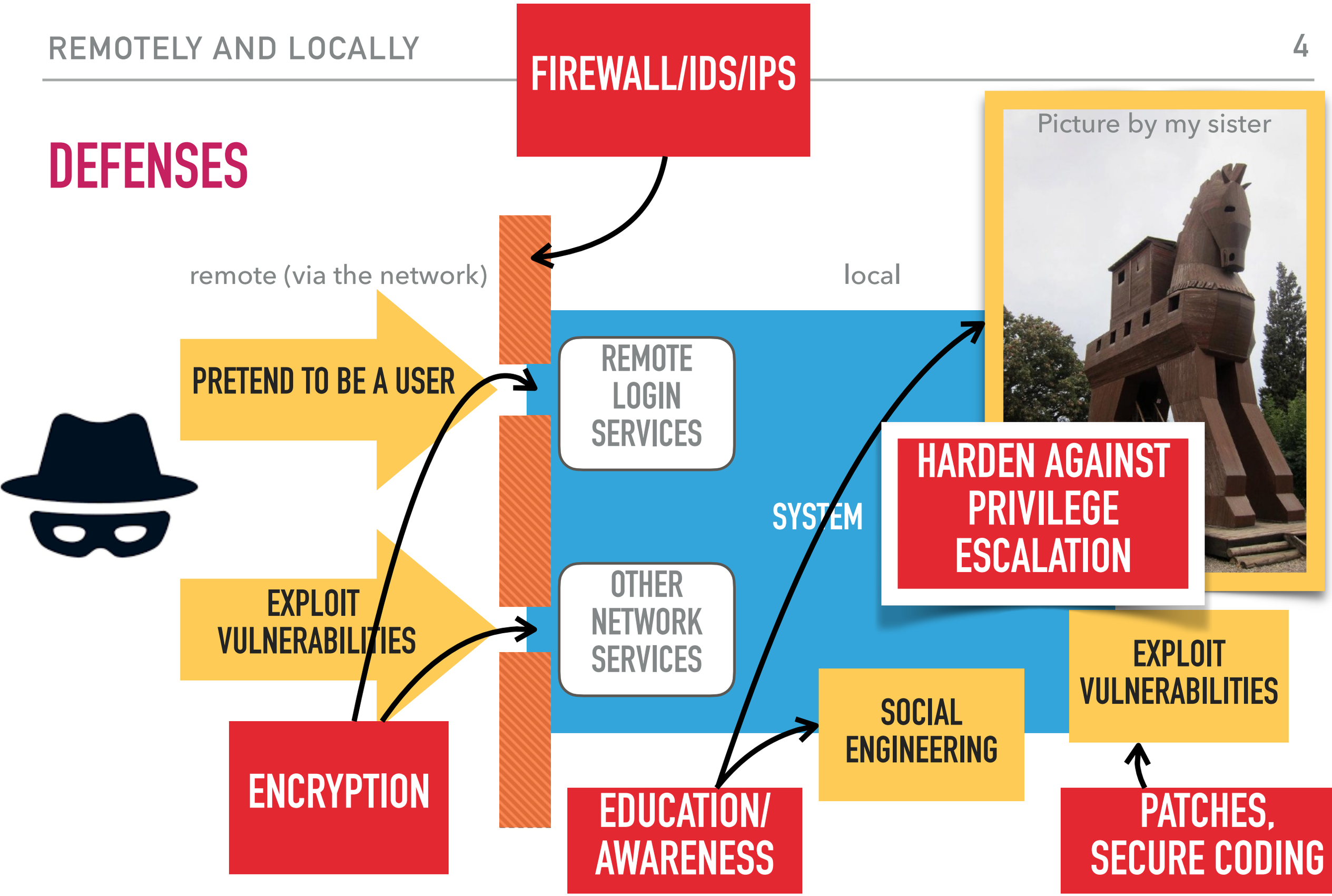
RECAP LAST WEEK'S ACTIVITY

- Recon
  - Social engineering
  - nmap
- Prevention of recon

ACTIVE OS FINGERPRINTING: HOW

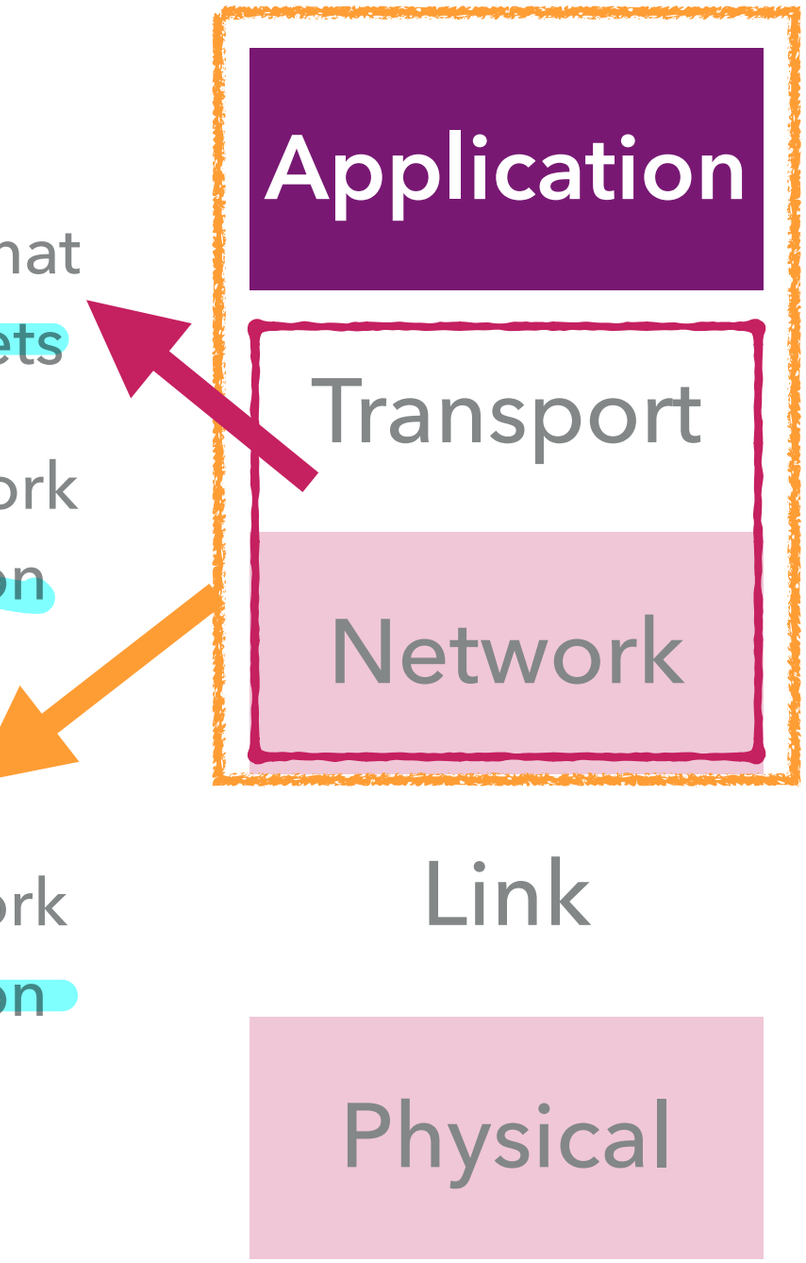
- Different OS's have different TCP/IP behavior
- Send the target a bunch of 'crafted' TCP packets and observe the response
- Map back to known fingerprints to determine OS

DEFENSES


FIREWALL/IDS/IPS
remote (via the network)
local
PRETEND TO BE A USER
REMOTE LOGIN SERVICES
SYSTEM
OTHER NETWORK SERVICES
EXPLOIT VULNERABILITIES
ENCRYPTION
EDUCATION/ AWARENESS
SOCIAL ENGINEERING
HARDEN AGAINST PRIVILEGE ESCALATION
EXPLOIT VULNERABILITIES
PATCHES, SECURE CODING
Picture by my sister

FIREWALL VS. INTRUSION DETECTION SYSTEM VS. INTRUSION PREVENTION SYSTEM

- Firewall: Analyze packet headers for IP addresses (network layer) and port numbers (transport layer) that match pre-configured rules to DROP/ACCEPT packets
- IDS: Analyze packet headers for IP addresses (network layer), port numbers (transport layer), and application data (application layer) that match rules and generates logs of the event
- IPS: Analyze packet headers for IP addresses (network layer), port numbers (transport layer), and application data (application layer) that match rules and DROP packets that match



FIREWALL EFFECTIVENESS IS LIMITED

- Firewalls are a partial fix, but widely used.
- Issue: adversary may be within firewalled network.
- Issue: hard to determine if packet is "malicious" or not.
- Issue: even for fields that are present (src/dst), hard to authenticate.
- TCP/IP's design not a good match for firewall--like filtering techniques.
  - E.g., IP packet fragmentation: TCP ports in one packet, payload in another.

Keep in mind....

SECURITY PROBLEM

INHERENT IN THE DESIGN

"PROTOCOL-LEVEL PROBLEM" VS.

IMPLEMENTATION PROBLEM "BUG"

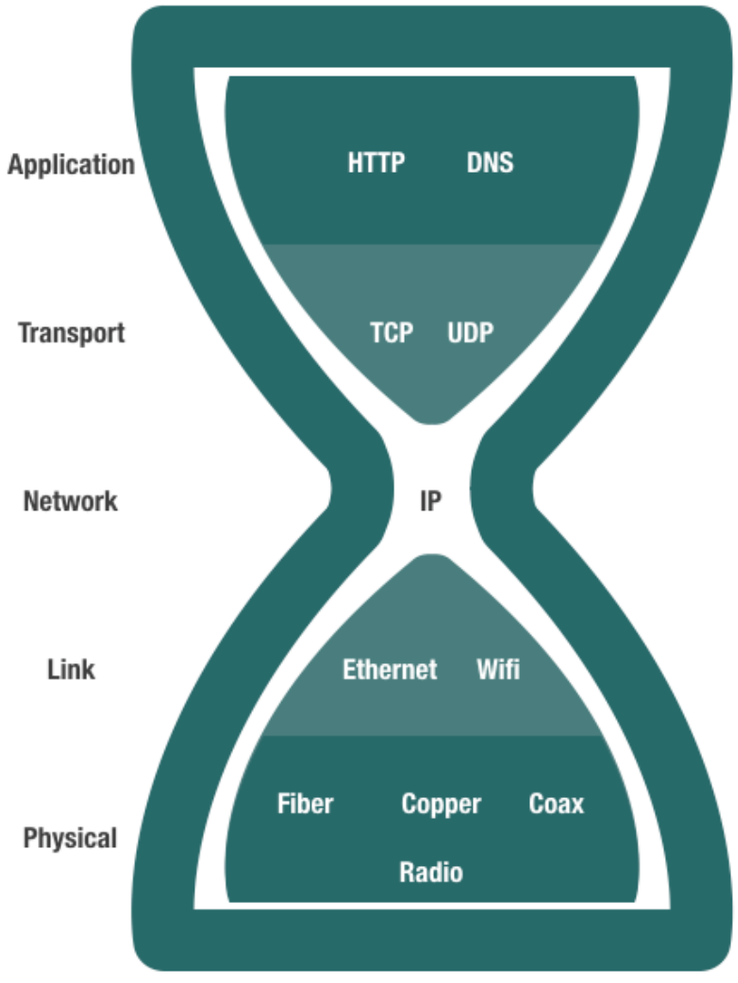
kunwadee (AT) cp.eng.chula.ac.th

THREAT MODEL FOR NETWORK SECURITY

- Adversary can intercept / modify network traffic.
- Adversary can send packets.
- Adversary has full control of their own machines.
- Adversary can participate in protocols (usually).
  - Often not feasible to keep bad guys out of a large system.

TRANSPORT LAYER

Properties	UDP	TCP
Connections		
Packet boundary		
Reliability		
Ordering		
Broadcast		

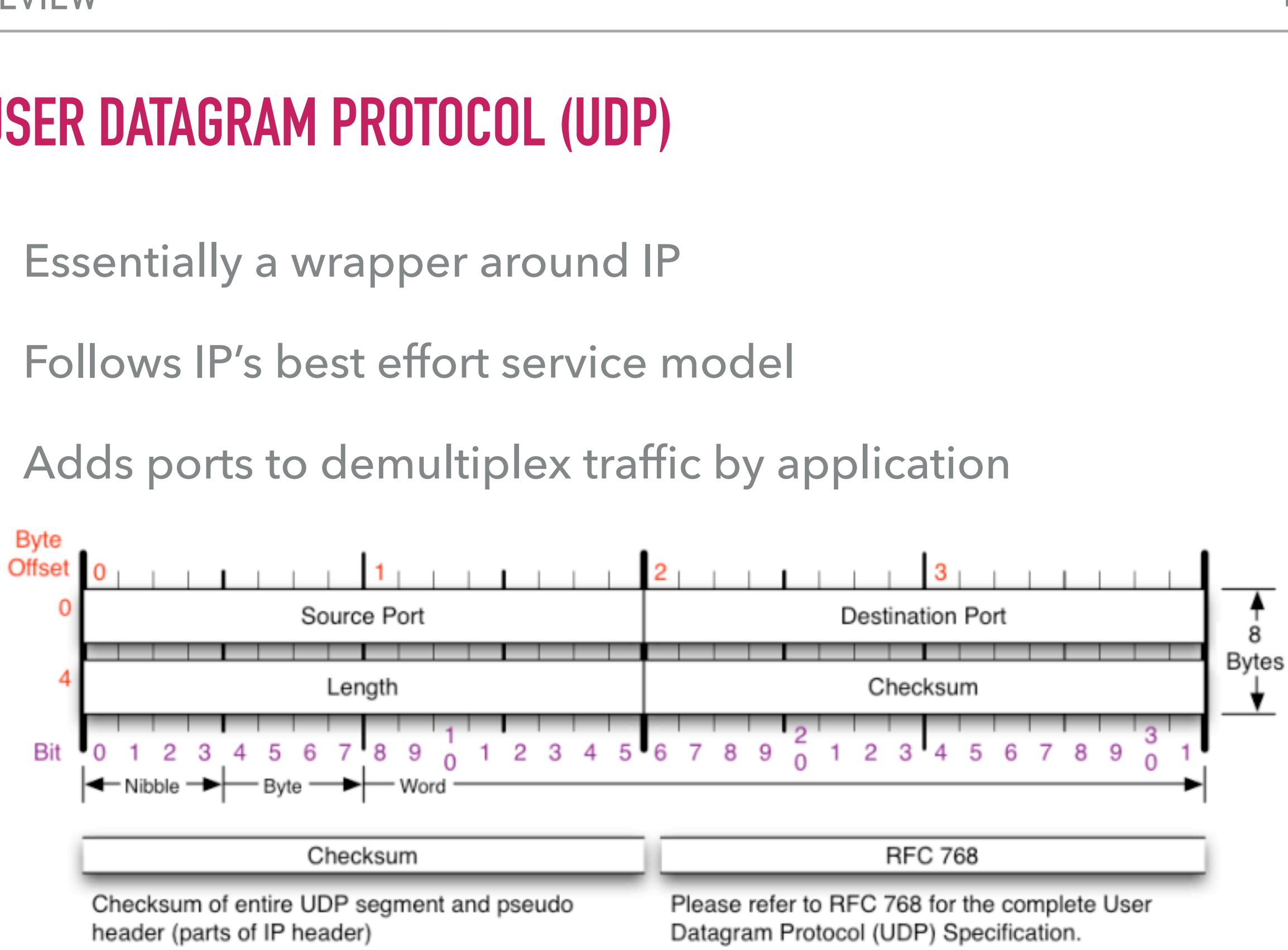


PORT NUMBERS

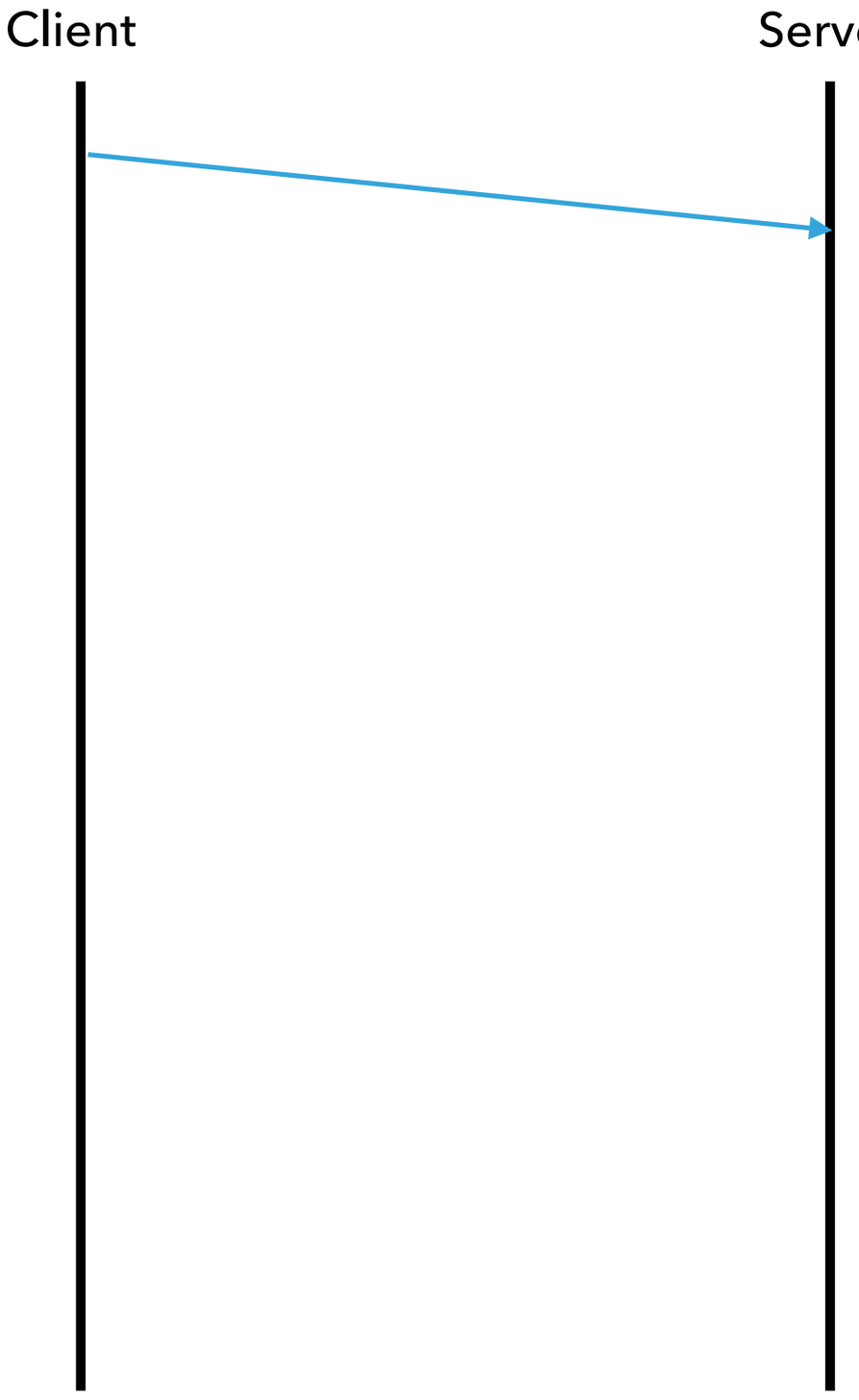
- Each application (e.g., HTTP server) on a host is identified by a port number
  - IP address is the address of the host
  - Port number identifies the process (application) running on the host
- TCP connection established between port A on host X to port B on host Y
- Ports are 1–65535 (16 bits)
- Some destination port numbers used for specific applications by convention
  - 80 HTTP (Web)
  - 443 HTTPS (Secure Web)
  - 25 SMTP (mail delivery)
  - 67 DHCP (host config)
  - 22 SSH (secure shell)
  - 23 Telnet

USER DATAGRAM PROTOCOL (UDP)

- Essentially a wrapper around IP
- Follows IP's best effort service model
- Adds ports to demultiplex traffic by application

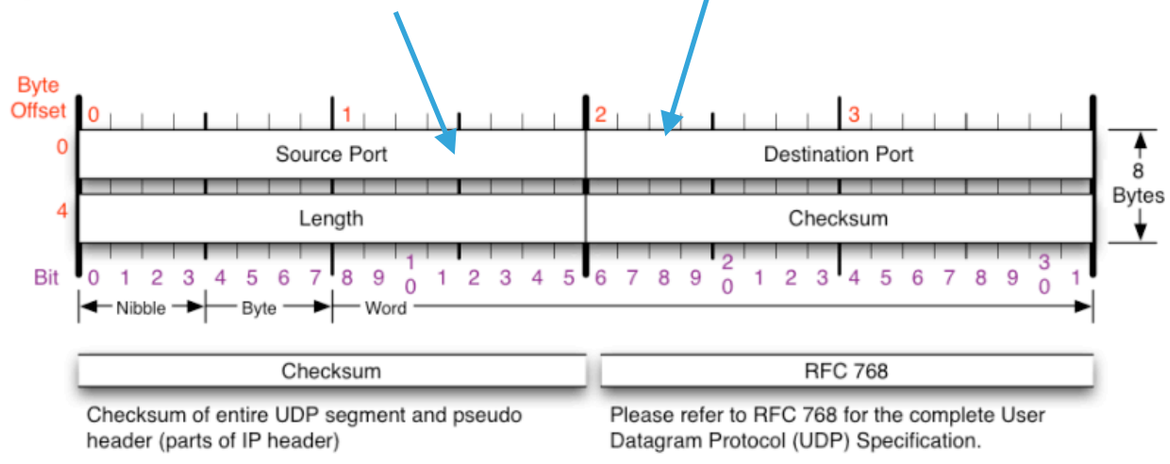


UDP PORT NUMBERS



client's source port number is automatically assigned by the client's OS

server's port number (i.e., port 53)



- Common UDP applications
  - DNS
  - QUIC
  - Streaming/VoIP

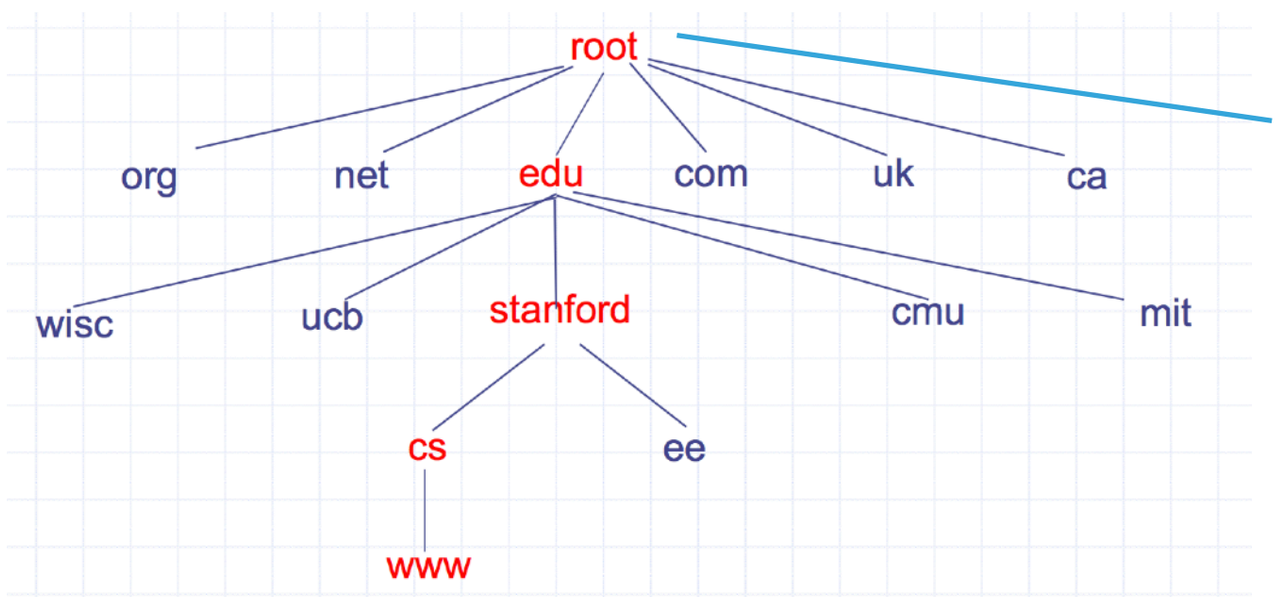
1. DNS CACHE POISONING
2. DNS SPOOFING (KAMINSKY ATTACK)
3. DNS REBINDING
4. DOS/DDOS

UDP KNOWN ISSUES

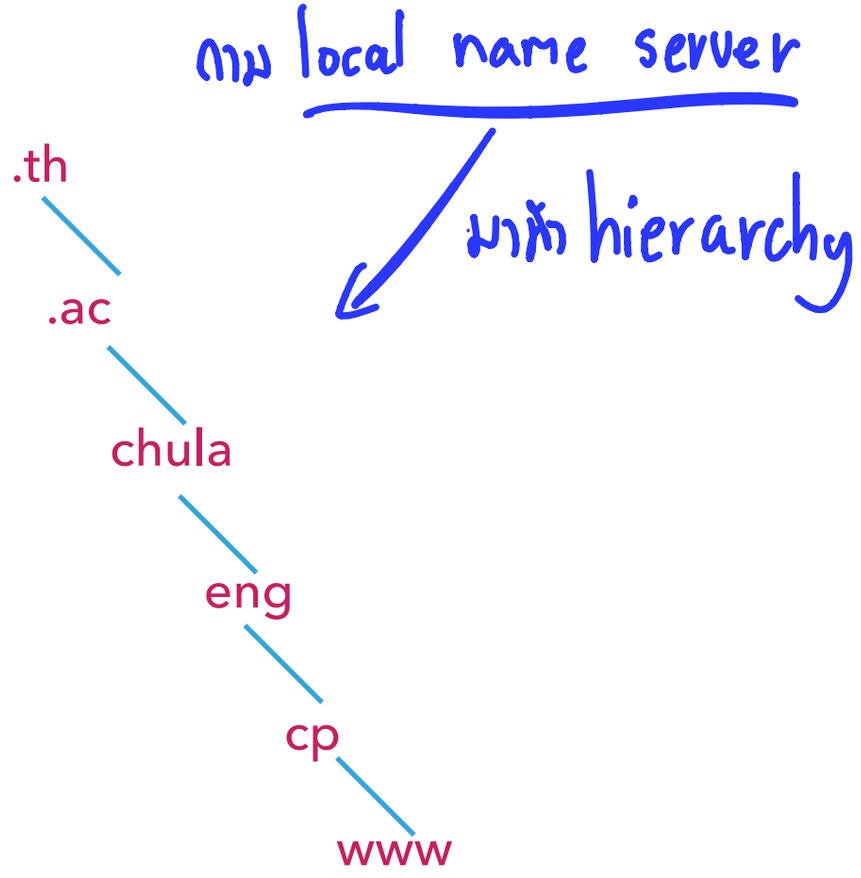
kunwadee (AT) cp.eng.chula.ac.th

DOMAIN NAME SYSTEM (DNS)

- Application-layer protocols (and people) usually refer to Internet host by host name (e.g., google.com)
- DNS is a delegatable, hierarchical name space



www.cs.stanford.edu



www.cp.eng.chula.ac.th

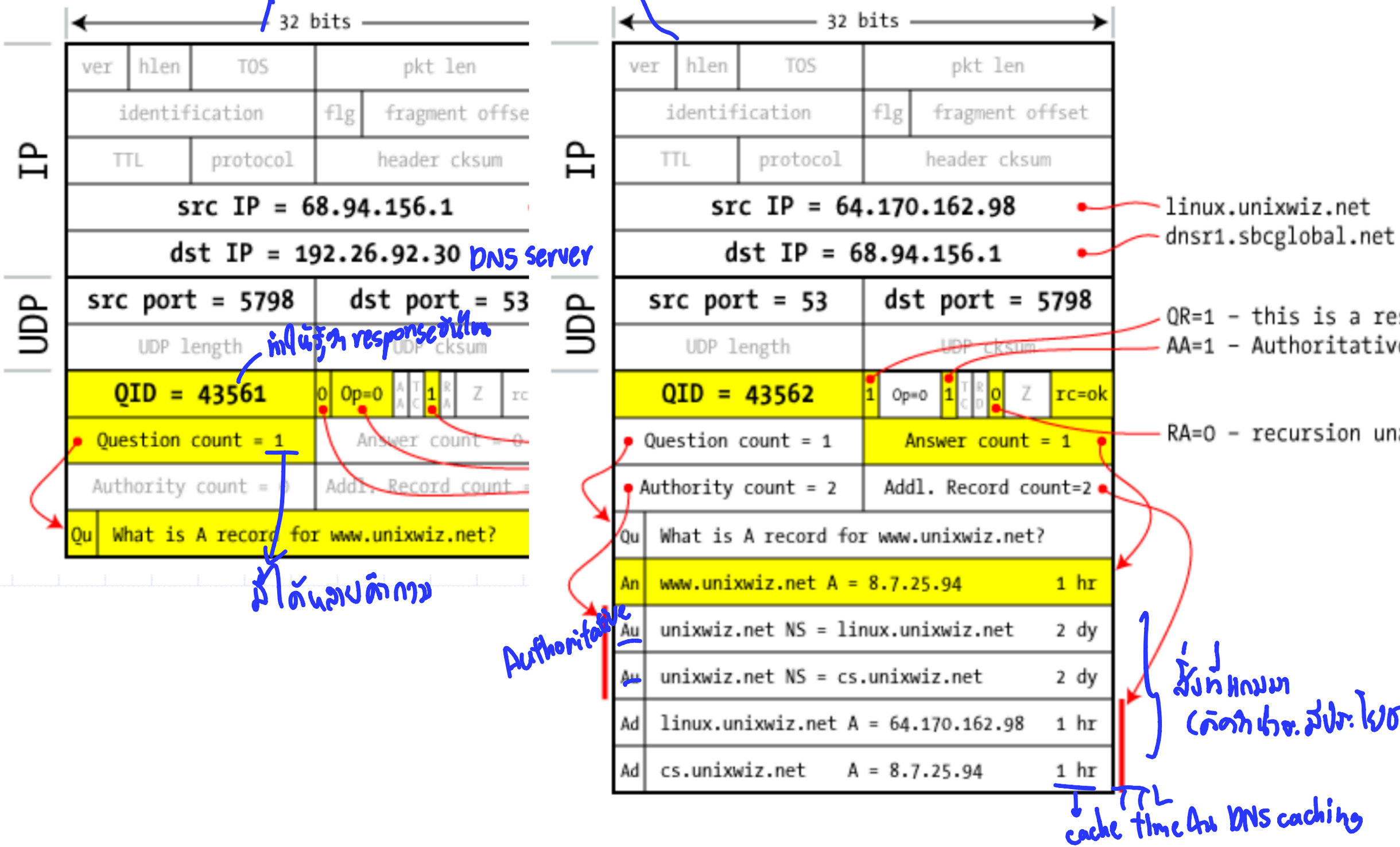
DNS RECORD

- A DNS server has a set of records it authoritatively knows about

```
 % dig chula.ac.th NS

; <<>> DiG 9.10.6 <<>> chula.ac.th NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47829
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;chula.ac.th.           IN NS

;; ANSWER SECTION:
chula.ac.th.    3600  IN NS ns.netserv.chula.ac.th.
chula.ac.th.    3600  IN NS explorer.netserv.chula.ac.th.
```

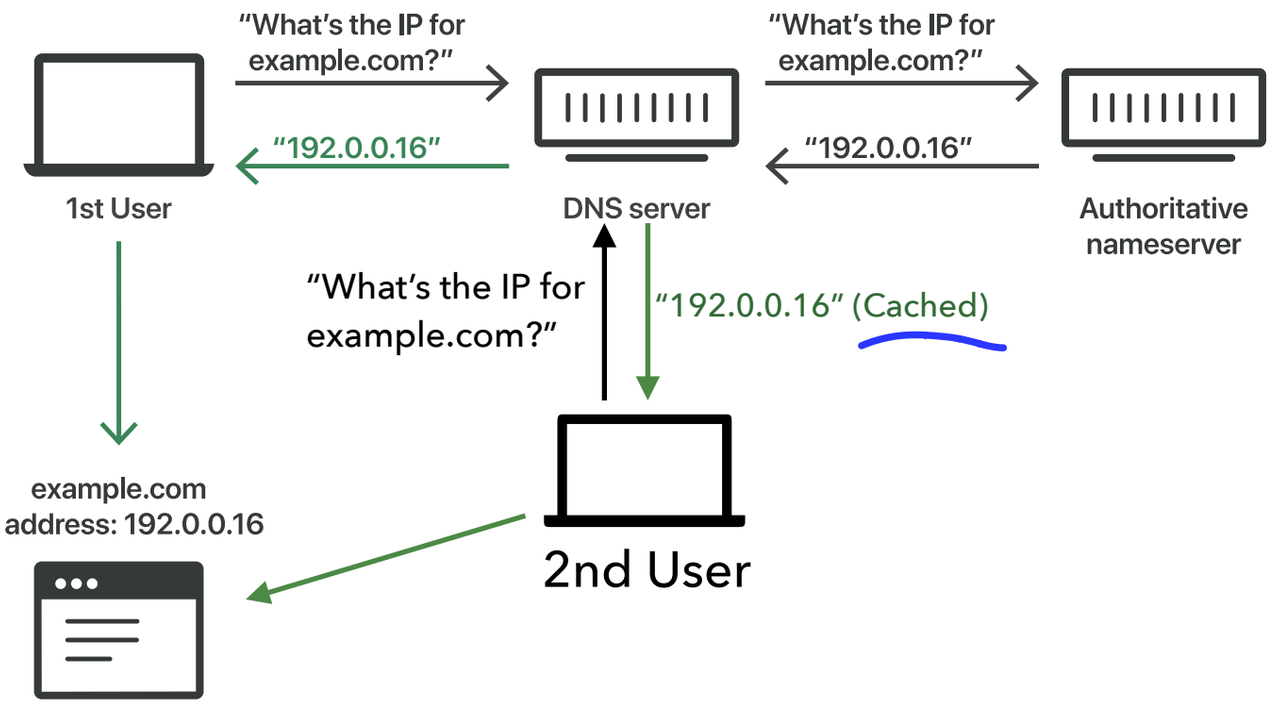
} authoritative

DNS REQUEST AND RESPONSE



DNS CACHING

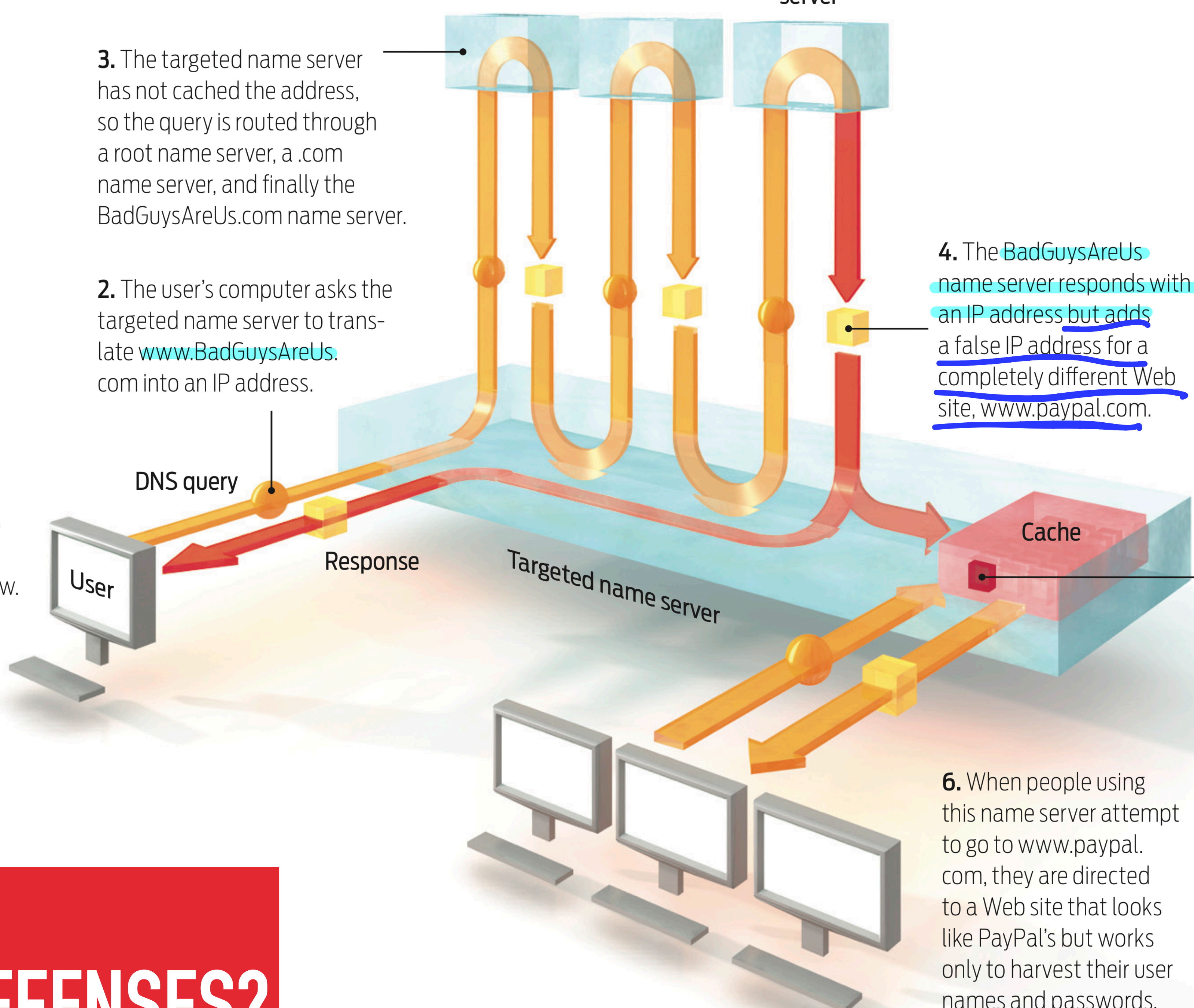
- DNS responses are cached
  - Quick response for repeated translations
  - NS records for domains also cached
- DNS negative queries are cached
  - Save time for nonexistent sites, e.g. misspelling
- Cached data periodically times out
  - Lifetime (TTL) of data controlled by owner of data
  - TTL passed with every record



DNS SECURITY

- Users/hosts trust the host-address mapping provided by DNS
- Used as basis for many security policies: Browser same origin policy, URL address bar
- Interception of requests or compromise of DNS servers can result in incorrect or malicious responses

Early Attack Strategy



1. A user loads a Web page containing an image hosted at www.BadGuysAreUs.com.

2. The user's computer asks the targeted name server to translate www.BadGuysAreUs.com into an IP address.

3. The targeted name server has not cached the address, so the query is routed through a root name server, a .com name server, and finally the BadGuysAreUs.com name server.

4. The BadGuysAreUs name server responds with an IP address but adds a false IP address for a completely different Web site, www.paypal.com.

poisoning

5. The targeted name server stores the false IP address for paypal.com.

6. When people using this name server attempt to go to www.paypal.com, they are directed to a Web site that looks like PayPal's but works only to harvest their user names and passwords.

DEFENSES?

Sol
1. ไม่ให้แคช : traffic, slow resp
2. ควบคุมของแคช : แคชเฉพาะของที่ควรแคช (เกี่ยวข้อง)
↳ อยู่ใต้ชื่อมัน

DNS CACHE POISONING ใส่ของปลอมใน DNS cache

- DNS query results include Additional Records section
  - Provide records for anticipated next resolution step
- Early servers accepted and cached all additional records provided in query response

GLUE RECORDS ปองกัน

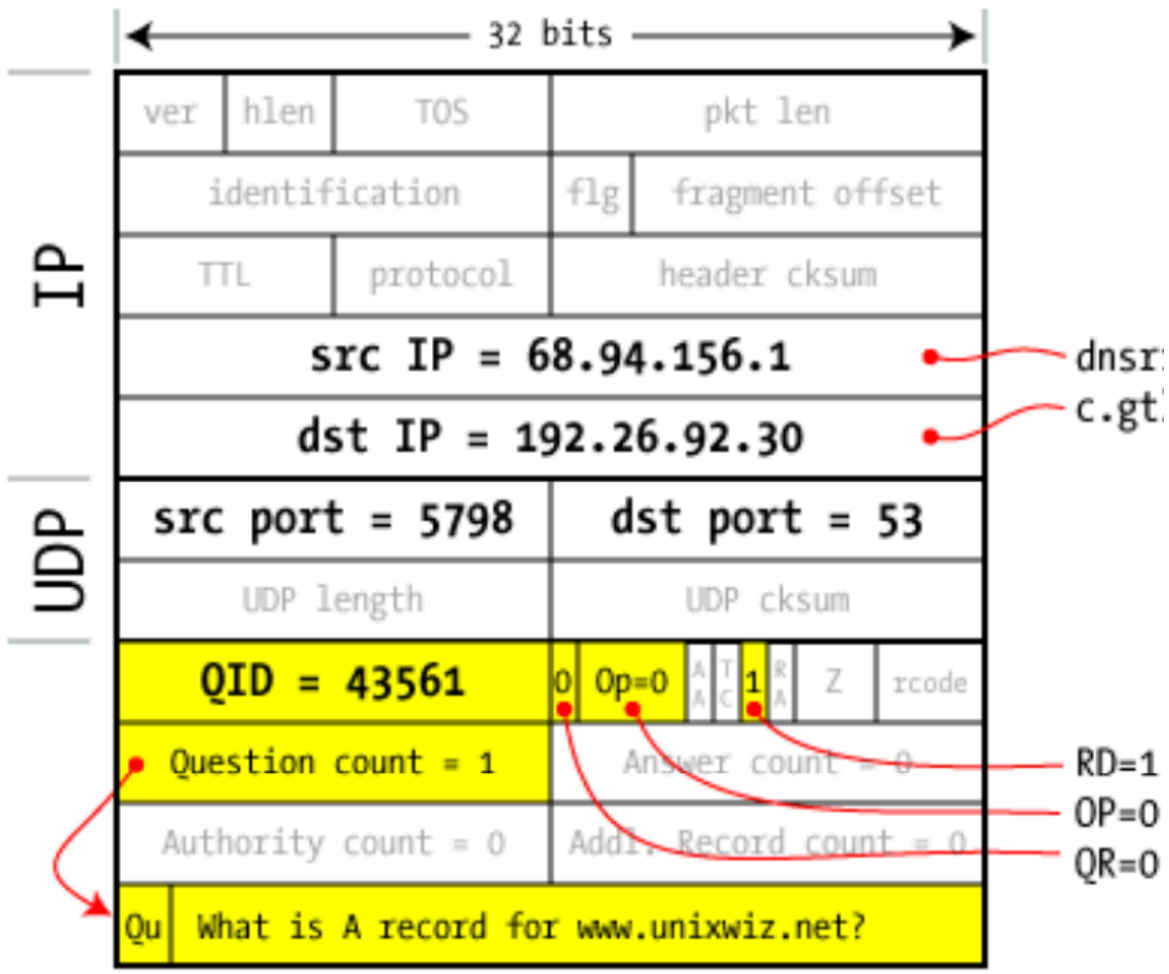
- Can we just stop using additional section?
  - Only accept answers from authoritative servers?
- Glue records: non-authoritative records necessary to contact next hop in resolution chain
  - Necessary given current design of DNS
- Bailiwick Checking: Only accept additional records that are for a domain in the original question.

DNS SPOOFING

: ปลอมตัวเป็น DNS server เพื่อส่งคำตอบมา

- Scenario: DNS client issues query to server
- Attacker would like to inject a fake reply
  - Attacker does not see query or real response
- How does client authenticate response?

DNS SPOOFING

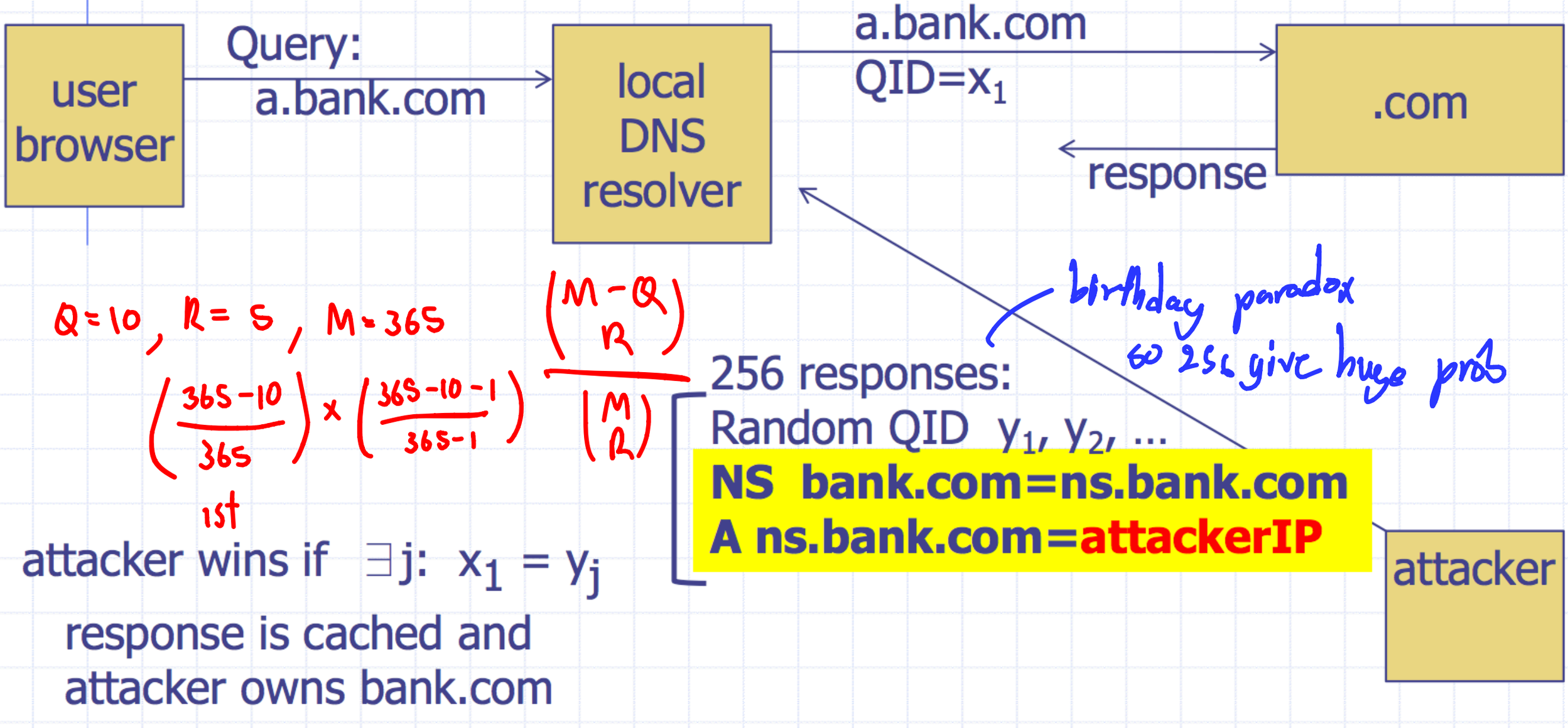


- How does client authenticate response?
  - UDP port numbers must match
- Destination port usually port 53 by convention
- 16-bit query ID must match only thing that need to ran

DEFENSES?

KAMINSKY ATTACK

- Victim machine visits attacker's web site, downloads Javascript

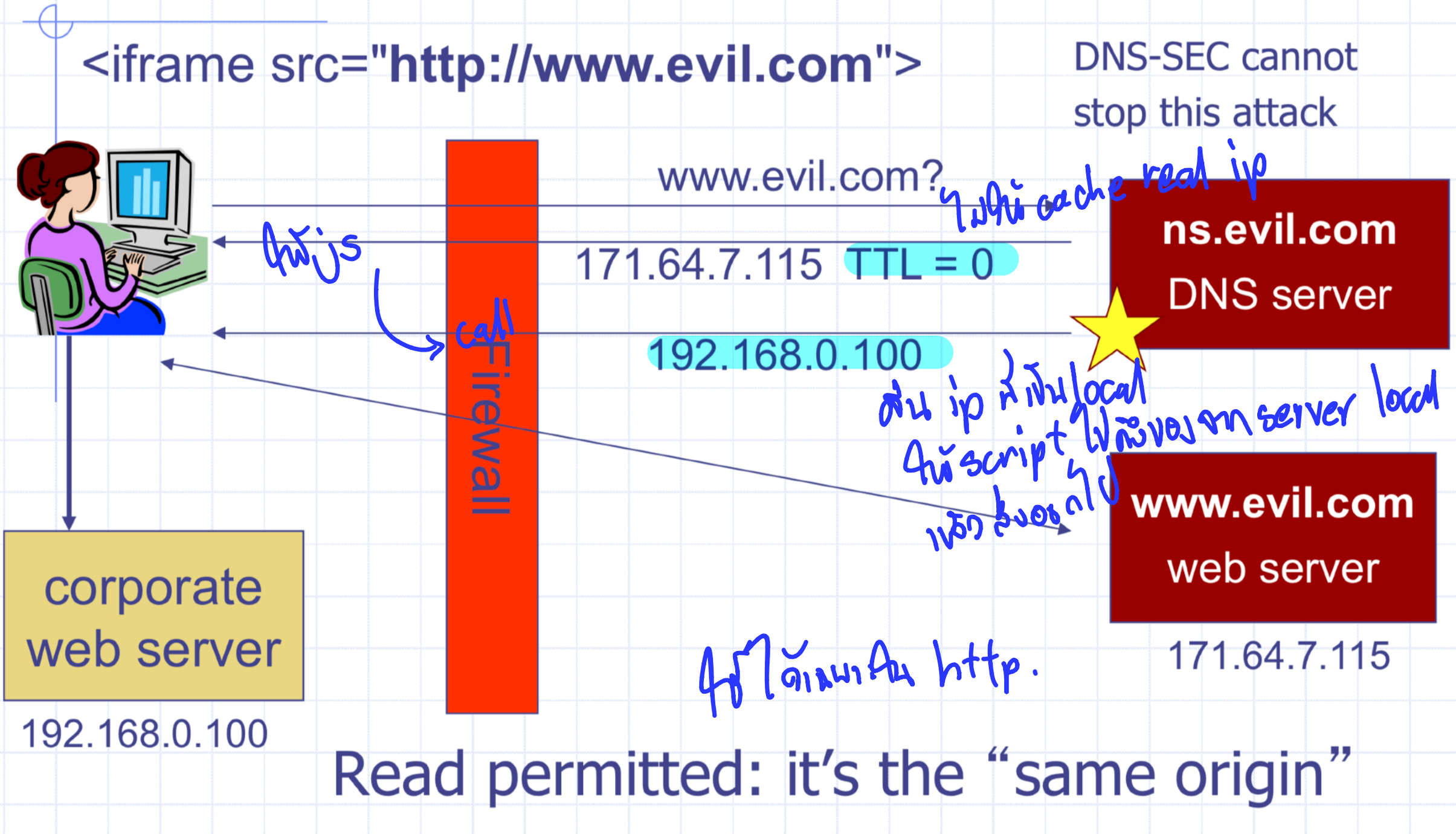


DEFENSES?

- Increase QueryID space. But how? Don't want to change packet.
  - Attack now takes several hours
- Randomize src port, additional bits of entropy
  - from fixed

DNS REBINDING

DEFENSES?



REBINDING DEFENSES

ไม่สนทางข้องกัน

- Browser Mitigations:
  - Refuse to switch IPs mid session ห้ามเปลี่ยน
  - Interacts poorly with proxies, VPNs, CDNs, etc
  - Not consistently implemented in any browser
- Server Defenses
  - Check Host header for unrecognized domains
  - Authenticate users with something else beyond IP address
- Firewall defenses
  - External names can’t resolve to internal addresses
  - Protects browsers inside the organization
- DNSSEC will not solve this problem

DNSSEC : ไม่แก้ปัญหาใดๆที่กล่าวมา

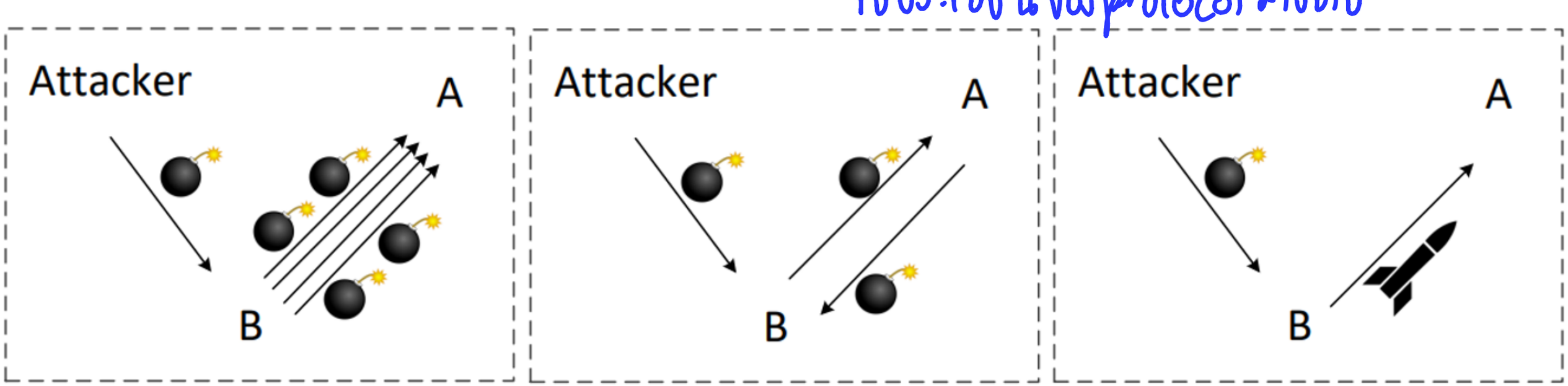
↳หรืออย่างเสียว : รู้หมด ถามตอบ, ใครตอบได้

- Adds authentication and integrity to DNS responses
- Authoritative DNS servers sign DNS responses using cryptographic key
- Clients can verify that a response is legitimate by checking signature through PKI similar to HTTPS
- Most people don’t use DNSSEC and never will. Use TLS instead.

UDP ATTACKS

- Mostly used for Denial-Of-Service (DOS) Attacks
- Strategies: amplify attacking power, "amplification"

ใช้ประโยชน์ของ protocol มาขยาย



(a) Turn one grenade into many grenades

Smurf, Fraggle ยิงสะท้อนกลับ

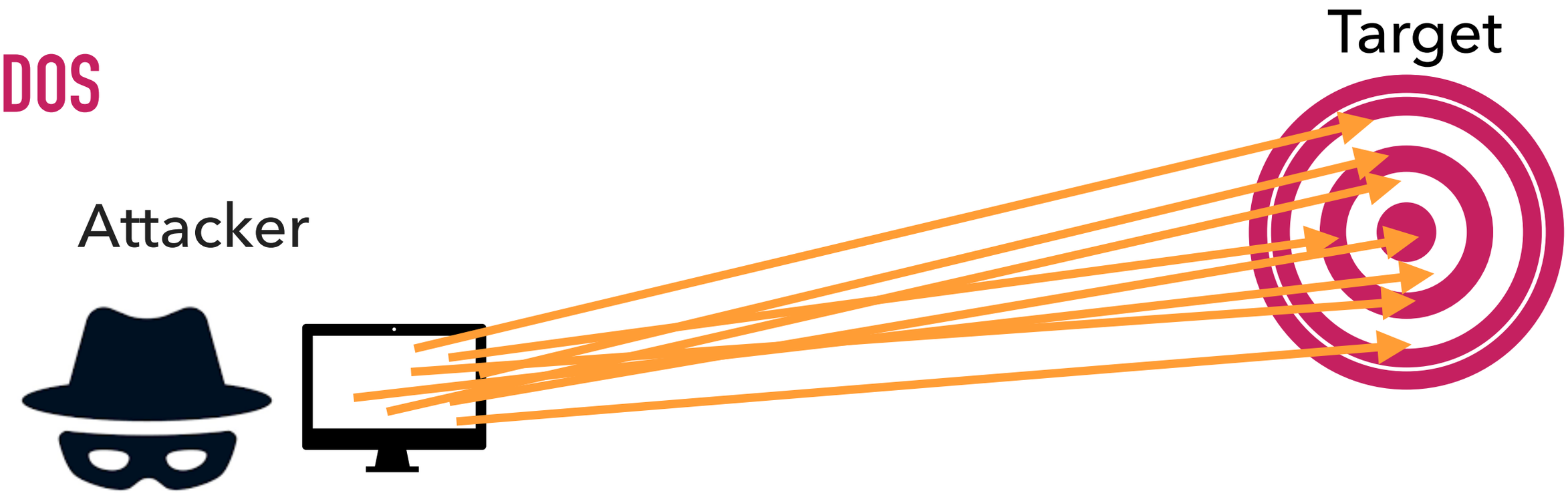
(b) Create a regenerable grenade

UDP Ping-Pong / ยิงวนเป็น loop Intinite

(c) Turn a grenade into a missile

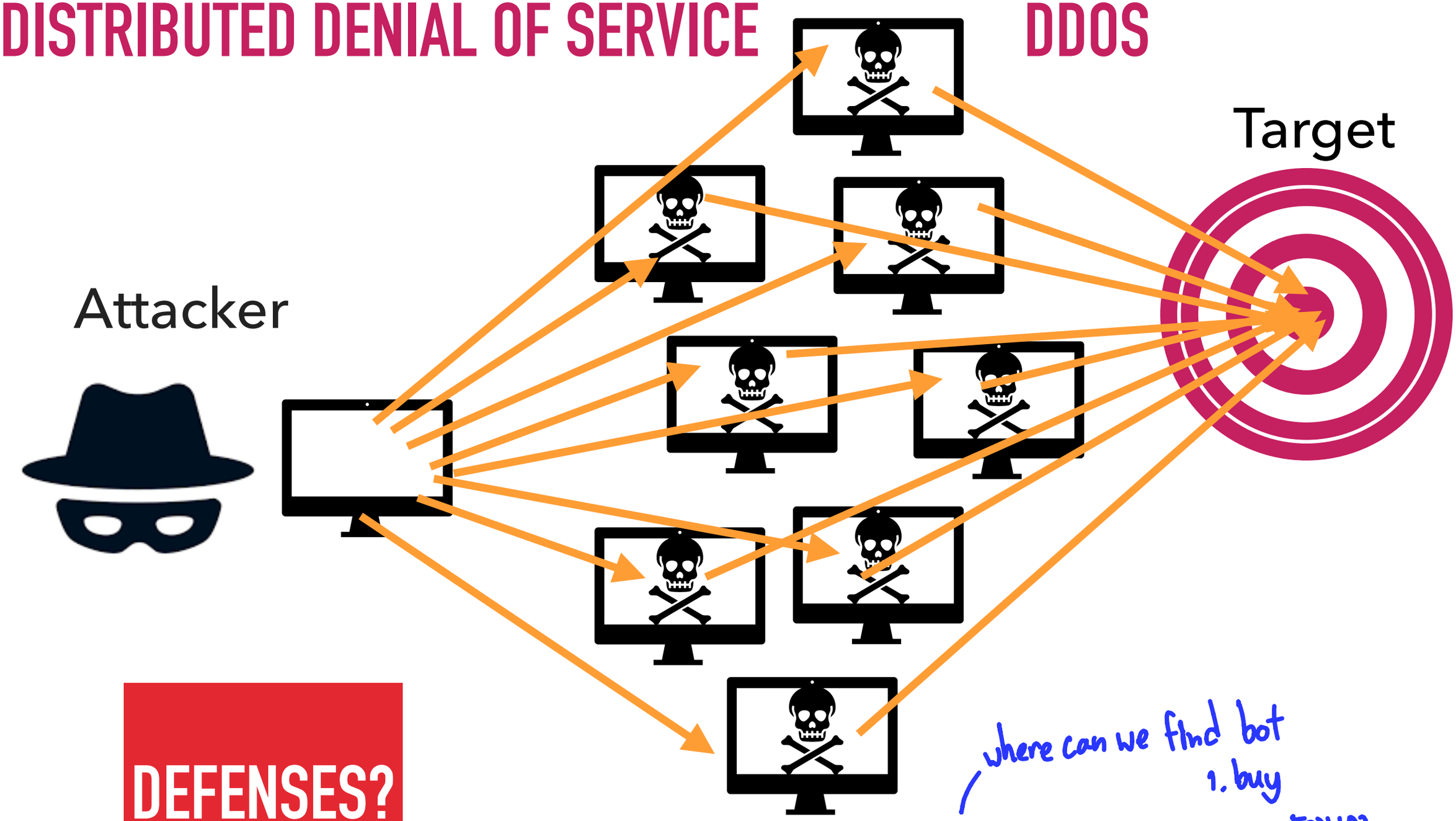
Amplification

DOS



- Goal: take large site offline by overwhelming it with network traffic such that they can't process real requests
- How: find mechanism where attacker doesn't have to spend a lot of effort, but requests are difficult/ expensive for victim to process
  - Design flaw that allows one machine to disrupt a service or implementation bug
  - Generally a protocol asymmetry, e.g., easy to send request, difficult to create response. Or requires server state.
  - Many exploits using popular protocols such as DNS, TCP, ICMP

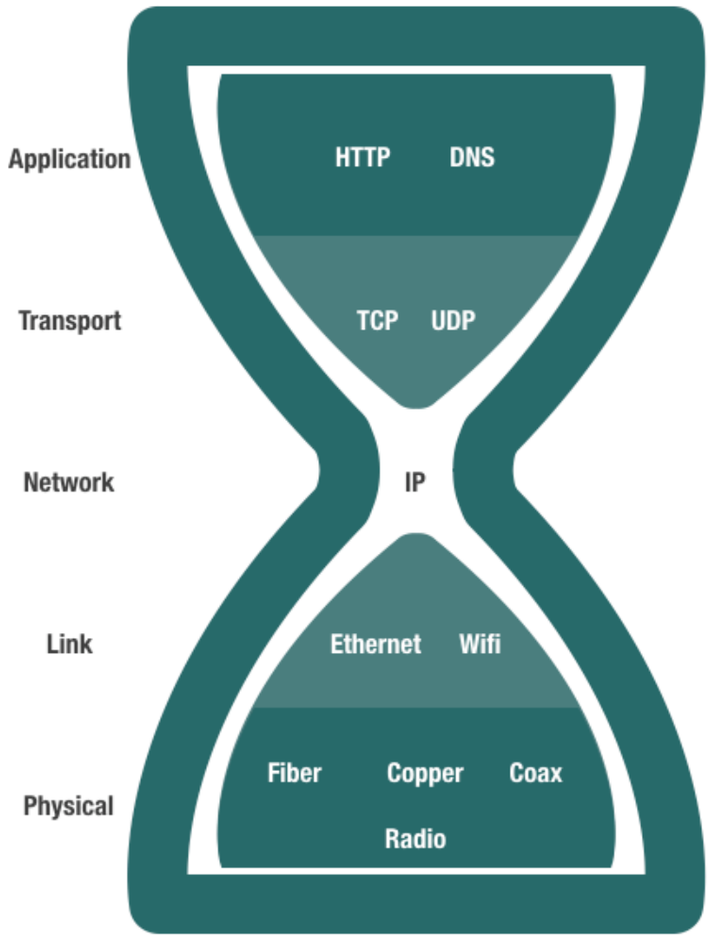
DISTRIBUTED DENIAL OF SERVICE DDOS



DEFENSES?

DENIAL OF SERVICE POSSIBLE AT EVERY LAYER

- Application Layer: require servers to perform expensive queries or cryptographic operations
- TCP/UDP: require servers to maintain large number of concurrent connections or state ทำให้ state เต็มจำนวนที่รับได้
- Link Layer: send too much traffic for switches/routers to handle



ขอให้ อะไรก็ล้อมรอบก่อนใหญ่มา

แก้ source ip เป็น victim ip

DDOS AMPLIFICATION + REFLECTOR ATTACKS

DEFENSES?

60-70x Increase in Size

Image: Cloudflare

Keep in mind....

SECURITY PROBLEM

INHERENT IN THE DESIGN

"PROTOCOL-LEVEL PROBLEM" VS.

IMPLEMENTATION PROBLEM "BUG"

kunwadee (AT) cp.eng.chula.ac.th

COMMON UDP AMPLIFIERS

- DNS: ANY query returns all records server has about a domain
- NTP: MONLIST returns list of last 600 clients who asked for the time recently

- Only works if you can receive a big response by sending a single packet – otherwise spoofing doesn't lead to effective DoS attacks.

AMPLIFICATION ATTACKS

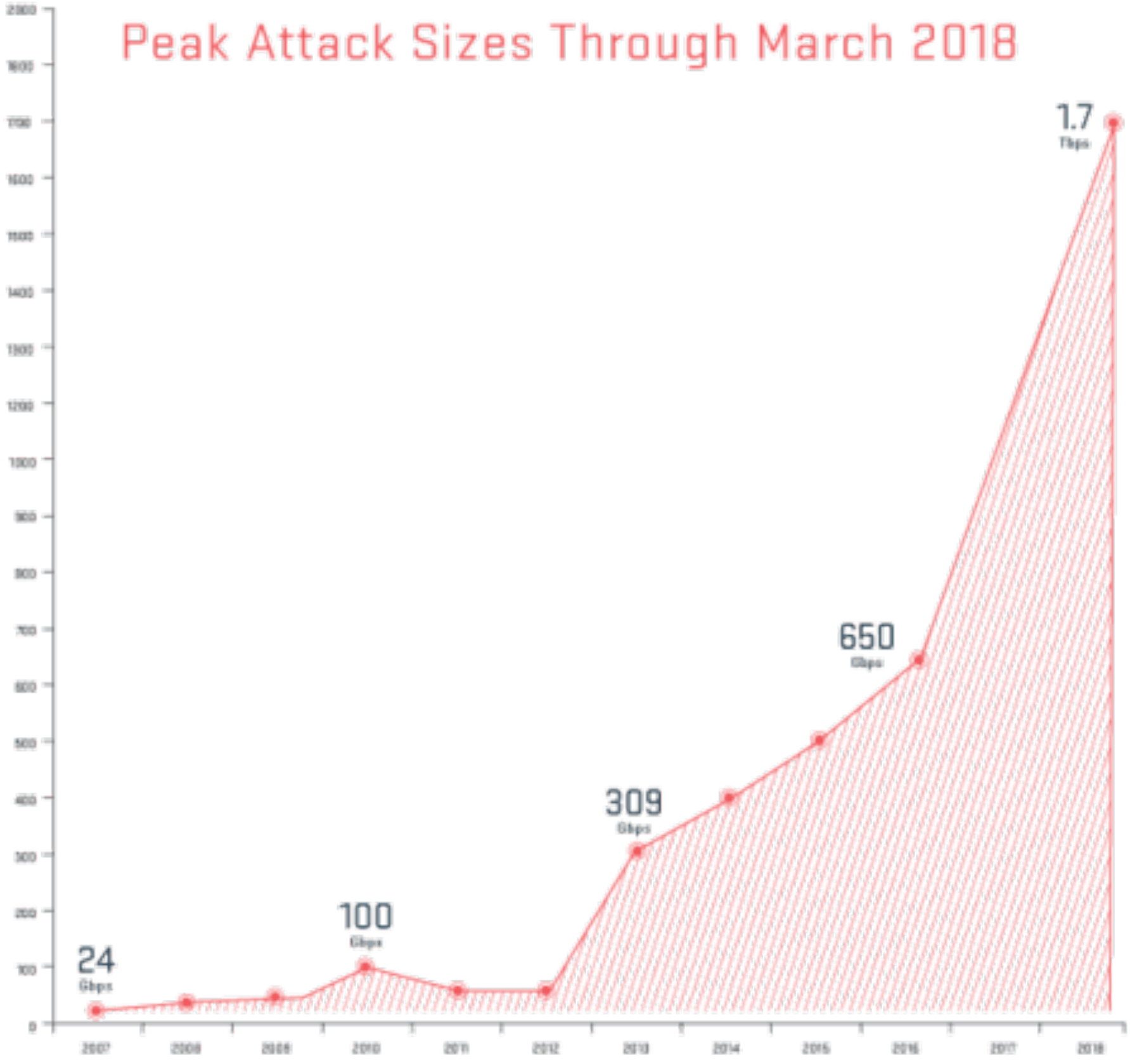
- 2013: DDoS attack generated 300 Gbps (DNS)
  - 31,000 misconfigured open resolvers, each at 10 Mbps
  - Source: 3 networks that allowed IP spoofing
- 2014: 400 Gbps DDoS attacked used 4500 NTP servers

AMPLIFICATION FACTOR

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [4]
NTP	556.9	see: TA14-013A [5]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange
Multicast DNS (mDNS)	2 to 10	Unicast query
RIPv1	131.24	Malformed request
Portmap (RPCbind)	7 to 28	Malformed request
LDAP	46 to 55	Malformed request [6]

MEMCACHE

- Memcache: retrieve large record
- The server responds by firing back as much as 50,000 times the data it received.
- Exist both a UDP and TCP version. Only works for UDP! TCP would require a three-way handshake and server would realize IP had been spoofed.



October 21, 2016

THE WALL STREET JOURNAL.

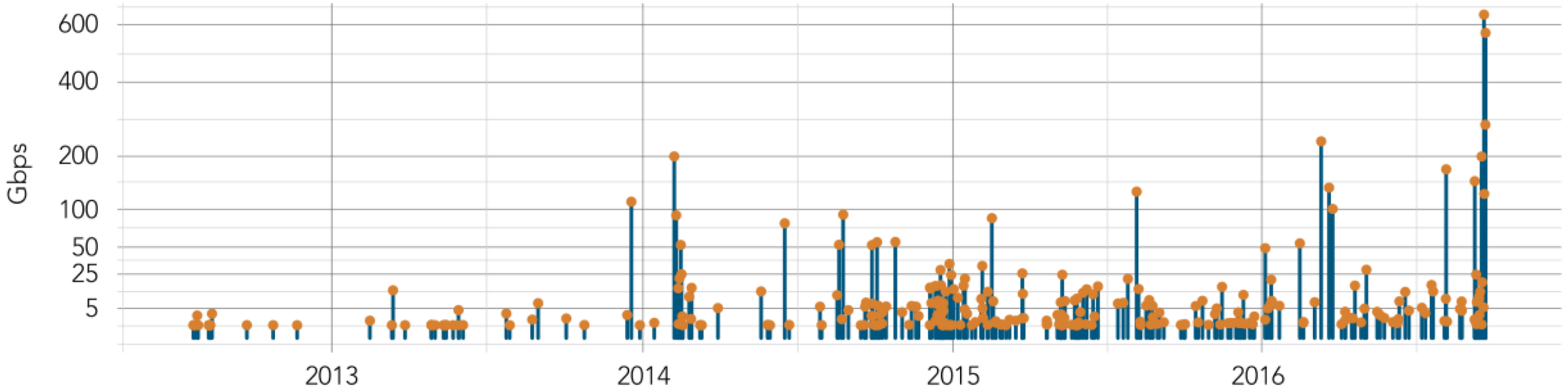
Cyberattack Knocks Out Access to Websites

Popular sites such as Twitter, Netflix and PayPal were unreachable for part of the day

twitter amazon web services™ PayPal NETFLIX SOUNDCLOUD

Spotify GitHub reddit New York Times

Attack on Dyn (DNS service provider)



> “The magnitude of the attacks seen during the final week were significantly larger than the majority of attacks Akamai sees on a regular basis. […] In fact, while the attack on September 20 was the largest attack ever mitigated by Akamai, the attack on September 22 would have qualified for the record at any other time, peaking at 555 Gbps.”

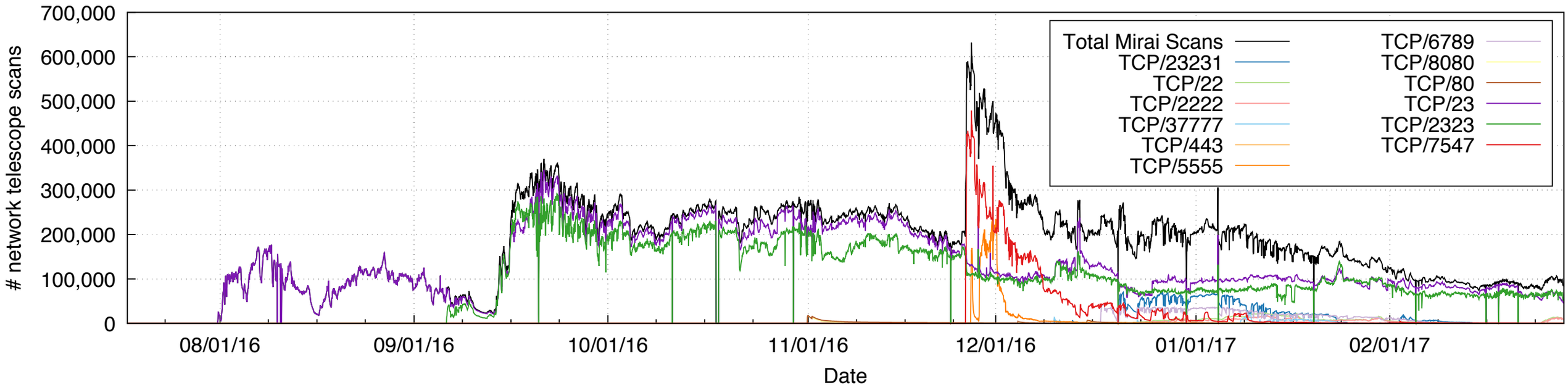
Source: 2017 Akamai State of the Internet

PASSWORD GUESSING

default password

Password	Device Type	Password	Device Type	Password	Device Type
123456	ACTi IP Camera	klv1234	HiSilicon IP Camera	1111	Xerox Printer
anko	ANKO Products DVR	jvbzd	HiSilicon IP Camera	Zte521	ZTE Router
pass	Axis IP Camera	admin	IPX-DDK Network Camera	1234	Unknown
888888	Dahua DVR	system	IQinVision Cameras	12345	Unknown
666666	Dahua DVR	meinsm	Mobotix Network Camera	admin1234	Unknown
vizxv	Dahua IP Camera	54321	Packet8 VOIP Phone	default	Unknown
7ujMko0vizxv	Dahua IP Camera	00000000	Panasonic Printer	fucker	Unknown
7ujMko0admin	Dahua IP Camera	realtek	RealTek Routers	guest	Unknown
666666	Dahua IP Camera	1111111	Samsung IP Camera	password	Unknown
dreambox	Dreambox TV Receiver	xmhdipc	Shenzhen Anran Camera	root	Unknown
juantech	Guangzhou Juan Optical	smcadmin	SMC Routers	service	Unknown
xc3511	H.264 Chinese DVR	ikwb	Toshiba Network Camera	support	Unknown
OxhlwSG8	HiSilicon IP Camera	ubnt	Ubiquiti AirOS Router	tech	Unknown
cat1029	HiSilicon IP Camera	supervisor	VideoIQ	user	Unknown
hi3518	HiSilicon IP Camera	<none>	Vivotek IP Camera	zlxx.	Unknown
klv123	HiSilicon IP Camera				

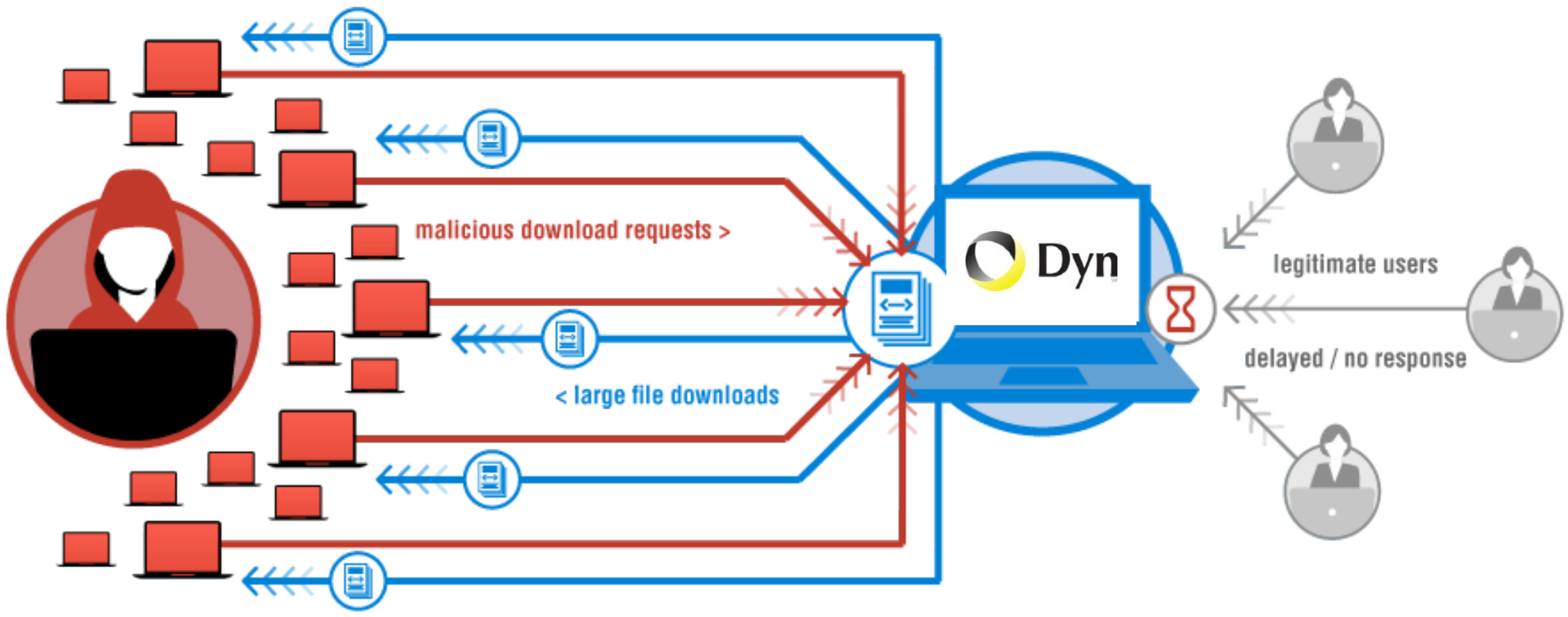
MIRAI POPULATION



~600K devices compromised

BOOTER SERVICES

$23.99 1 month	$34.99 1 month	$44.99 10 years
1 Month Gold	**1 Month Diamond**	**Lifetime Bronze**
Time per boot 2400 sec	Time per boot 3600 sec	Time per boot 600 sec
Concurrents 1	Concurrents 2	Concurrents 2
Total network 220Gbps	Total network 220Gbps	Total network 220Gbps
Tools Included	Tools Included	Tools Included
Support 24/7	Support 24/7	Support 24/7
Buy with Paypal bitcoin	Buy with Paypal bitcoin	Buy with Paypal bitcoin



> “We are still working on analyzing the data but the estimate at the time of this report is up to 100,000 malicious endpoints. […] There have been some reports of a magnitude in the 1.2 Tbps range; at this time we are unable to verify that claim.”

Image: Verisign

A BOTNET OF IOT DEVICES

≈ ~~200K Hosts~~
200K IoT devices

Not Amplification.
Flood with SYN, ACK, UDP, and GRE packets

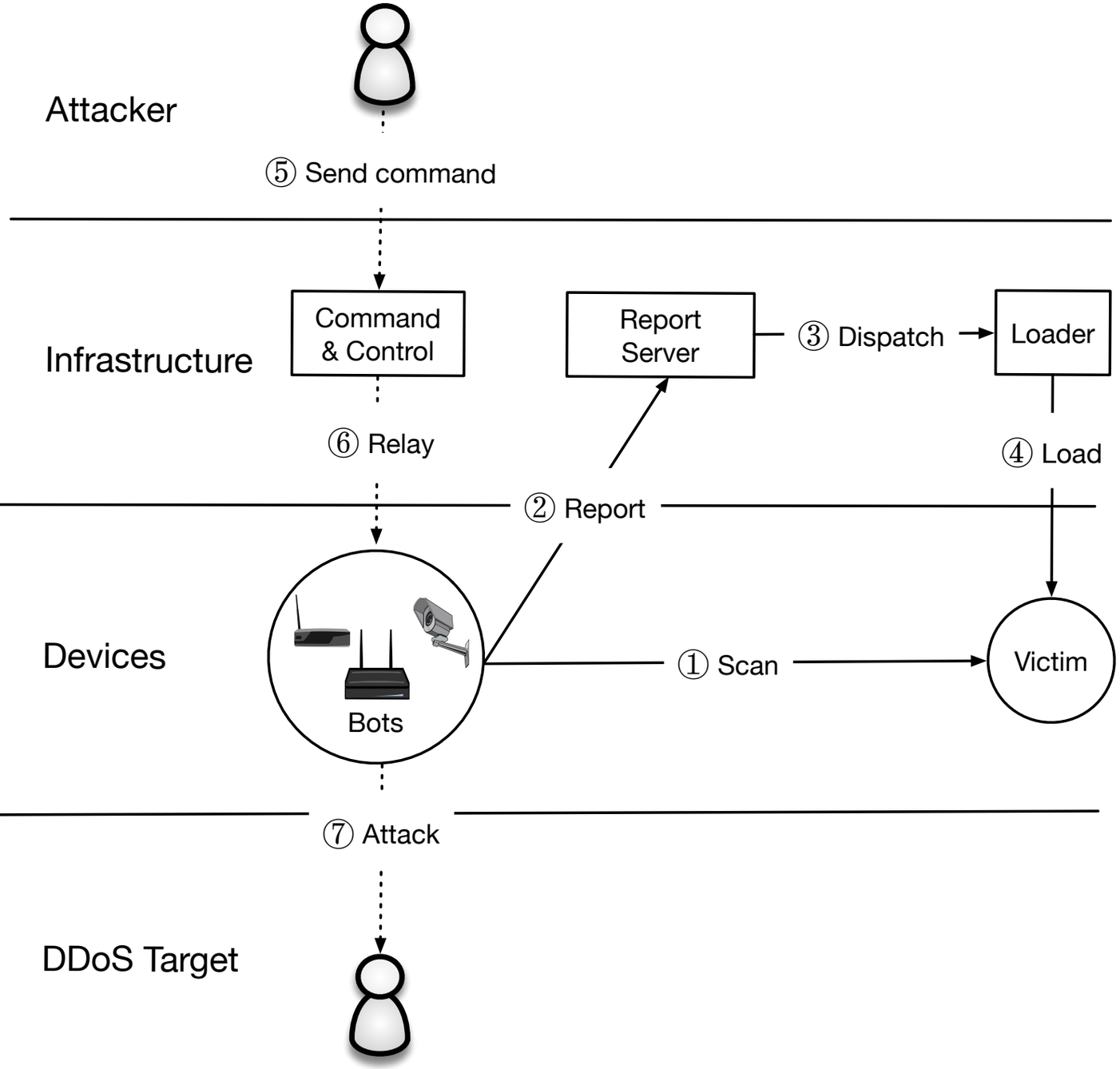
THE MIRAI MALWARE

Steps 5-7. Later, the **bot master** will issue commands to pause scanning and to start an attack

Attack Command:

- Action (e.g., START, STOP)
- Target IP(s)
- Attack Type (e.g., GRE, DNS, TCP)
- Attack Duration

DEFENSES?

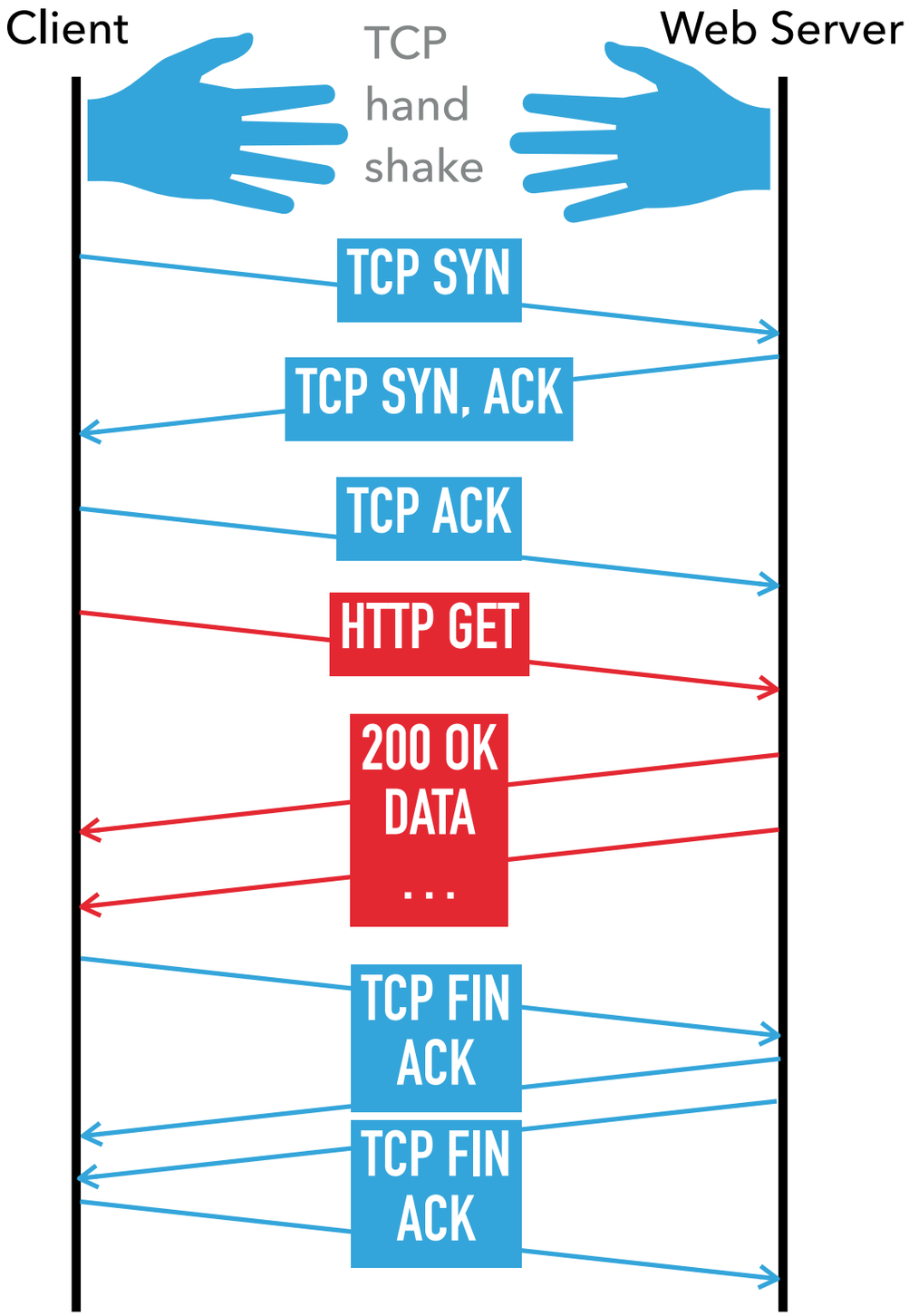


1. TCP SPOOFING
2. TCP RESET
3. SYN FLOOD ATTACK

TCP KNOWN ISSUES

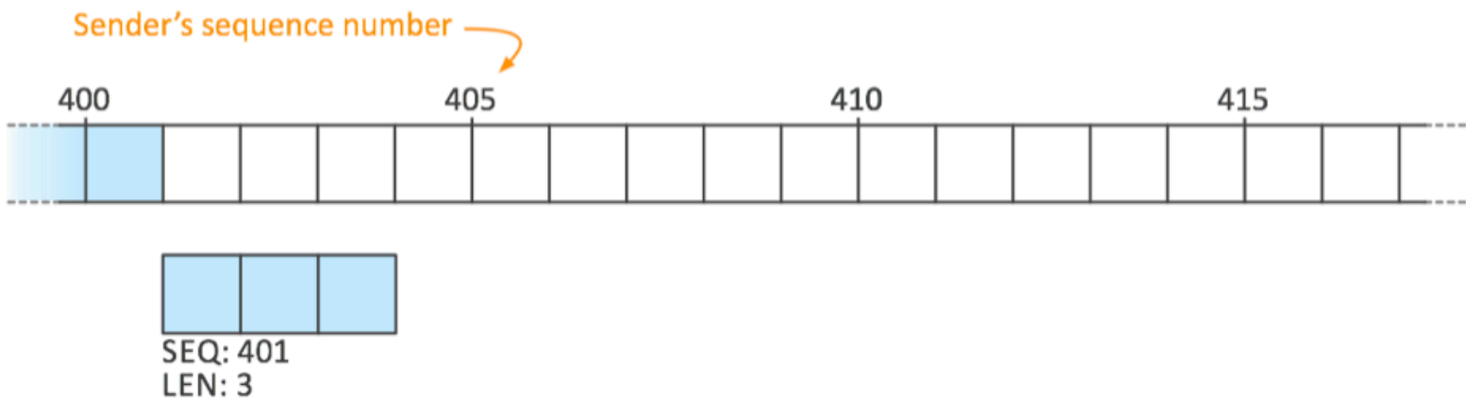
kunwadee (AT) cp.eng.chula.ac.th

TRANSMISSION CONTROL PROTOCOL (TCP)



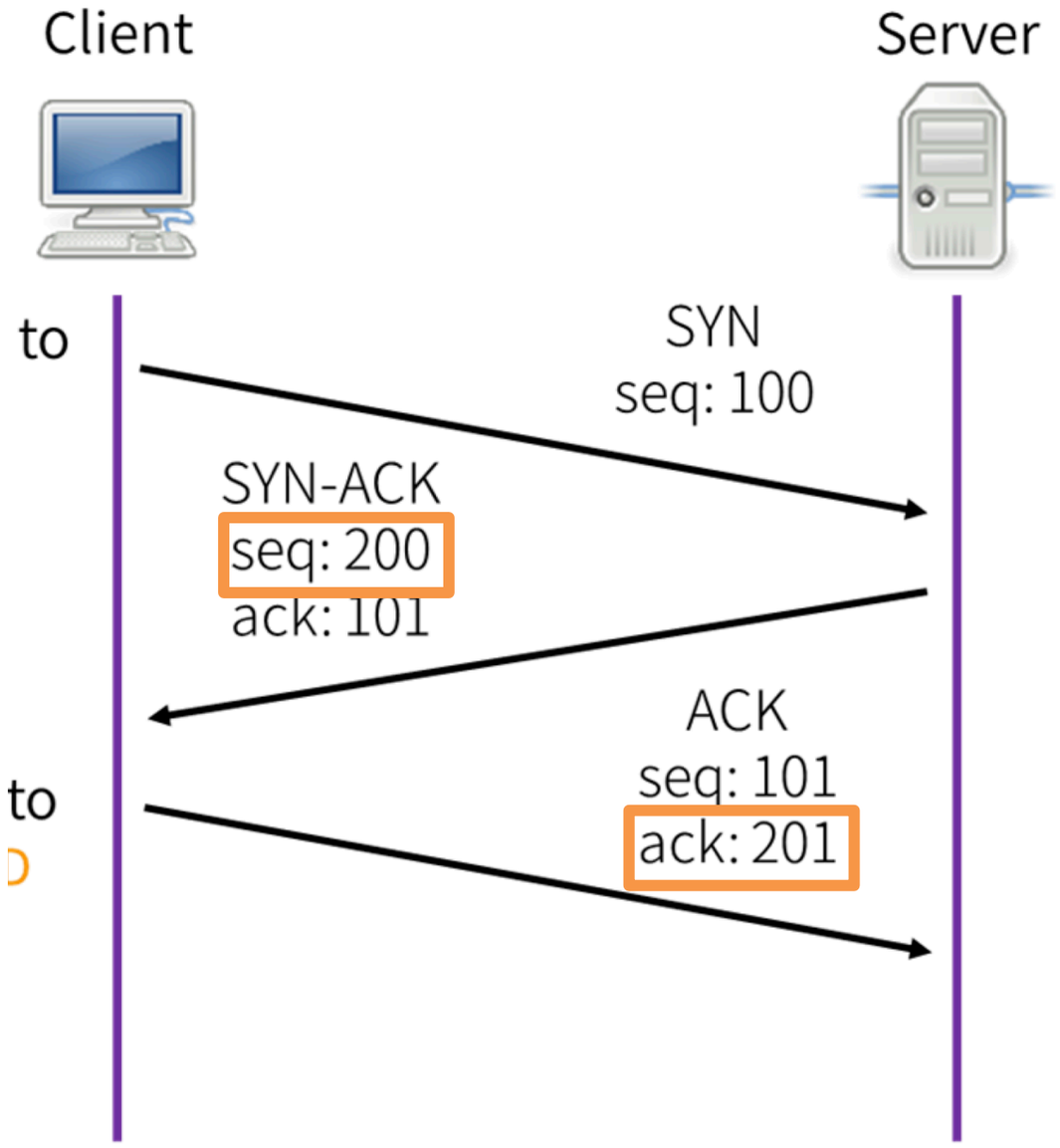
- Many applications want a stream of bytes delivered reliably and in-order between applications on different hosts
- Transmission Control Protocol (TCP) provides…
  - Connection-oriented protocol with explicit setup/teardown
  - Reliable in-order byte stream
  - Congestion control
- Despite IP packets being dropped, re-ordered, and duplicated (i.e., IP is best effort)

TCP SEQUENCE NUMBERS



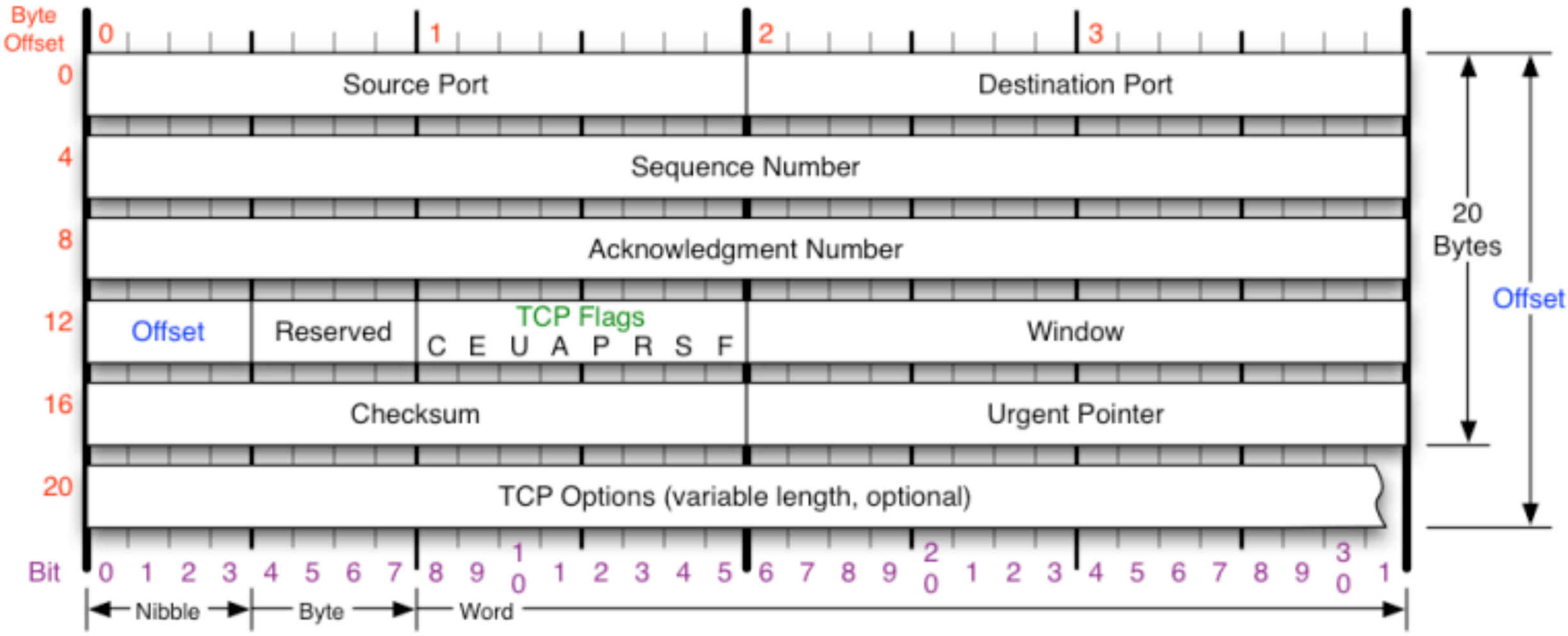
- Two data streams in a TCP session, one in each direction
- Bytes in data stream numbered with a 32-bit sequence number
- Every packet has sequence number that indicates where data belongs
- Receiver sends acknowledgement number that indicates data received

CAN WE IMPERSONATE ANOTHER HOST WHEN INITIATING A CONNECTION (AKA SPOOF TCP CONNECTIONS)?



- Off-path attacker can send initial SYN to server ..... but cannot complete three-way handshake without seeing the server's sequence number
- $1/2^{32}$ chance to guess right if initial sequence number chosen uniformly at random

TRANSMISSION CONTROL PROTOCOL (TCP)



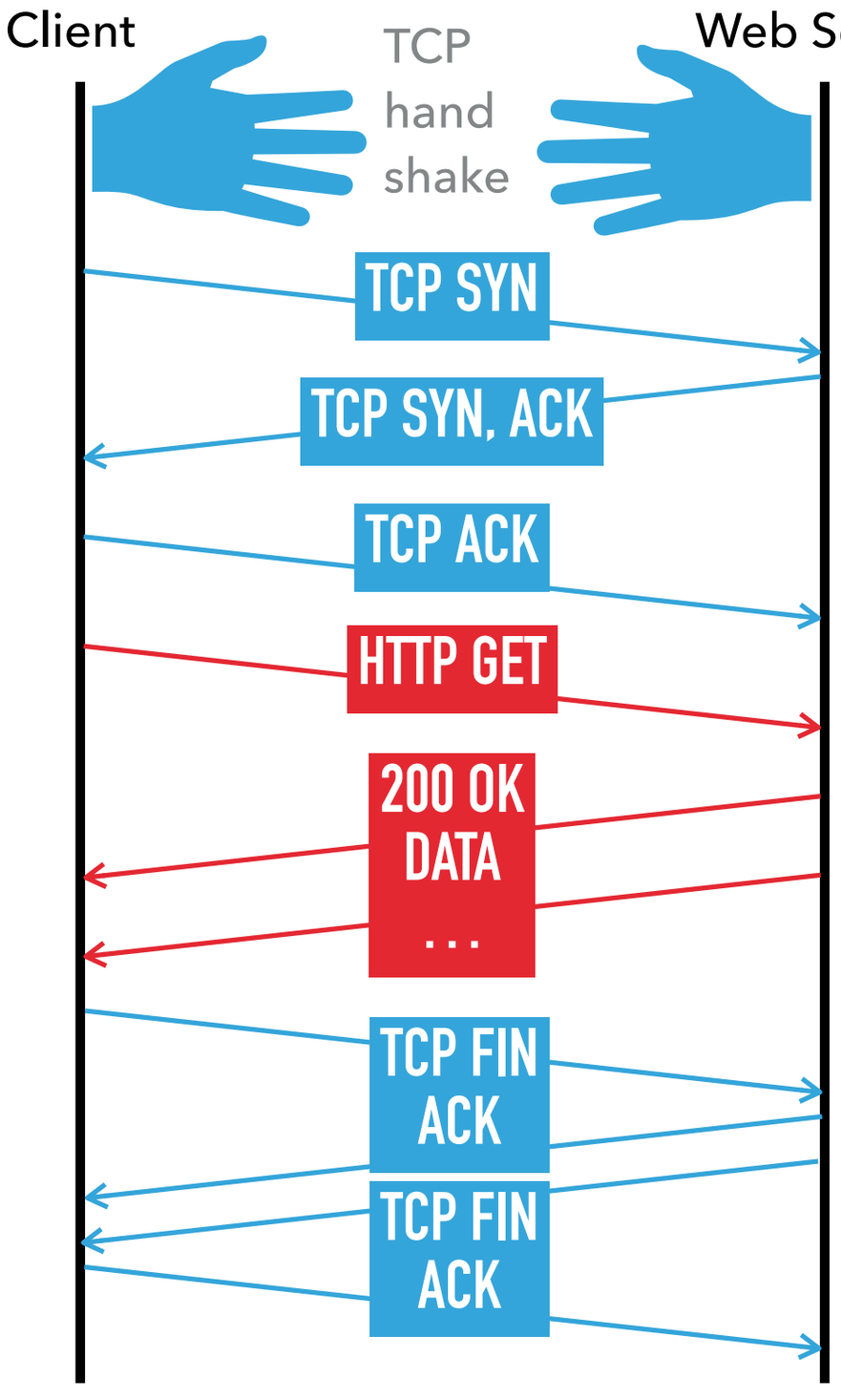
TCP CONNECTION RESET

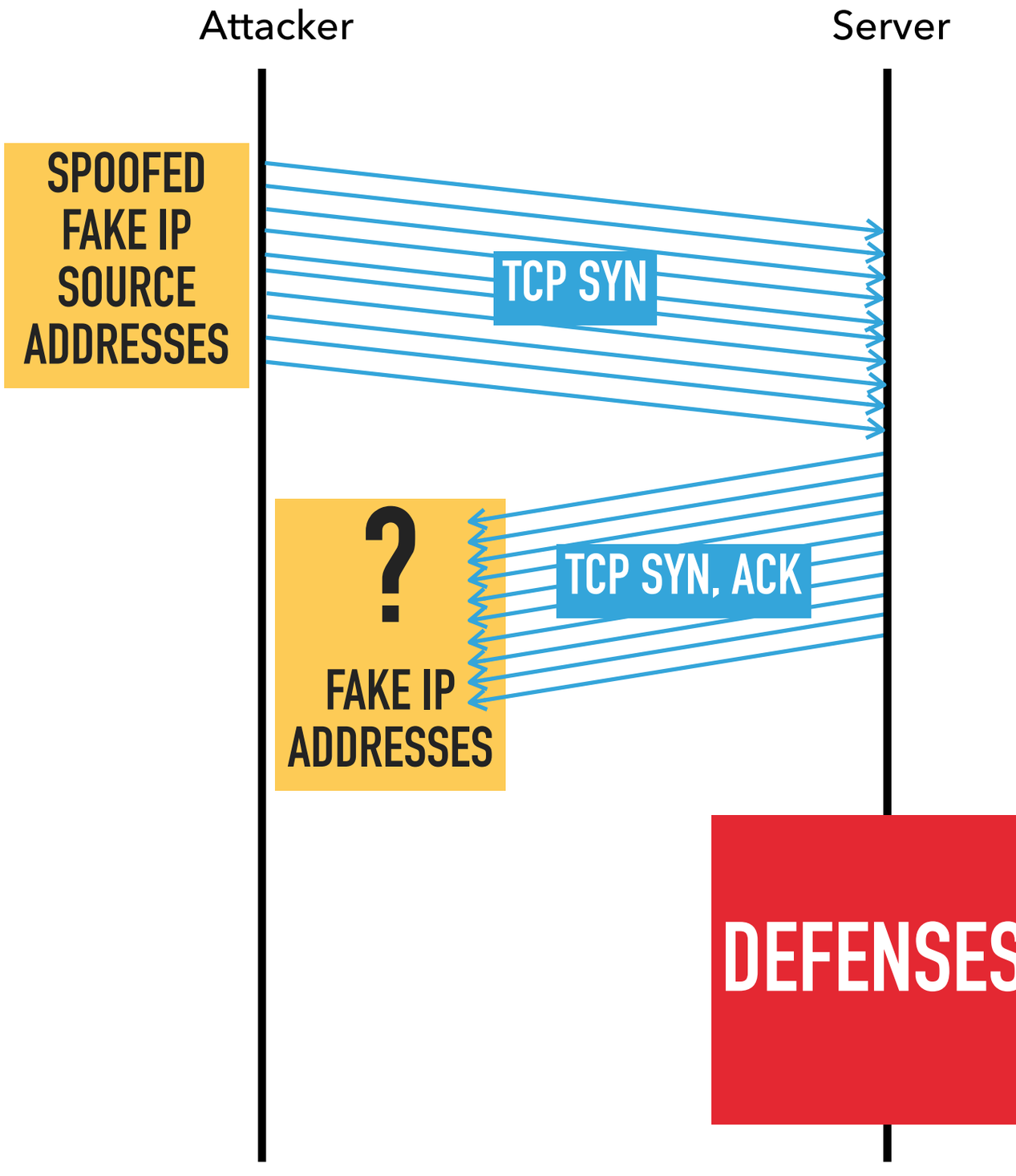
- TCP designed to handle possibility of spurious TCP packets (e.g. from previous connections)
- Packets that are invalid given current state of session generate a reset
  - If a connection exists, it is torn down
  - Packet with RST flag sent in response
- If a host receives a TCP packet with RST flag, it tears down the connection

CAN WE RESET AN EXISTING TCP CONNECTION?

- Need to know port numbers (16 bits)
  - Initiator's port number usually chosen random by OS
  - Responder's port number may be well-known port of service
- There is leeway in sequence numbers B will accept
  - Must be within window size (32-64K on most modern OSes)
- 1 in $2^{16+32}/W$ (where W is window size) chance to guess right

TCP SYN FLOOD ATTACK (PART II)





Keep in mind....

SECURITY PROBLEM

INHERENT IN THE DESIGN

"PROTOCOL-LEVEL PROBLEM" VS.

IMPLEMENTATION PROBLEM "BUG"

GOOD VS. BAD SOLUTIONS FOR SYN FLOOD ATTACKS

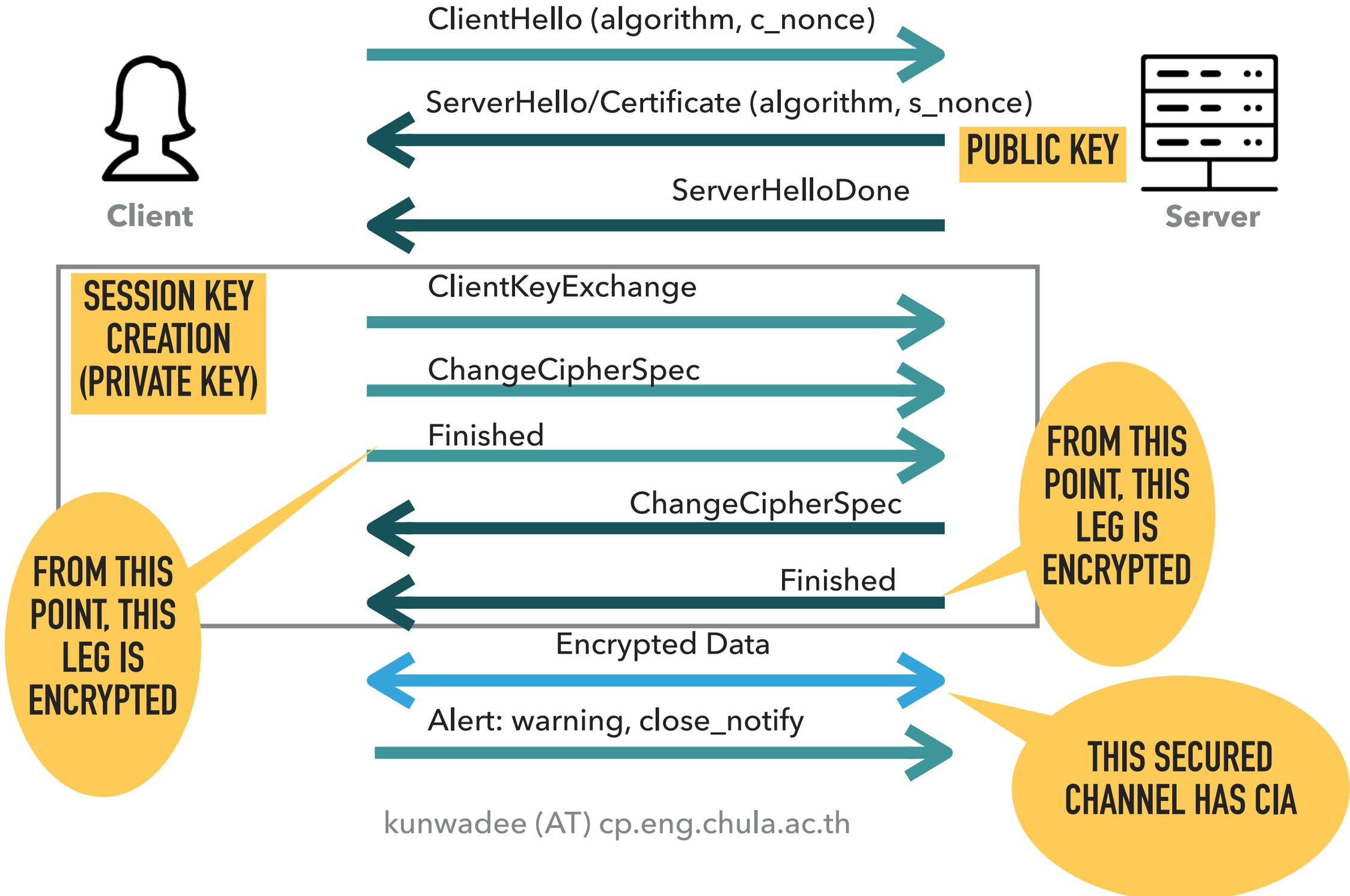
- Problem: server commits resources (memory) before confirming identify of client (when client responds)
- Solutions?
  - Increase backlog queue size
  - Decrease timeout
  - Avoid state until 3-way handshake completes

1. SSL HEART BLEED

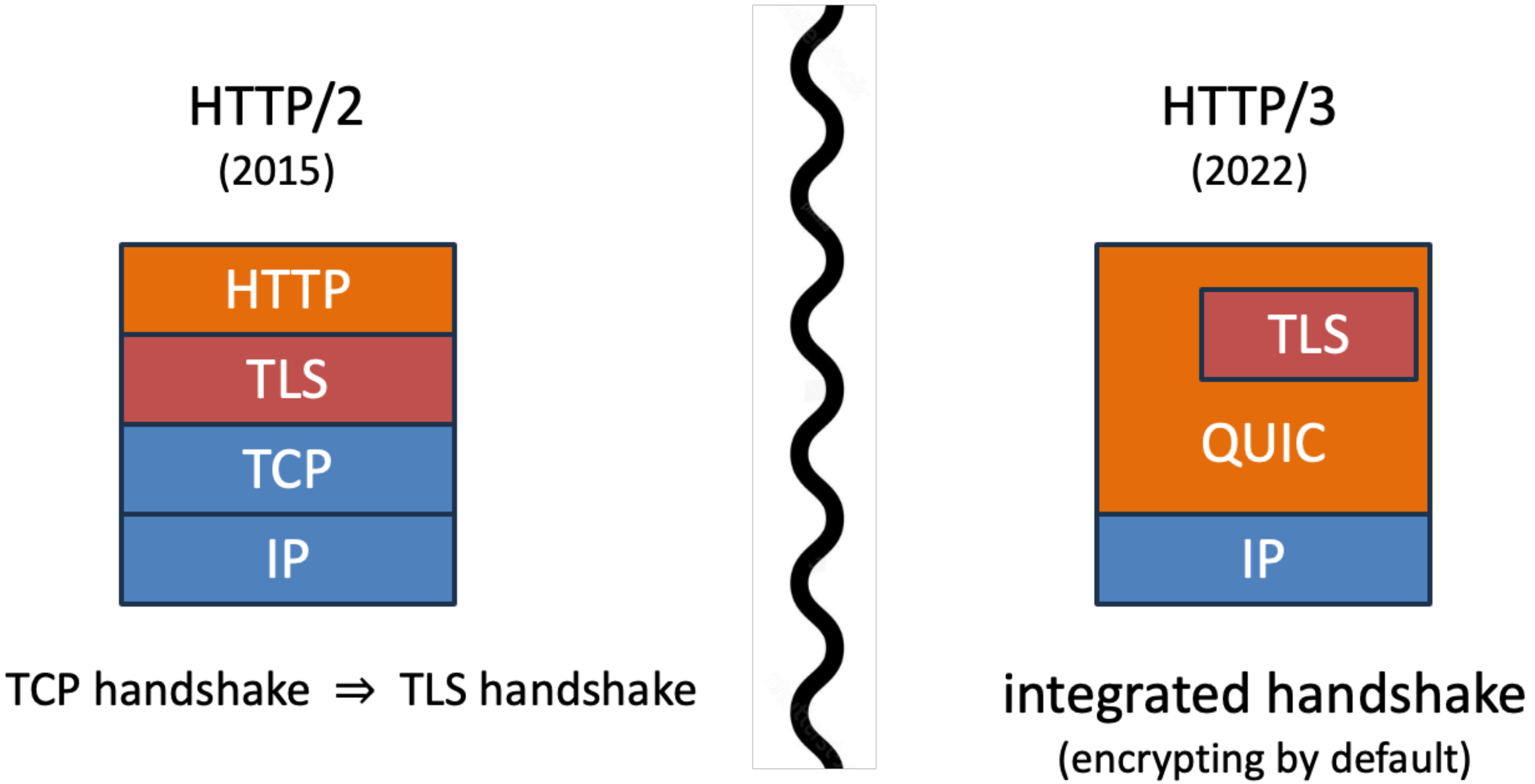
SSL KNOWN ISSUES

kunwadee (AT) cp.eng.chula.ac.th

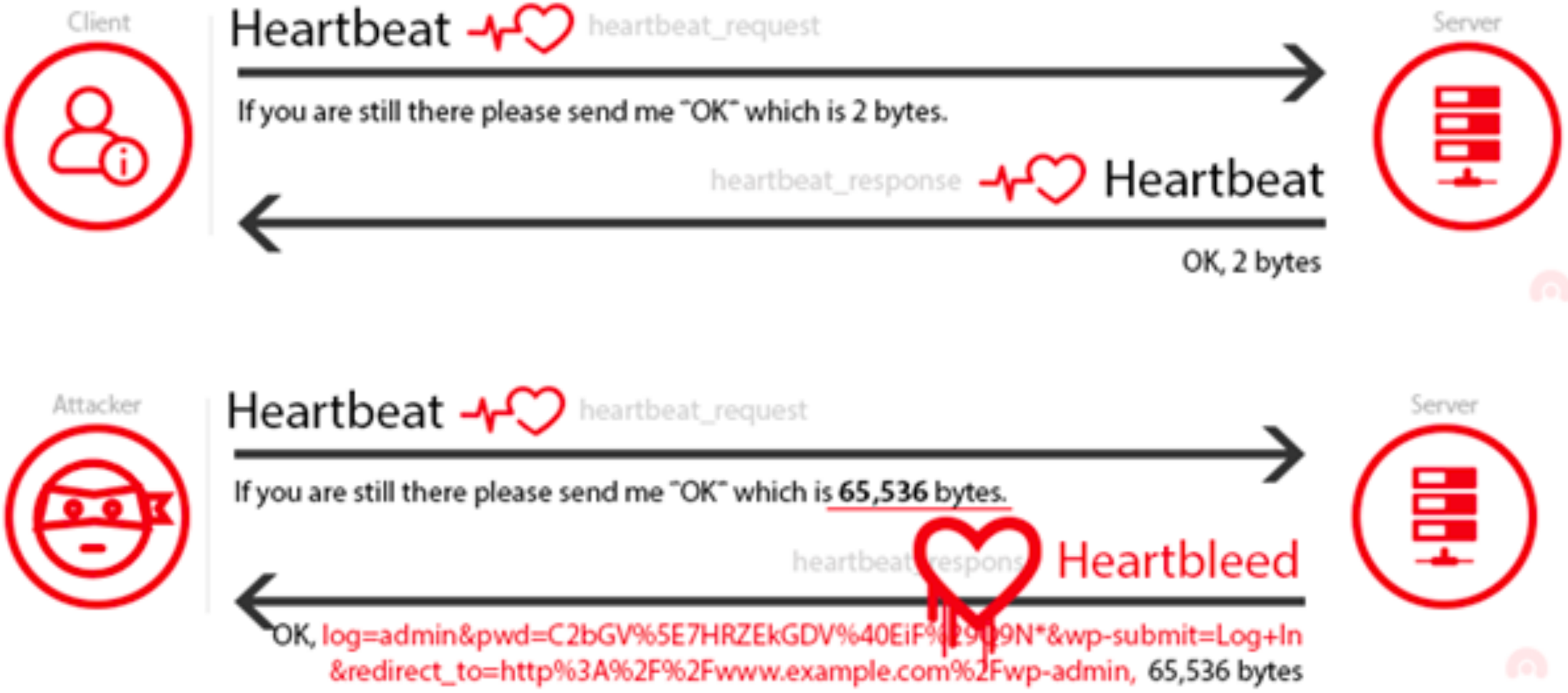
ENCRYPTION WITH TLS/SSL



INTEGRATING TLS WITH HTTP: HTTPS

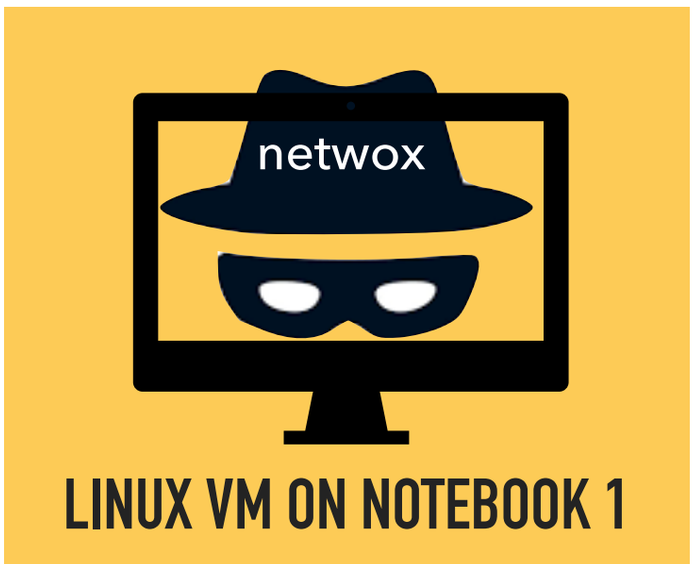


TLS/SSL HEARTBLEED (PART III)



Picture from acunetix

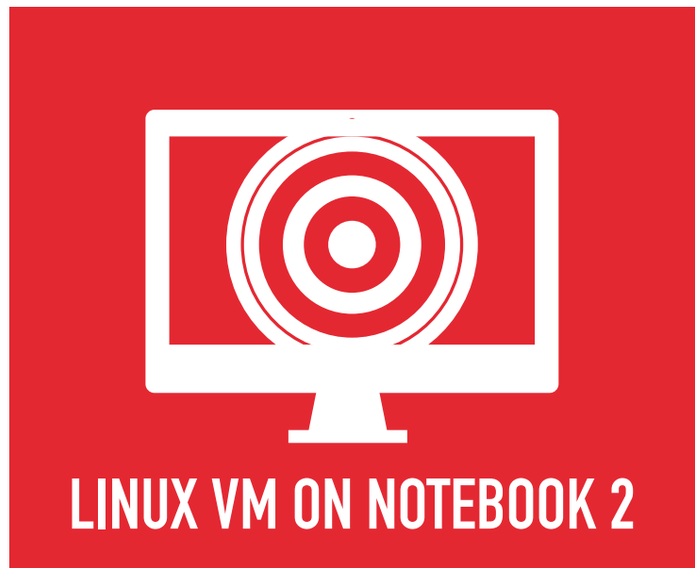
OPTION 1



SET BRIDGED NETWORK IN VIRTUALBOX

connected using
your own hotspot

(not chula wifi)

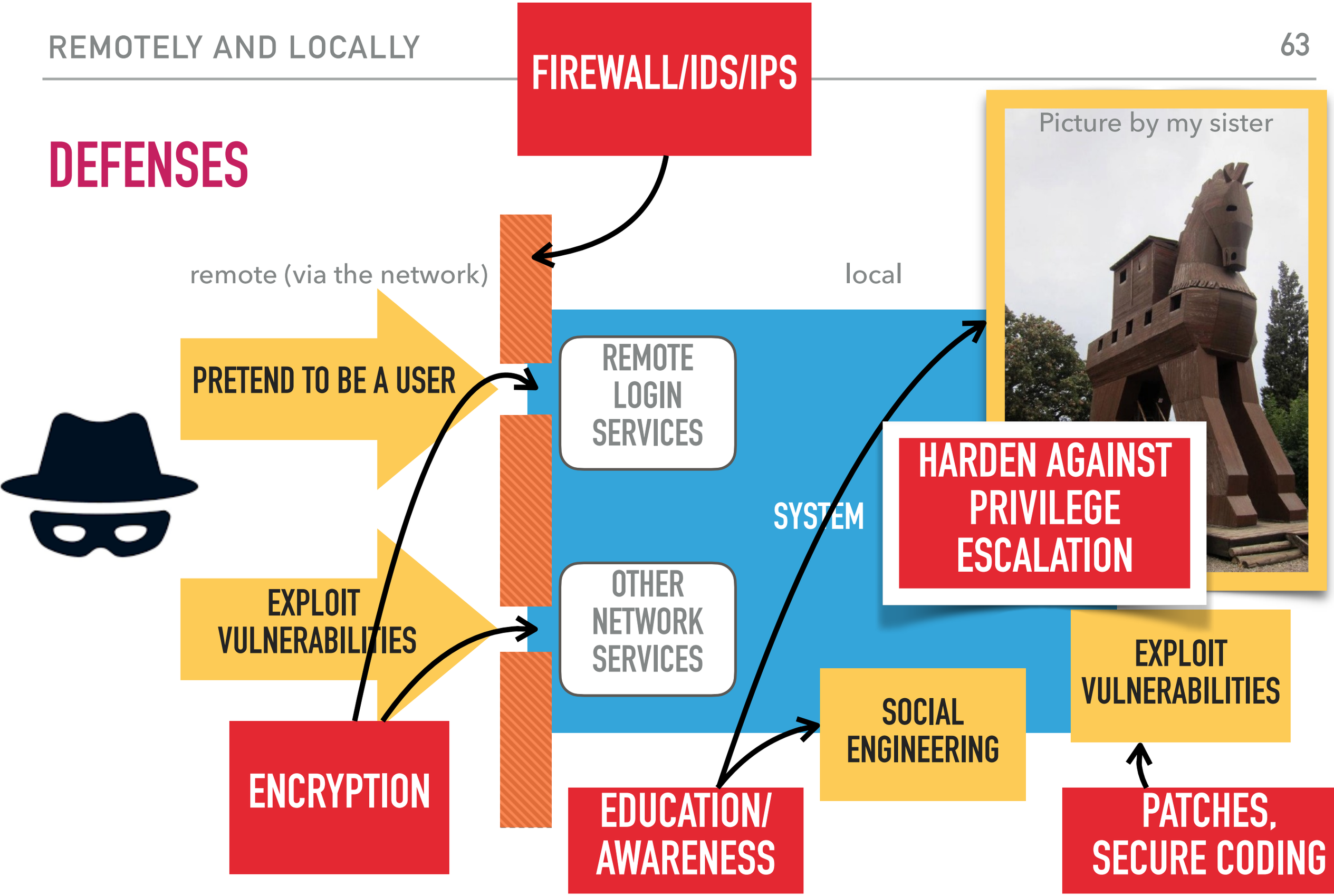


SET BRIDGED NETWORK IN VIRTUALBOX

ASSUME THE NETWORK IS OUT TO GET YOU.

kunwadee (AT) cp.eng.chula.ac.th

DEFENSES


FIREWALL/IDS/IPS
remote (via the network)
local
PRETEND TO BE A USER
REMOTE LOGIN SERVICES
SYSTEM
OTHER NETWORK SERVICES
EXPLOIT VULNERABILITIES
ENCRYPTION
EDUCATION/ AWARENESS
SOCIAL ENGINEERING
HARDEN AGAINST PRIVILEGE ESCALATION
Picture by my sister
EXPLOIT VULNERABILITIES
PATCHES, SECURE CODING

ARE THERE NO DEFENSES, BUT ONLY WAYS TO IMPROVE SECURITY?

- Protocol-compatible fixes to TCP implementations.
- Firewalls.
  - Partial fix, but widely used.
  - Issue: adversary may be within firewalled network.
  - Issue: hard to determine if packet is "malicious" or not.
  - Issue: even for fields that are present (src/dst), hard to authenticate.
- TCP/IP's design not a good match for firewall-like filtering techniques.
  - E.g., IP packet fragmentation: TCP ports in one packet, payload in another.
- Implement security on top of TCP/IP: SSL/TLS, Kerberos, SSH, etc.
- Use cryptography (encryption, signing, MACs, etc).
  - Quite a hard problem: protocol design, key distribution, trust, etc.
- Some kinds of security hard to provide on top: DoS-resistance, routing.
- Deployment of replacement protocols: SBGP, DNSSEC.

CREDITS

- Some slides for this lecture are modified from
  - Stanford University Security Class
  - Syracuse University SEED Project
  - MIT System Security Class