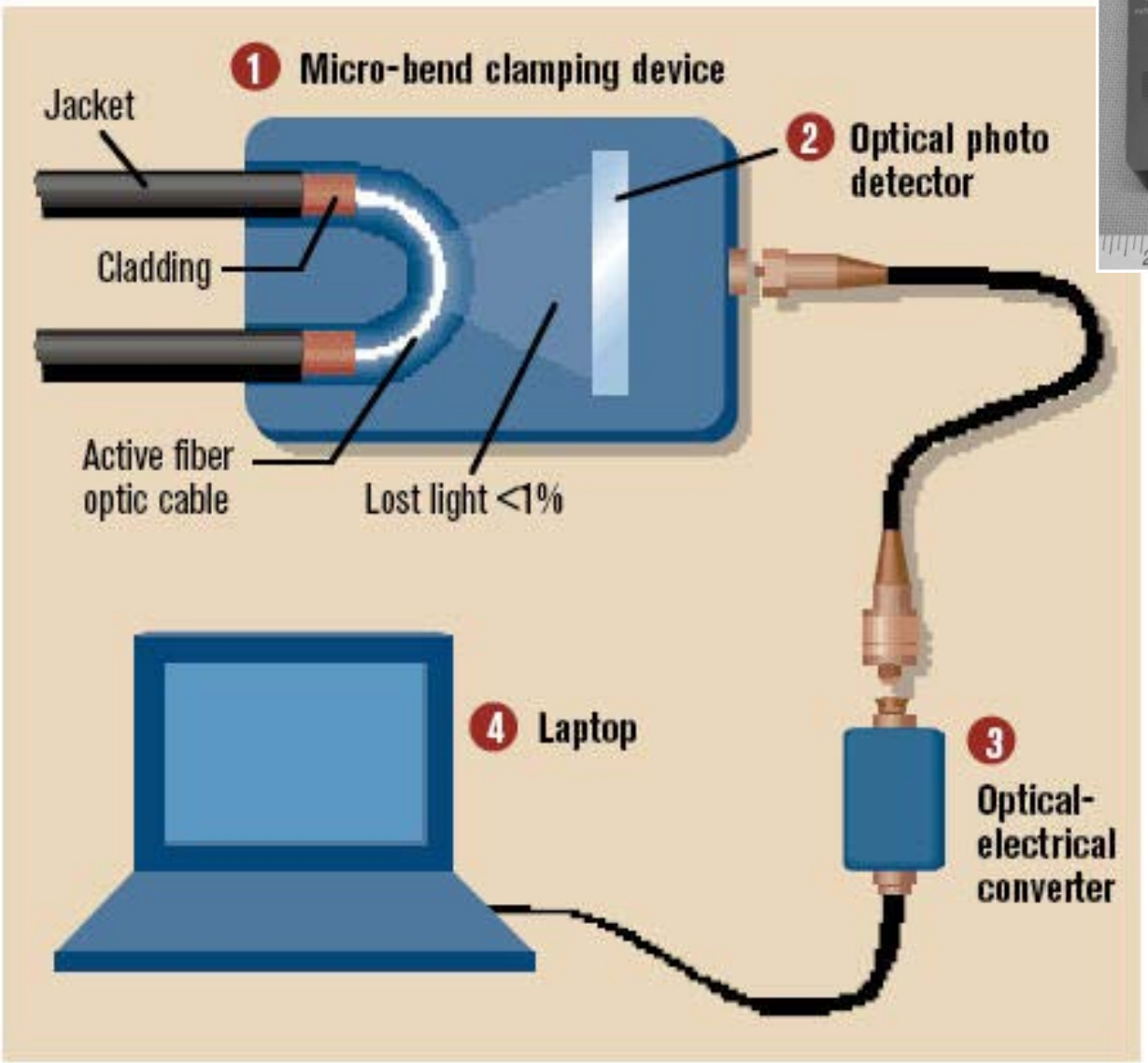
CS 161: Computer Security

Lecture 12

October 15, 2015

Stealing Photons



Operation Ivy Bells

By Matthew Carle
Military.com

At the beginning of the 1970's, divers from the specially-equipped submarine, USS Halibut (SSN 587), left their decompression chamber to start a bold and dangerous mission, code named "Ivy Bells".

The Regulus guided missile submarine, USS Halibut (SSN 587) which carried out Operation Ivy Bells.

In an effort to alter the balance of Cold War, these men scoured the ocean floor for a five-inch diameter cable carry secret Soviet communications between military bases.

The divers found the cable and installed a 20-foot long listening device on the cable. designed to attach to the cable without piercing the casing, the device recorded all communications that occurred. If the cable malfunctioned and the Soviets raised it for repair, the bug, by design, would fall to the bottom of the ocean. Each month Navy divers retrieved the recordings and installed a new set of tapes.

Upon their return to the United States, intelligence agents from the NSA analyzed the recordings and tried to decipher any encrypted information. The Soviets apparently were confident in the security of their communications lines, as a surprising amount of sensitive information traveled through the lines without encryption.

prison. The original tap that was discovered by the Soviets is now on exhibit at the KGB museum in Moscow.

Link Layer Threat Disruption

- Attackers can “jam” packets they don’t like (integrity)
- Attackers can overwhelm signaling (e.g., WiFi radio signals)

- There’s also the heavy handed approach…

Sabotage attacks knock out phone service

Nanette Asimov, Ryan Kim,Kevin Fagan, Chronicle Staff Writers
Friday, April 10, 2009

PRINT E-MAIL SHARE COMMENTS (477) FONT | SIZE:

(04-10) 04:00 PDT SAN JOSE --

Police are hunting for vandals who chopped fiber-optic cables and killed landlines, cell phones and Internet service for tens of thousands of people in Santa Clara, Santa Cruz and San Benito counties on Thursday.

IMAGES

View More Images

MORE NEWS

- Toyota seeks damage control, in public and private 02.09.10
- Snow shuts down federal government, life goes on 02.09.10
- Iran boosts nuclear enrichment, drawing warnings 02.09.10

The sabotage essentially froze operations in parts of the three counties at hospitals, stores, banks and police and fire departments that rely on 911 calls, computerized medical records, ATMs and credit and debit cards.

The full extent of the havoc might not be known for days, emergency officials said as they finished repairing the damage late Thursday.

Whatever the final toll, one thing is certain: Whoeve did this is in a world of trouble if he, she or they get caught.

"I pity the individuals who have done this," said San Jose Police Chief Rob Davis.

Ten fiber-optic cables carrying were cut at four locations in the predawn darkness. Residential and business customers quickly found that telephone service was perhaps more laced into their everyday needs than they thought. Suddenly they couldn't draw out money, send text messages, check e-mail or Web sites, call anyone for help, or eve check on friends or relatives down the road.

Several people had to be driven to hospitals because they were unable to summon ambulances. Many businesses lapsed into idleness for hours, without the ability to contact associates or customers.

More than 50,000 landline customers lost service - some were residential, others were business lines that needed the connections for ATMs, Internet and bank card transactions. One line alone could affect hundreds of users.

UPDATE LOOK Vancouver's Venues Shine Up

NEWS | LOCAL BEAT

$250K Reward Out for Vandals Who Cut AT&T Lines

Local emergency declared during outage

By LORI PREUITT

Updated 2:12 PM PST, Fri, Apr 10, 2009

PRINT EMAIL SHARE BUZZ UP! TWITTER FACEBOOK

AT&T is now offering a $250,000 reward for information leading to the arrest of whoever is responsible for severing lines fiber optic cables in San Jose tha left much of the area without phone or cell service Thursday.

John Britton of AT&T said the reward is the largest ever offered by the company.

Link-Layer Threat: Spoofing

- Attack can inject spoofed packets, and lie about the source address

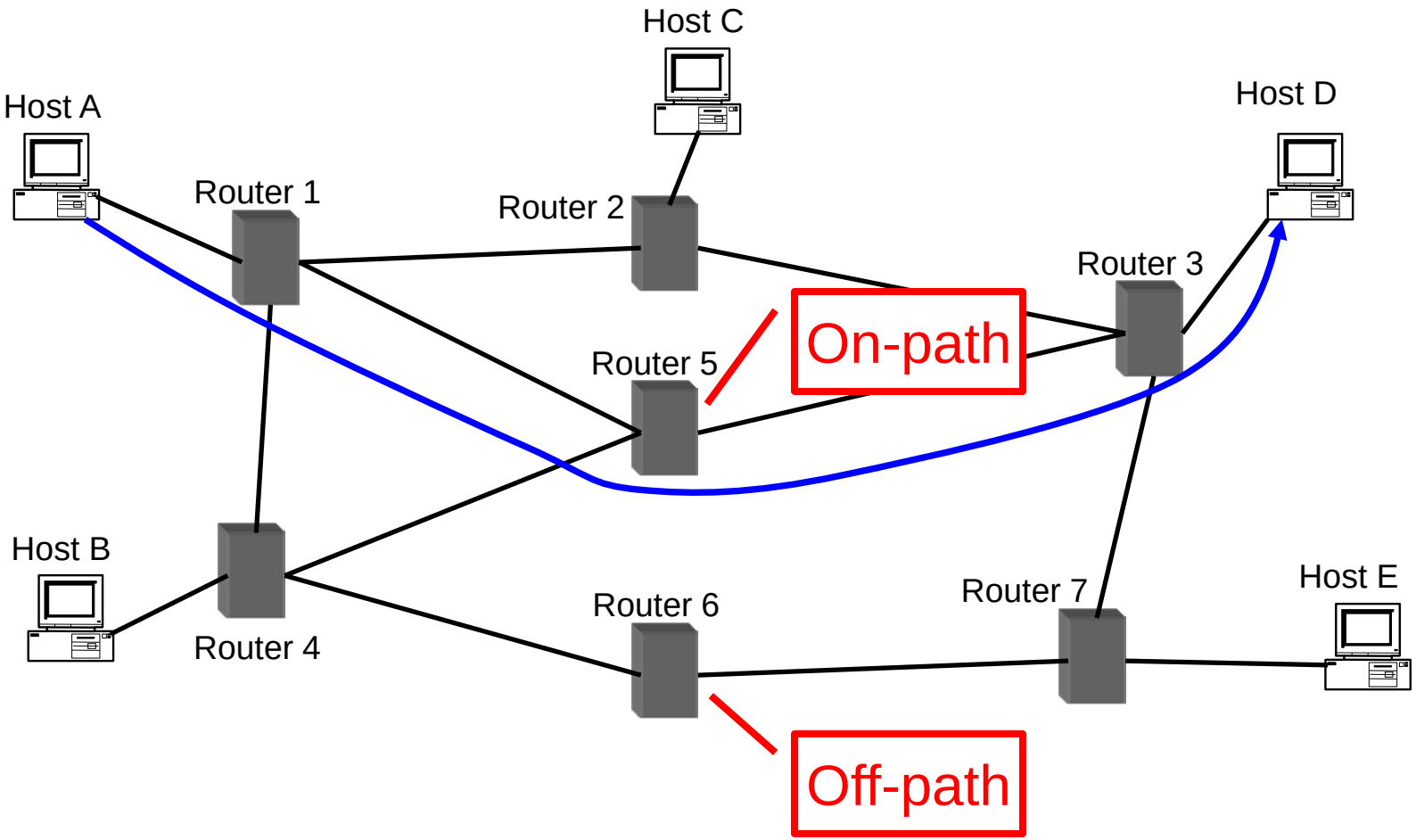
D	C	Hello world!

Physical/Link-Layer Threats: Spoofing

- Physical access allows attacker to create any message it likes
  - With a bogus source address: spoofing
  - May require root/administrative access
- Particularly powerful combined w/eavesdropping
  - Attacker understands state of victim's communication
  - Crafts communication to exploit it
- Spoofing w/o eavesdropping
  - *Blind spoofing*

On-path vs Off-path Spoofing

Host A communicates with Host D



Spoofing on the Internet

- On-path attackers see victim's traffic
  - Spoofing is easy
- Off-path attackers cannot see victim's traffic
  - Blind spoofing
  - Must infer packet header values
  - We care about work factor
  - Brute force: try all 16 bit (65,536) values
  - When we say attacker "can spoof" we mean "can spoof with a reasonable chance of success"

Layer 3: General Threats?

7	**Application**
4	**Transport**
3	**(Inter)Network**
2	**Link**
1	**Physical**

Bridges multiple "subnets" to provide end-to-end internet connectivity between nodes

4-bit Version	4-bit Header Length	8-bit Type of Service (TOS)	16-bit Total Length (Bytes)
16-bit Identification		3-bit Flags	13-bit Fragment Offset
8-bit Time to Live (TTL)	8-bit Protocol	16-bit Header Checksum	
32-bit Source IP Address			
32-bit Destination IP Address			
Payload			

IP = Internet Protocol

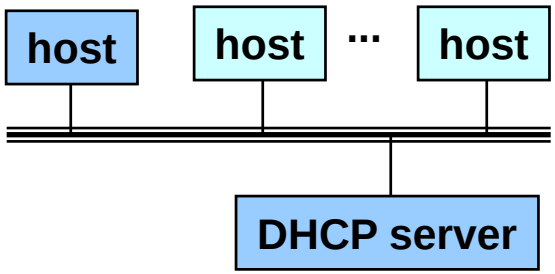
IP-Layer Threats

- Can set arbitrary source address
  - Spoofing
    - Blind or with “sniffing”
- Can set arbitrary destination address
  - “Scanning”: brute force searching for hosts
- Can “flood”: send many packets
  - IP has no general mechanism for tracking overuse
  - IP has no general mechanism for tracking consent
  - Hard to tell source of flood
- Can manipulate routing
  - Bring traffic to self for eavesdropping (not easy)

LAN Bootstrapping: DHCP

- New host doesn't have an IP address yet
  - So, host doesn't know what source address to use
- Host doesn't know *who to ask* for an IP address
  - So, host doesn't know what destination address to use

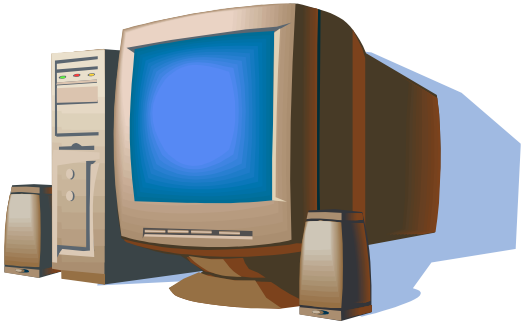
- Solution: shout to "**discover**" server that can help
  - Broadcast a server-discovery message (layer 2)
  - Server(s) sends a reply offering an address



Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

DHCP request (broadcast)

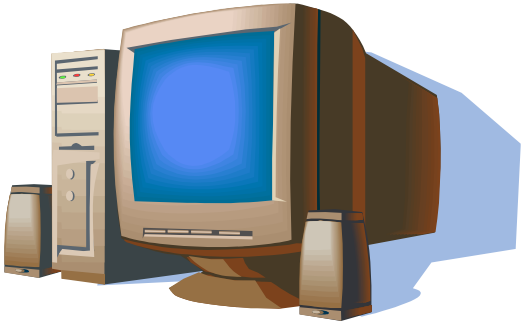
DHCP ACK

Threats?

Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

DHCP request (broadcast)

DHCP ACK

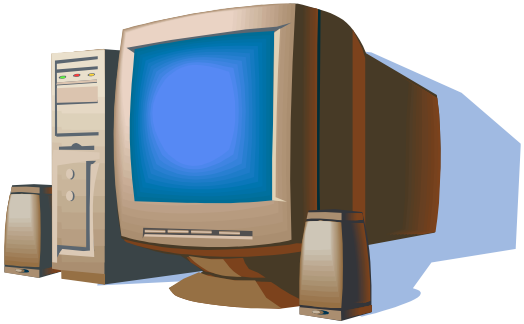
Attacker on same subnet can **hear** new host's DHCP request

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

DHCP request (broadcast)

DHCP ACK

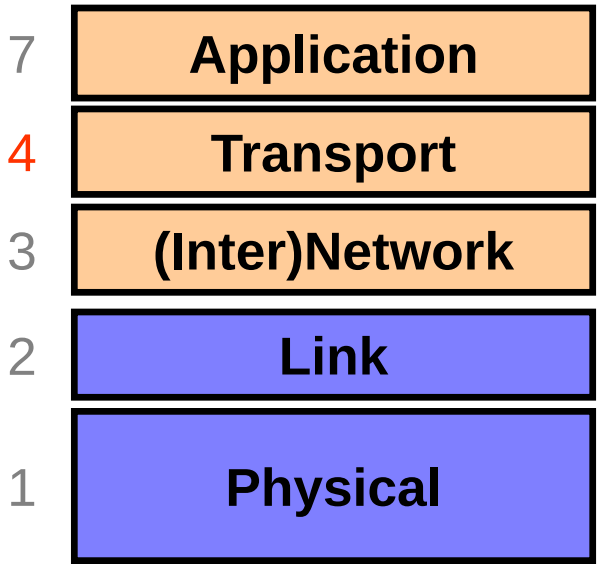
"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

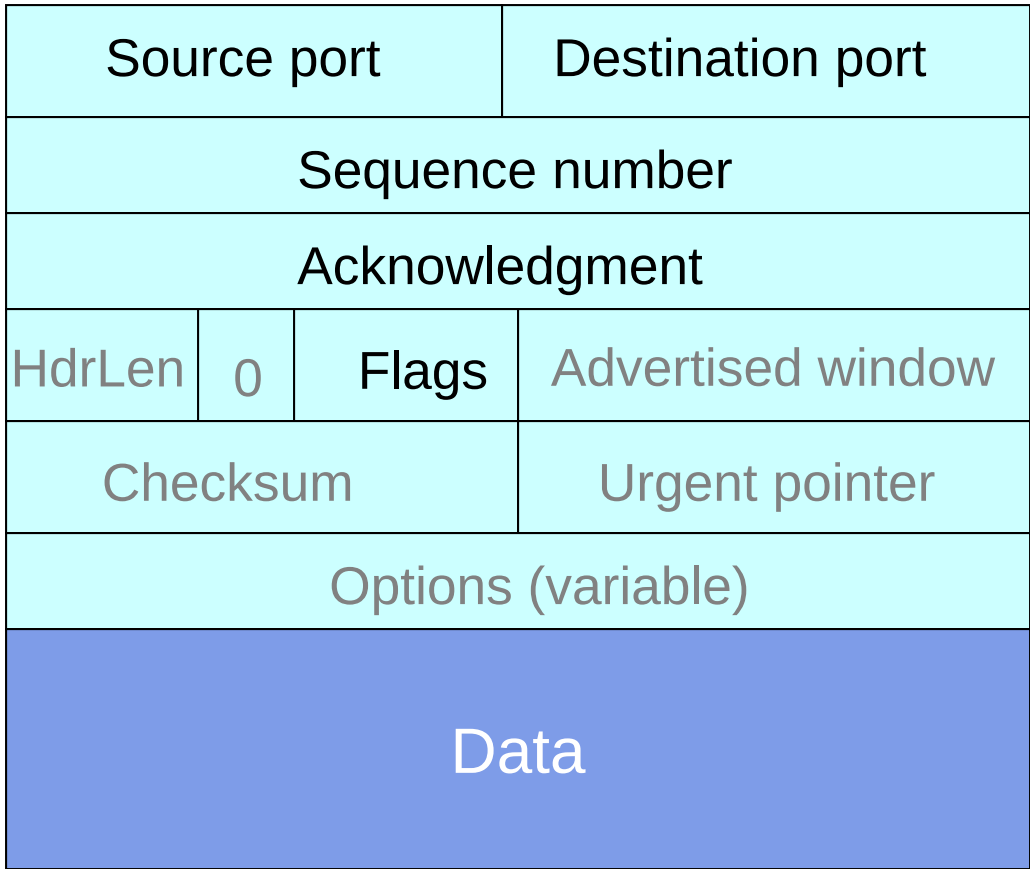
Attacker can **race** the actual server; if they win, replace DNS server and/or gateway router

DHCP Threats

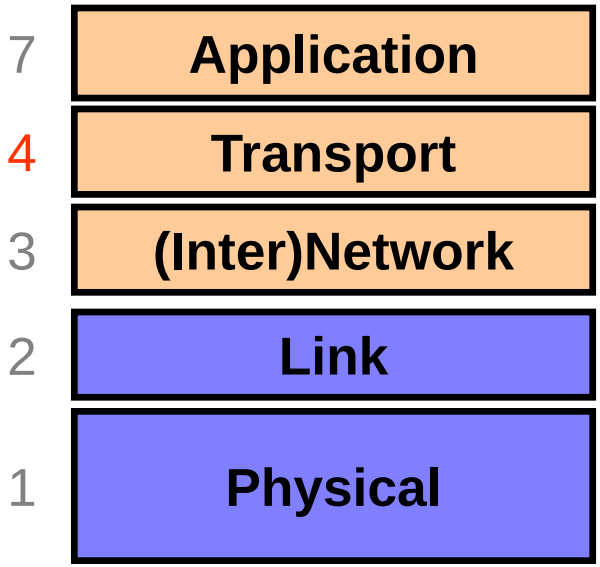
- Substitute a fake DNS server
  - Redirect any of a host's lookups
- Substitute a fake gateway router
  - Intercept all of a host's off-subnet traffic
    - (even if not preceded by DNS lookup)
  - Relay contents to remote server
    - (allows full modification)
  - Allows "man in the middle attack"
    - Undetectable
      - DHCP can have multiple replies benignly
- Fixing this is hard

TCP

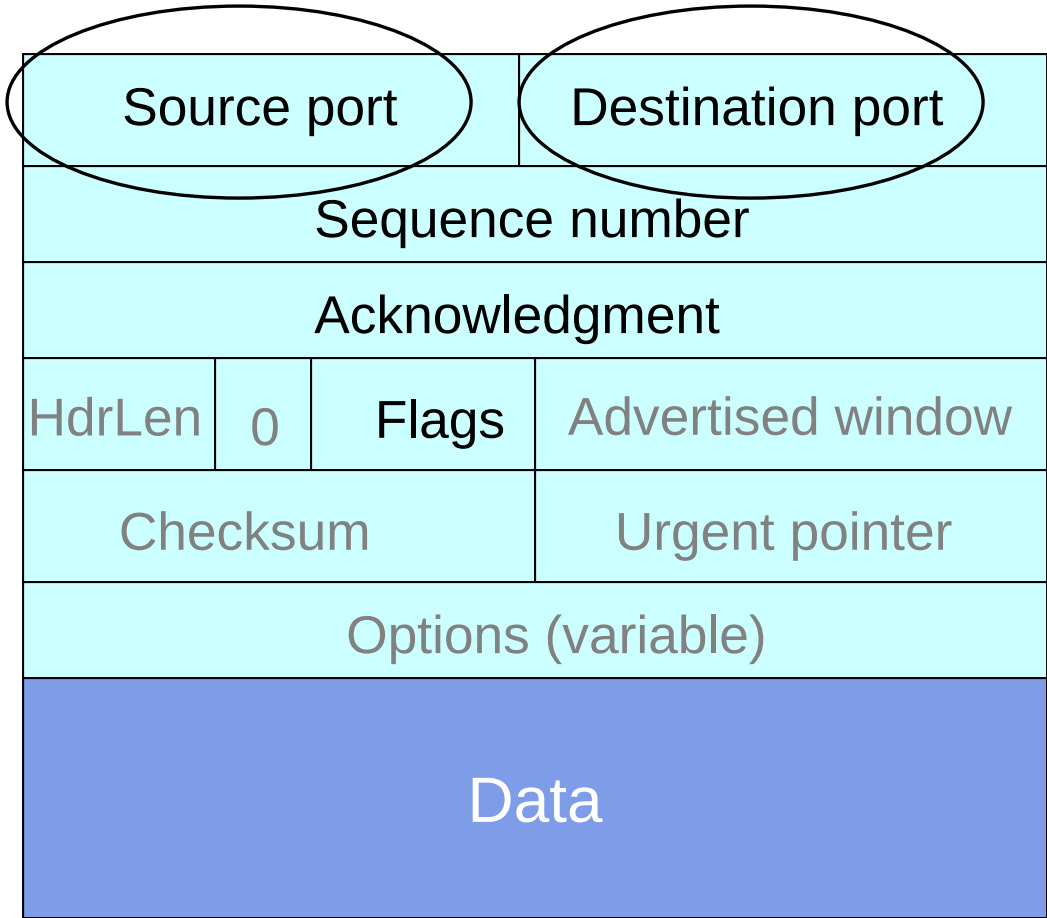

7
Application
4
Transport
3
(Inter)Network
2
Link
1
Physical


Source port
Destination port
Sequence number
Acknowledgment
HdrLen
0
Flags
Advertised window
Checksum
Urgent pointer
Options (variable)
Data

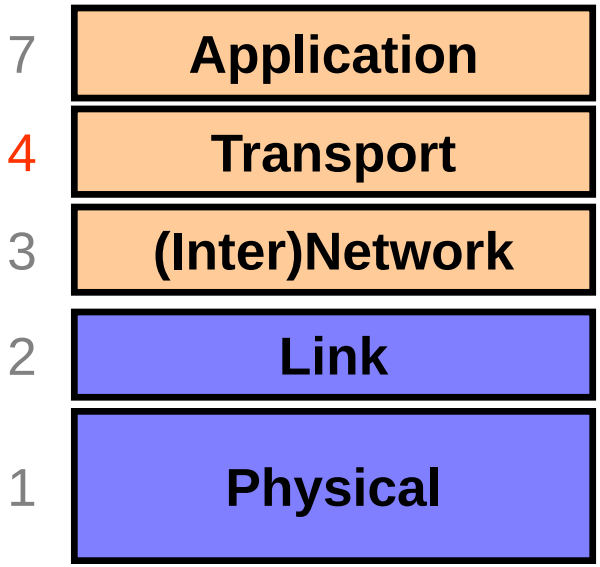
TCP



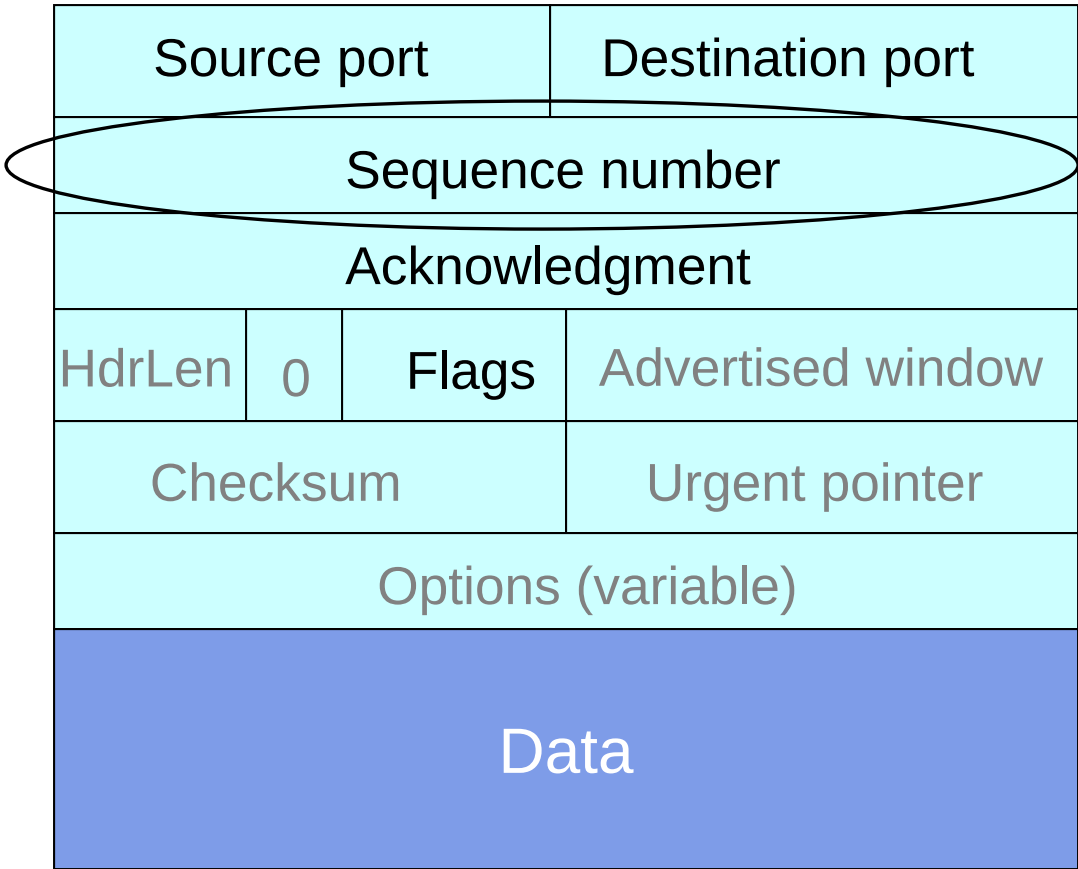
These plus IP addresses define a given connection



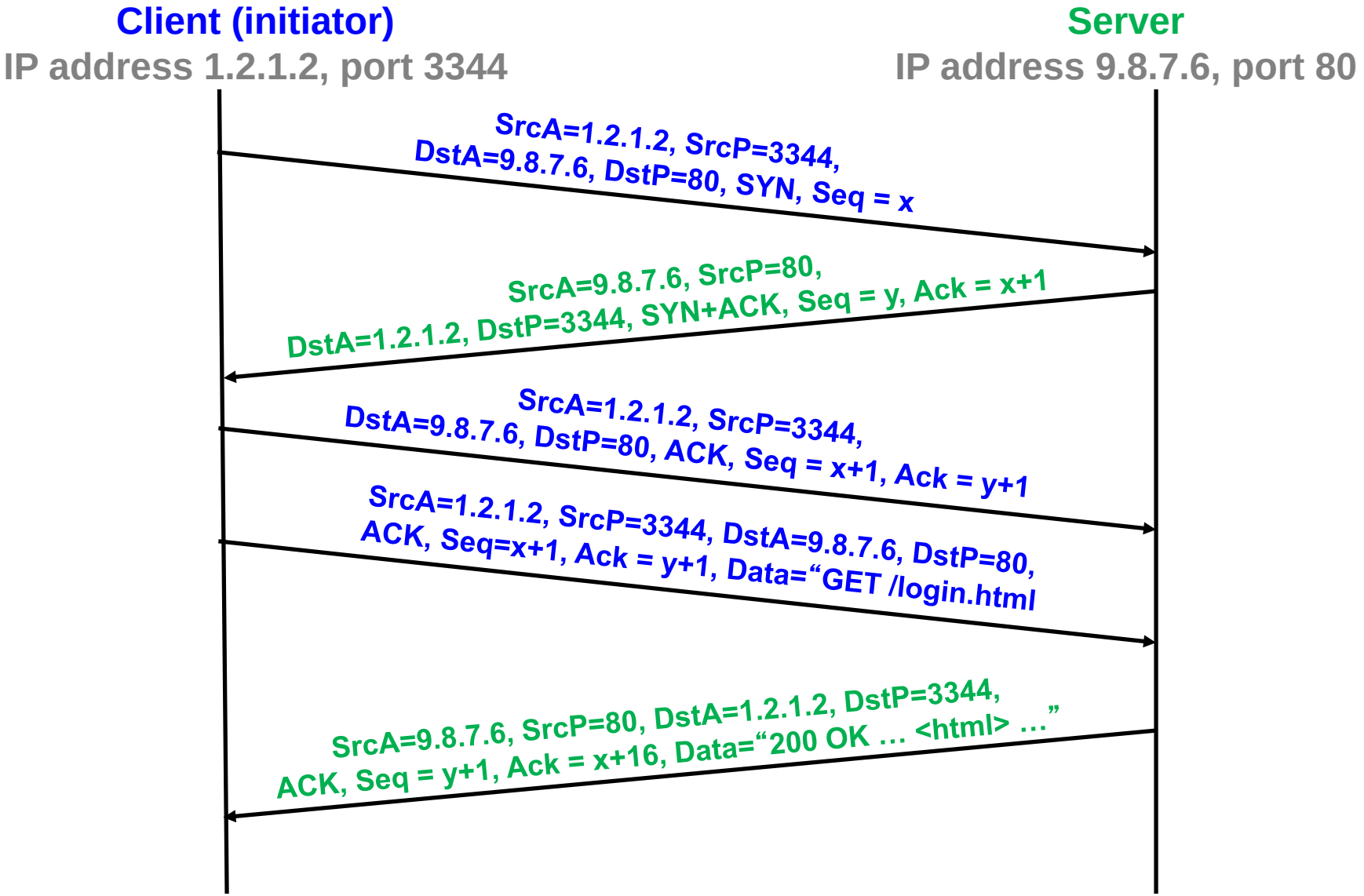
TCP



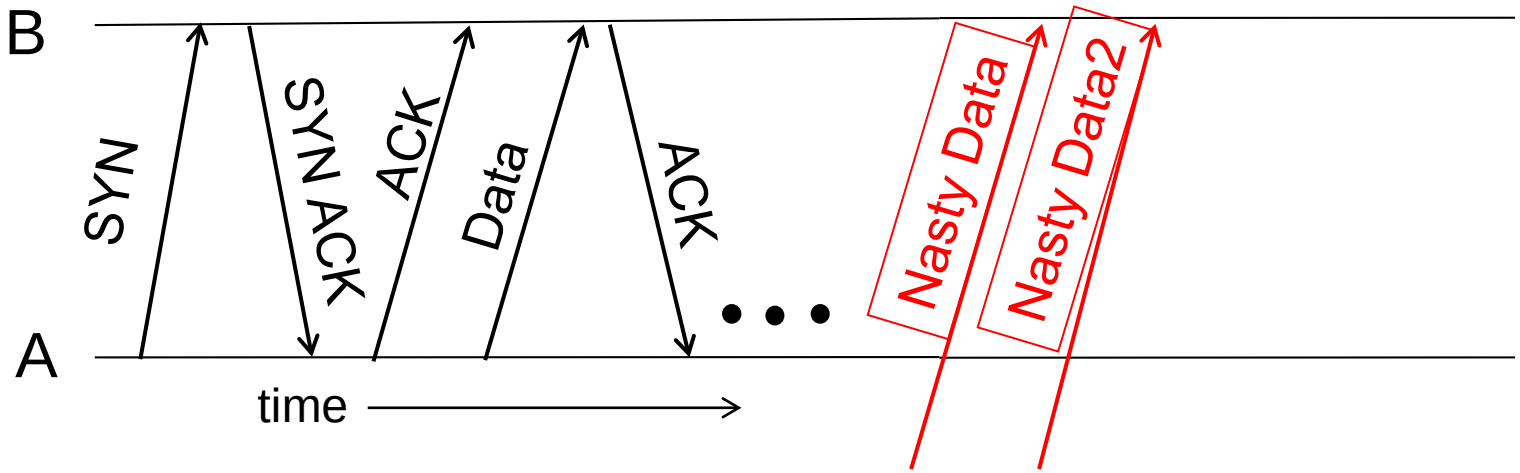
Defines where this packet fits within the sender's bytestream



TCP Conn. Setup & Data Exchange

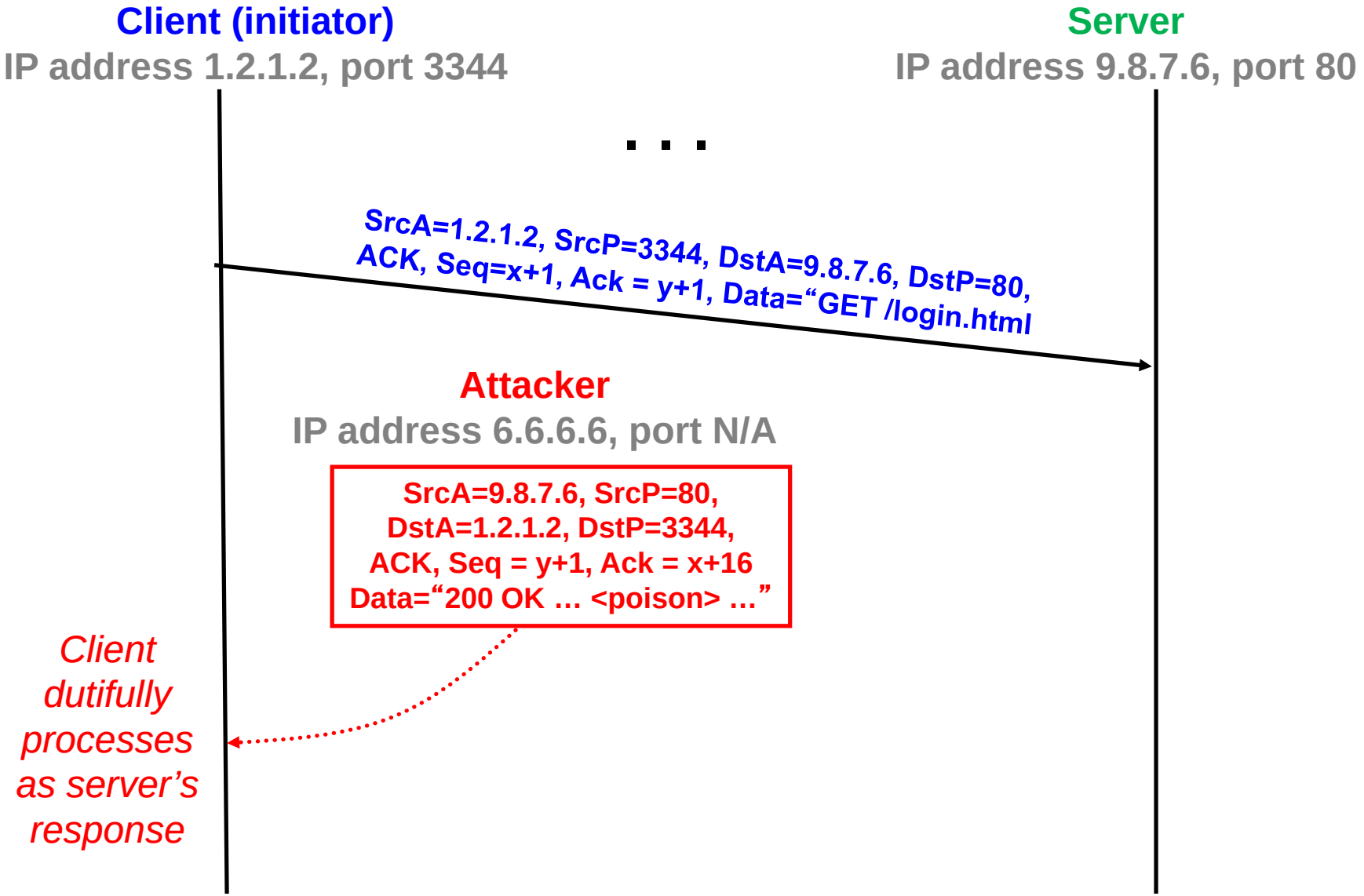


TCP Threat: Data Injection

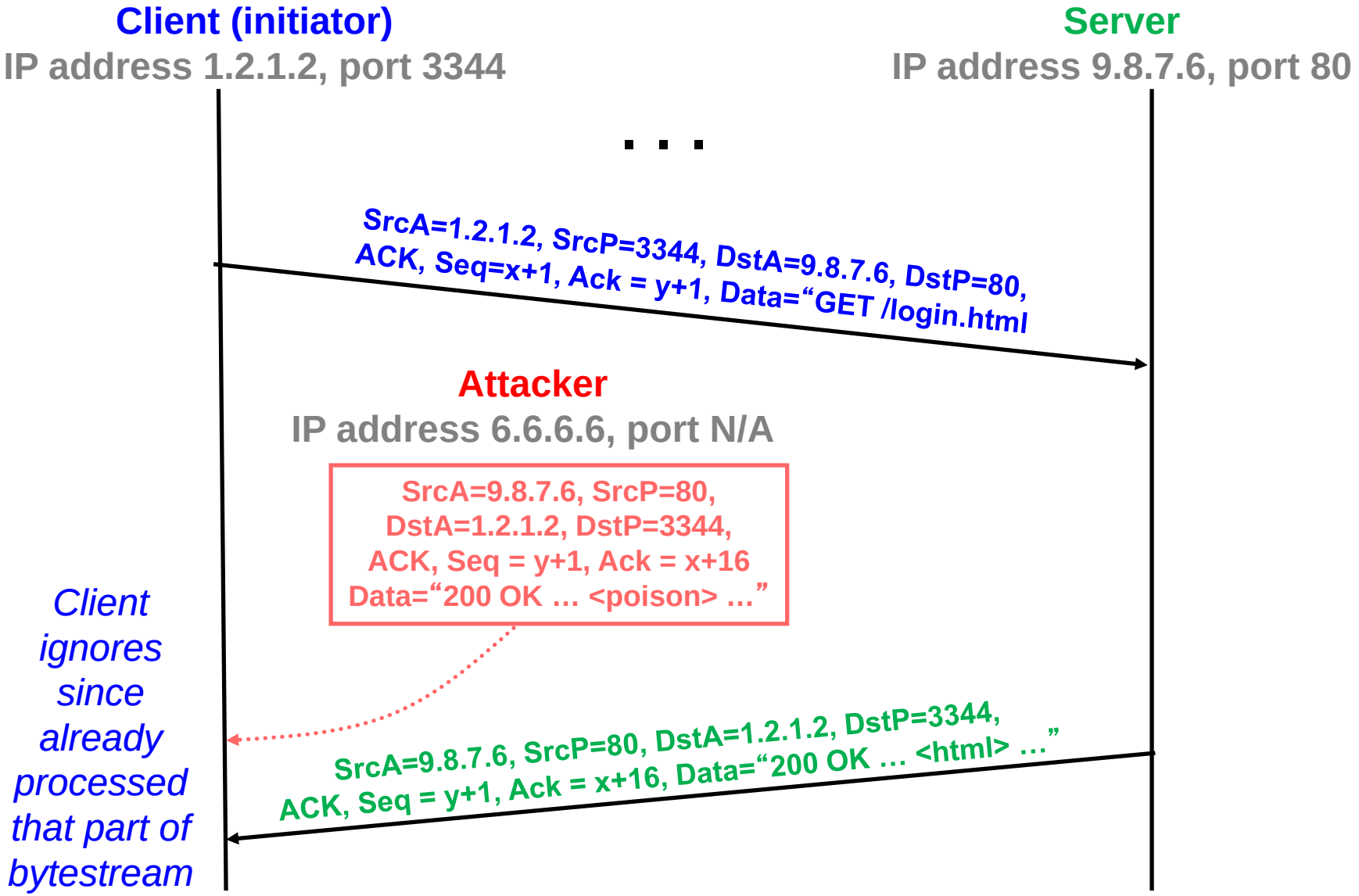


- If attacker knows ports & sequence numbers (e.g., on-path attacker), attacker can inject data into any TCP connection
  - Receiver B is none the wiser
- Termed TCP connection hijacking (or “session hijacking”)
  - A general means to take over an already-established connection
- We are toast if an attacker can see our TCP traffic
  - Because then they immediately know the port & sequence numbers

TCP *Data Injection*



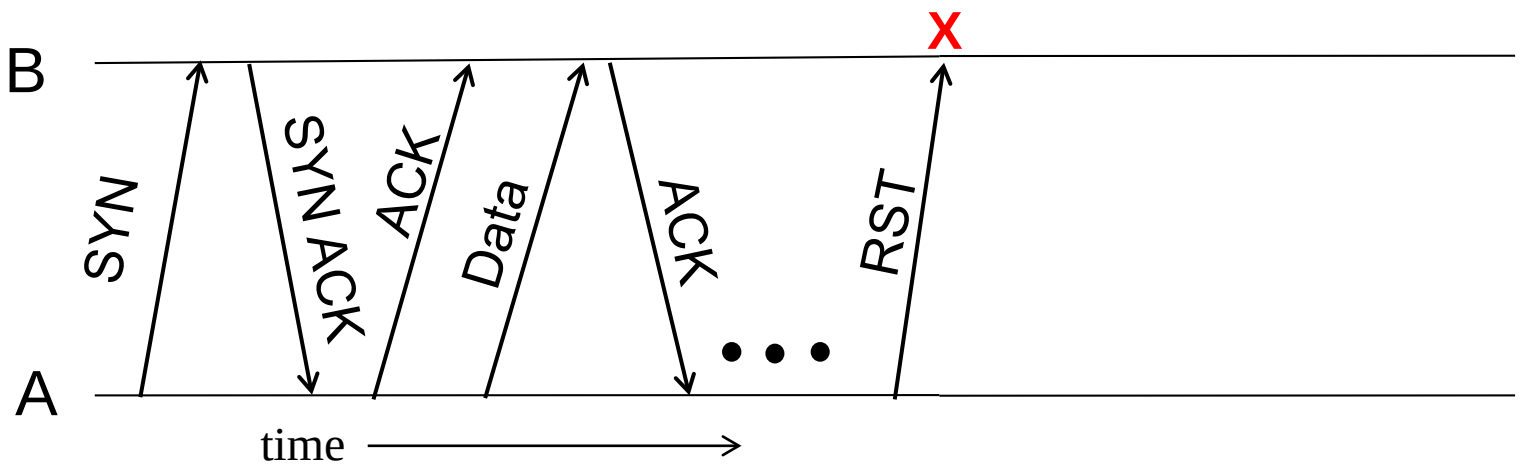
TCP *Data Injection*



TCP Threat disruption

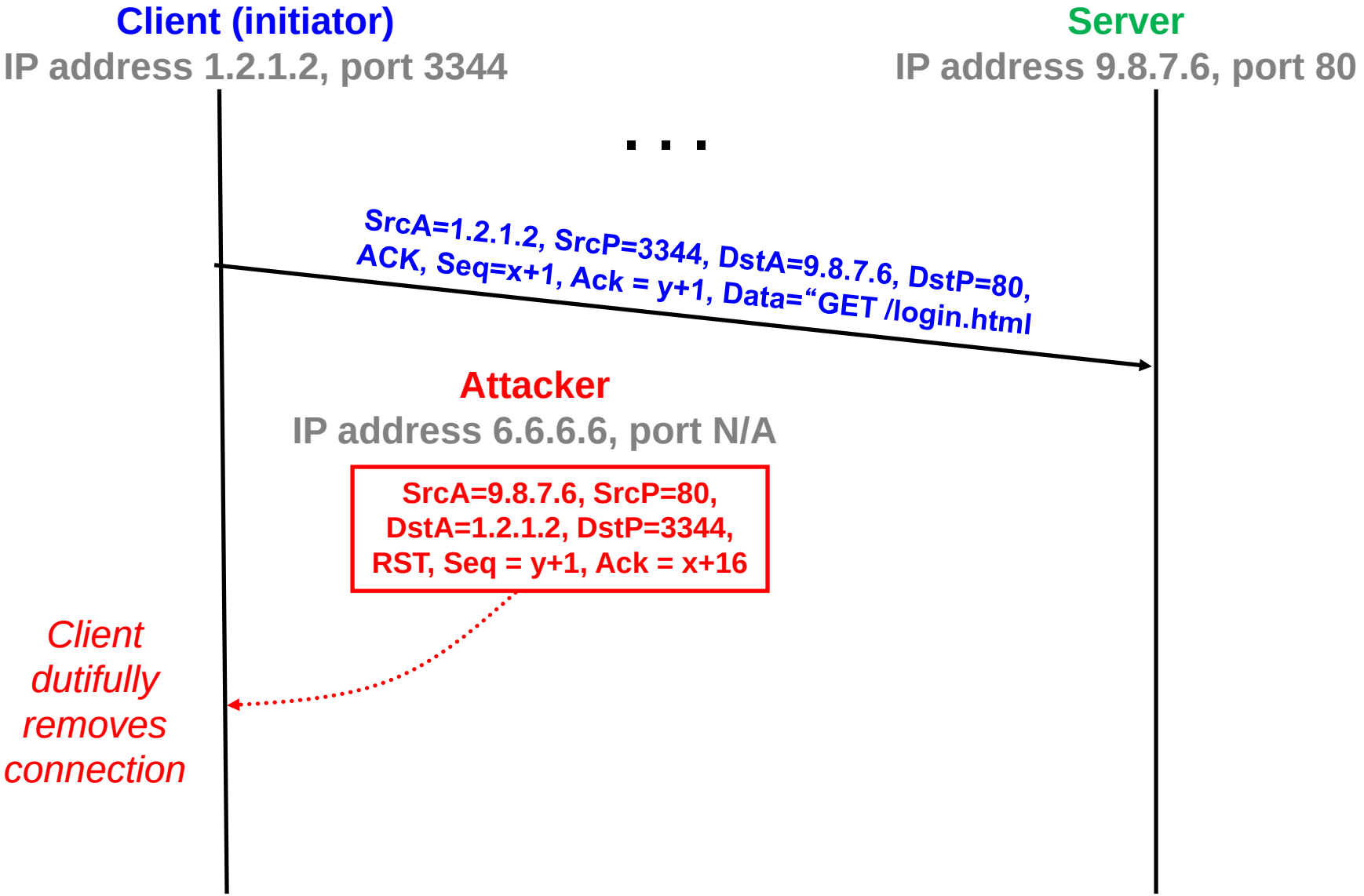
- Can on-path attack shutdown a TCP connection?
- Yes: it can infer the port and sequence numbers
  - And insert fake data too
- (Great Firewall of China)
  - Normally TCP closes connection with FIN packet
    - Reliably delivered, other side must ACK
  - But RST will immediately terminate connection
    - Used for dead processes or inconsistent data
    - Unilateral
    - Requires correct sequence number

Abrupt Termination

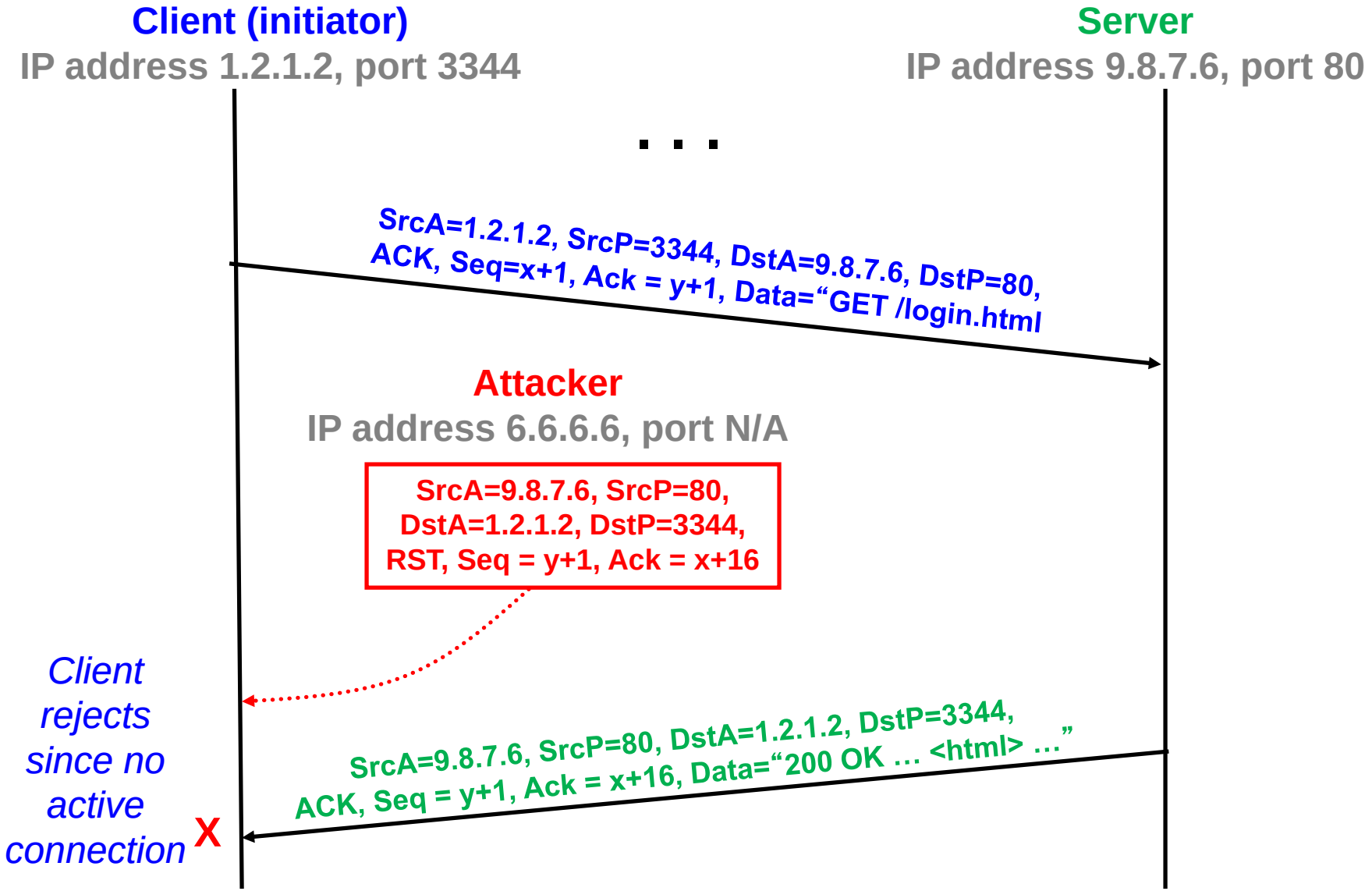


- A sends a TCP packet with RESET (**RST**) flag to B
  - E.g., because app. process on A crashed
  - (Could instead be that B sends a RST to A)
- Assuming that the sequence numbers in the **RST** fit with what B expects, That's It:
  - B's user-level process receives: **`ECONNRESET`**
  - No further communication on connection is possible

TCP *RST Injection*



TCP *RST Injection*



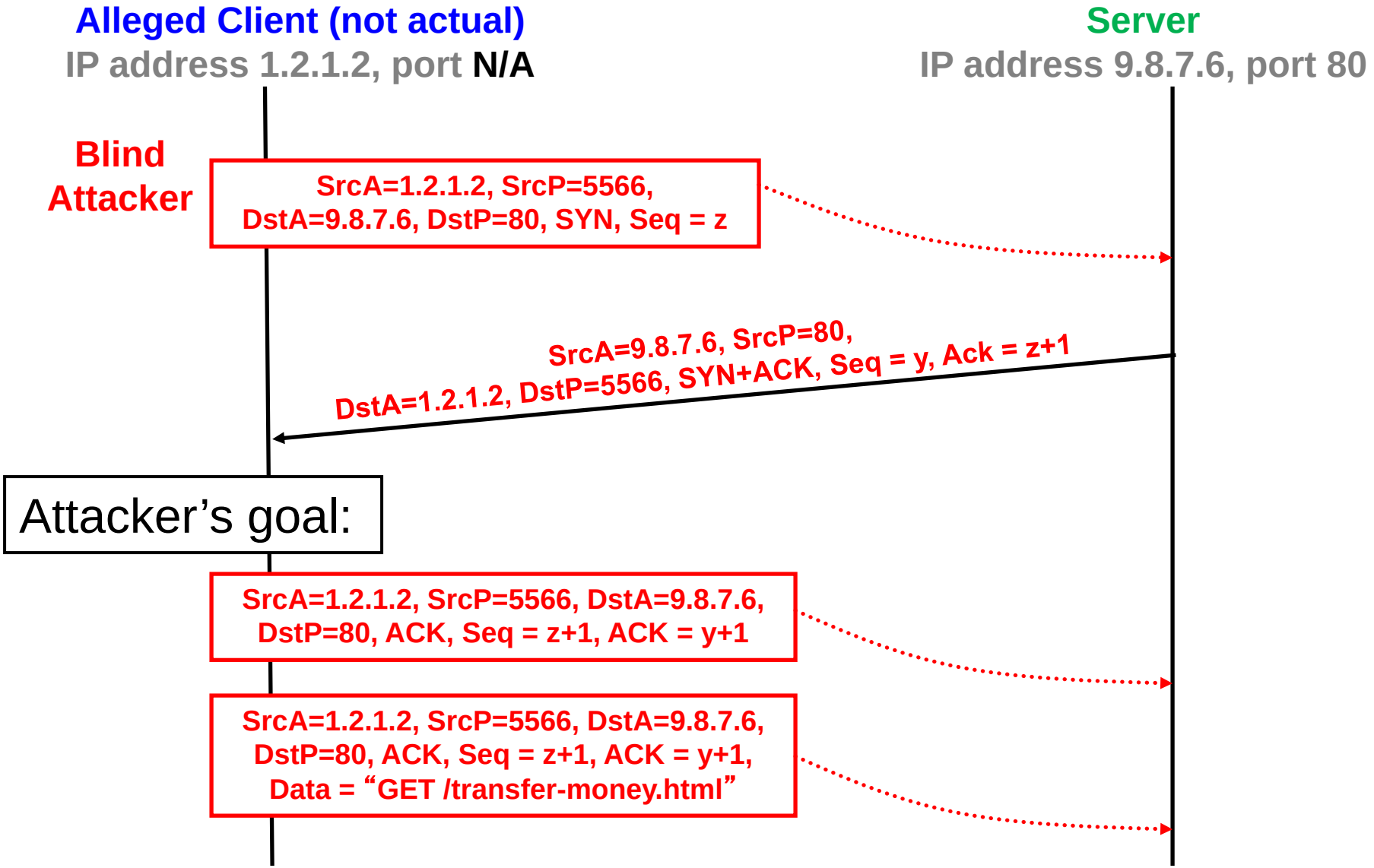
TCP Threat: Blind Hijacking

- Can off-path attack inject into a TCP connection?
- Yes, if it can infer or guess port & sequence #s

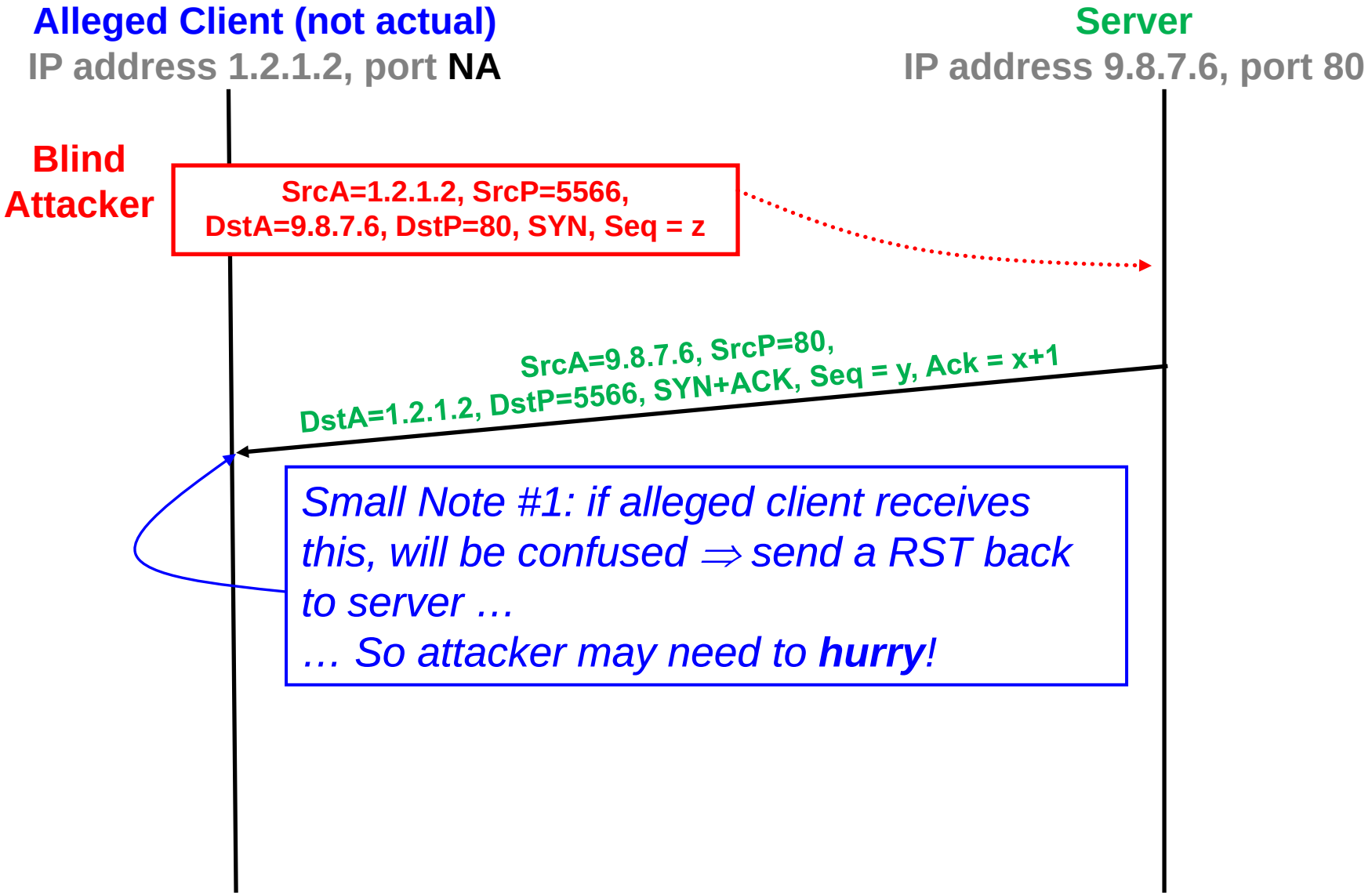
TCP Threat: Blind Spoofing

- Can off-path attack create fake TCP connection?
- Yes, if it can infer or guess port & sequence #s
- Why would attacker want to do this?
  - Perhaps to leverage trust associated with IP address
  - Perhaps to frame an IP address with an attack

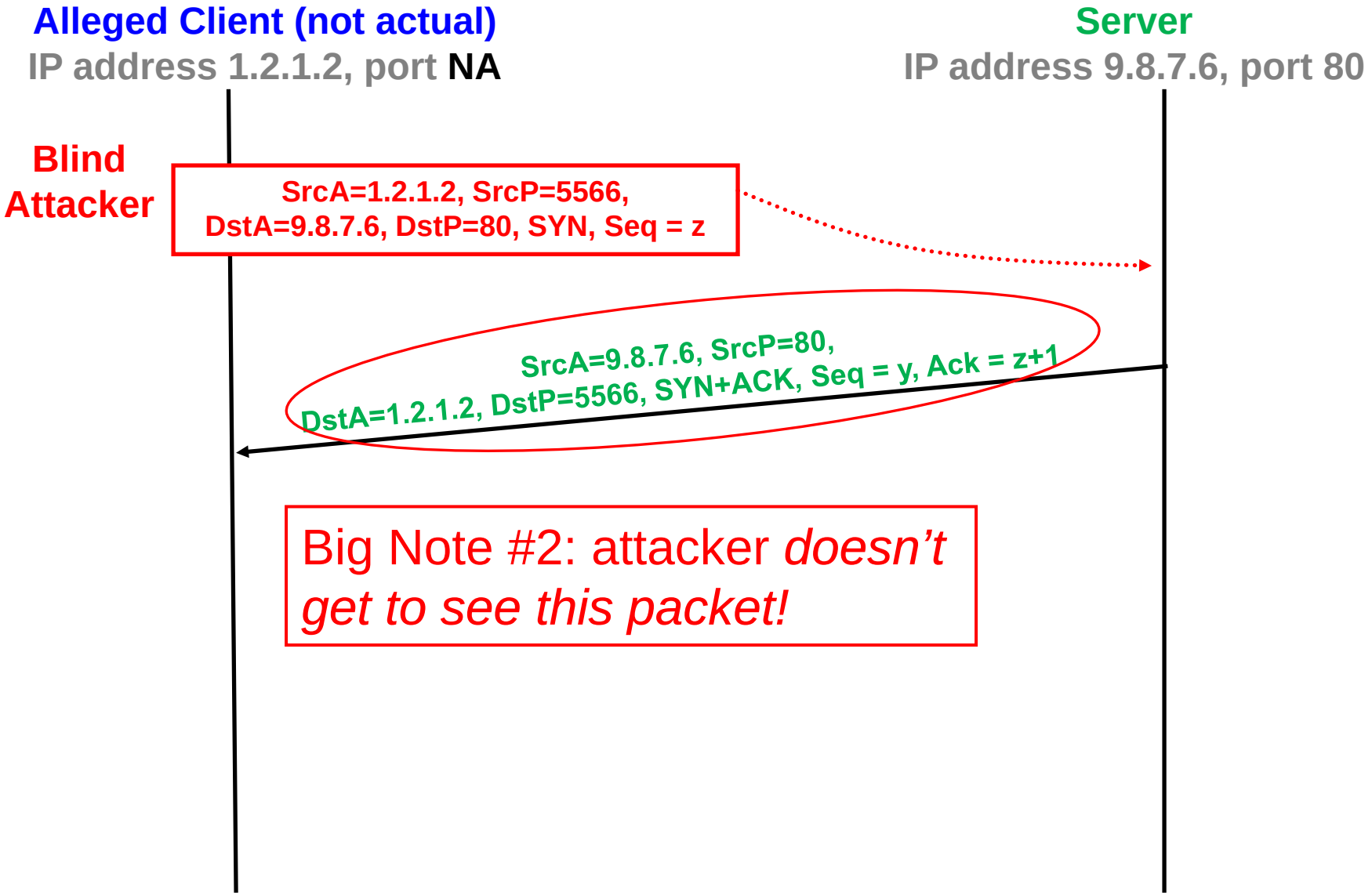
Blind Spoofing on TCP Handshake



Blind Spoofing on TCP Handshake

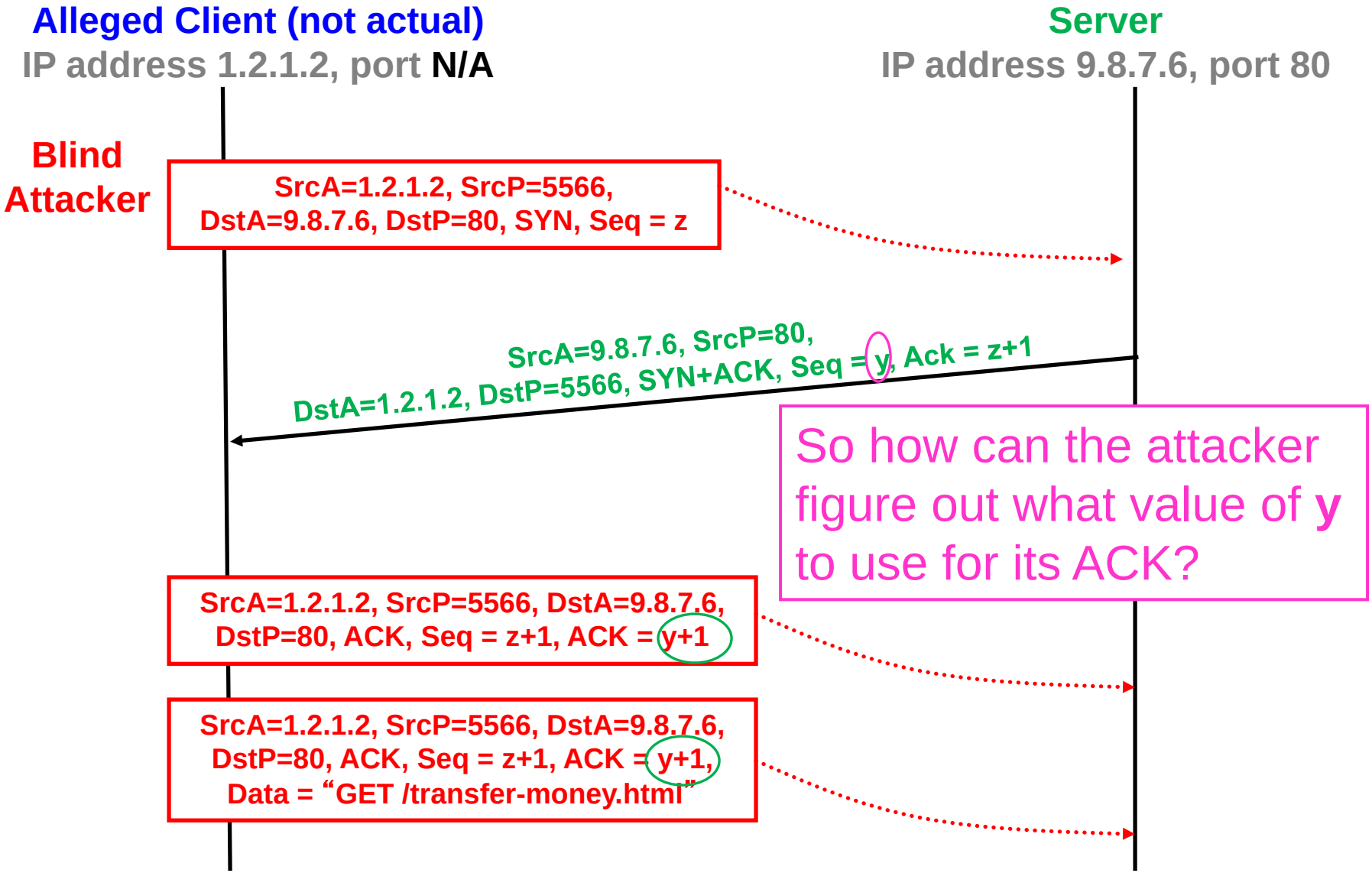


Blind Spoofing on TCP Handshake

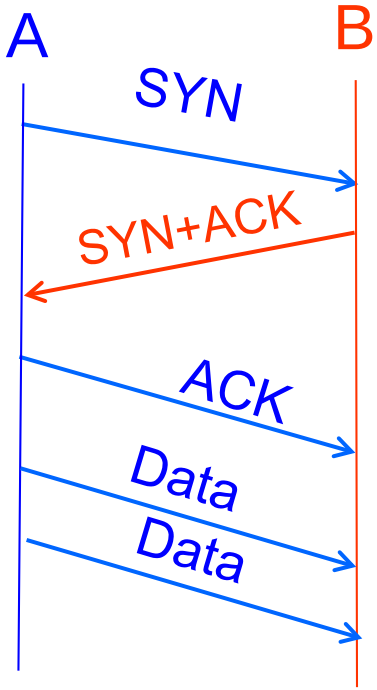


Big Note #2: attacker *doesn't get to see this packet!*

Blind Spoofing on TCP Handshake



Reminder: Establishing a TCP Connection



Each host tells its *Initial Sequence Number* (ISN) to the other host.

(Spec says to pick based on local clock)

Hmm, any way for the attacker to know ***this?***

How Do We Fix This?

Use a (Pseudo)-*Random* ISN

Sure - make a non-spoofed connection *first*, and see what server used for ISN then!

Summary of TCP Security Issues

- Observable TCP can be manipulated
  - Can be terminated by forging RST packet
  - Inject data in either direction by forging packets
  - Works because sequence #s are known
  - Remains a major threat today
- If ISNs can be predicted, easy to blind spoof
  - Undermines trust based on IP addresses
  - IP addressed can be “framed”
  - Fixed (mostly) today by using random ISNs

Summary of IP Security Issues

- No security against on-path attackers
  - Can sniff, inject packets, spoof TCP, hijack TCP, man-in-the-middle
  - Example: wireless networks
  - Example: malicious network operator
- Partial security against off-path attackers
  - TCP is reasonably secure
  - UDP and IP are not secure

Attacks on Availability

- Denial-of-Service (DoS)
- Preventing legitimate users from using a service

- We need to consider our threat model
- What might motivate a DoS attack?

Botnets Beat Spartan Laser on *Halo 3*

By Kevin Poulsen February 4, 2009 | 12:13 pm | Categories: Cybarmageddon!

What's the most powerful weapon you can wield when playing *Halo 3* online?

I know. You can control the entire map with a battle rifle and a couple of sticky grenades. But that teeny-bopper you just pwned has you beat with the tiny botnet he leased with his allowance money.

KrebsonSecurity

In-depth security news and investigation

There are dozens of underground forums where members advertise their ability to execute debilitating "distributed denial-of-service" or DDoS attacks for a price. DDoS attack services tend to charge the same prices, and the average rate for taking a Web site offline is surprisingly affordable: about $5 to $10 per hour; $40 to $50 per day; $350-$400 a week; and upwards of $1,200 per month.

An ad for a DDoS attack service.

Of course, it pays to read the fine print before you enter into any contract. Most DDoS services charge varying rates depending on the complexity of the target's infrastructure, and how much lead time the attack service is given to size up the mark. Still, buying in bulk always helps: One service advertised on several fraud forums offered discounts for regular and wholesale customers.

Extortion via DDoS on the rise

By Denise Pappalardo and Ellen Messmer, Network World, 05/16/05

Criminals are increasingly targeting corporations with distributed denial-of-service attacks designed not to disrupt business networks but to extort thousands of dollars from the companies.

Ivan Maksakov, Alexander Petrov and Denis Stepanov were accused of receiving $4 million from firms that they threatened with cyberattacks.

The trio concentrated on U.K. Internet gambling sites, according to the prosecution. One bookmaker, which refused to pay a demand for $10,000, was attacked and brought offline--which reportedly cost it more than $200,000 a day in lost business.

NOV 06

8

DDoS makes a phishing e-mail look real

Posted by Munir Kotadia @ 12:00

0 comments

Just as Internet users learn that clicking on a link in an e-mail purporting to come from their bank is a bad idea, phishers seem to be developing a new tactic -- launch a DDoS attack on the Web site of the company whose customers they are targeting and then send e-mails "explaining" the outage and offering an "alternative" URL.

November 17th, 2008

Anti fraud site hit by a DDoS attack

Posted by Dancho Danchev @ 4:01 pm

Categories: Botnets, Denial of Service (DoS), Hackers, Malware, Pen testing...

Tags: Security, Cybercrime, DDoS, Fraud, Bobbear...

9 TalkBacks

ADD YOUR OPINION

SHARE

PRINT

E-MAIL

WORTHWHILE? 4 VOTES

The popular British anti-fraud site **Bobbear.co.uk** is currently under a DDoS attack (distributed denial of service attack) , originally launched last Wednesday, and is continuing to hit the site with 3/4 million hits daily from hundreds of thousands of malware infected hosts mostly based in Asia and Eastern Europe, according to the site's owner. Targeted DDoS attacks against anti-fraud and volunteer cybercrime fighting communities clearly indicate the impact these communities have on the revenue stream of scammers, and with Bobbear attracting such a high profile underground attention, the site is indeed doing a very good job.

Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites

Ethan Zuckerman, Hal Roberts, Ryan McGrady, Jillian York, John Palfrey[†]

The Berkman Center for Internet & Society at Harvard University

December 2010

---

9. In the past year, has your site been subjected to a denial of service attack, meaning an attacker prevented or attempted to prevent access to your site altogether?

#	Answer	Bar	Response	%
1	yes		21	62%
2	no		8	24%
3	not sure		5	15%
	Total		34	

Row over Korean election DDoS attack heats up

Ruling party staffer accused of disrupting Seoul mayoral by-election

By **John Leyden** • **Get more from this author**

Posted in Security, 7th December 2011 09:23 GMT

Free whitepaper – IBM System Networking RackSwitch G8124

A political scandal is brewing in Korea over alleged denial of service attacks against the National Election Commission (NEC) website.

Police have arrested the 27-year-old personal assistant of ruling Grand National Party politician Choi Gu-sik over the alleged cyber-assault, which disrupted a Seoul mayoral by-election back in October.

However, security experts said that they doubt the suspect, identified only by his surname "Gong", had the technical expertise or resources needed to pull off the sophisticated attack.

Gong continues to protest his innocence, a factor that has led opposition politicians to speculate that he is covering up for higher-ranking officials who ordered the attack.

Democratic Party politician Baek Won-woo told *The HankYoreh*: “We need to determine quickly and precisely whether there was someone up the line who ordered the attack, and whether there was compensation.” ®

Russia accused of unleashing cyberwar to disable Estonia

- Parliament, ministries, banks, media targeted
- Nato experts sent in to strengthen defences

Ian Traynor in Brussels
The Guardian, Thursday 17 May 2007
Article history

Bronze Soldier, the Soviet war memorial removed from Tallinn. Nisametdinov/AP

A three-week wave of massive cyber-attacks on the small Baltic country of Estonia, the first known incidence of such an assault on a state, is causing alarm across the western alliance, with Nato urgently examining the offensive and its implications.

August 11th, 2008

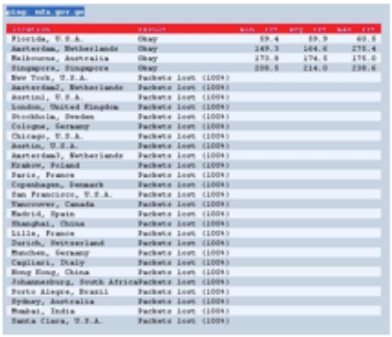
Coordinated Russia vs Georgia cyber attack in progress

Posted by Dancho Danchev @ 4:23 pm

Categories: Black Hat, Botnets, Denial of Service (DoS), Governments, Hackers...
Tags: Security, Cyber Warfare, DDoS, Georgia, South Osetia...

62 TalkBacks ADD YOUR OPINION | SHARE | PRINT | E-MAIL | WORTHWHILE? +18 24 VOTES

In the wake of the Russian-Georgian conflict, a week worth of speculations around Russian Internet forums have finally materialized into a coordinated cyber attack against Georgia's Internet infrastructure. The attacks have already managed to compromise several government web sites, with continuing DDoS attacks against numerous other Georgian government sites, prompting the government to switch to hosting locations to the U.S, with Georgia's Ministry of Foreign Affairs undertaking a desperate step in order to disseminate real-time information by moving to a Blogspot account.



Posted on Tuesday, August 12th, 2008 | Bookmark on del.icio.us

Georgia DDoS Attacks - A Quick Summary of Observations

by Jose Nazario

The clashes between Russia and Georgia over the region of South Ossetia have been shadowed by attacks on the Internet. As we noted in July, the Georgia presidential website fell victim to attack during a war of words. A number of DDoS attacks have

> Raw statistics of the attack traffic paint a pretty intense picture. We can discern that the attacks would cause injury to almost any common website.

Average peak bits per second per attack	211.66 Mbps
Largest attack, peak bits per second	814.33 Mbps
Average attack duration	2 hours 15 minutes
Longest attack duration	6 hour

ATLAS Peak Monitored Attack Sizes Month-By-Month (January 2009-Present)

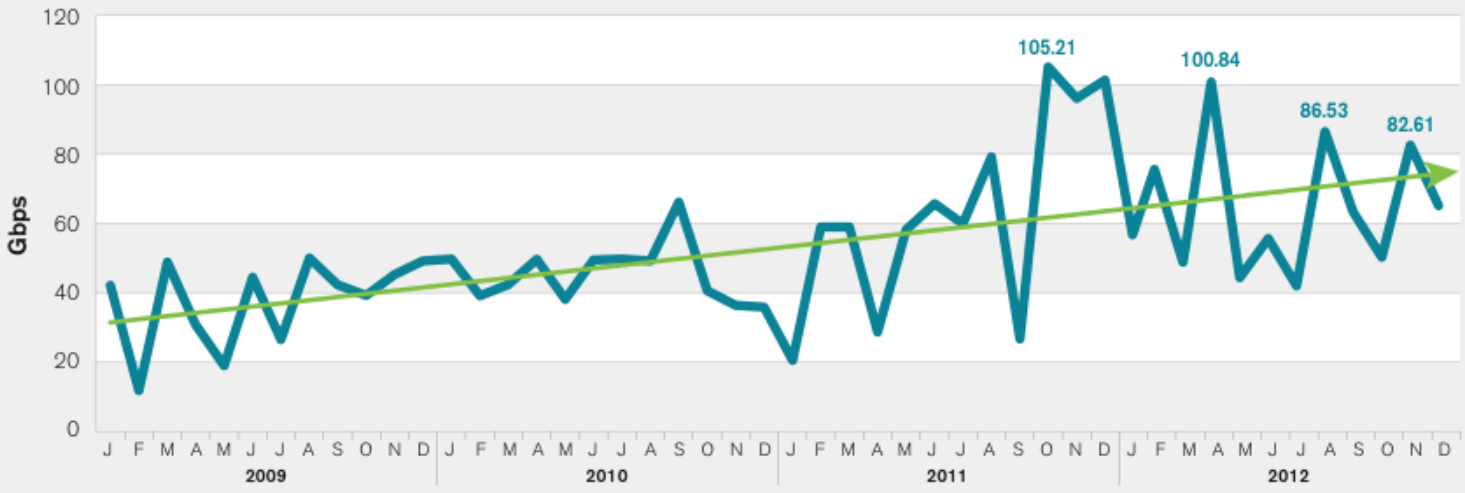


Figure 17 *Source: Arbor Networks, Inc.*

ATLAS Average Monitored Attack Sizes Month-By-Month (January 2009-Present)

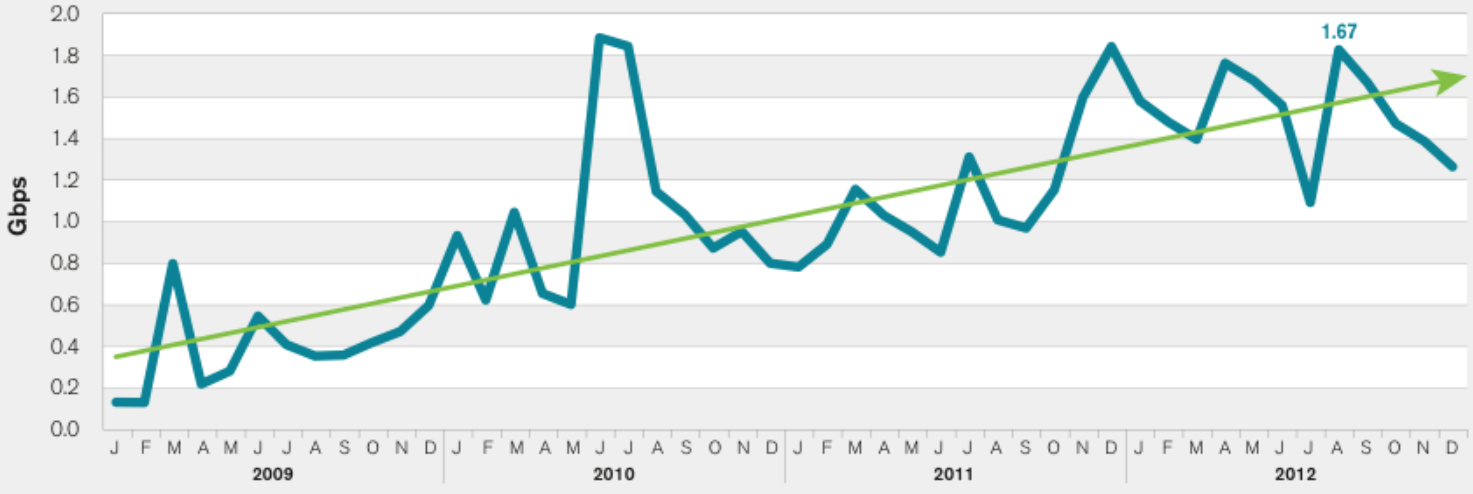


Figure 18 *Source: Arbor Networks, Inc.*

Most Significant Operational Threats

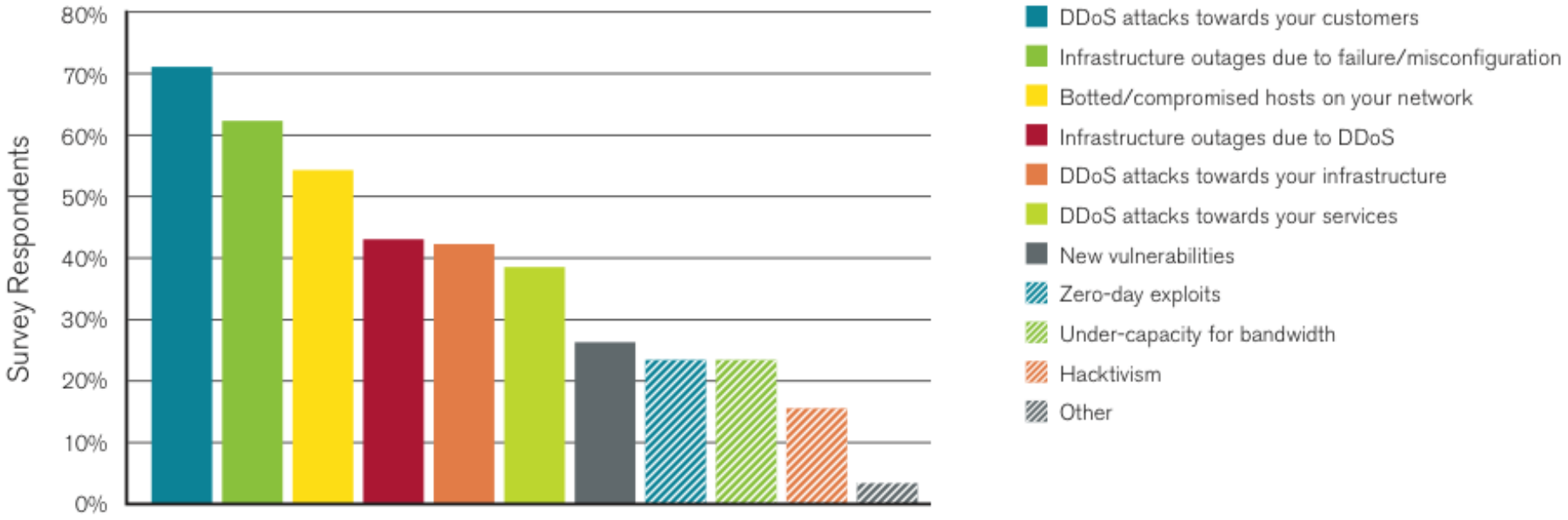


Figure 6 *Source: Arbor Networks, Inc.*

Motivations for DoS

- Showing off / entertainment / ego
- Competitive advantage
  - Maybe commercial, maybe just to win
- Vendetta / denial-of-money
- Extortion
- Political statements
- Impair defenses
- Espionage
- Warfare

Network-level DoS

- Can exhaust network resources by
- Flooding with lots of packets (brute-force)
- DDoS: flood with packets from many sources
- Amplification: Third parties amplify traffic

DoS & Networks

- How could you DoS a target's Internet access?
  - Send many packets
  - Internet lacks isolation between different users
- What resources does attacker need?
  - Bandwidth = bottleneck link of target connection
    - Attacker sends maximum-sized packets
  - Or overwhelm bottleneck router packet rate
    - Attacker sends minimum-sized packets to maximize packet arrival rate

Defending Against Network DoS

- Suppose an attacker has high bandwidth (a “big pipe”)
- It sends packets to the target at a high rate
- How can the target defend against onslaught?
  - Install a network filter to discard any packets that arrive with attacker’s IP address as their source
    - E.g., `drop * 66.31.1.37:* -> *:*`
    - Or it can leverage any other pattern in the flooding traffic that’s not in benign traffic
  - Attacker’s IP address = means of identifying misbehaving user

Filtering is not easy

- DoS filters can be easily evaded
- Spoof source address
  - Filtering impossible
  - Best hope: attacker's ISP has anti-spoofing tests
    - About 75% do
- Use many hosts to send traffic
  - Distributed Denial-of-Service = DDoS ("dee-doss")
  - Requires defender to install complex filters
  - How many hosts are enough?
  - Today they are cheap to acquire

Not Level Playing Field

- Asymmetries allow attackers to consume victim resources with little comparable effort
  - Makes DoS easier to launch
  - Defense costs much more than attack

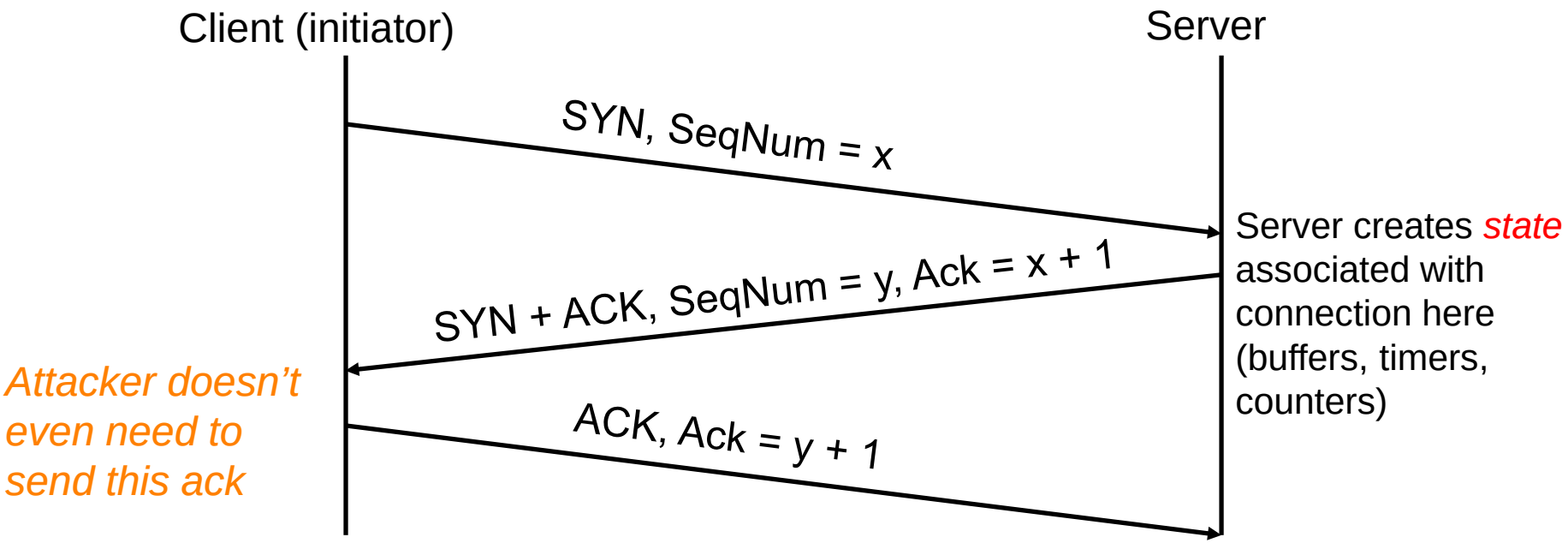
- Particularly dangerous form of asymmetry: amplification
  - Attacker leverages third party resources to increase workload

Amplification

- Amplification example: DNS lookups
- Reply is generally larger than request
- Attacker spoofs DNS request from third party DNS
- Blind spoofing
- Uses UDP (can’t establish TCP conn.)
- Victim doesn’t see spoofed source addresses
- Addresses are those of actual intermediary systems

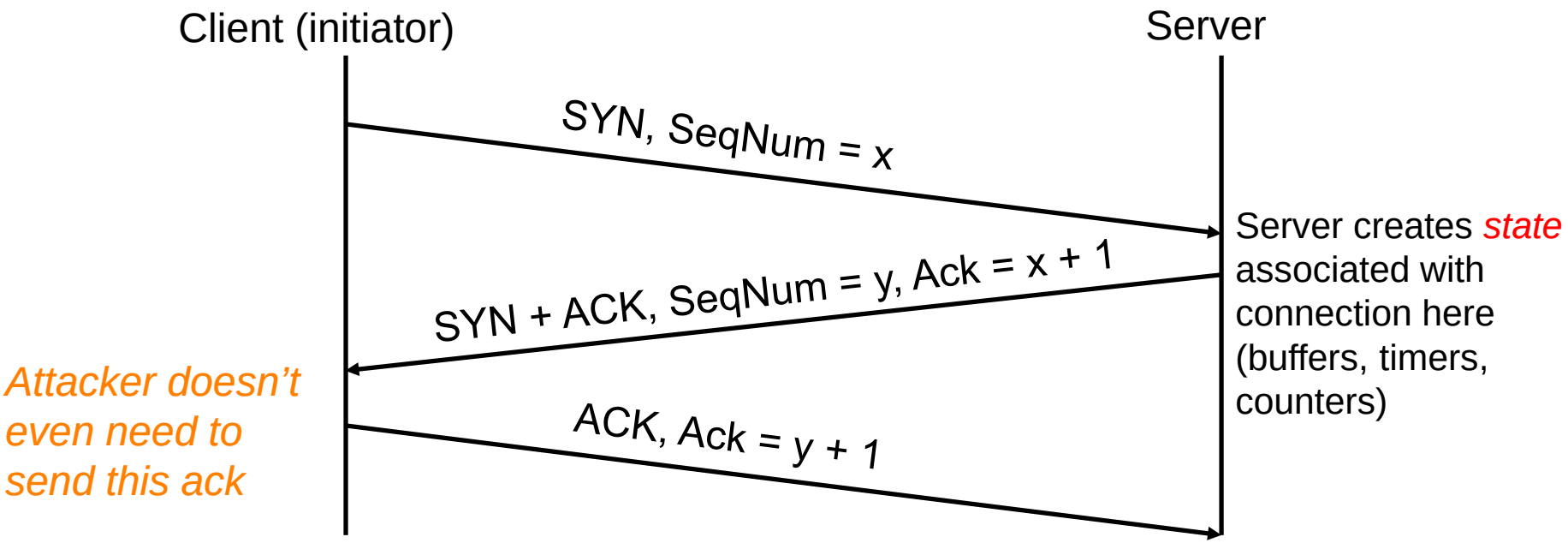
Transport-Level Denial-of-Service

- Recall TCP's 3-way connection establishment handshake
  - Goal: agree on initial sequence numbers



Transport-Level Denial-of-Service

- Recall TCP's 3-way connection establishment handshake
  - Goal: agree on initial sequence numbers
- So a single SYN from an attacker suffices to force the server to spend some memory



TCP *SYN Flooding*

- Attacker targets memory rather than network capacity
- Every (unique) SYN that the attacker sends burdens the target
- What should target do when it has no more memory for a new connection?
  - No good answer
- Refuse new connection?
  - Legit new users can’t access service
- Evict old connections to make room?
  - Legit old users get kicked off

TCP SYN Flooding Defense

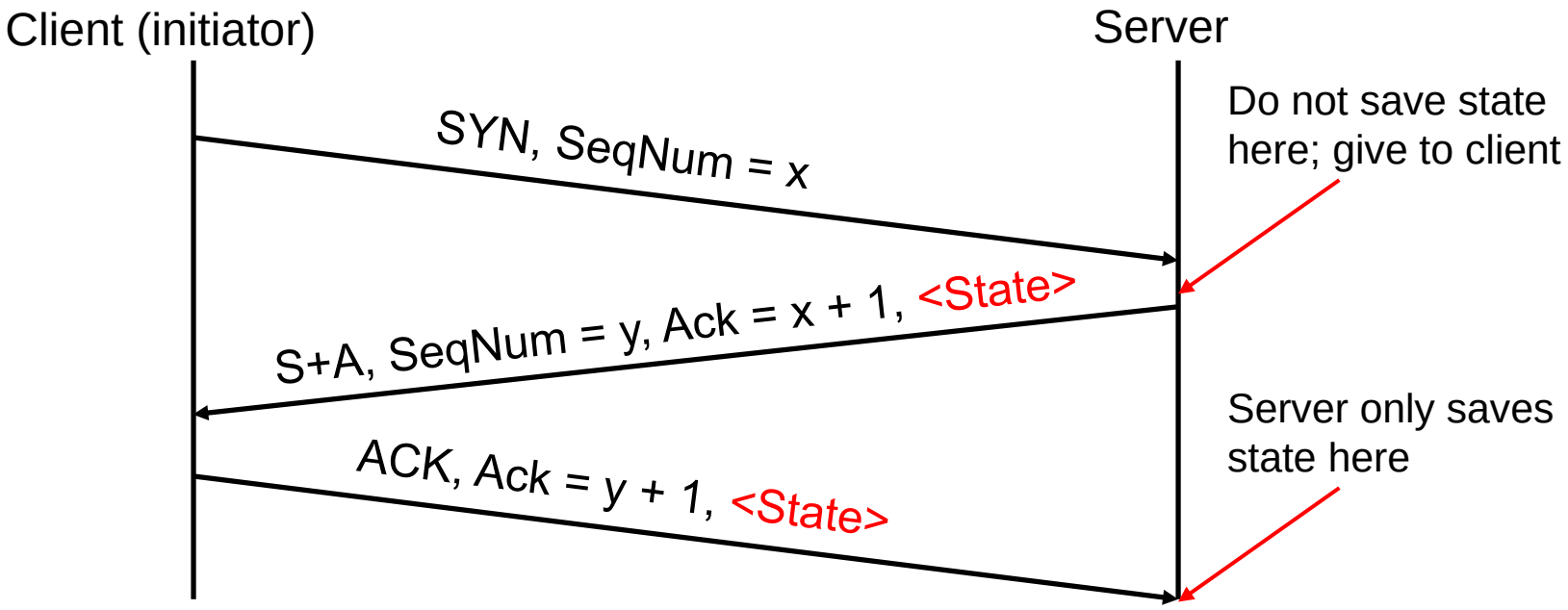
- How can the target defend itself?
- Approach #1: tons of memory
  - How much is enough?
  - Depends on resources attacker can bring to bear (threat model), which might be hard to know

TCP SYN Flooding Defense

- Approach #2: identify bad actors & refuse connections
  - Hard because identification is on IP address
    - We cannot require a password because doing so requires an established connection!
  - For a public Internet service, who knows which addresses customers might come from?
  - Plus: attacker can spoof addresses since they don't need to complete TCP 3-way handshake
- Approach #3: don't keep state!
  - "SYN cookies"; only works for spoofed SYN flooding

SYN Flooding Defense: Idealized

- Server: when SYN arrives, rather than keeping state locally, send it to the client …
- Client needs to return the state in order to established connection



SYN Flooding Defense: Idealized

- Server: when SYN arrives, rather than keeping state locally, send it to the client …
- Clien to estab

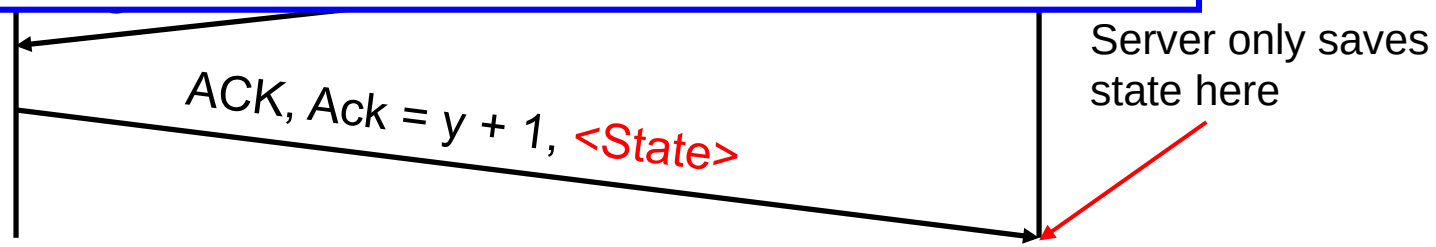
Problem: the world isn't so ideal!

TCP doesn't include an easy way to add a new **<State>** field like this.

Is there any way to get the same functionality without having to change TCP clients?

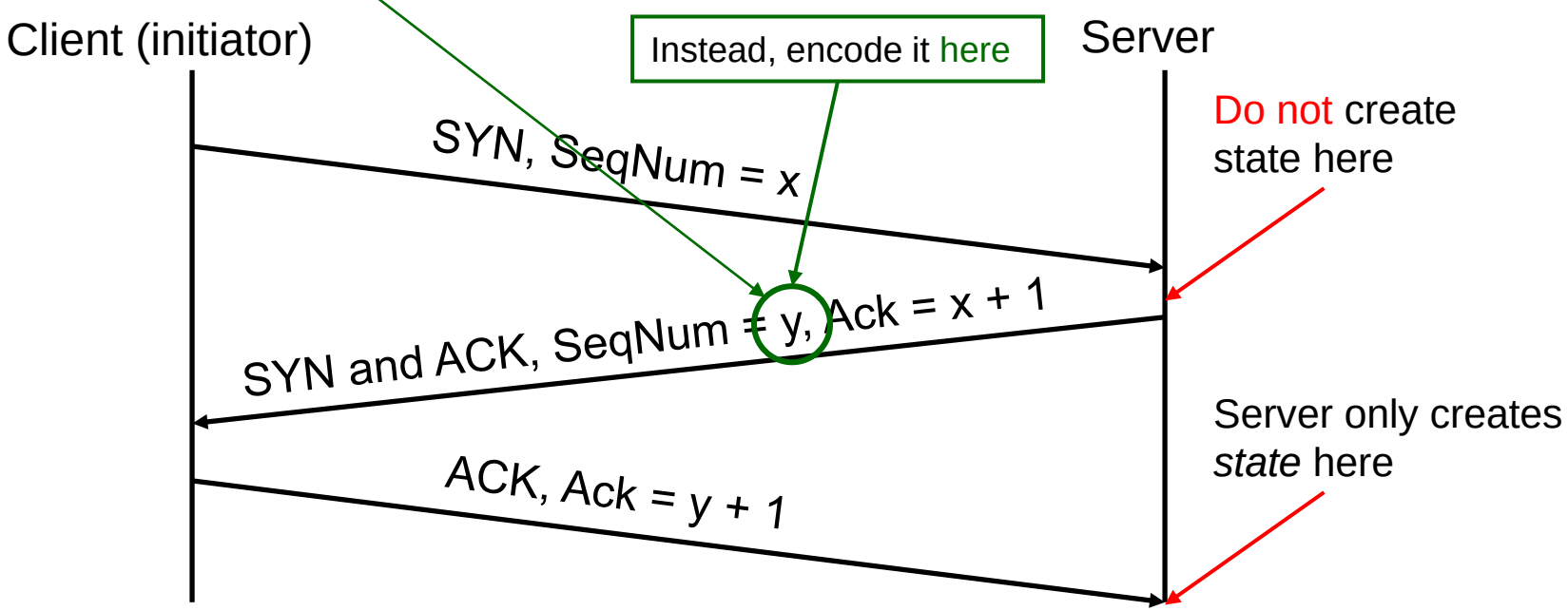
Client

t save state give to client



Practical Defense: SYN Cookies

- Server: when SYN arrives, encode connection state entirely within SYN-ACK's sequence # y
  - y = encoding of necessary state, using server secret
- When ACK of SYN-ACK arrives, server only creates state if value of y from it agrees w/ secret



SYN Cookies: Discussion

- Illustrates general strategy: rather than holding state, encode it so that it is returned when needed
- For SYN cookies, attacker must complete 3-way handshake in order to burden server
  - Can’t use spoofed source addresses
- Note #1: strategy requires that you have enough bits to encode all the state
  - (This is just barely the case for SYN cookies)
- Note #2: if it’s expensive to generate or check the cookie, then it’s not a win

Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service’s processing capacity
- There are many ways to do so, often at little expense to attacker compared to target (asymmetry)

reddit hot new browse stats

This link runs a slooow SQL query on the RIAA's server. Don't click it; that would be wrong. (tinyurl.com)

814 points posted 8 days ago by keyboard_user 211 comments

The link sends a request to the web server that requires heavy processing by its “backend database”.

Algorithmic complexity attacks

- Attacker can try to trigger worst-case complexity of algorithms / data structures
- Example: You have a hash table.
  Expected time: $O(1)$ Worst-case: $O(n)$
- Attacker picks inputs that cause hash collisions.
  Time per lookup: $O(n)$
  Total time to do n operations: $O(n^2)$
- Solution? Use algorithms with good worst-case running time.

Application-Layer DoS

- Rather than exhausting network or memory resources, attacker can overwhelm a service's processing capacity
- There are many ways to do so, often at little expense to attacker compared to target (asymmetry)
- Defenses against such attacks?
- Approach #1: Only let legit users issue expensive requests
  - Relies on being able to identify/authenticate them
  - Note: that this itself might be expensive!
- Approach #2: Force legit users to "burn" cash
- Approach #3: Over-provisioning ($$$)

DoS Defense in General Terms

- Defending against program flaws requires:
  - Careful design and coding/testing/review
  - Consideration of behavior of defense mechanisms
    - E.g. buffer overflow detector that when triggered halts execution to prevent code injection $\Rightarrow$ denial-of-service
- Defending resources from exhaustion is hard. Requires:
  - Isolation and scheduling mechanisms
    - Keep adversary's consumption from affecting others
  - Reliable identification of different users