Network Attacks

CS 161 - Computer Security
Profs. Vern Paxson & David Wagner

TAs: John Bethencourt, Erika Chin, Matthew Finifter, Cynthia Sturton, Joel Weinberger

http://inst.eecs.berkeley.edu/~cs161/

Feb 10, 2010

Announcements / Game Plan

- Homework #1 due tomorrow (Thurs 2/11, 11:59PM)
  - Turn in via hardcopy to drop box in 283 Soda

- Project #1 now out, due Thurs 2/18
  - Turn in electronically

- Goal for today: a look at network attacks
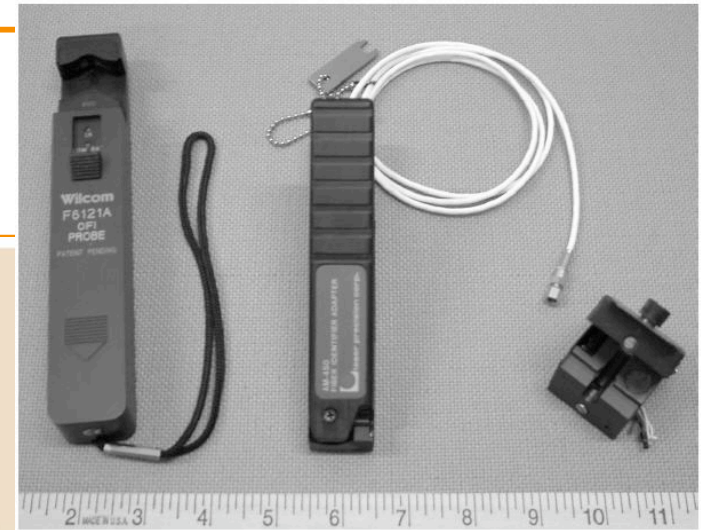 - With a focus on network layers 1-4

Layers 1 & 2: General Threats?

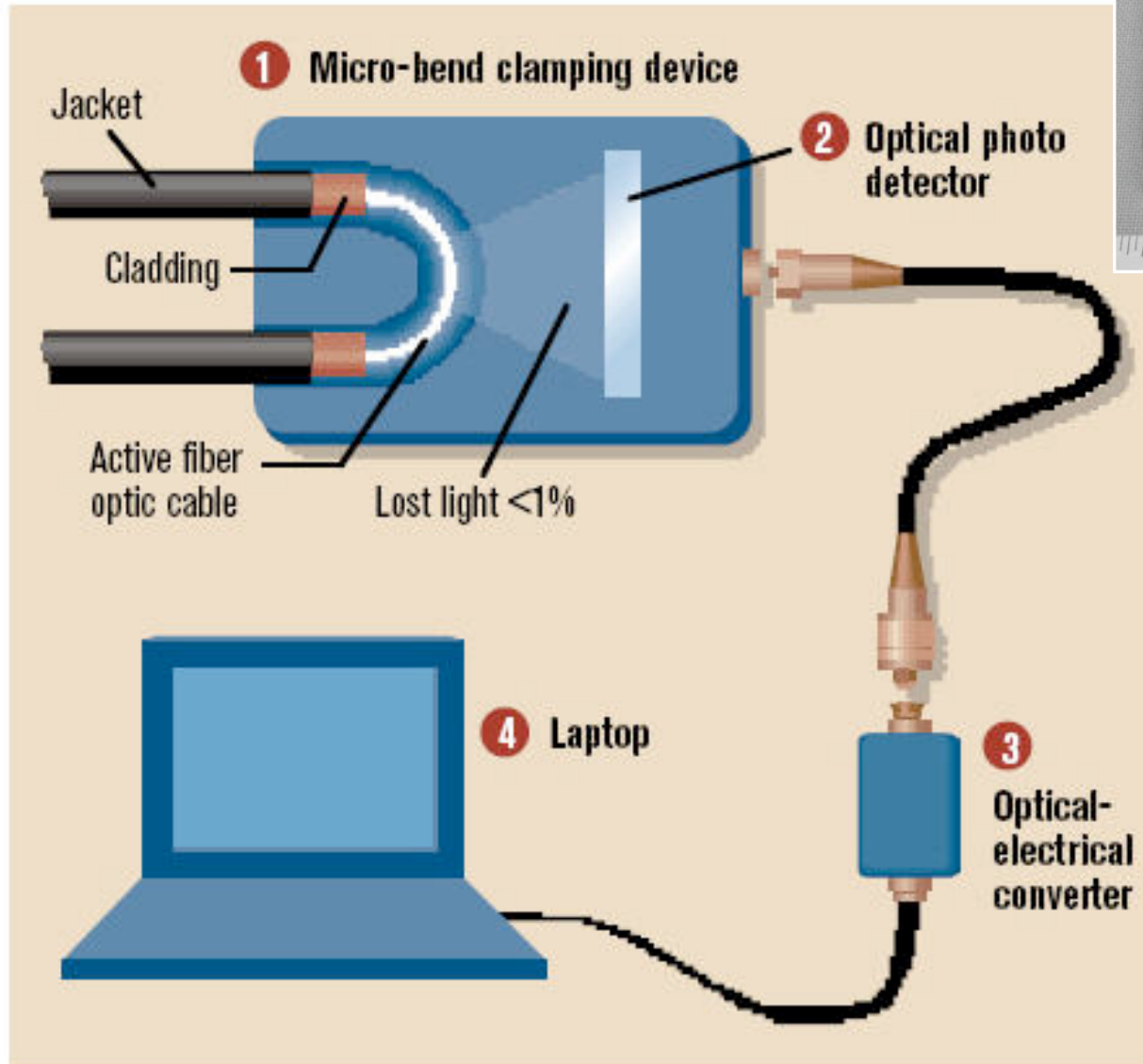|	
7	**Application**
4	**Transport**
3	**(Inter)Network**
2	**Link**
1	**Physical**
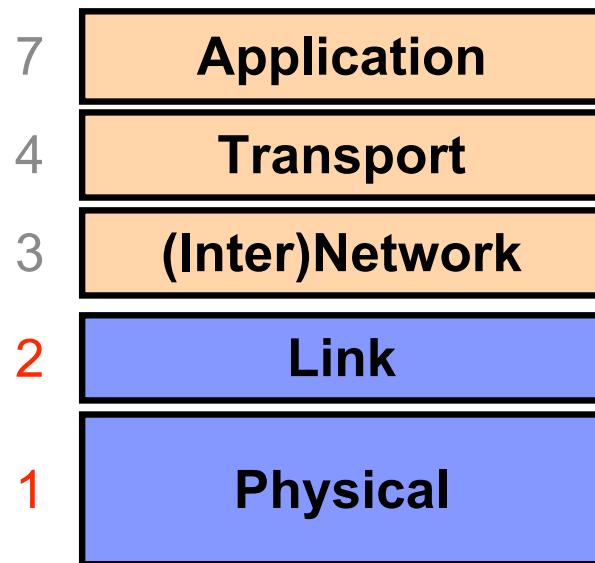
Framing and transmission of a collection of bits into individual messages sent across a single "subnetwork" (one physical technology)

Encoding bits to send them over a single **physical link** e.g. patterns of
voltage levels /
photon intensities /
RF modulation

Physical/Link-Layer Threats: *Eavesdropping*

- For subnets using broadcast technologies (e.g., WiFi, some types of Ethernet), get it for "free"
  - Each attached system 's NIC (= Network Interface Card) can capture any communication on the subnet
  - Some handy tools for doing so
    - o Wireshark
    - o tcpdump / windump
    - o bro (demo)

- For any technology, routers (and internal "switches") can look at / export traffic they forward

- You can also "tap" a link
  - Insert a device to mirror physical signal
  - Or: just steal it!

Stealing Photons

1. Micro-bend clamping device

Jacket

Cladding

Active fiber optic cable

Lost light <1%

2. Optical photo detector

3. Optical-electrical converter

4. Laptop

5

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.

6

Physical/Link-Layer Threats: *Disruption*

- With physical access to a subnetwork, attacker can
  - Overwhelm its signaling
    - E.g., jam WiFi's RF
  - Send messages that violate the Layer-2 protocol's rules
    - E.g., send messages > maximum allowed size, sever timing synchronization, ignore fairness rules

- Routers & switches can simply "drop" traffic

- 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: Whoever 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 even 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.

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.

Physical/Link-Layer Threats: *Injection*

- With physical access to a subnetwork, attacker can create any message they like

- May require root/administrator access to have full freedom

- Particularly powerful when combined with *eavesdropping*
  - Can manipulate existing communications

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

IP = Internet Protocol

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					

Network-Layer Threats

- ## Major:
  - ### Can set arbitrary source address
    - o "*Spoofing*" - receiver has no idea who you are
  - ### Can set arbitrary destination address
    - o Enables "*scanning*" - brute force searching for hosts

- ## Lesser: (FYI; don't worry about unless later explicitly covered)
  - ### Fragmentation mechanism can evade network monitoring
  - ### Identification field leaks information
  - ### Time To Live allows discovery of topology
  - ### TOS can let you steal high priority service
  - ### IP "options" can reroute traffic

11

Layer 4: General Threats?

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

End-to-end communication between processes (TCP, UDP)

Source port	Destination port
Sequence number	
Acknowledgment	

HdrLen	0	Flags	Advertised window
Checksum			Urgent pointer

Options (variable)
Data
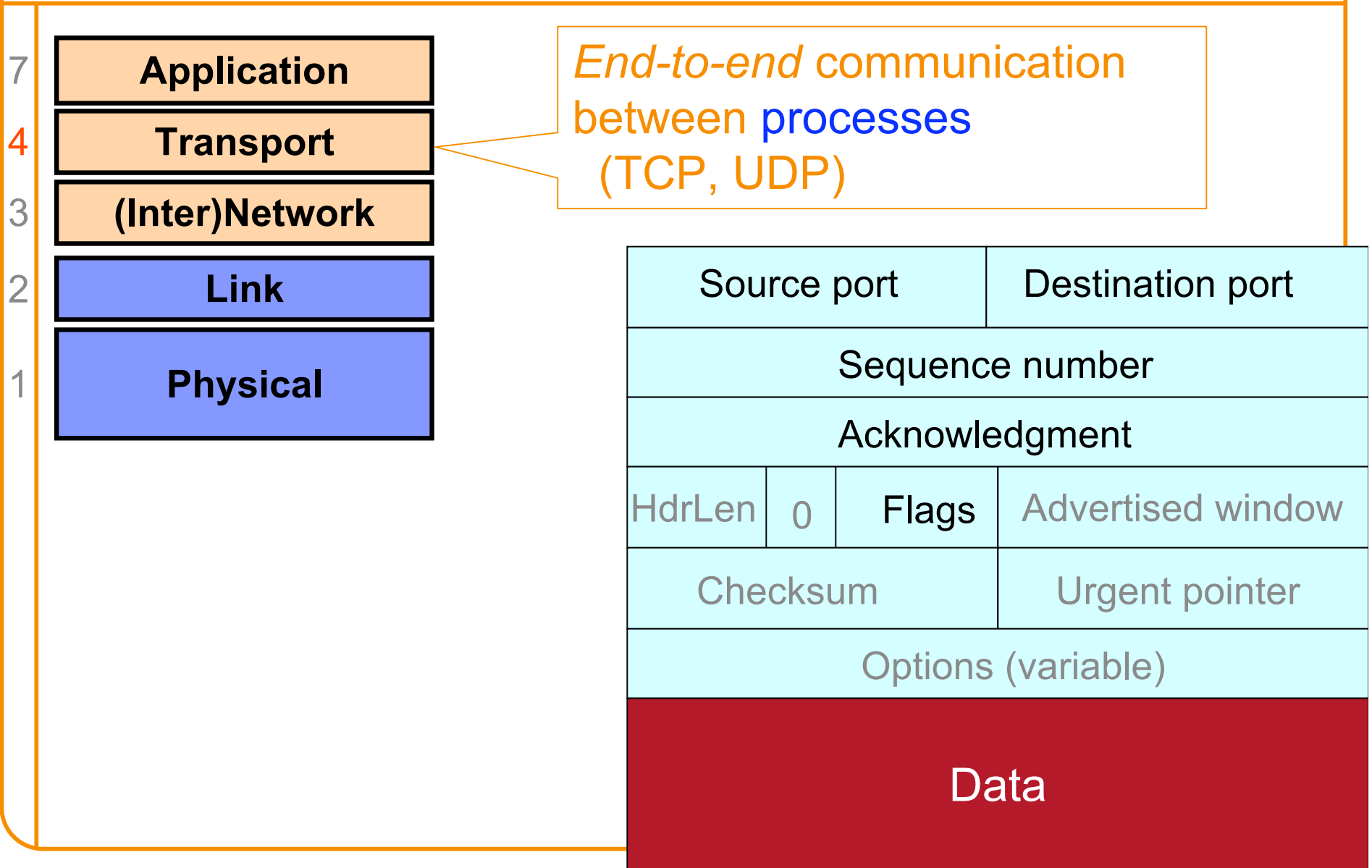
TCP Threat: Disruption

- Normally, TCP finishes ("closes") a connection by each side sending a `FIN` control message
  - Reliably delivered, since other side must <u>ack</u>

- But: if a TCP endpoint finds unable to continue (process dies; info from other "peer" is inconsistent), it abruptly terminates by sending a `RST` control message
  - Unilateral
  - Takes effect immediately (no ack needed)
  - Only accepted by peer if has correct sequence numbers

- So: if attacker knows sequence numbers …

Tools For Disruption Demo

- **netcat** (sometimes "nc")
  - Can listen or send on arbitrary TCP port

- **telnet** (std. Unix utility)
  - Sends ASCII to arbitrary TCP port

- **bro** (bro-ids.org)
  - Programmable network analyzer/monitor

- **inject**
  - Custom Unix utility for forging packets

```
s = socket(AF_INET,
 SOCK_RAW, IPPROTO_RAW);
...
char pkt[pktlen];
struct ip *ip =
    (struct ip *) pkt;
...
ip->ip_v = IPVERSION;
ip->ip_len = pktlen;
ip->ip_off = 0;
ip->ip_src = from;
ip->ip_dst = to;
ip->ip_hl = 5;
ip->ip_p = IPPROTO_TCP;
ip->ip_ttl = 255;
```
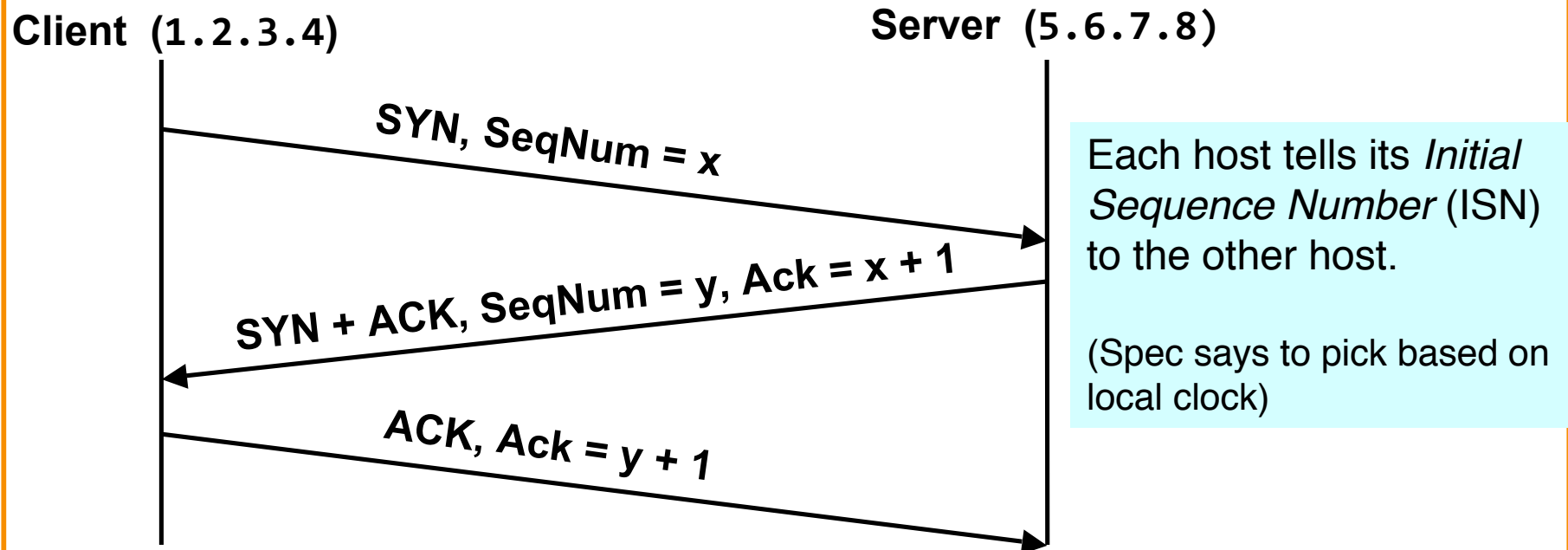
TCP Threat: Injection

- If attacker knows sequence numbers, can inject whatever they like into TCP connection

- Instead of a RST, how about data?

- Note: *desynchronizes* client & server
  - They have inconsistent views of the byte stream and what acknowledgments refer to
  - However, if you've already killed one end with a spoofed RST, doesn't matter

$\Rightarrow$ TCP *session hijacking*
  - General means to take over an already-established connection!
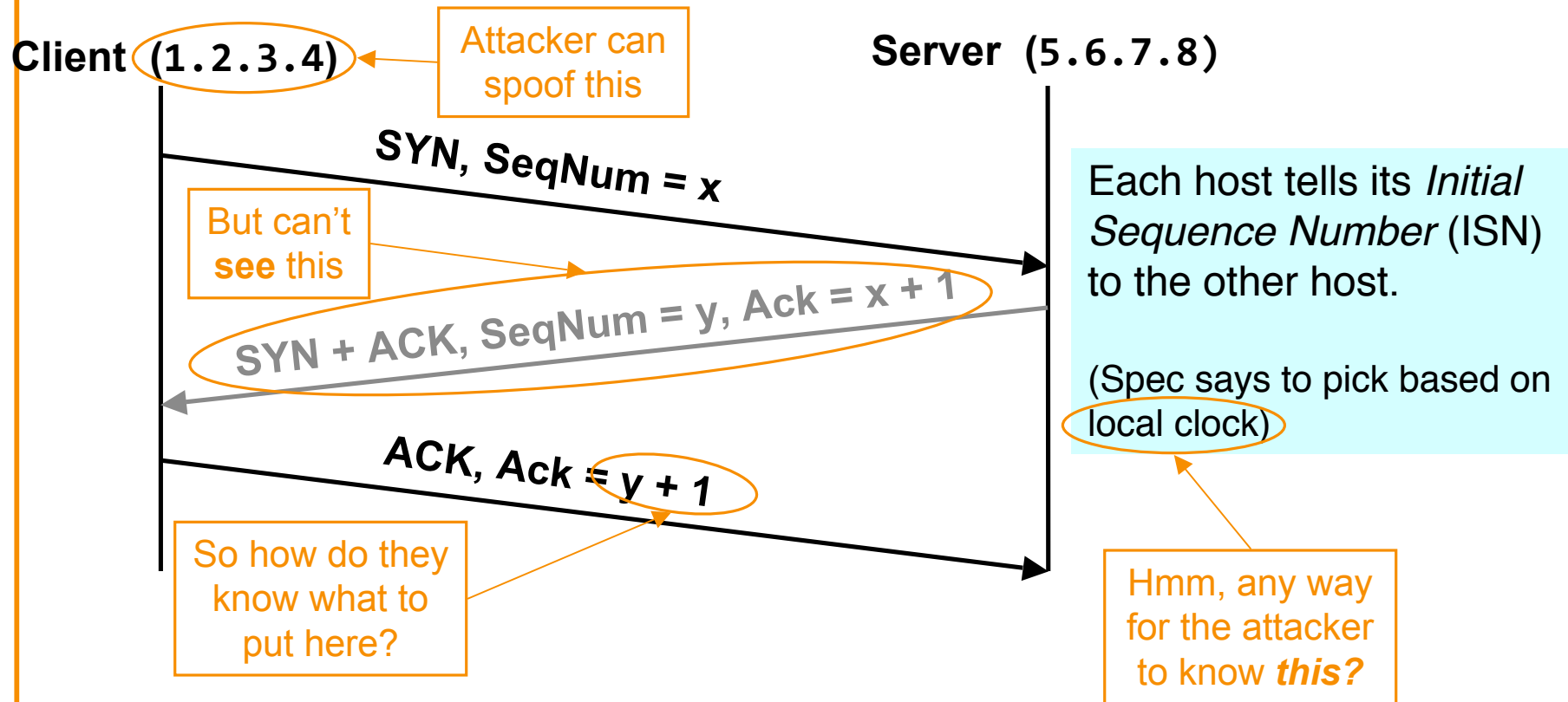 - We are toast if an attacker can see our TCP traffic

15

TCP Threat: Blind Spoofing

- TCP connection establishment:

Client (1.2.3.4)   **Server (5.6.7.8)**

$SYN, SeqNum = x$

$SYN + ACK, SeqNum = y, Ack = x + 1$

$ACK, Ack = y + 1$

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

(Spec says to pick based on local clock)

- How can an attacker create an *apparent* connection from 1.2.3.4 to 5.6.7.8 even if they can't see the *real* 1.2.3.4's traffic?

Blind Spoofing: Attacker's Viewpoint

Client (1.2.3.4)

Attacker can spoof this

Server (5.6.7.8)

SYN, SeqNum = x

But can't **see** this

SYN + ACK, SeqNum = y, Ack = x + 1

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

(Spec says to pick based on local clock)

ACK, Ack = y + 1

So how do they know what to put here?

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

How Do We Fix This?

Use a *random* ISN

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