

Network Security



Dina Katabi

dk@mit.edu

nms.csail.mit.edu/~dina

Network Attacks Are Common

- ❖ Attack Types:
 - ❖ Spam
 - ❖ Denial of service attacks
 - ❖ Worms & Viruses
 - ❖ and others
- ❖ Attack targets
 - ❖ Hosts including attacks on Web servers, TCP, etc.
 - ❖ Links
 - ❖ Routers
 - ❖ DNS
 - ❖ And others
- ❖ Who are the attackers?
 - ❖ Script kiddies
 - ❖ Professionals who do it for money

How confidential is traffic in this lecture room?

- ❖ `sudo tcpdump -s 0 -Ai en1`
 - ❖ Complete trace of all packets on wireless interface
 - ❖ You shouldn't do this

- ❖ Example:

```
13:57:53.794429 IP 18.188.69.36.mdns >  
224.0.0.251.mdns: 0 [4a] [4q] SRV? Ben's  
music._daap._tcp.local. TXT? Ben's  
music._daap._tcp.local. A? ben-powerbook-g4-  
15.local. AAAA? ben-powerbook-g4-15.local. (367)
```

Example Data inside packet

GET /Slashdot/slashdot HTTP/1.1

Host: rss.slashdot.org

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X; en-US; rv:1.8.1.14)
Gecko/20080404 Firefox/2.0.0.14

Accept:
text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Connection: keep-alive

X-Moz: livebookmarks

Cookie: __utma=9273847.1144108930.1176828748.1210531979.1210543936.424;
__utmz=9273847.1205865901.368.13.utmcsr=google|utmccn=(organic)|
utmcmd=organic|
utmctr=generating%2B3d%2Bmodels%2Bfrom%2Bstill%2Bimages;

6.033 Related

Massachusetts Institute of Technology
Department of Electrical Engineering and Computer Science



Hal Abelson

Portrait by [Philip Greenspun](#)

Hal Abelson is Class of 1922 Professor of Computer Science and Engineering in the [Department of Electrical Engineering and Computer Science](#) at [MIT](#).

Hal Abelson
MIT Computer Science and Artificial Intelligence Laboratory
Room 386, The Stata Center
32 Vassar Street
Cambridge, MA 02139
Phone: (617) 253-5856
Fax: (617) 258-8682
Email: hal at MIT dot edu

- [Stodgy biography](#) for public consumption.
- [What I'm doing](#) these days
- [Selected publications](#)
- [Obligatory baby picture](#)

Not so related



Home

Videos

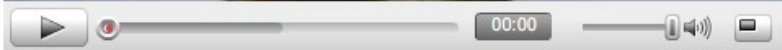
Videos

Search

settings
advanced search

Upload

Rick Astley-Never Gonna Give You Up



Rate: ★★★★★
22,325 ratings

Views: 8,032,148
watch in high quality

Share

Favorite

Playlists

Flag

Email

MySpace

Facebook

(more share options)

Commentary

Statistics & Data

Video Responses: 14

Text Comments: 46,240



RICK ASTLEY
RINGTONES

music.weclub.com

Ads by Goooooogle

Advertisement



From: YTRickRollsYou

Joined: 1 month ago

Videos: 4

Subscribe

Added: March 25, 2008 (More info)

Rick Astley Never Gonna Give You Up

Embed:

Embedding disabled by request

Music Available At: amazonmp3

More From: YTRickRollsYou



Rick Astley-Cry For Help

04:54 From: YTRickRollsYou

Views: 85,659



Rick Astley-Hold Me In Your Arms

04:24 From: YTRickRollsYou

Views: 58,620

iChat is Plaintext

- ❖ None this year, but last year...
- ❖ `strings log.dump | grep ichatballoon | cut -d\> -f 4-`

A: it's just better not to reveal personal information

B: why?

A: I dunno, identity theft and stuff

B: oh, okay

A: maybe I just won't worry about it

GMail is not encrypted by default

- ❖ Completely in the clear:
 - ❖ Contacts lists
 - ❖ GCalendar events
- ❖ GZipped text but can ungzip
 - ❖ Inbox entries
 - ❖ Mail messages

May 4

Semmie Kim

Bored on a Sunday night?? Take a break!

Dear Student: We would appreciate your input and help -- please take this survey! Our apologies ...

☐

May 4

David Templeton

Technique YEARBOOKS available in the student center this week

Technique 2008, the Yearbook of MIT, will be available in the student center for the next two ...

☐

May 4

Ali Wyne

Spring 2008 Issue of MIT International Review Available!

Hi, folks. The Spring 2008 issue of The MIT International Review (MITIR) is available at [http ...](http://...)

☐

May 4

Vanessa Perez

Chocolate Fountain in 5E

Hurry

☐

May 4

Sun Kim

Senate Meeting Monday May 5 with Dean Schmill

Hev all. Sun here. I am wondering if anyone is going to the Senate meeting tomorrow night ...

☐

May 4

David Karger

dp2 early draft

I know dp2 is due thursday. But please, if possible, bring an early draft of your submission on ...

☐

...nor is Google Docs

STRIPING IMPLEMENTATION

I. SYSTEM PREPARATION

To perform TCP connection striping, the system first establishes multiple TCP connections to stripe over. To accomplish this,

6.033 DP2 - Design Report Outline

INTRO

System summary (striping)
Failures, transparency, & reliability
Brief performance & tradeoffs

DESIGN DESCRIPTION (walkthrough of striping btwn. Client/Server)

Striping setup

- (Client-side)

1. Striping setup
2. Striping
3. Periodic scan
4. Striping
5. Striping
6. Striping
7. Striping
8. Striping

- (Server-side)

1. Striping
2. Striping
3. Striping
4. Striping
5. Striping
6. Striping
7. Striping
8. Striping
9. Striping
10. Striping

II. CLIENT-DESTINATION

(too late to spy on DP2!)

Solution?

- ❖ Don't use access sensitive data over an unencrypted connection
 - ❖ Good thing we don't use Google Docs to manage grades... or do we?
- ❖ Change `http://` to `https://`
 - ❖ Works for Gmail, Google Docs
 - ❖ Not in general

Use SSL for MIT/CSAIL mail

- ❖ At least one staff member forgot to turn on SSL for outgoing mail

Message-Id: <0F7F7068-C5E0-4C9D-B59E-DC8FC4958CAC@csail.mit.edu>

From: XXX

To: XXX, XXX

Content-Type: text/plain; charset=US-ASCII; format=flowed; delpsp=yes

Content-Transfer-Encoding: 7bit

Mime-Version: 1.0 (Apple Message framework v919.2)

Subject: hal abelson lecture now

Date: Mon, 12 May 2008 14:15:36 -0400

X-Mailer: Apple Mail (2.919.2)

Hal Abelson is giving a guest lecture in 6.033 right now on ethics and law in computer systems. It's pretty good so far if you're looking to kill time.

32-123

(hang on, i think it might be getting into actual work-related stuff now... might still be interesting tho)

Mounting An Attack

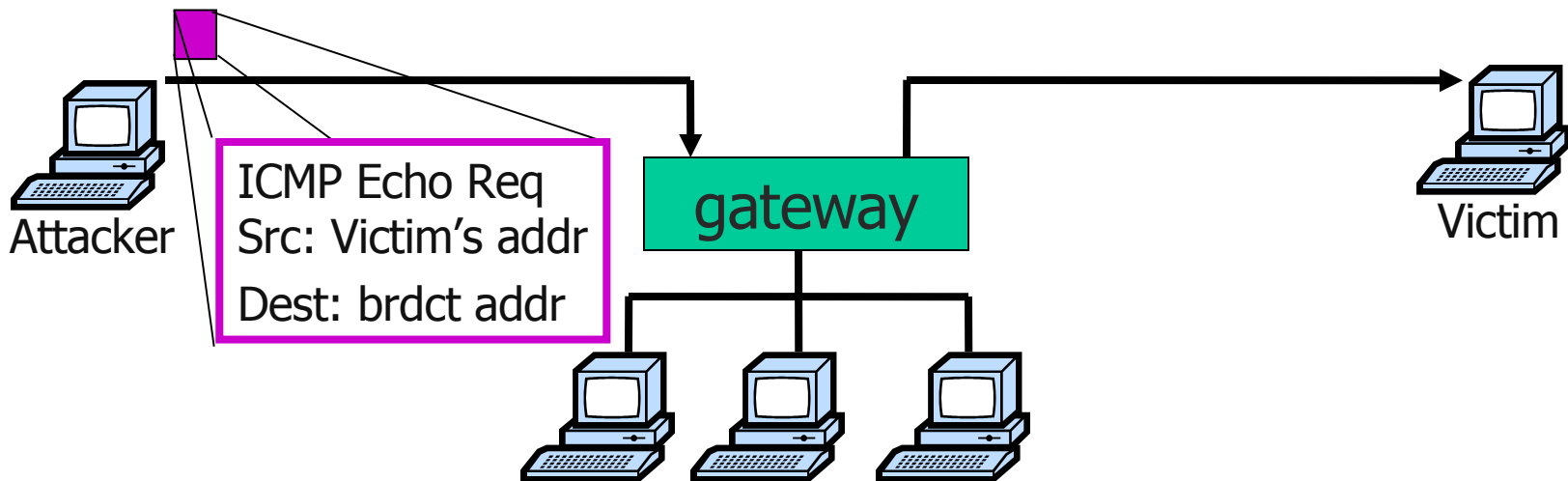
Attacker's Goals

- ❖ Hide
- ❖ Maximize damage

These goals are essential to understand what makes an attack effective and how to counter attacks

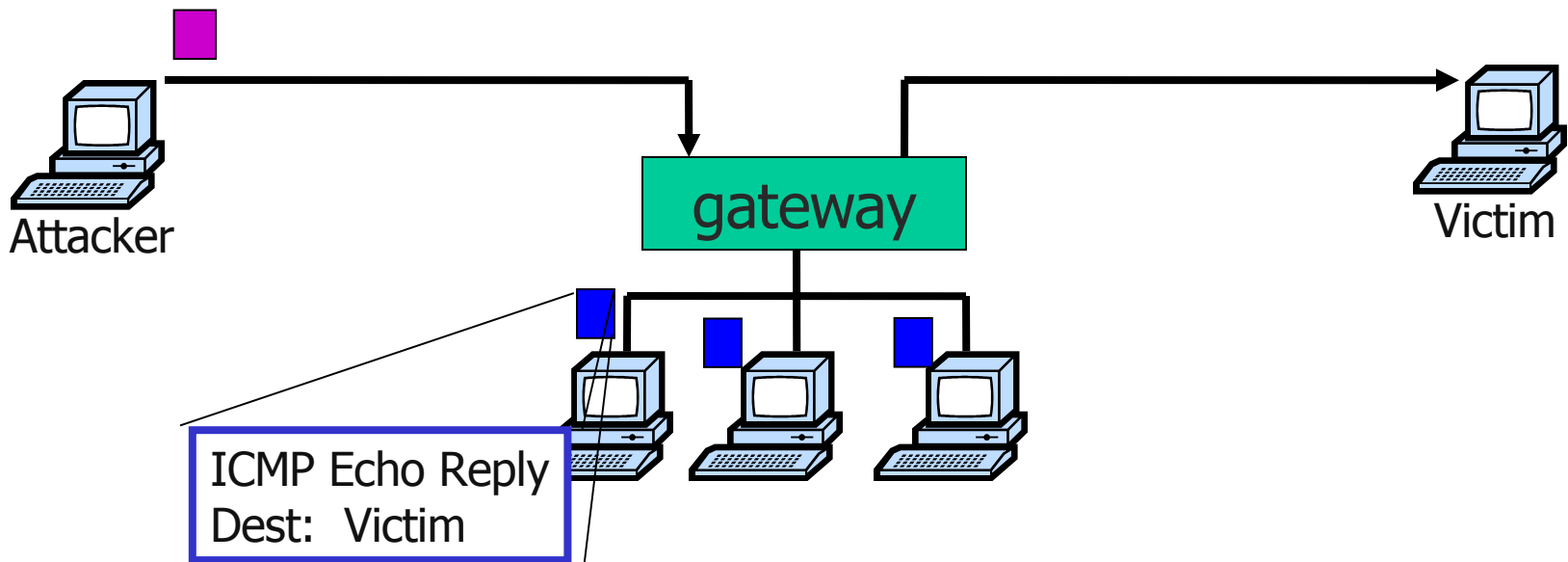
Attacker Wants to Hide

- ❖ Spoof the source (IP address, email account, ...)
- ❖ Indirection
 - ❖ Reflector attacks: E.g., Smurf Attack

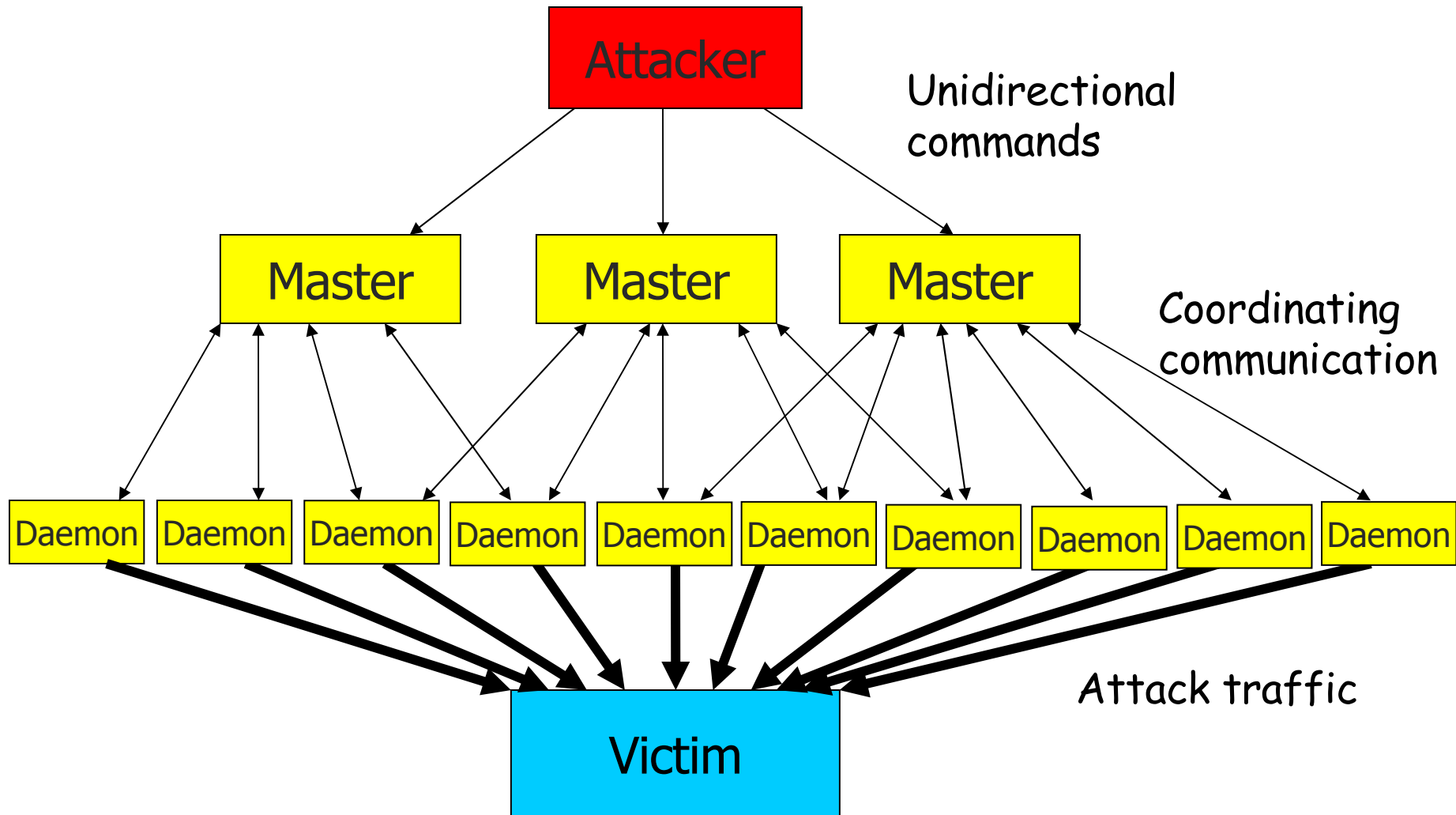


Attacker Wants to Hide

- ❖ Spoof the source (IP address, email account, ...)
- ❖ Indirection
 - ❖ Reflector attacks: E.g., Smurf Attack



Increase Damage → Go Fully Distributed
→ Use a Botnet



Some Distributed Denial of Service (DDoS) Tools

- ❖ Many public tools for flooding a victim with unwanted traffic
- ❖ Trin00 (Trinoo)
 - ❖ Client ported to Windows
- ❖ TFN - Tribe Flood Network
 - ❖ TFN2K - Updated for 2000
- ❖ Stacheldraht
 - ❖ German for "Barbed Wire"

Trinoo Transcript

Connection to port (default 27665/tcp)

```
attacker$ telnet 10.0.0.1 27665
```

```
Trying 10.0.0.1
```

```
Connected to 10.0.0.1
```

```
Escape character is '^]'.  
Kwijibo
```

```
Connection closed by foreign host. . . .
```

```
attacker$ telnet 10.0.0.1 27665
```

```
Trying 10.0.0.1
```

```
Connected to 10.0.0.1
```

```
Escape character is '^]'.  
Betaalmostdone
```

```
trinoo v1.07d2+f3+c..[rpm8d/cb4Sx/]
```

```
trinoo>
```

Trin00 Commands

- ❖ `dos <IP>` - command to initiate a DoS against the targeted <IP> address
- ❖ `mdos <IP1:IP2:IP3>` - sends command to attack three IP addresses, sequentially
- ❖ `die` - shut down the master
- ❖ `mdie <password>` - if correct password specified, packet is sent out to all daemon nodes to shutdown
- ❖ `mping` - ping sent to all nodes in the daemon list
- ❖ `killdead` - delete daemon nodes from list that didn't reply to ping
- ❖ `bcast` - gives a list of all active daemons
- ❖ `mstop` - Attempts to stop an active DoS attack. Never implemented by the author(s), but the command is there

Bots Stories

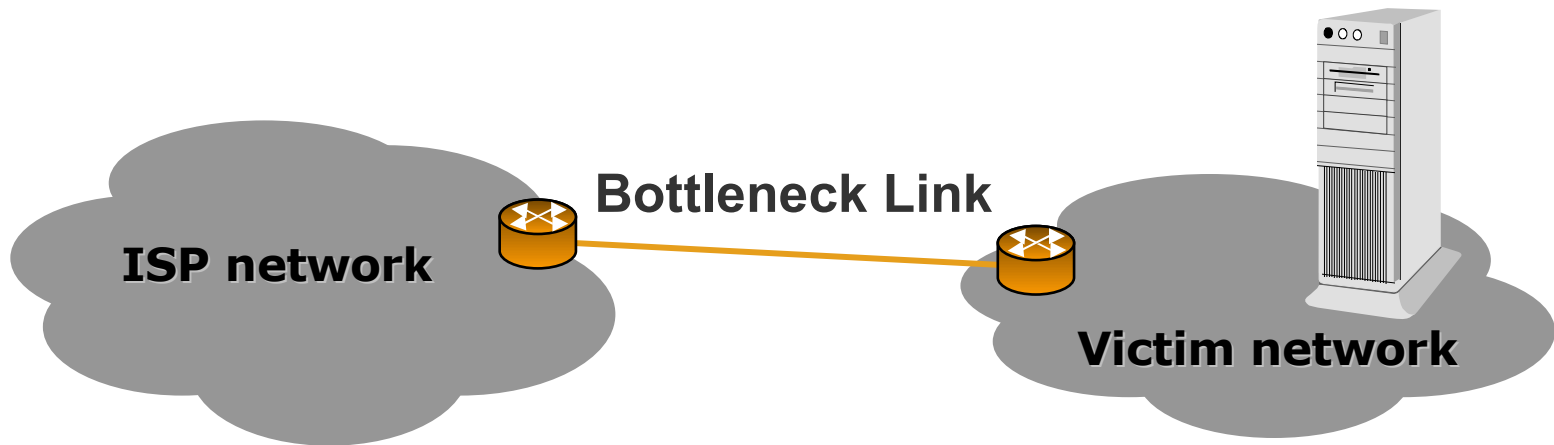
- ❖ Bots are common
- ❖ In 2006, every day 30,000 machines become zombies
- ❖ Bots of 20,000+ machines are reported
- ❖ Bots are rented by the hour
- ❖ Bots are used for a variety of attacks, DDoS, Spam, as web servers which serve illegal content,...

Attacks

Attacks on Bandwidth

- ❖ Brute force attack
- ❖ Attacker sends traffic to consume link bandwidth

Defending against bandwidth attacks is hard

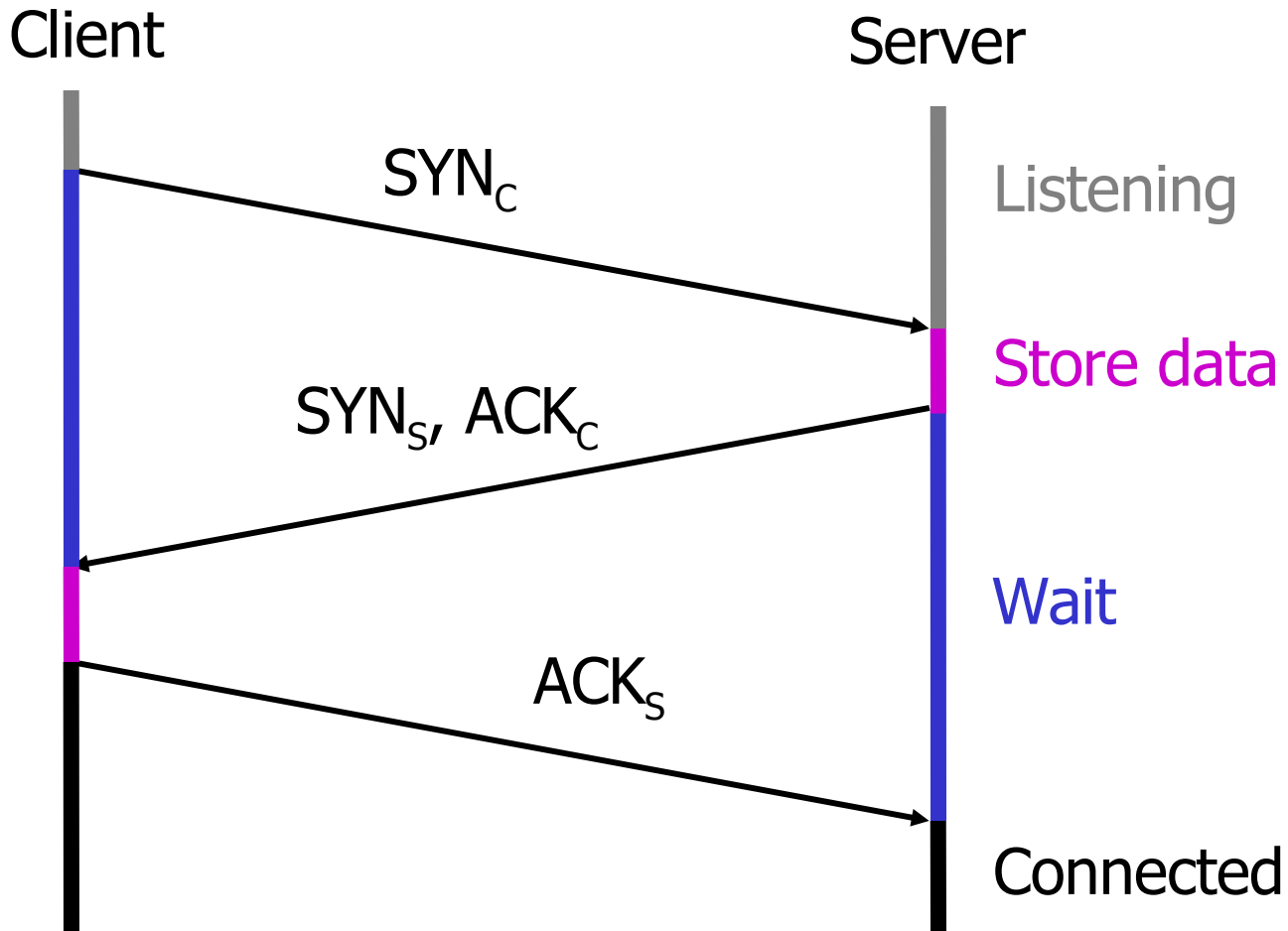


- ❖ Should drop packets before the bottleneck, i.e., at ISP
- ❖ But
 - ❖ ISPs are not willing to deploy complex filters for each client
 - ❖ ISPs have no strong incentive; they charge clients for traffic
- ❖ Big companies defend themselves by using very high bandwidth access links

Attacks on TCP

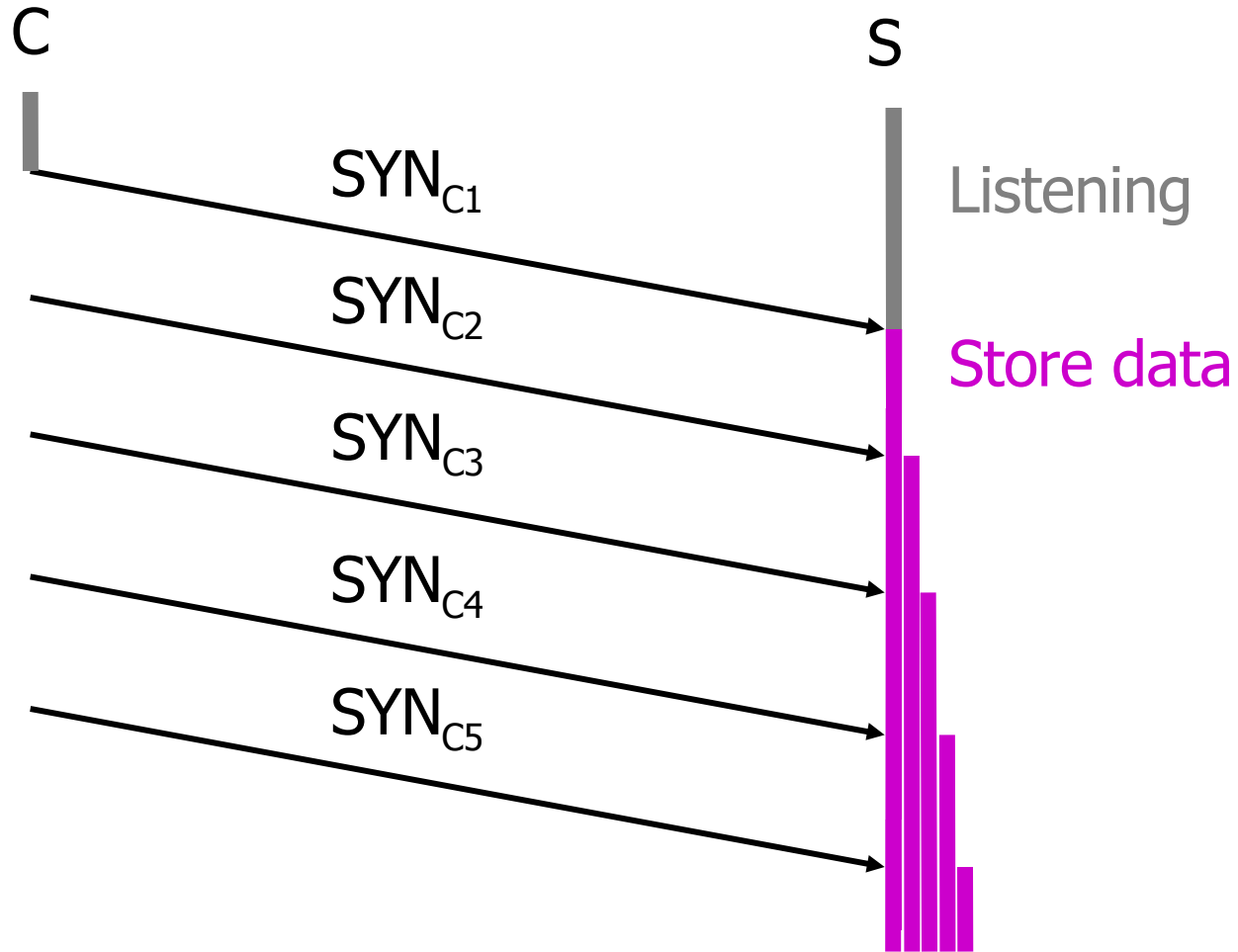
TCP DoS Attacks:

TCP SYN Flood



TCP DoS Attacks:

TCP SYN Flood



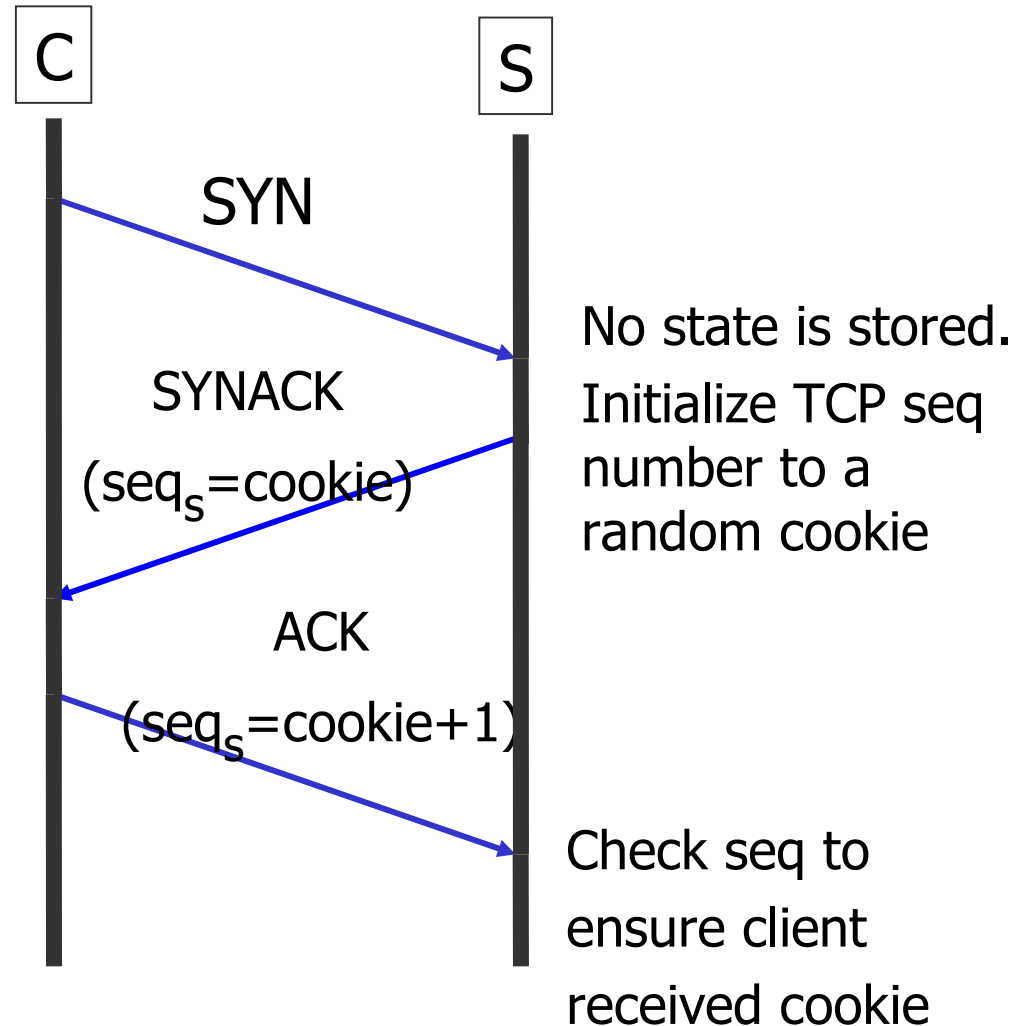
TCP DoS Attacks:

TCP SYN Flood

- ❖ Usually targets connection memory → Too many half-open connections
- ❖ Potential victim is any TCP-based server such as a Web server, FTP server, or mail server
- ❖ To check for SYN flood attacks
 - ❖ Run `netstat -s |grep "listenqueue overflows"` and check whether many connections are in "SYN_RECEIVED"
- ❖ How can the server deal with it?
 - ❖ Server times out half-open connection
 - ❖ **SYN cookies** and SYN caches prevent spoofed IP attacks

SYN Cookie

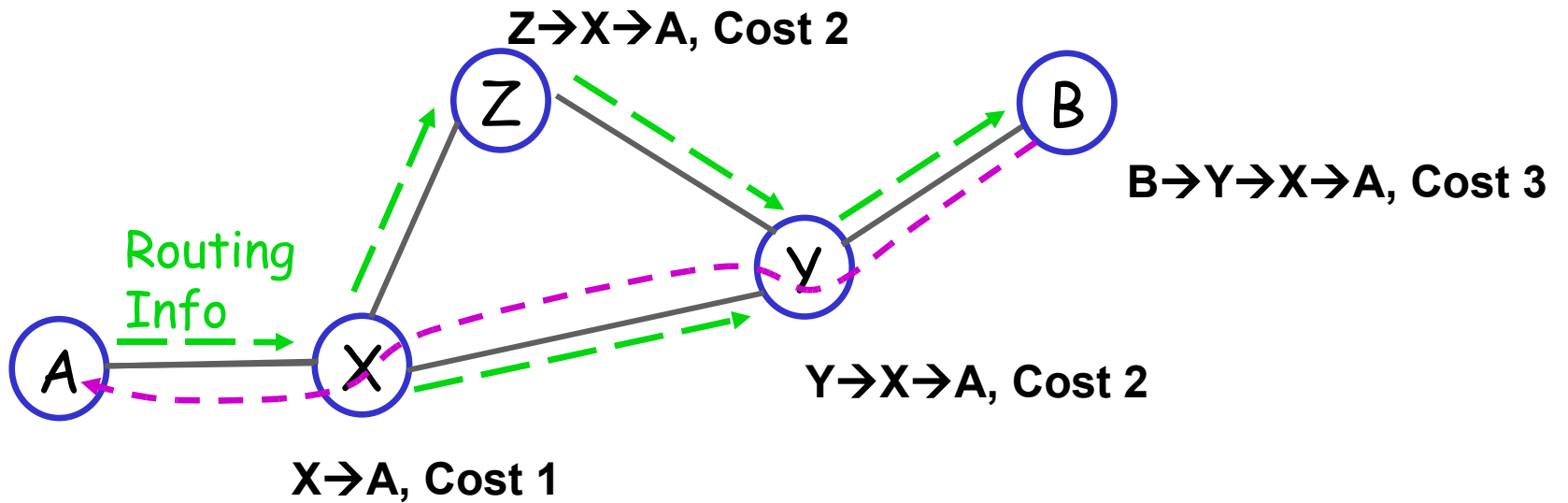
- ❖ Ensures source IP is not spoofed
- ❖ Server delays resource reservation until it checks that the client can receive a packet at the claimed source address



Attacks on Routers

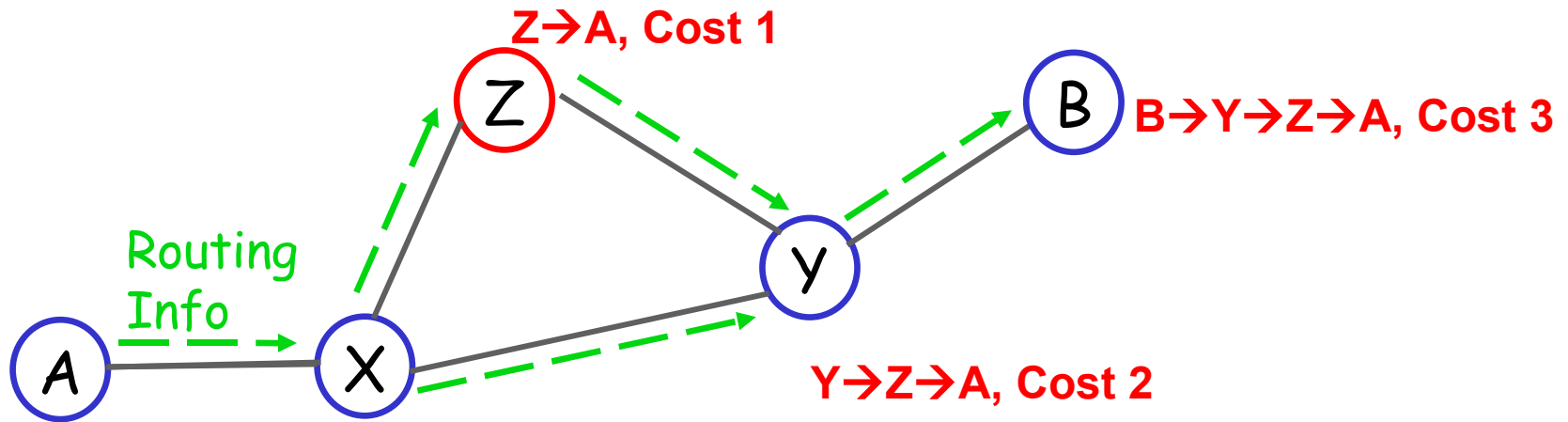
Attacks on Routers:

Routing Protocols



Attacks on Routers:

Attacks on Routing Table



- ❖ Attacker needs to get access to a router
- ❖ Attacks
 - ❖ Prefix hijacking by announcing a more desirable route
 - Z can lie about its route to A
 - ❖ Overload routers CPU by too many routing churns
 - ❖ Overload the routing table with too many routes
 - Causes router to run out of memory or CPU power for processing routes
 - E.g., AS7007

Attacks on Routers:

Countering Routing Table Attacks

- ❖ Authenticate peer routers
- ❖ Secure BGP [Kent et al]
 - ❖ Every ISP sign their advertisements creating a chain of accountability (e.g., Y sends { X: {A}_X }_Y)
 - ❖ Too many signatures → too slow
 - With no authentication needs a few usec; MD5 ~100 usec; RSA ~1 sec

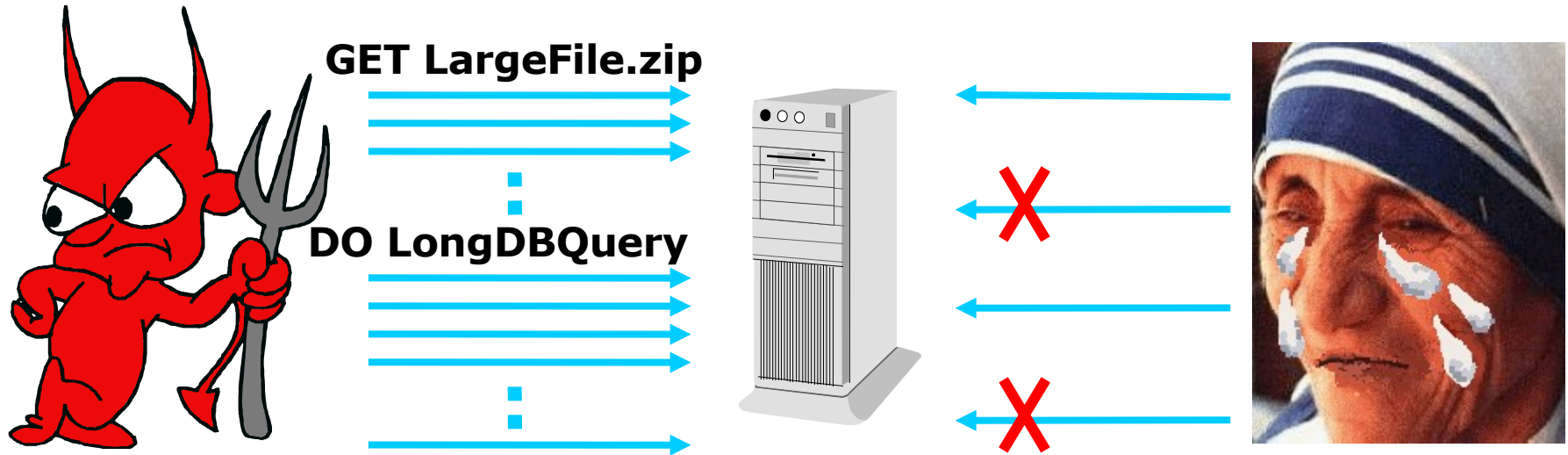
DoS Attacks on Web Servers

DoS Attacks on Web Servers

- ❖ Most known attacks
 - ❖ E.g., Yahoo, Amazon, ...
 - ❖ Moore et al report over 12,000 attacks in 3-week, intensity as high as 600,000 pkts/s
- ❖ Recently taking the form of Cyber Mafia
 - ❖ Pay us \$50,000 to protect you from attacks similar to the one on last Tuesday
- ❖ Becoming more distributed
 - ❖ Less spoofing of IP addresses

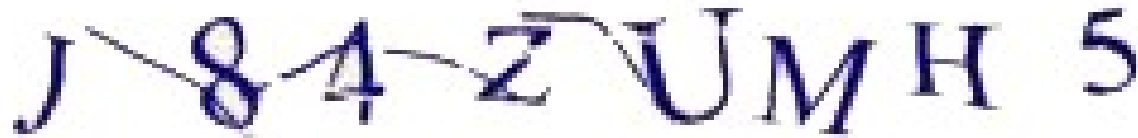
DoS Attacks on Servers:

Attacks that Mimic Legitimate Traffic



- ❖ Attacker compromises many machines causing them to flood victim with HTTP requests (e.g., MyDoom worm)
- ❖ Attacked resources
 - ❖ DB and Disk bandwidth
 - ❖ Socket buffers, processes, ...
 - ❖ Dynamic content, password checking, etc.
- ❖ Hard to detect; attack traffic is indistinguishable from legitimate traffic

CAPTCH-Based Solution



J 8 4 z U M H 5

Suspected attack! To access `www.foo.com`
enter the above letters:

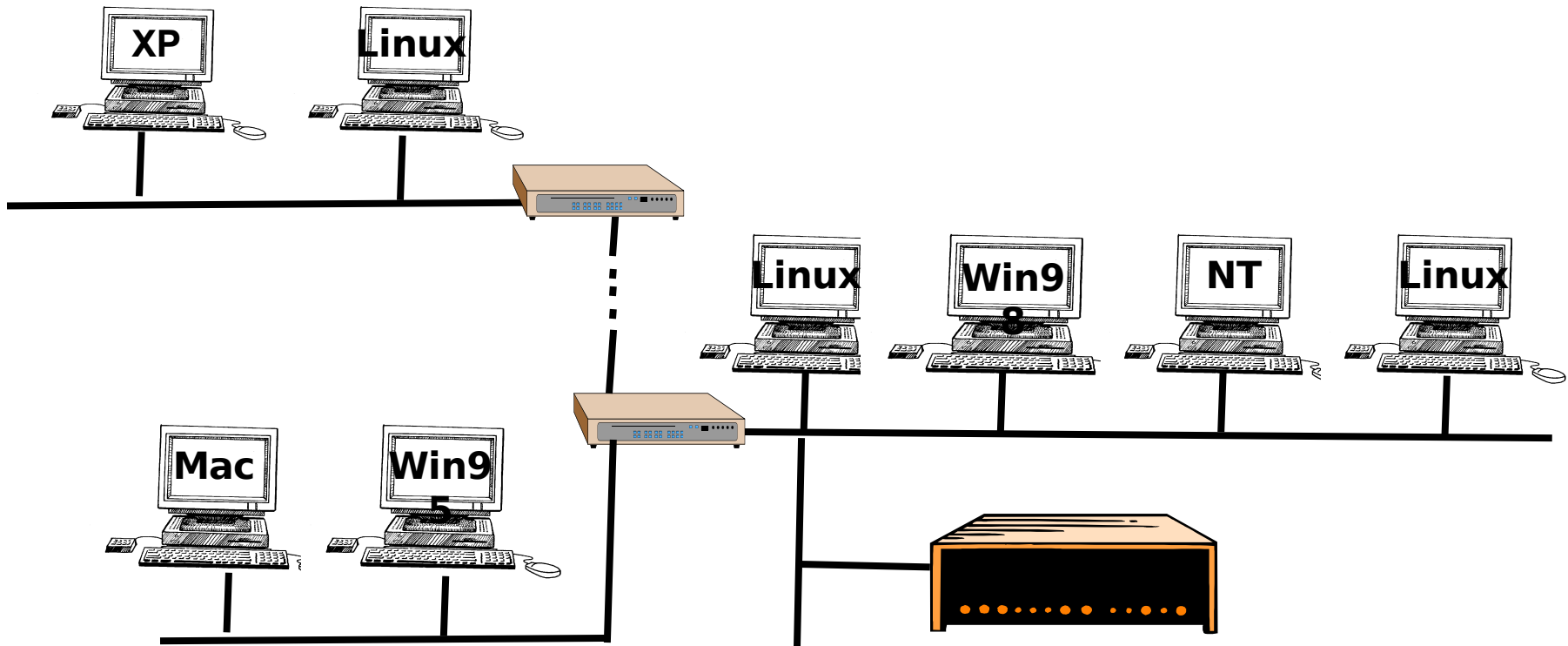
- ❖ Need to ensure:
 - ❖ Cheap ways to send test and check answer
 - ❖ Some people can't or don't want to answer graphical tests but are legitimate users (e.g., Blind users)

Detection

Detection Issues

- ❖ Detecting What?
 - ❖ Detecting the offending packets
 - ❖ Some attack characteristics (e.g., how many zombies)
 - ❖ The occurrence of an attack
- ❖ Offline vs. realtime
 - ❖ Realtime detection may help in throttling the attack while forensics might help in suing the attacker
- ❖ Detection cost
 - ❖ Can attacker mount an attack on the detection mechanism? How would that affect the protected system?

Network Intrusion Detection



- ❖ NIDS box monitors traffic entering and leaving your network
- ❖ In contrast to firewalls, NIDS are passive

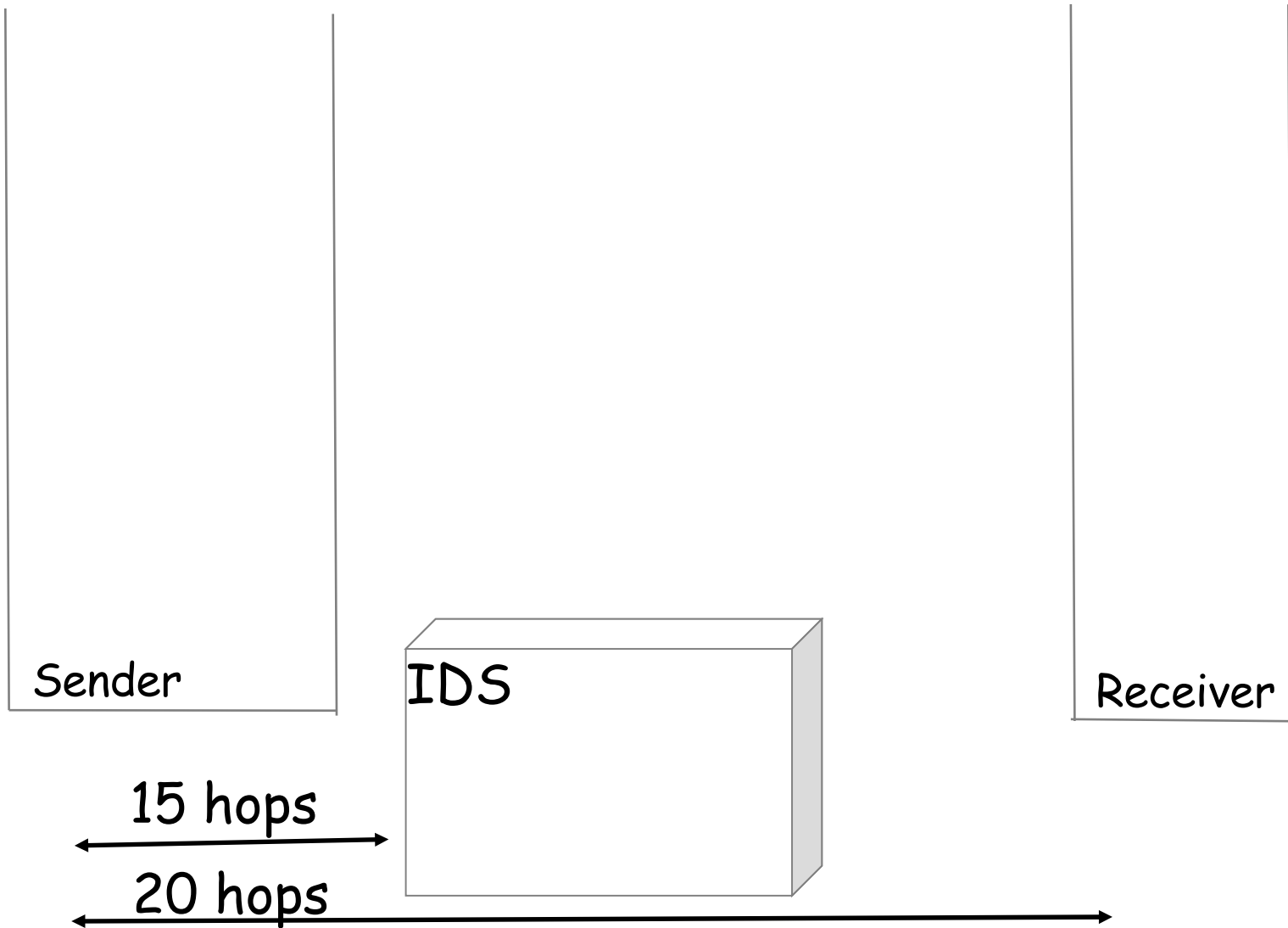
Approaches to Intrusion Detection

1. Signature Based: Keeps a DB of known attack signatures and matches traffic against DB (e.g., Bro, Snort)
 - ❖ **Pros**
 - Easy to understand the outcome
 - More accurate in detecting known attacks
 - ❖ **Cons**
 - Can't discover new attacks
2. Anomaly Based: Matches traffic against a model of normal traffic and flags abnormalities (e.g., EMERALD)
 - ❖ **Pros**
 - Can deal with new attacks
 - ❖ **Cons**
 - Modeling normal. it is hard to describe what is normal
 - Limits new applications
 - Less accurate detection of known attacks
3. Hybrid: Matches against DB of known attacks. If no match, it checks for anomaly

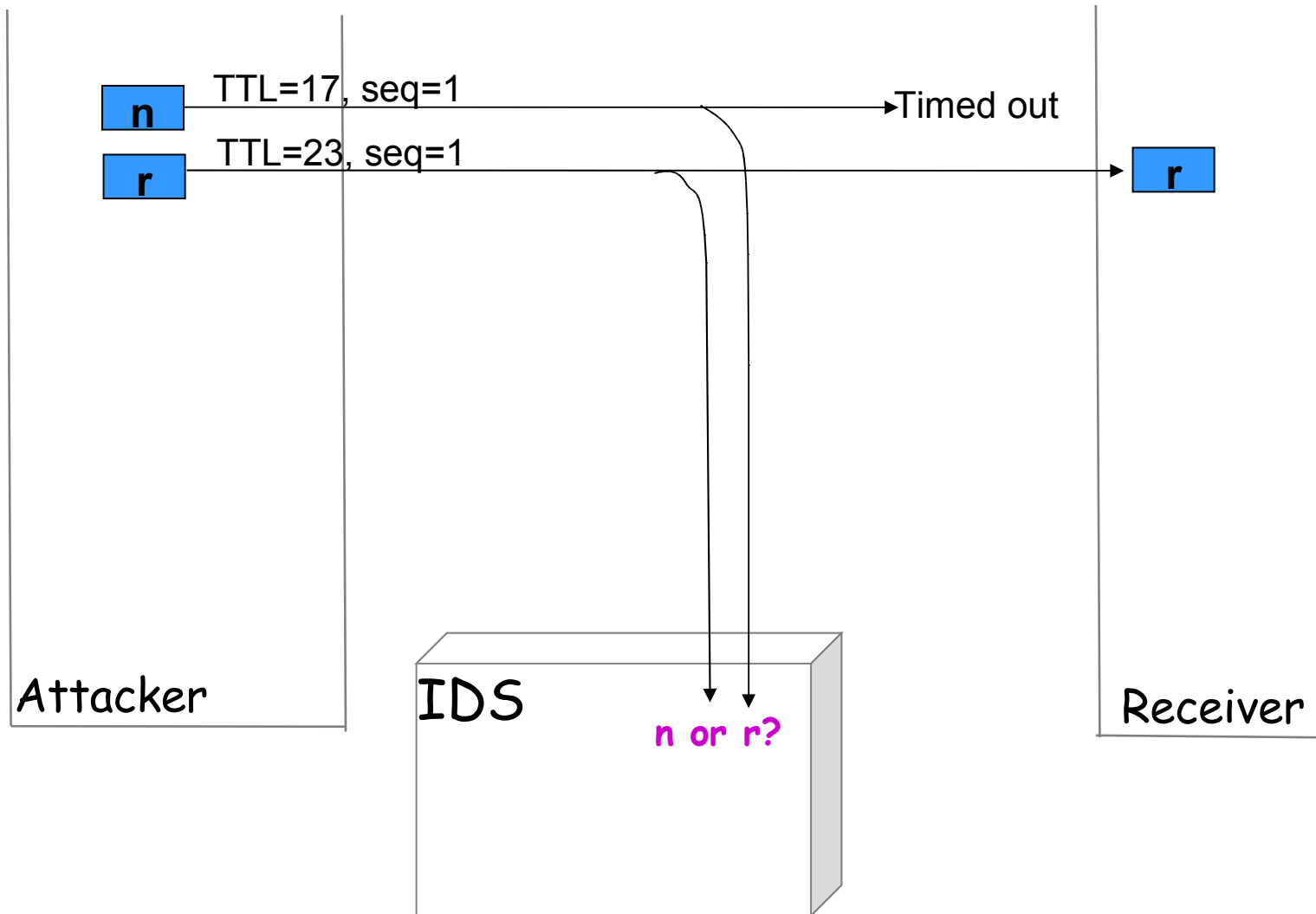
Evasion Problem in NIDS

- ❖ Consider scanning traffic for a particular string (“USER root”)
- ❖ Easiest: scan for the text in each packet
 - ❖ No good: text might be split across multiple packets
- ❖ Okay, remember text from previous packet
 - ❖ No good: out-of-order delivery
- ❖ Okay, fully reassemble byte stream
 - ❖ Costs state
 - ❖ and still evadable

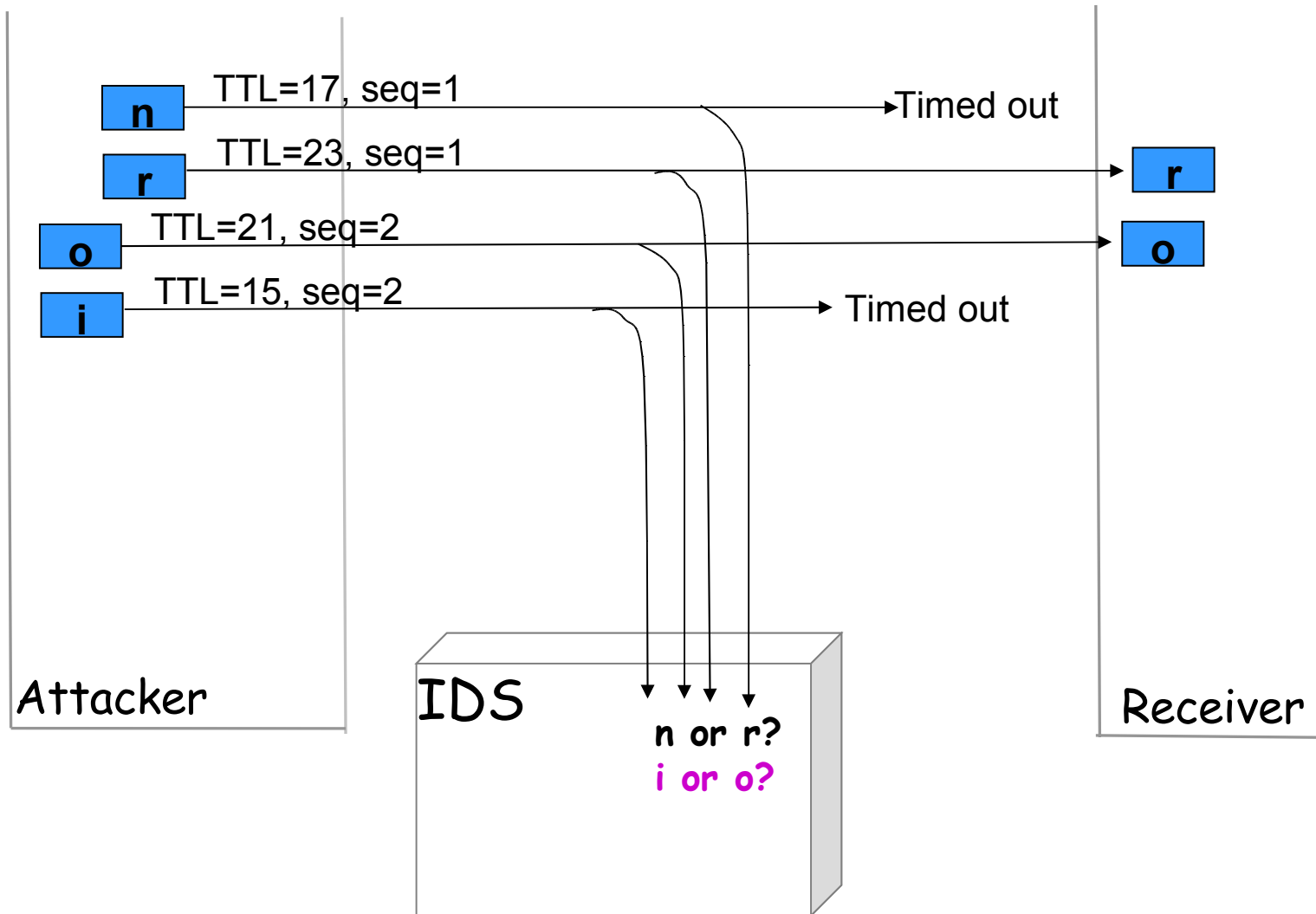
Evading Detection Via Ambiguous TCP Retransmission



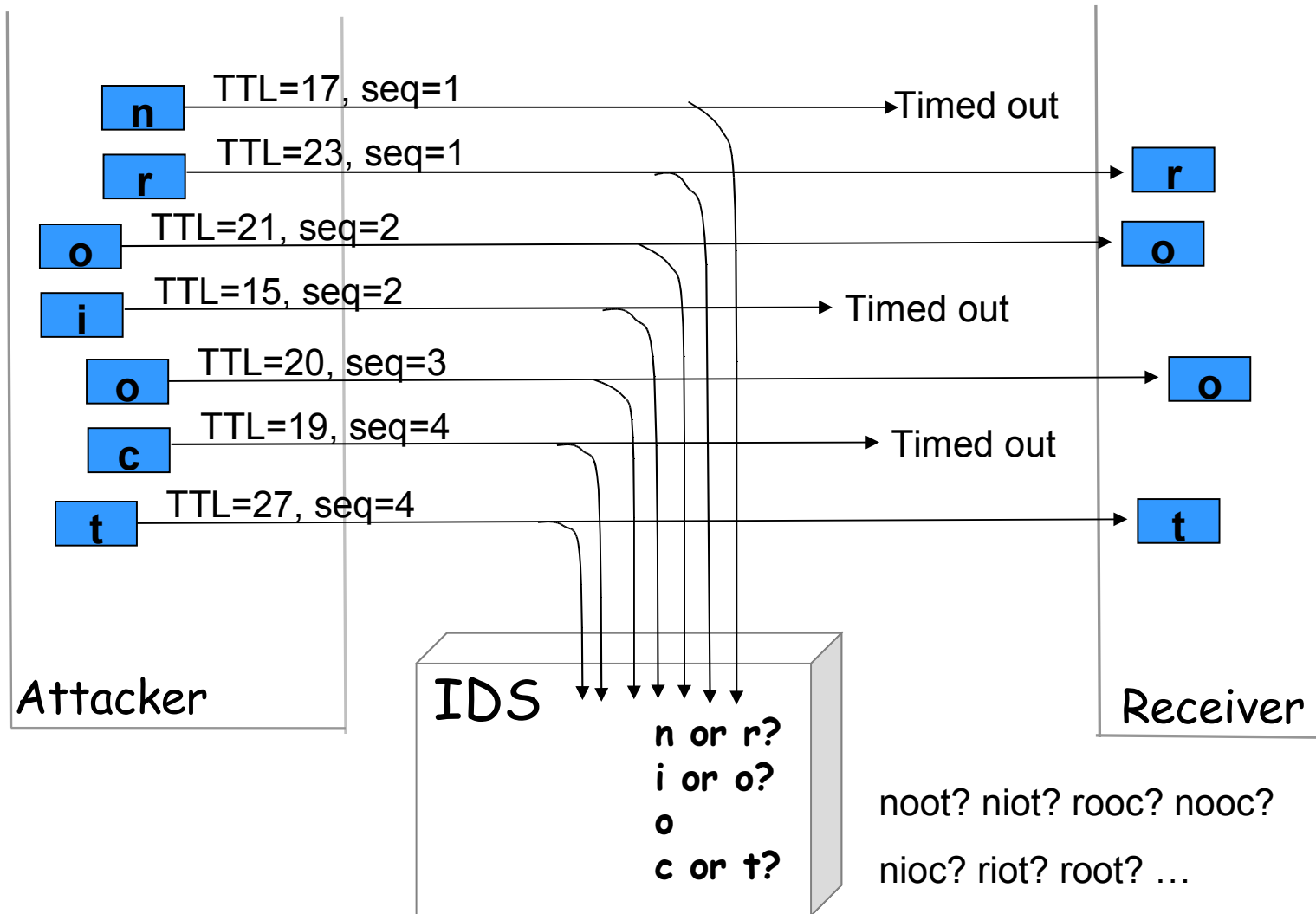
Evading Detection Via Ambiguous TCP Retransmission



Evading Detection Via Ambiguous TCP Retransmission



Evading Detection Via Ambiguous TCP Retransmission



Bypassing NIDS

- ❖ Evasion
- ❖ Insertion
- ❖ DoS it
- ❖ Hack it
- ❖ Cause many false alarms until admin stops paying attention