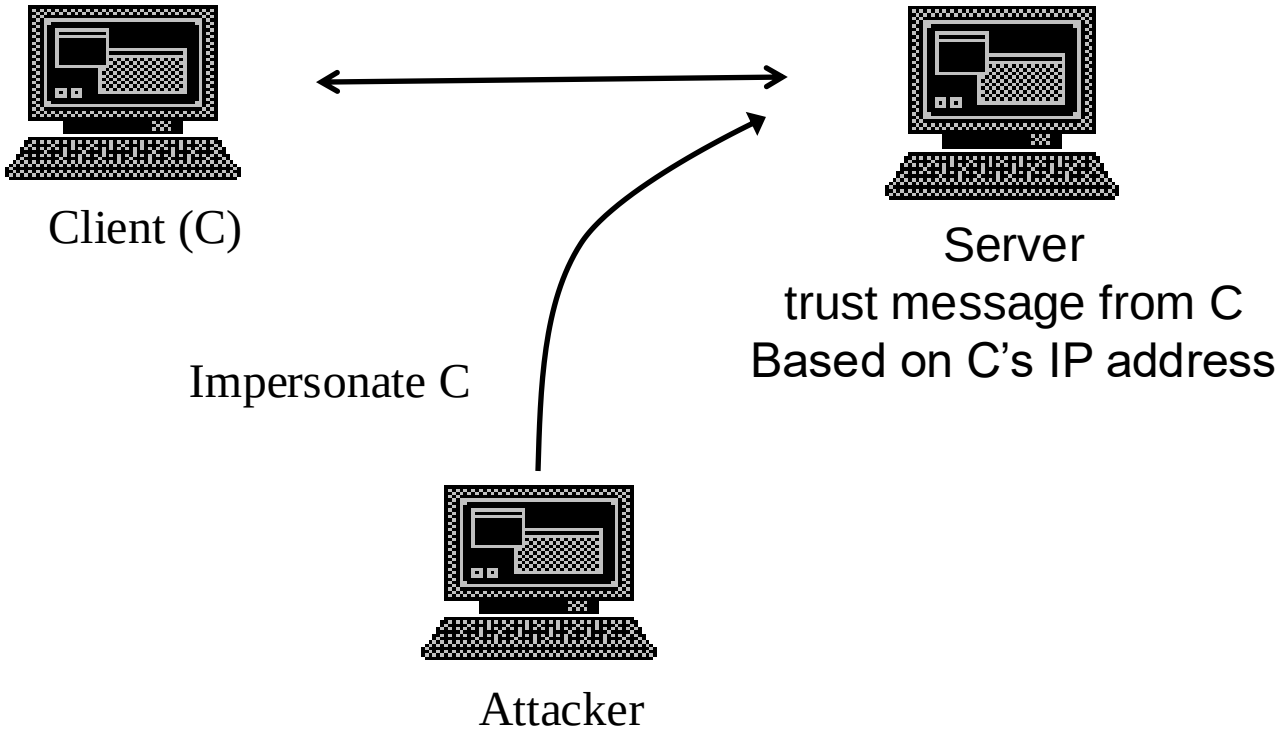
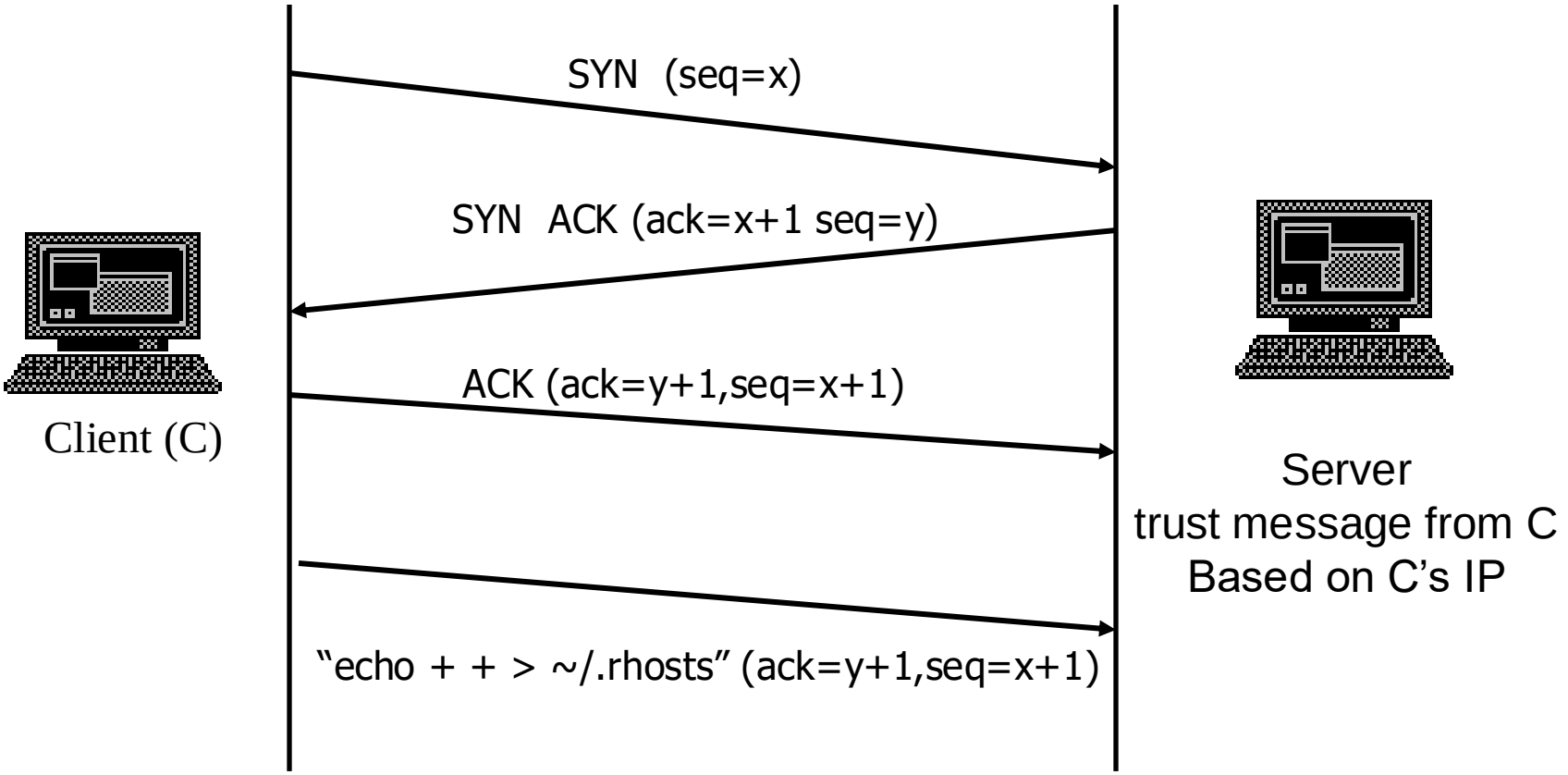
TCP Session Hijacking

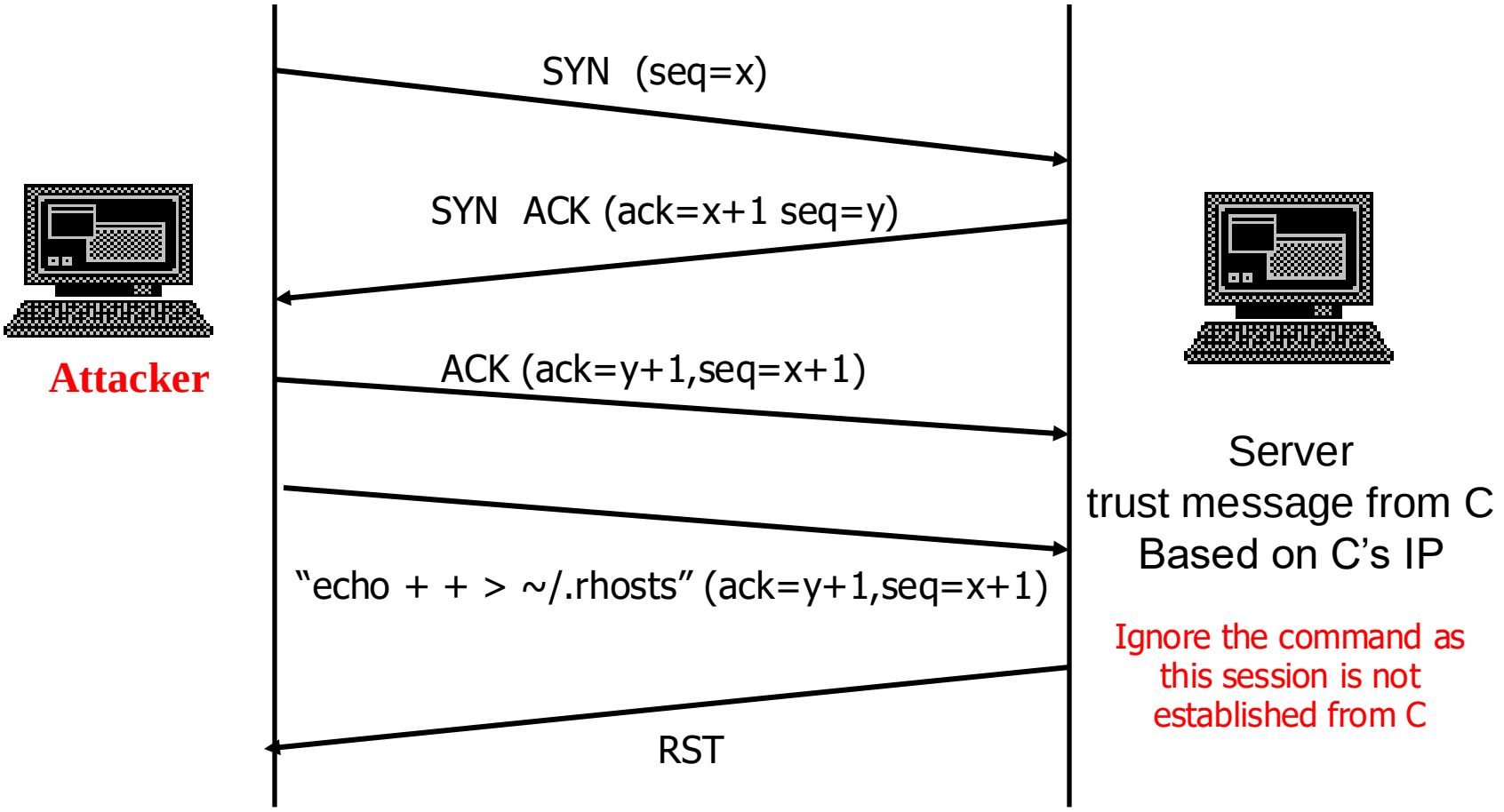
- An attacker takes over a TCP session between two machines.



TCP Session Hijacking

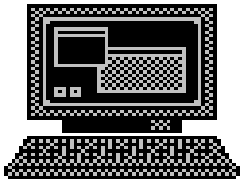


TCP Session Hijacking

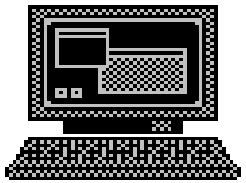


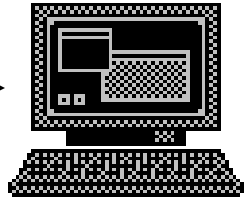
TCP Session Hijacking

- IP Spoofing



Client (C)



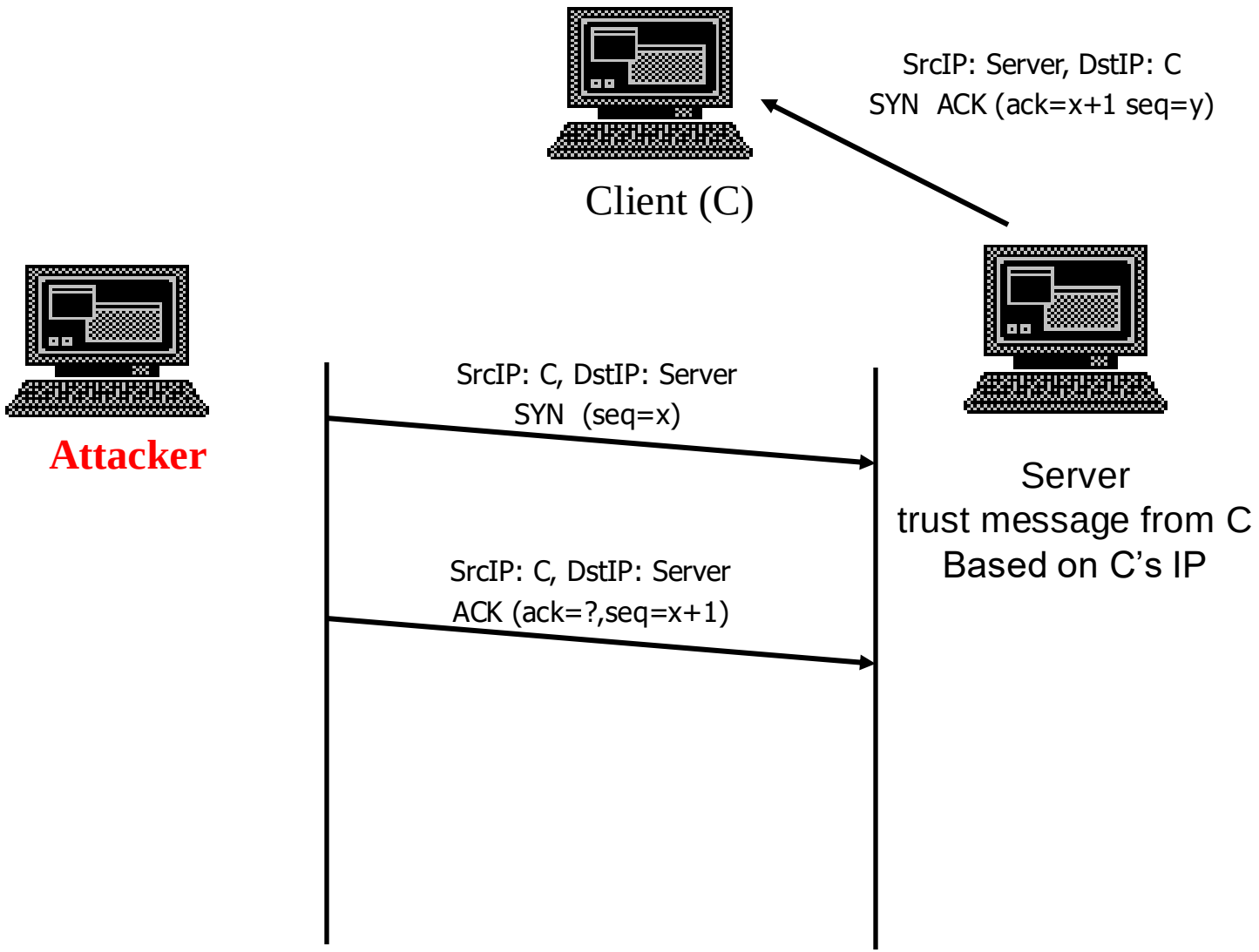


Attacker

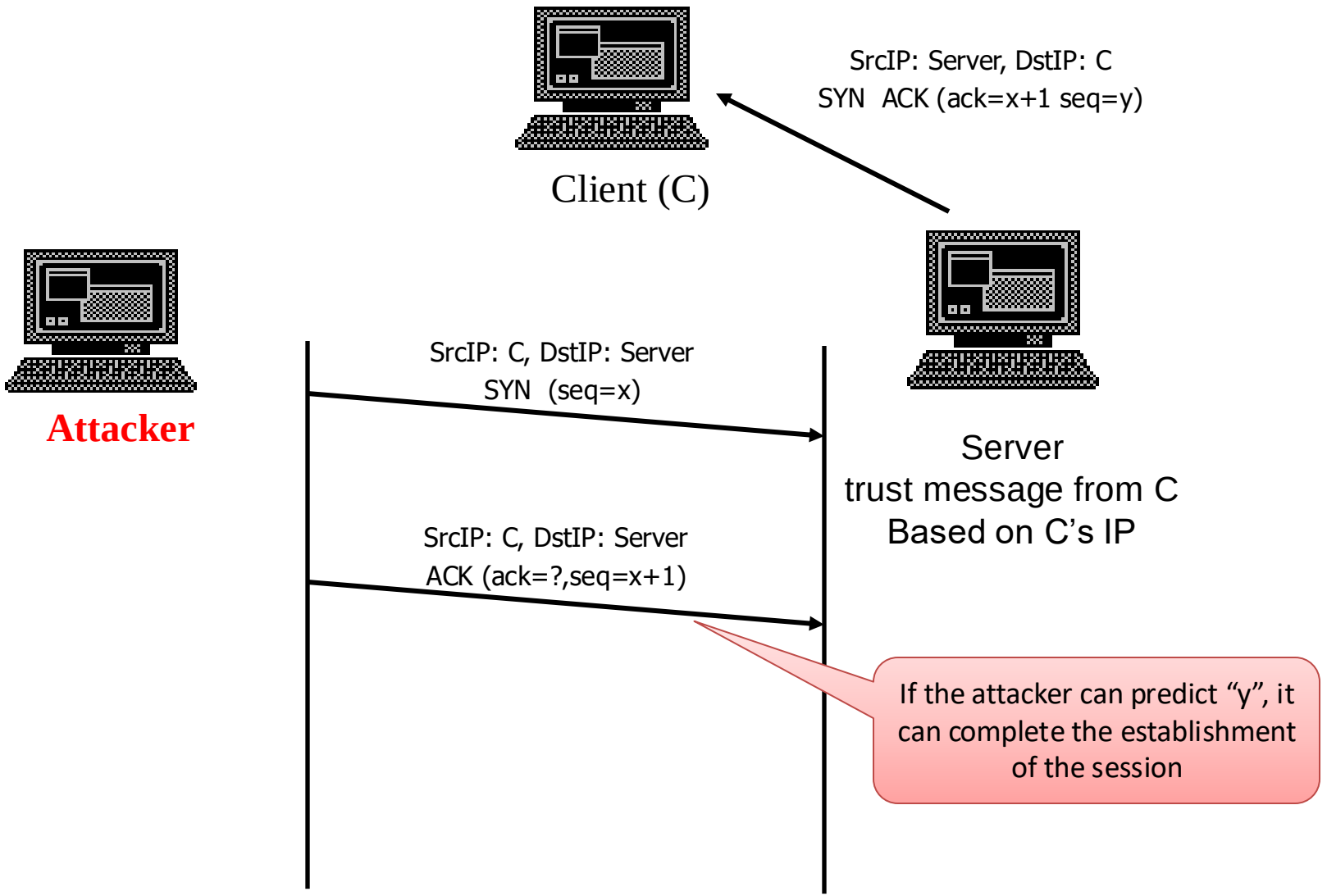
SrcIP	DstIP	IP Payload
C's IP	Server IP	……

Server
trust message from C
Based on C's IP

TCP Session Hijacking



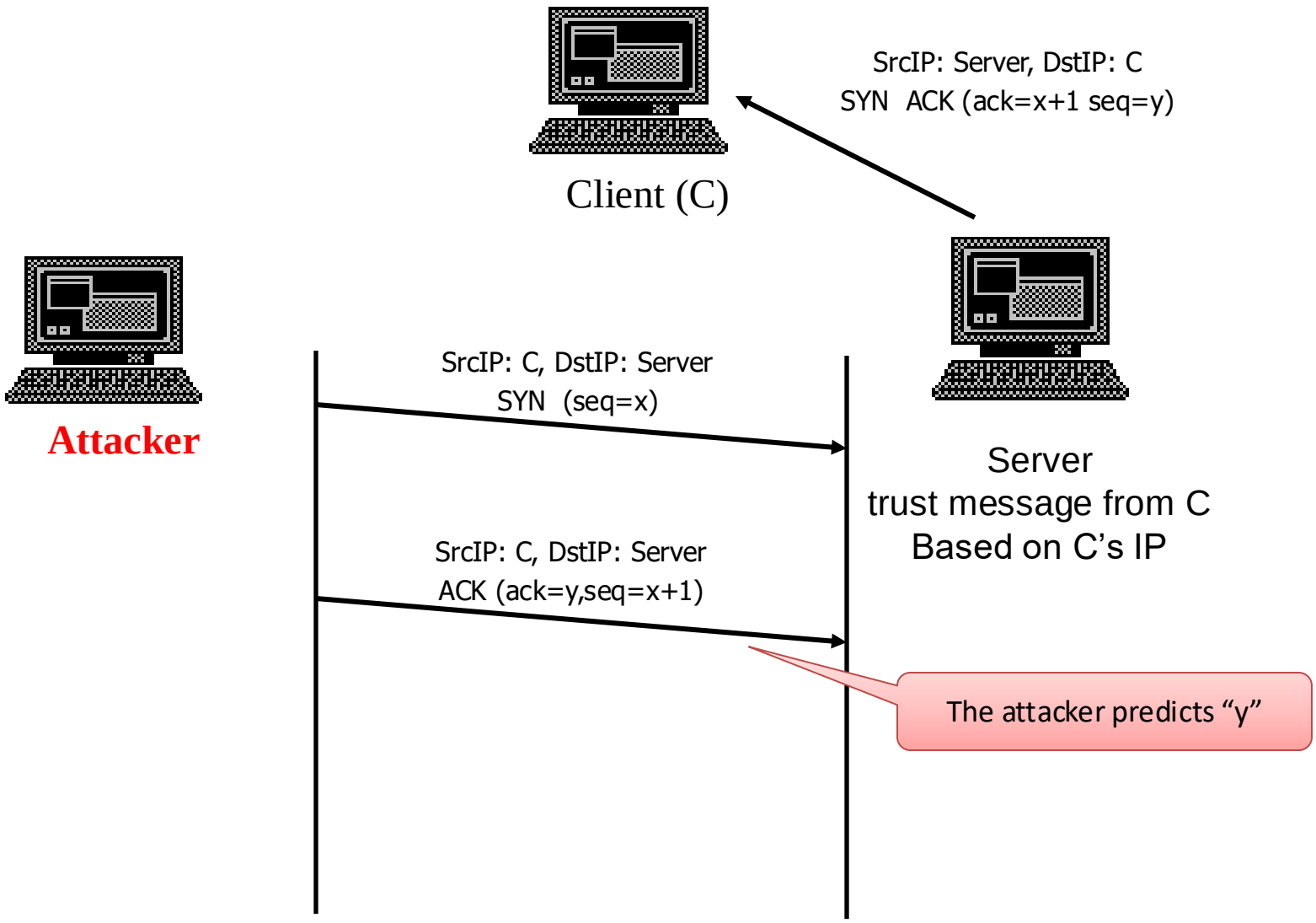
TCP Session Hijacking



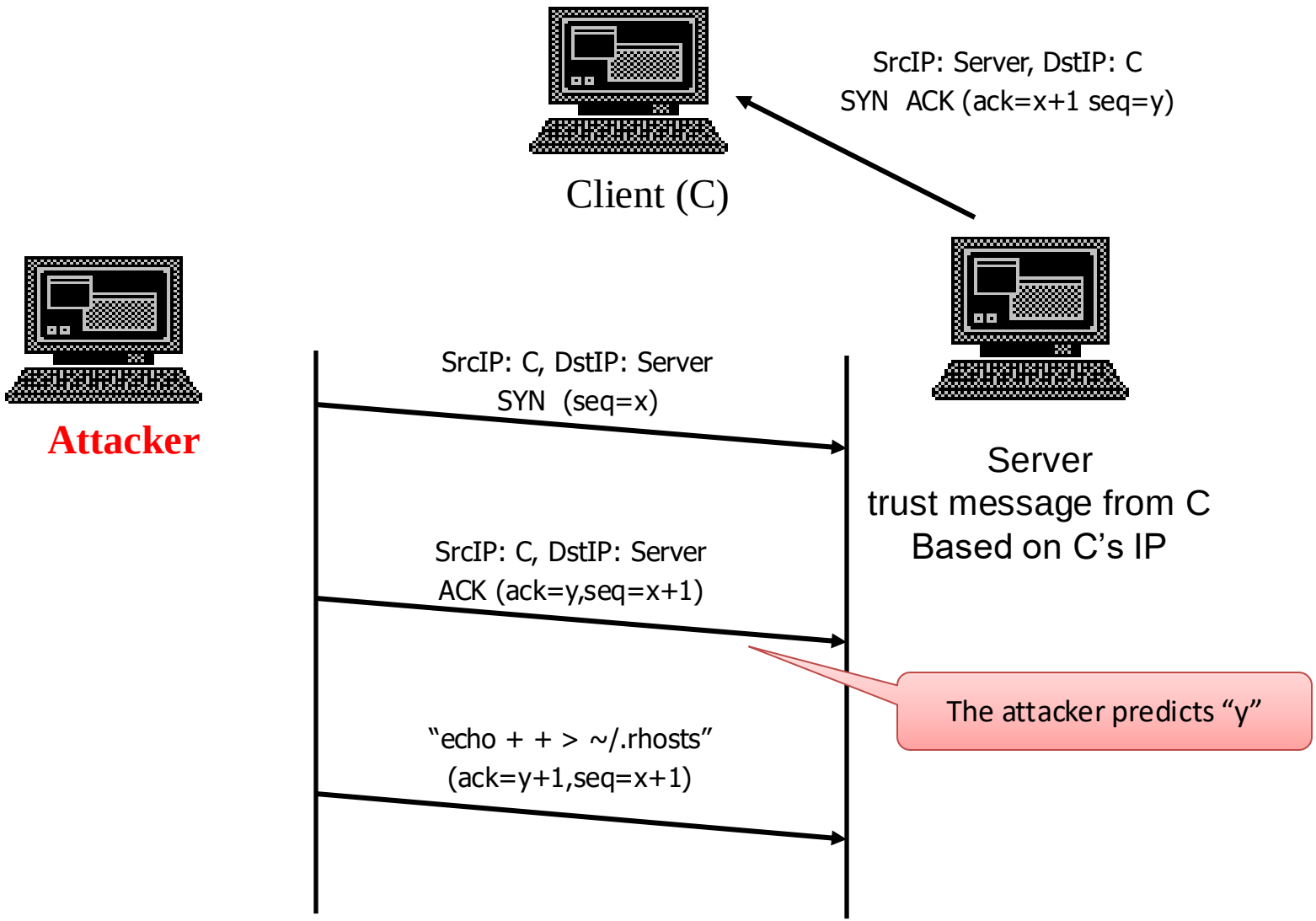
Predict the Initial Sequence Number in Berkeley-Derived Systems

- The Berkeley-derived kernels
  - Increment the initial sequence number variable by a constant once per second(e.g., 128,000)
  - Increment the initial sequence number variable by another constant for each new connection (e.g., 64,000)
- Attacker can
  - initiate a legitimate connection and observe the initial sequence number used
  - then calculate the initial sequence number used for the next connection attempt

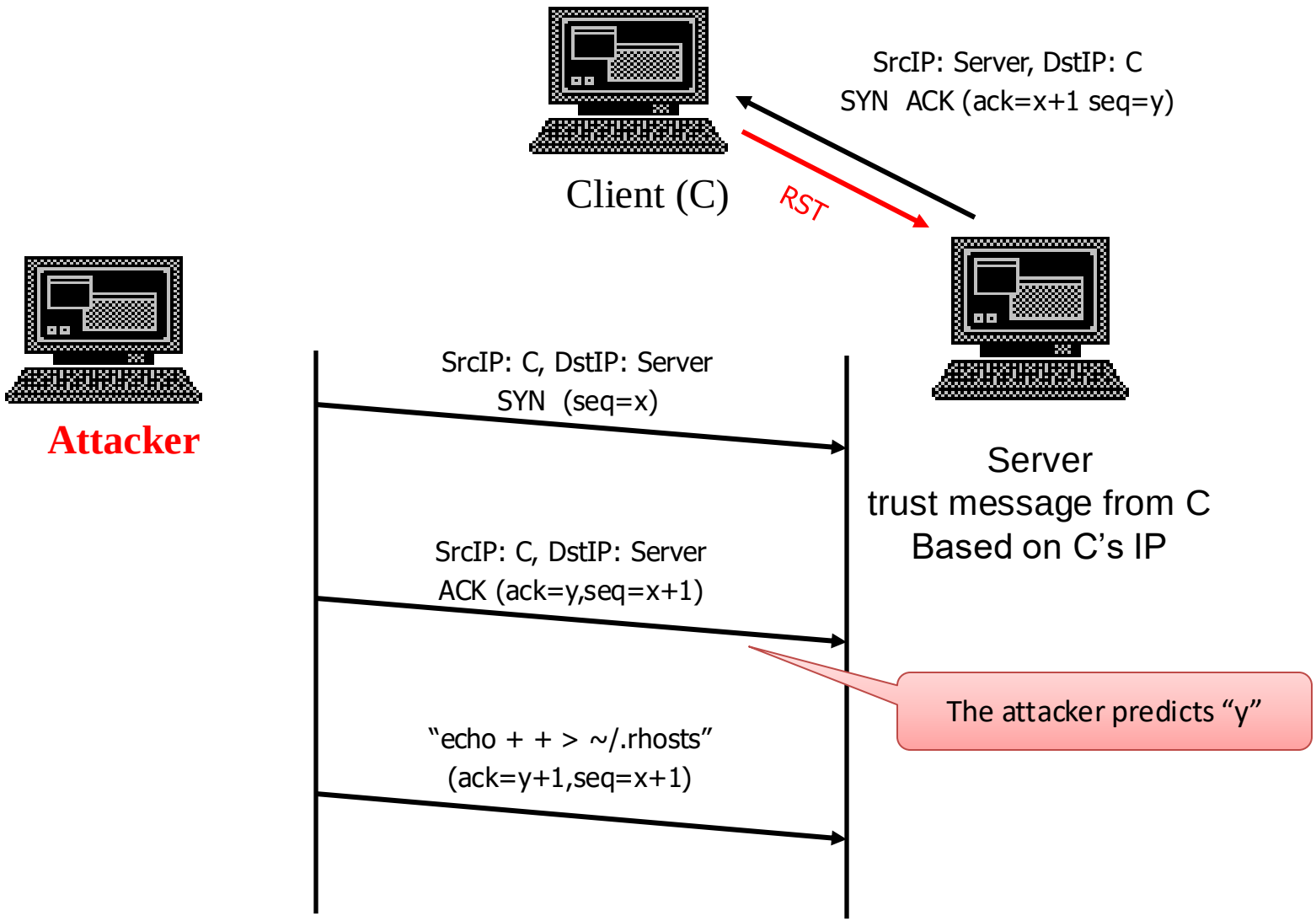
TCP Session Hijacking



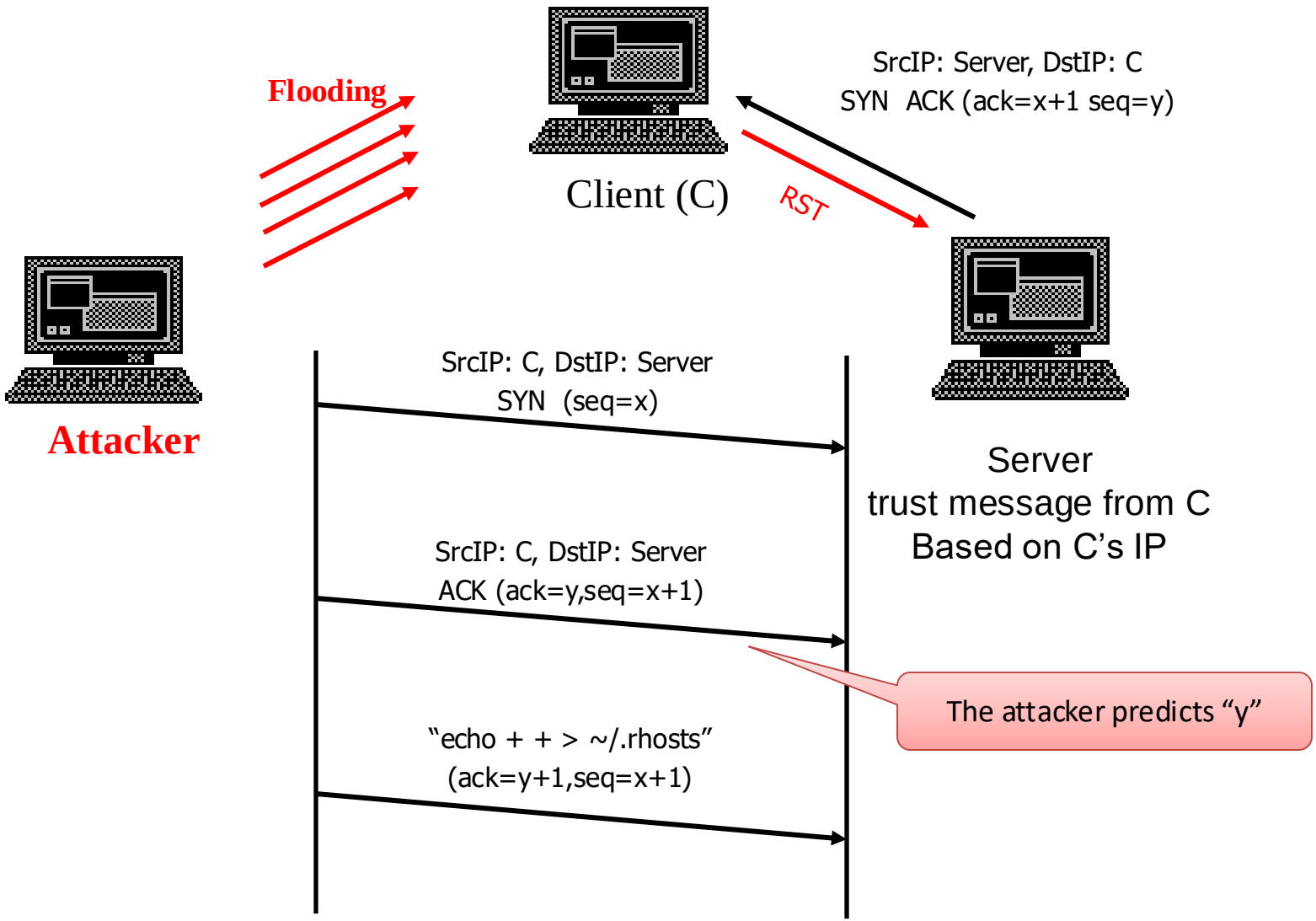
TCP Session Hijacking



TCP Session Hijacking



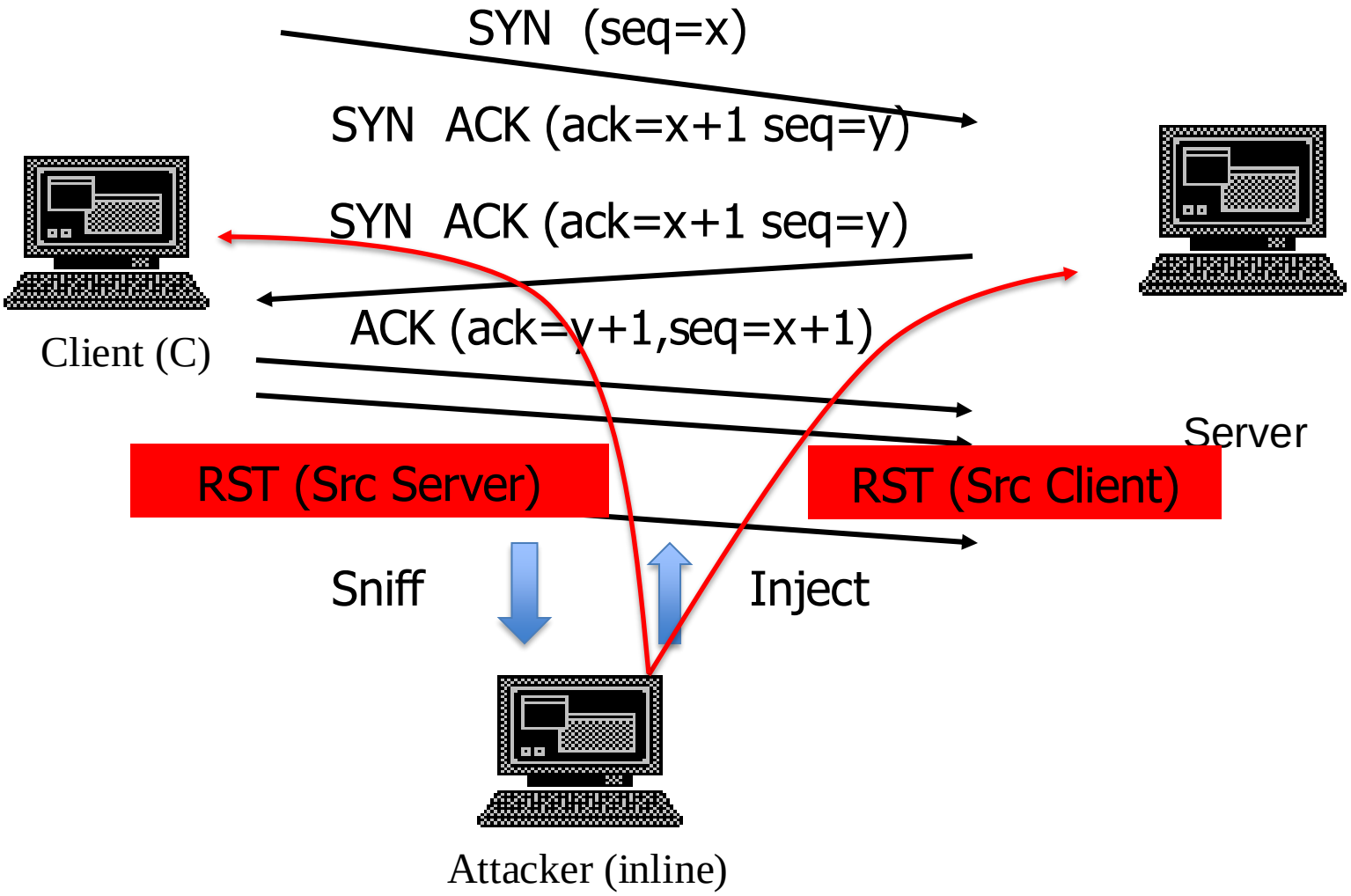
TCP Session Hijacking



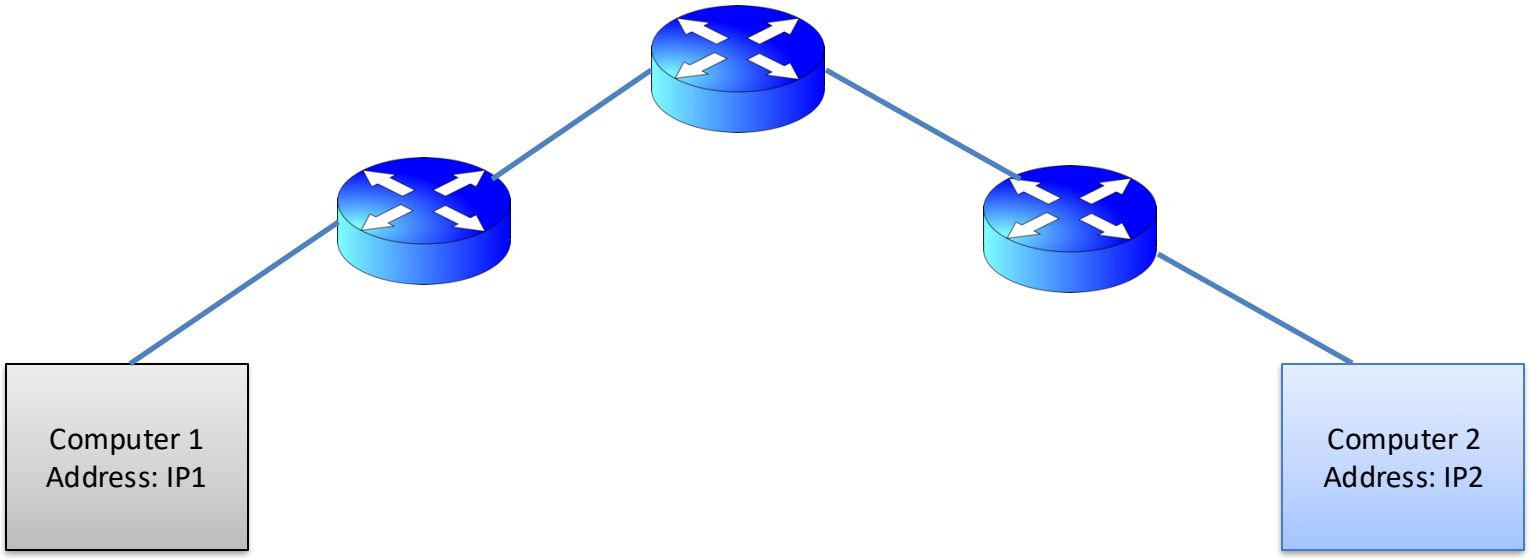
TCP RST

- A TCP reset basically kills a TCP connection instantly.
  - If the RST bit is set to 1, it indicates to the receiving computer that the computer should immediately stop using the TCP connection; it should not send any more packets using the connection's identifying numbers, called ports, and discard any further packets it receives with headers indicating they belong to that connection.

Malicious Usage: RST Reset

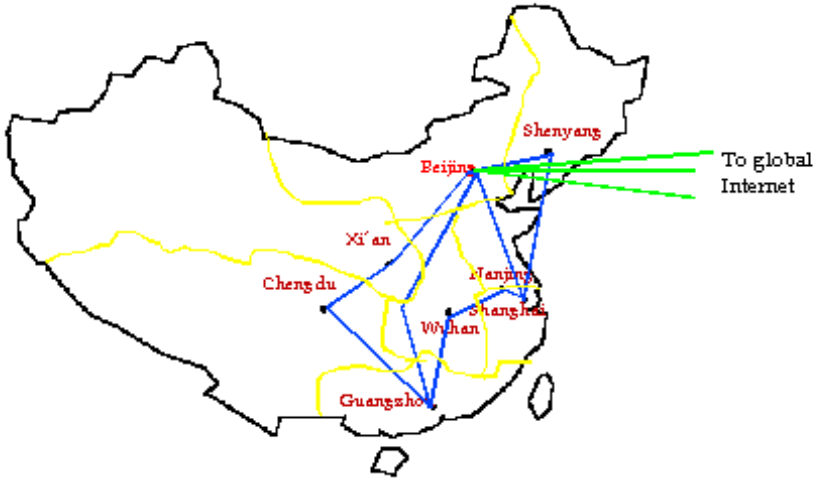


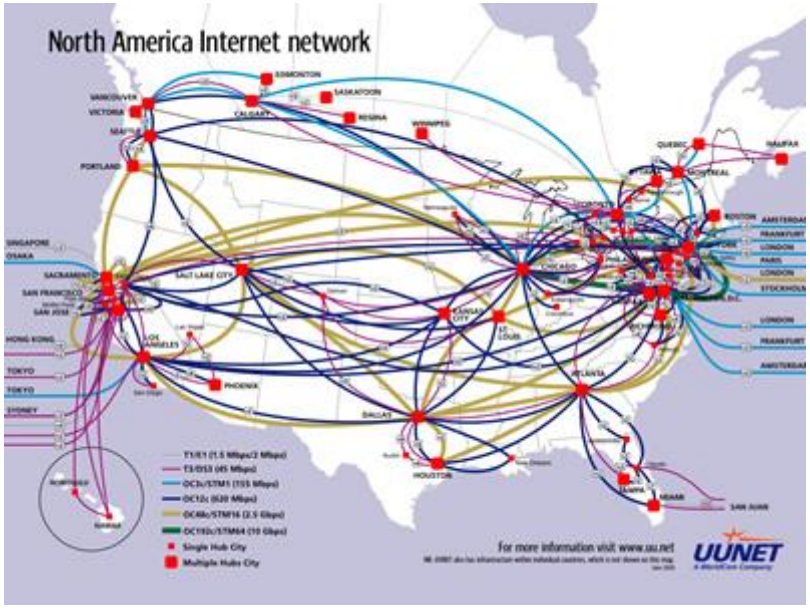
Who is “Malicious”/Malicious?



Who is “Malicious”/Malicious?

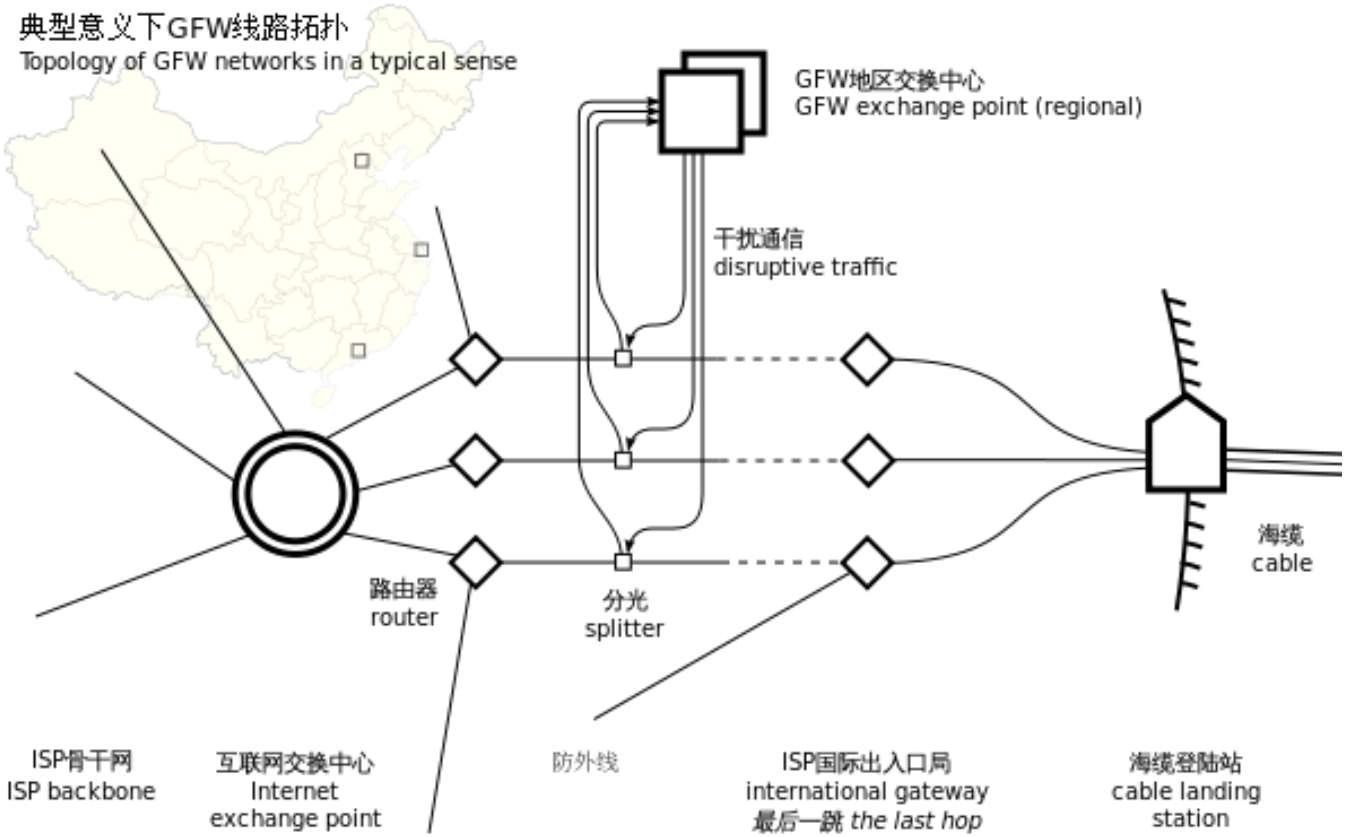
- The “Great Fire Wall” (active now).
- Comcast’s actions to disrupt P2P connections (around 2007).





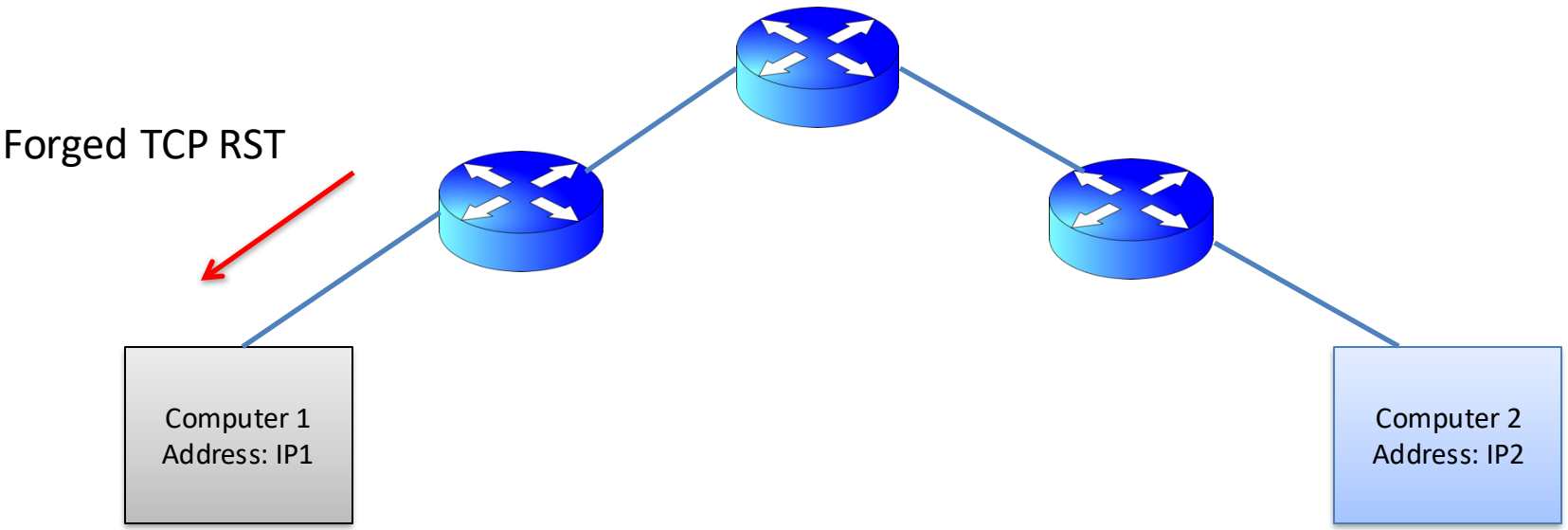
RST Reset

- Great Firewall (from wiki)



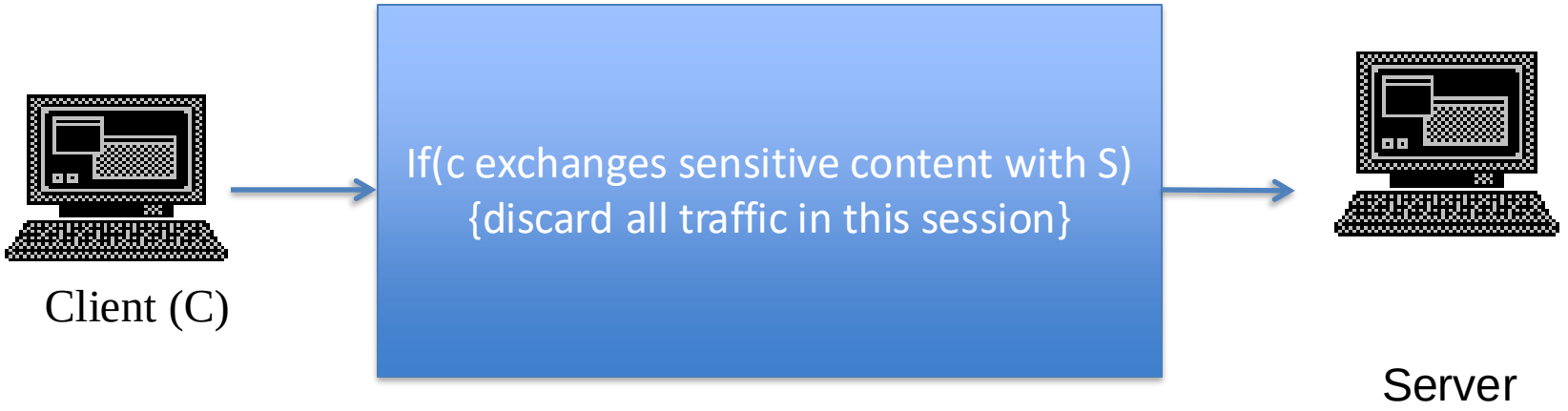
The Paper

- “Detecting Forged TCP Reset Packets”, N. Weaver, Robin Sommer, and Vern Paxson.



Discussion

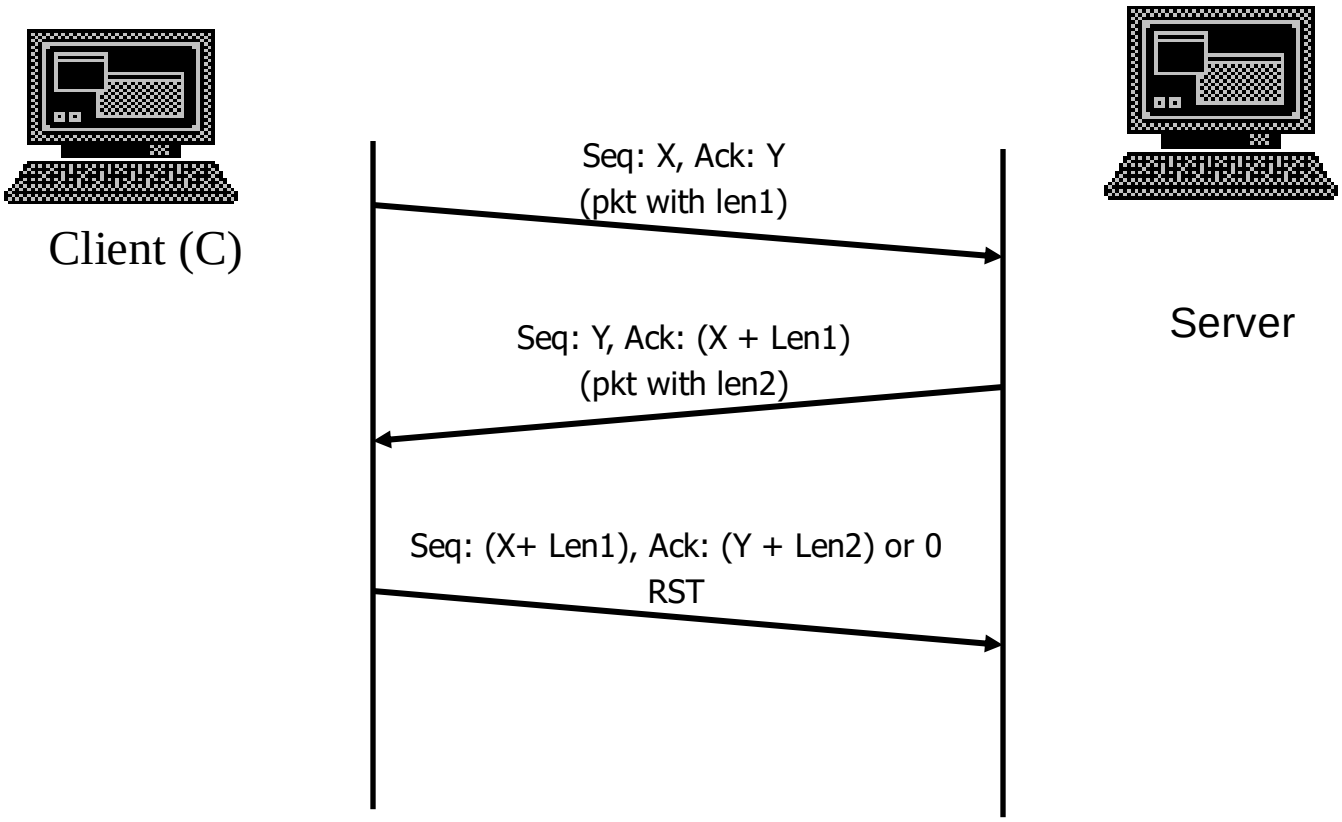
- Why don't they design GFW like this (inline interruption) rather than RST-based method (out-of-band interruption)?



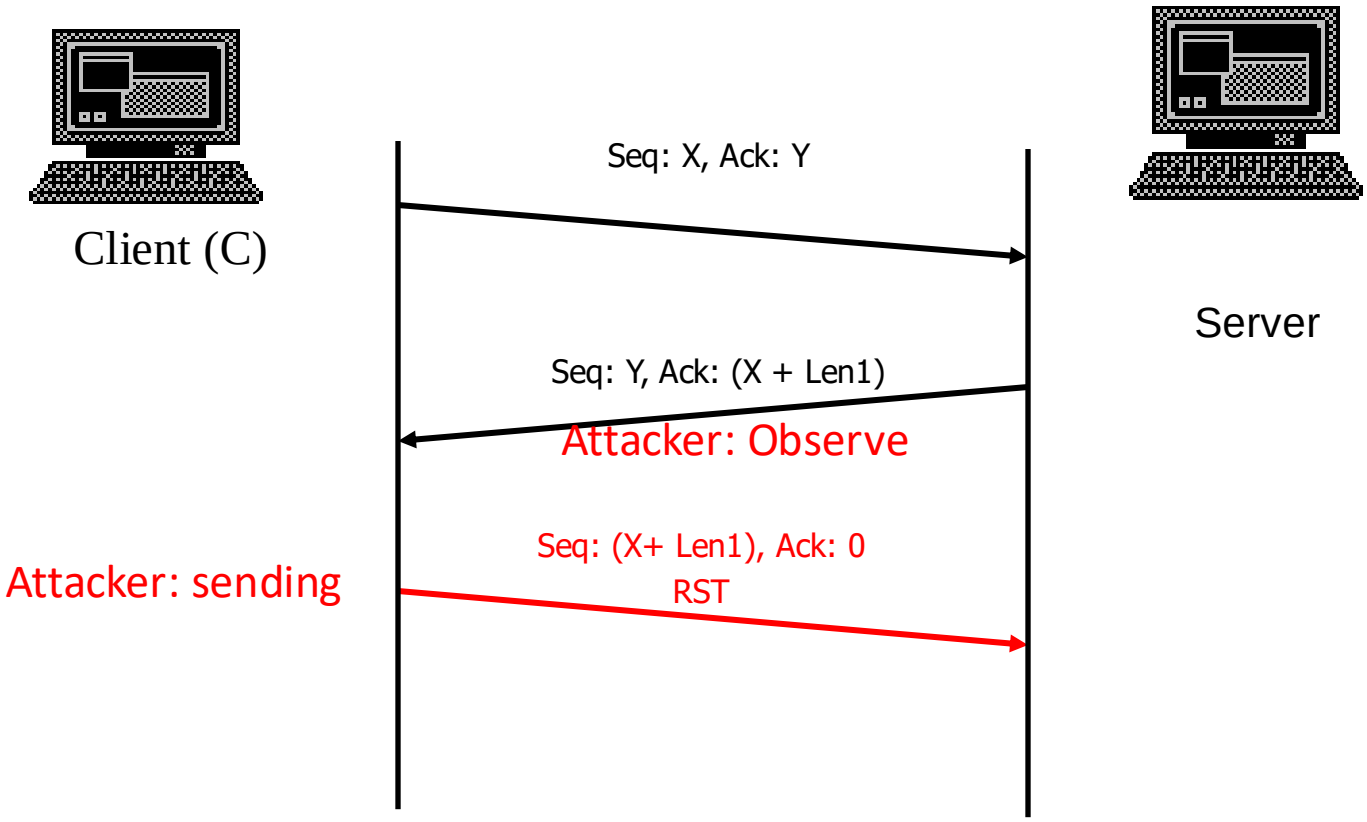
Discussion

- Why does GFW send RST packets to both client and server?
  - GFW can send RST to only client. It should be enough to terminate the connection.

The Normal Case of RST



The Injection of RST

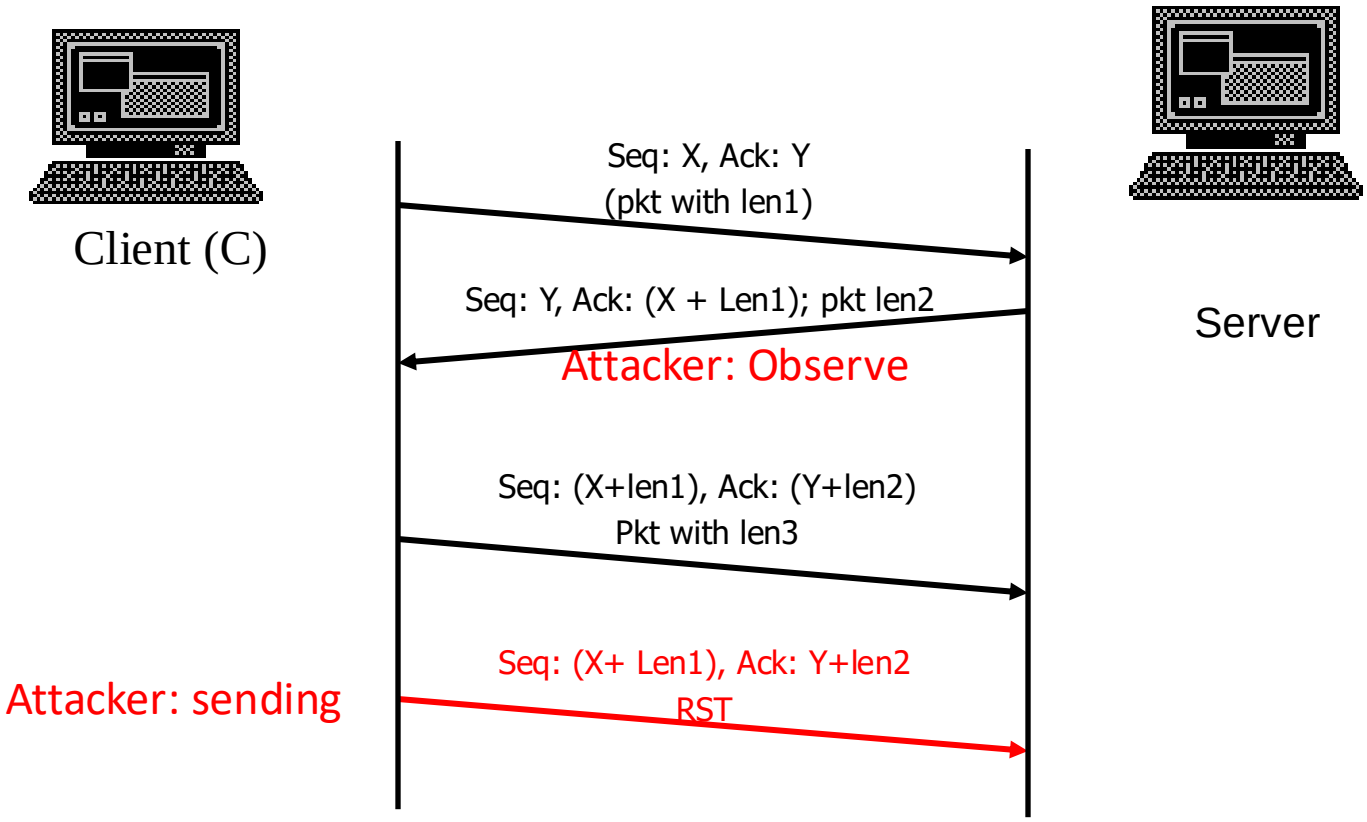


What is the problem?

Race Condition

- The sender can send a few (decided by both congestion control and flow control algorithms) packets with out receiving acknowledgments.
  - Seq number < Min(window-size, rwnd)
    - Window-size for congestion control, decided by the sender of the packet
    - rwnd for flow control, decider by the receiver of the packet.

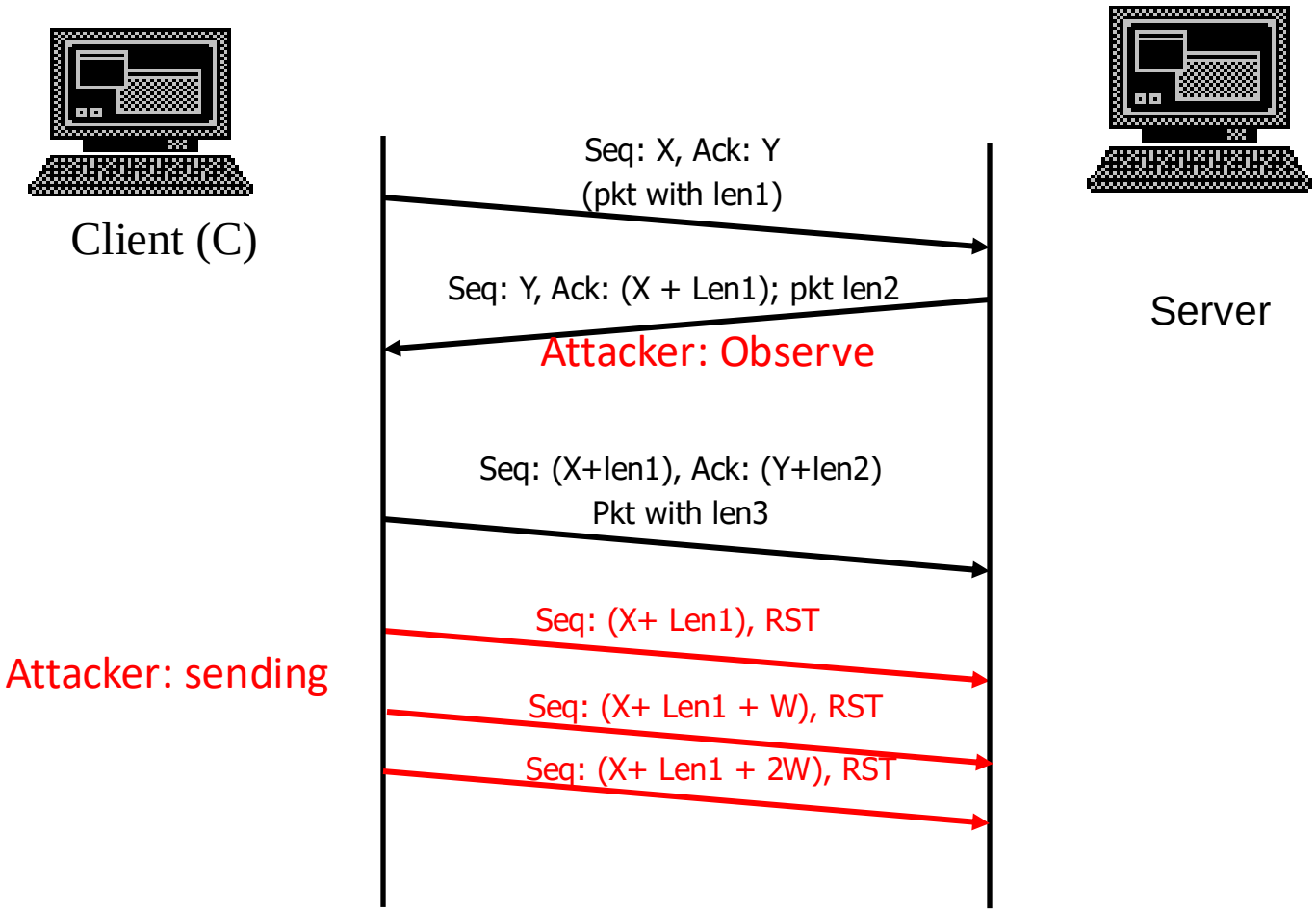
The Challenge



What is the problem?

Objective: X+len1+len3 <= seq <= X+len1+len3+rwnd

The Solution



Objective: X+len1+len3 <= seq <= X+len1+len3+rwnd

Detection Rules

- RST_SEQ_DATA:
  - The RST packet is “out of sequence”, with the receiver observing a sequence number less than the preceding data packet would suggest.
  - What doesn’t it happen for normal cases?
- DATA_SEQ_RST:
  - The receiver will see further data packets from the sender *after* it has already received the RST.
  - What doesn’t it happen for normal cases?

Detection Rules

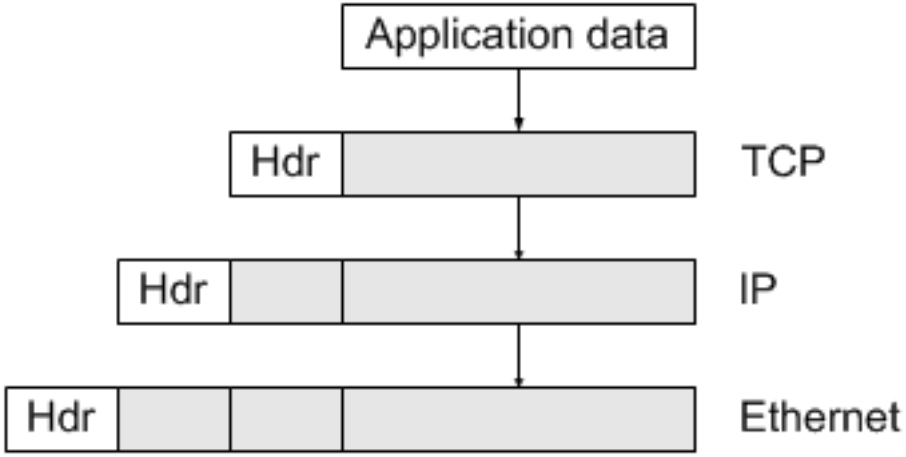
- RST_SEQ_CHANGE:
  - Back-to-pack pairs of RSTs in which the second RST has a sequence number higher than the first, and that exceeds the current maximum sequence number.
  - What doesn't it happen for normal cases?

Detection Rules

- RST_ACK_CHANGE:
  - Nonsensical ACK numbers
- SYN_RST
  - SYNs immediately followed by RST
- SYN_ACK_RST
  - SYN/ACKs immediately followed by RST

Application Layer Attacks

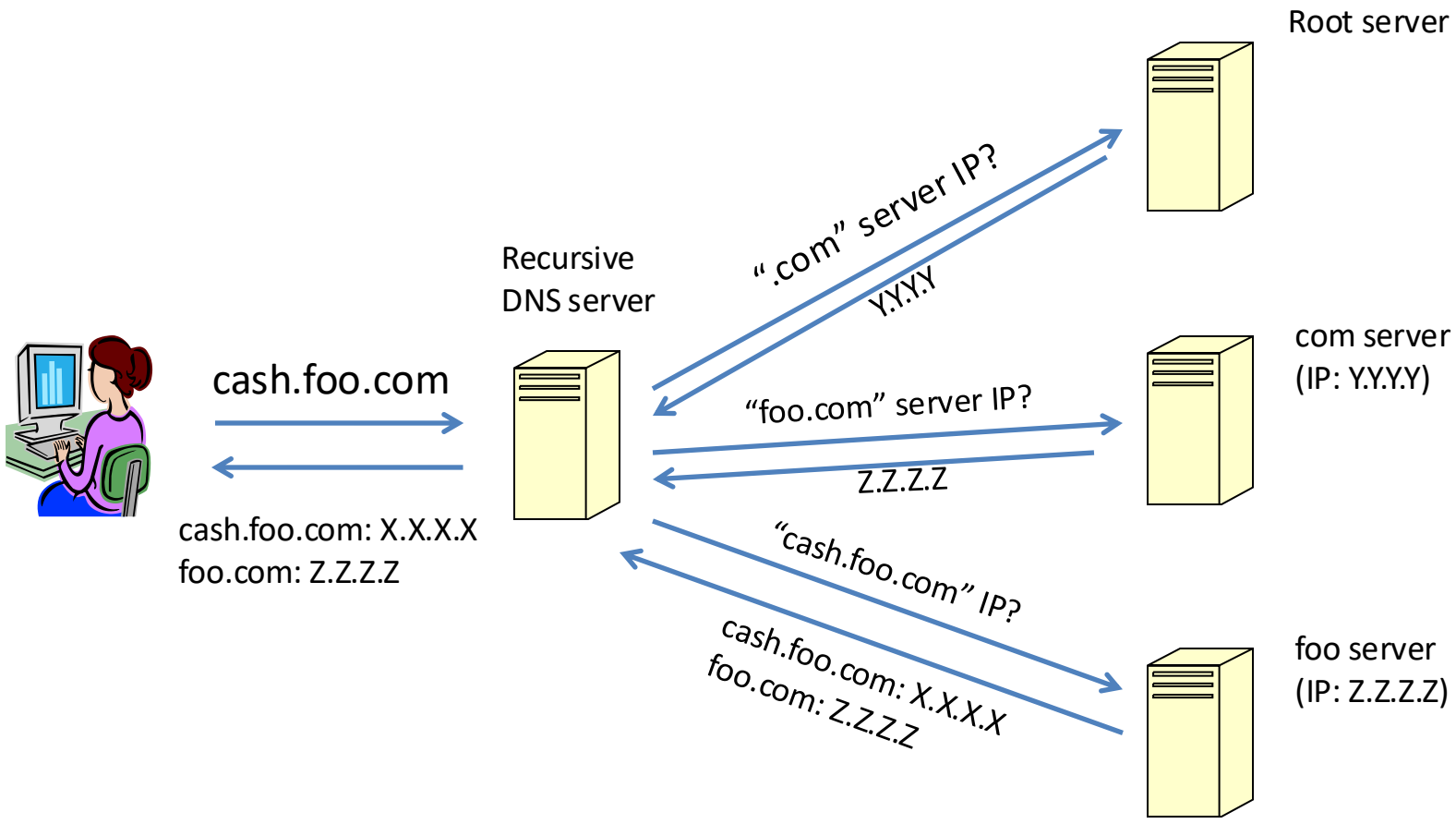
- The Application Layer
  - A variety of protocols
  - DNS



Domain Name System (DNS)

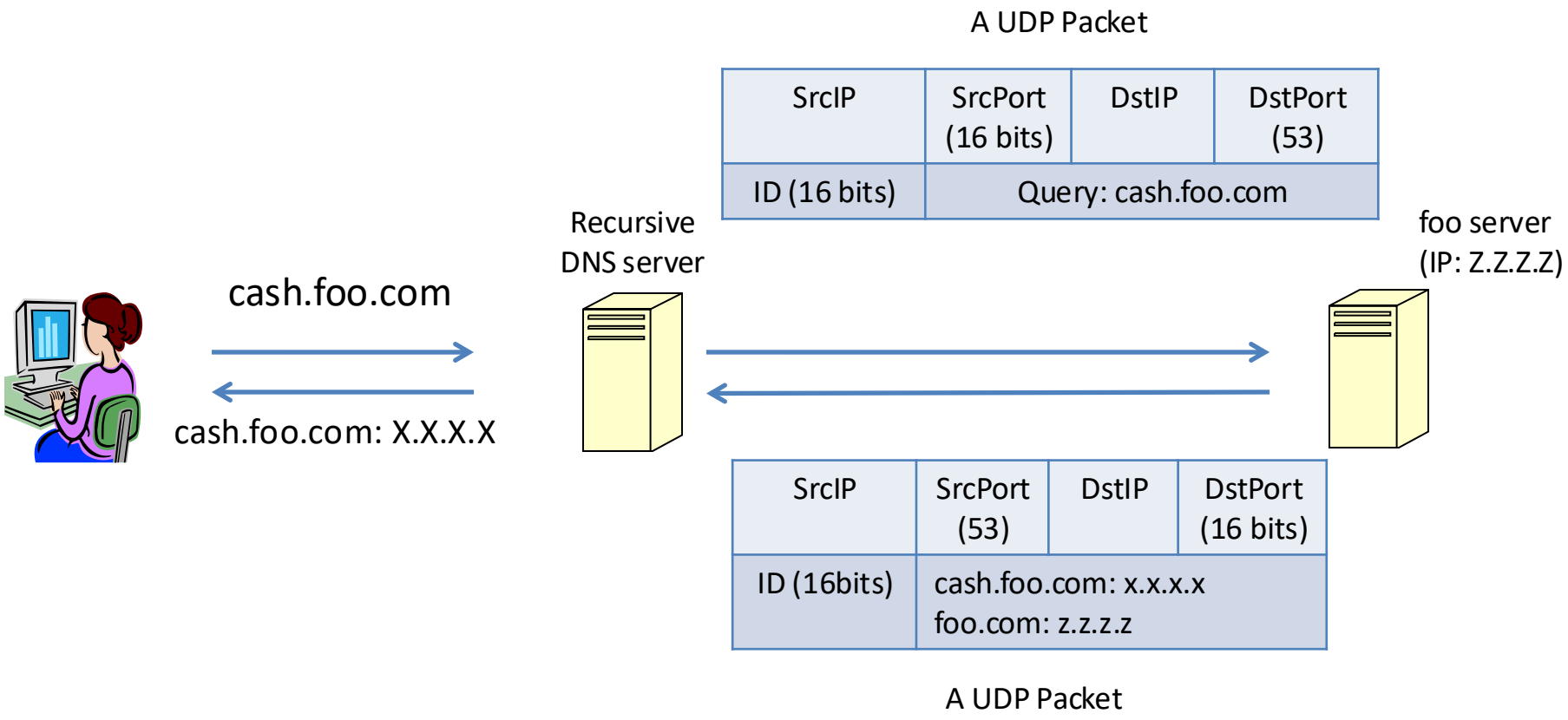
- Indispensable component for the Internet
  - www.google.com -> 173.194.75.106
- Used by a huge percentage of Internet applications
  - Browsers
  - FTP
  - Instant Messengers

How DNS Works



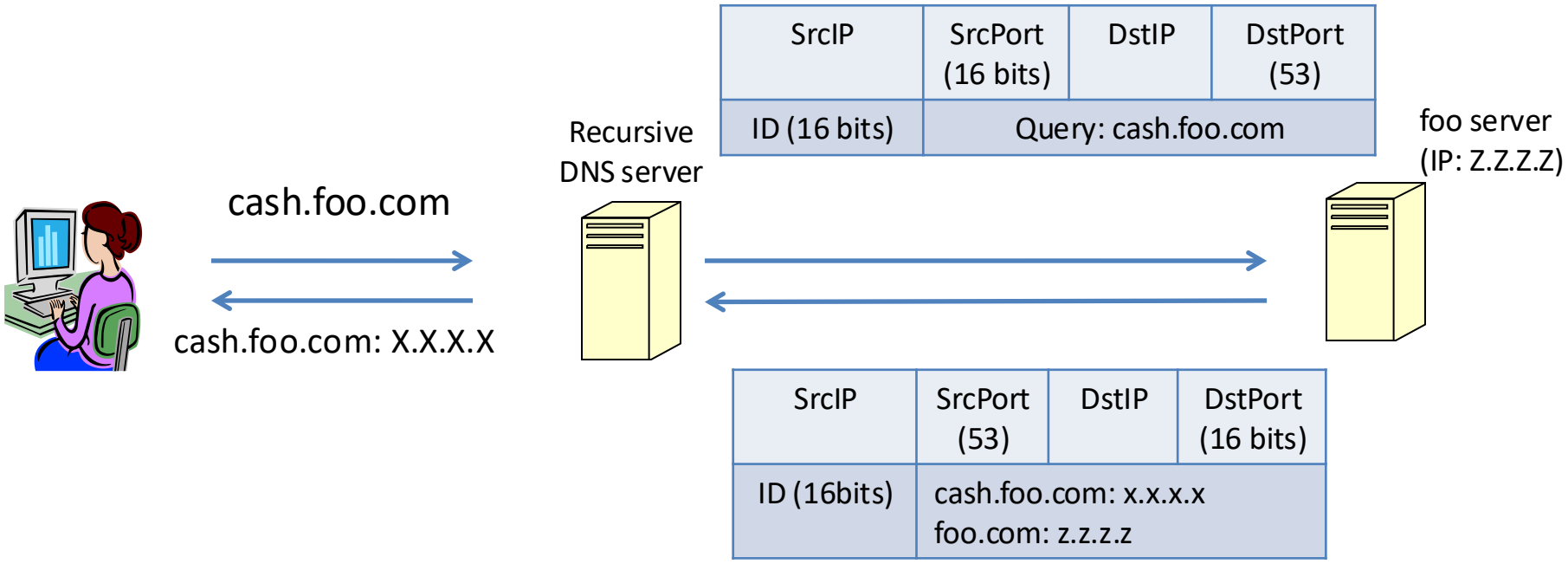
Domain	IP
cash.foo.com	X.X.X.X

How DNS Works

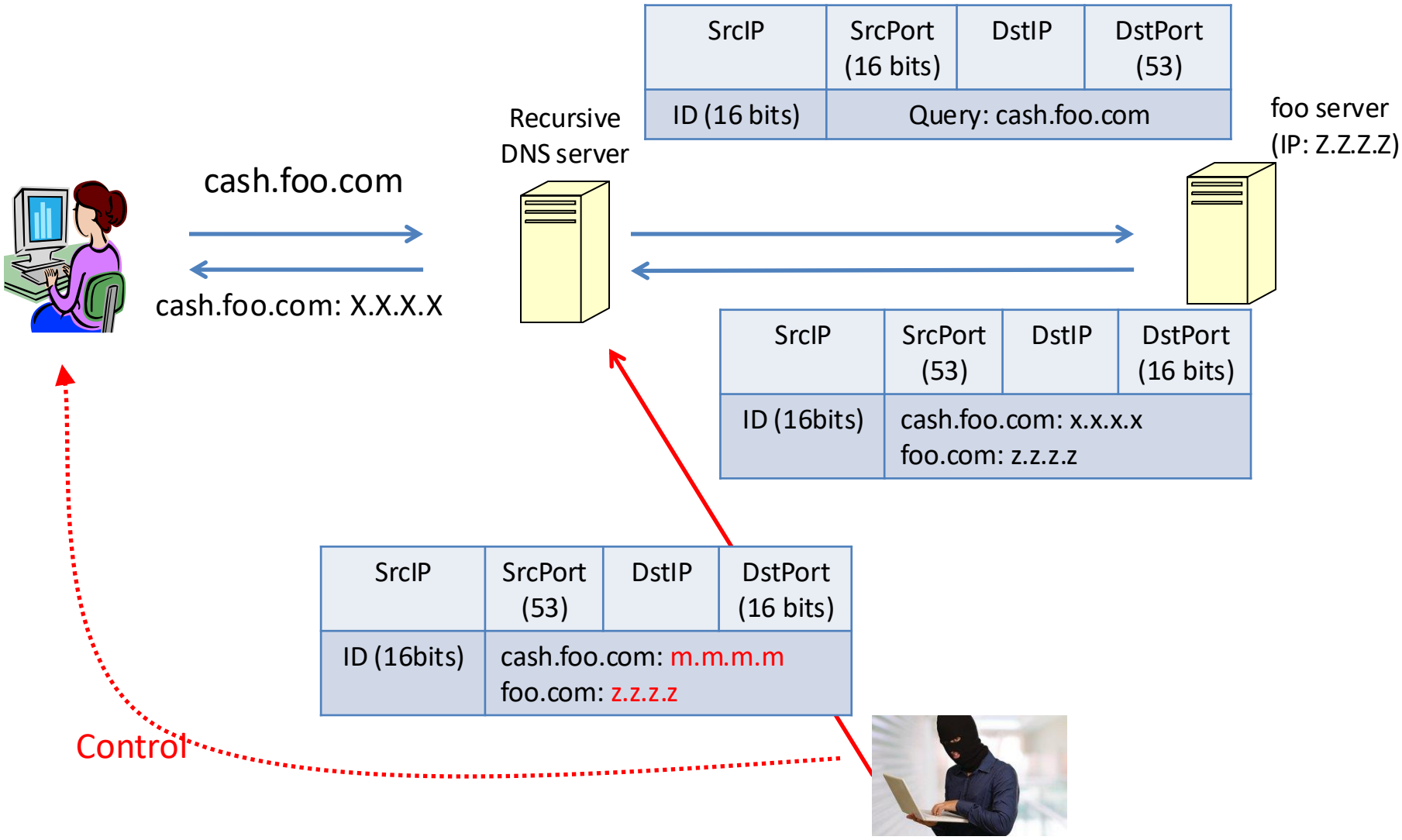


DNS Poisoning Attack

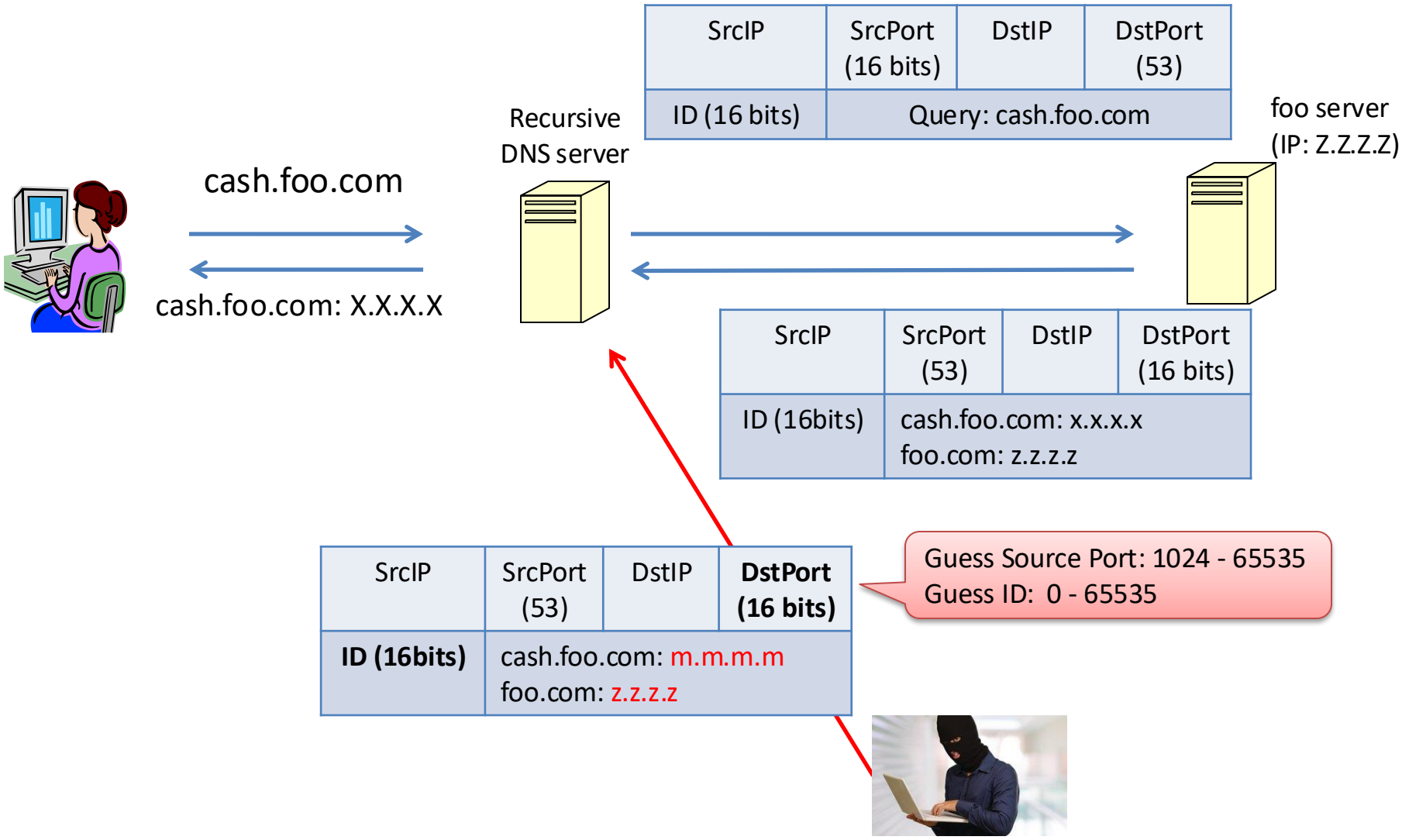
- How a recursive server accepts a response from the authoritative server



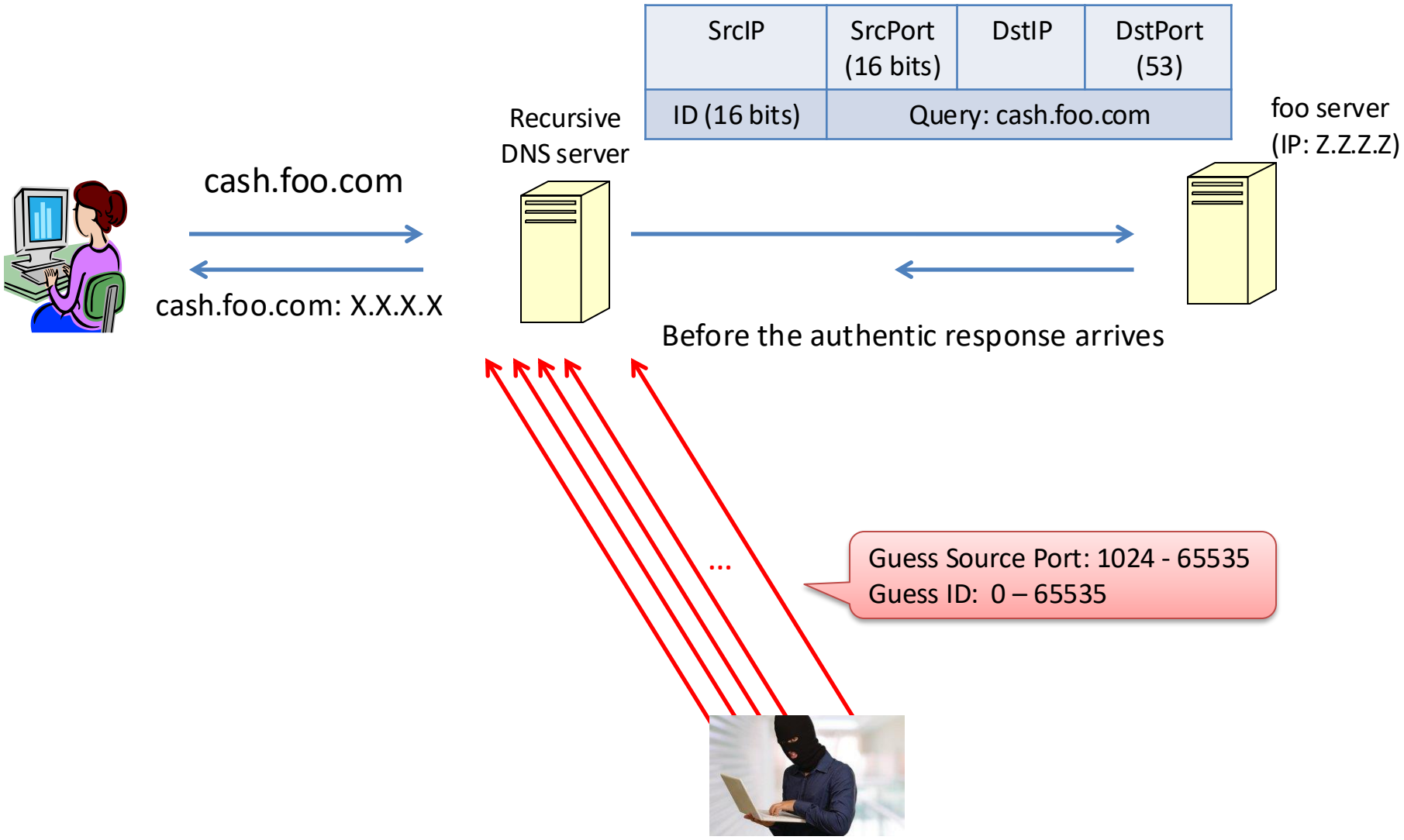
DNS Poisoning Attack



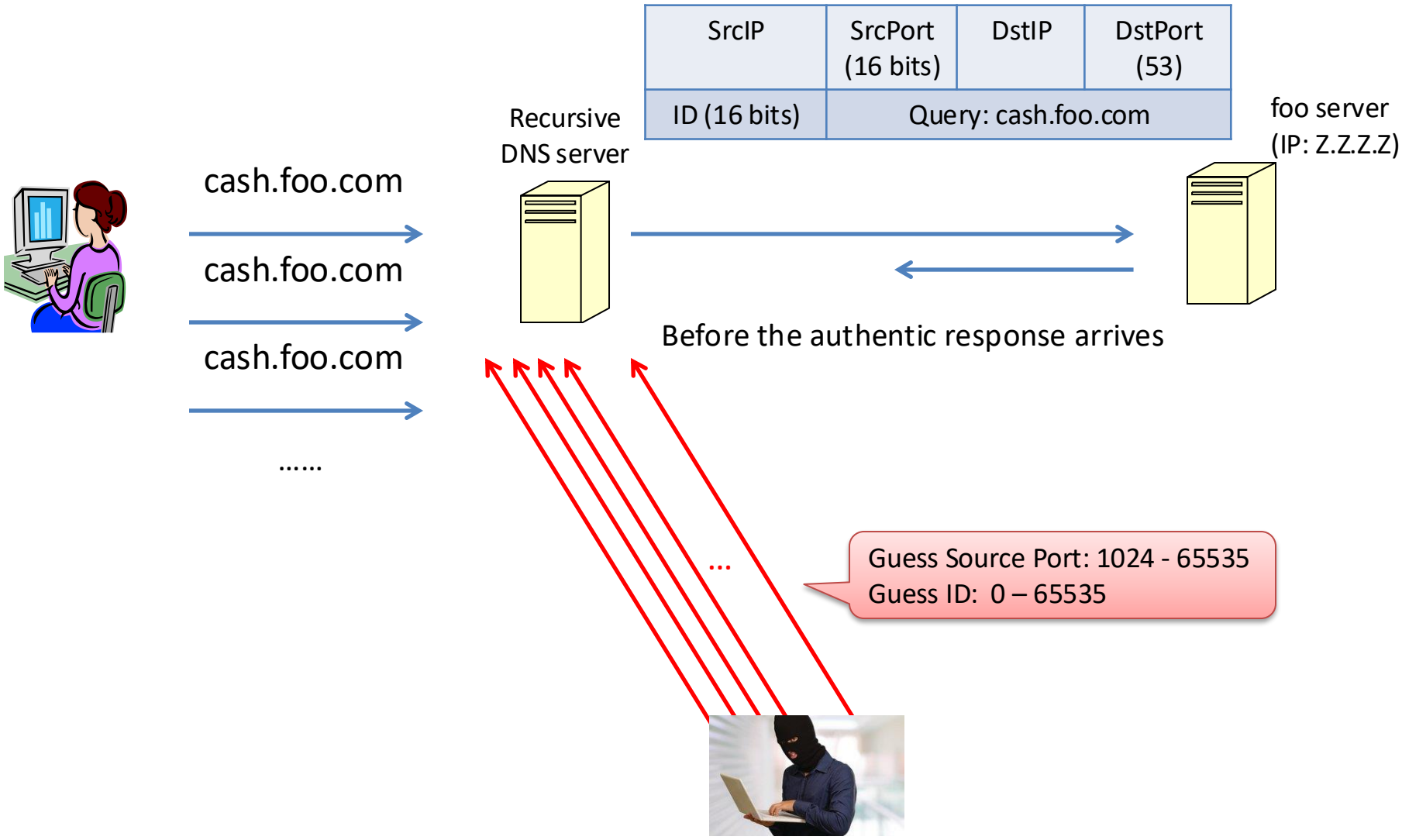
The Challenges for Attackers



The Challenges for Attackers



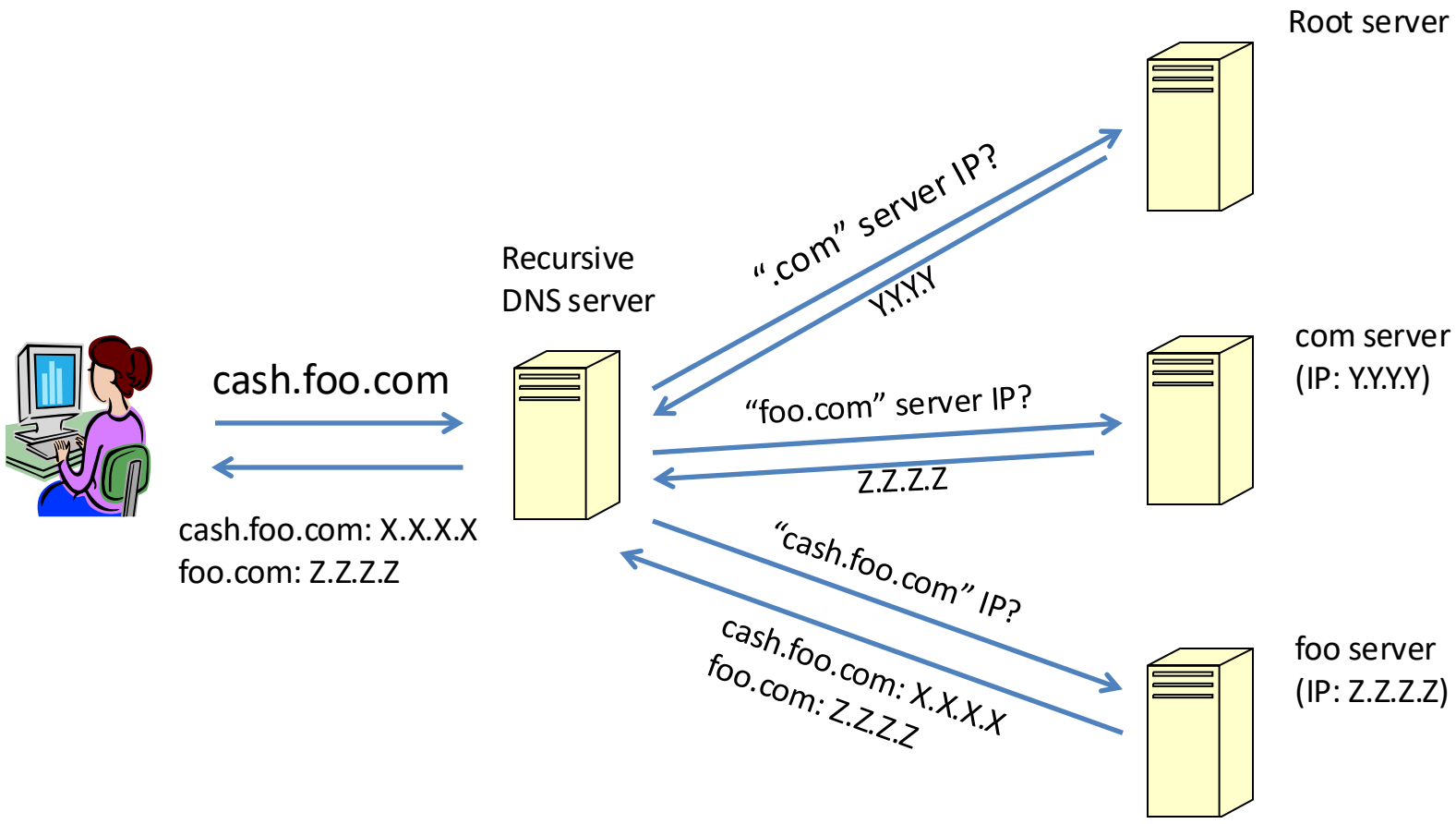
How to Address Challenges?



Inline DNS Injection

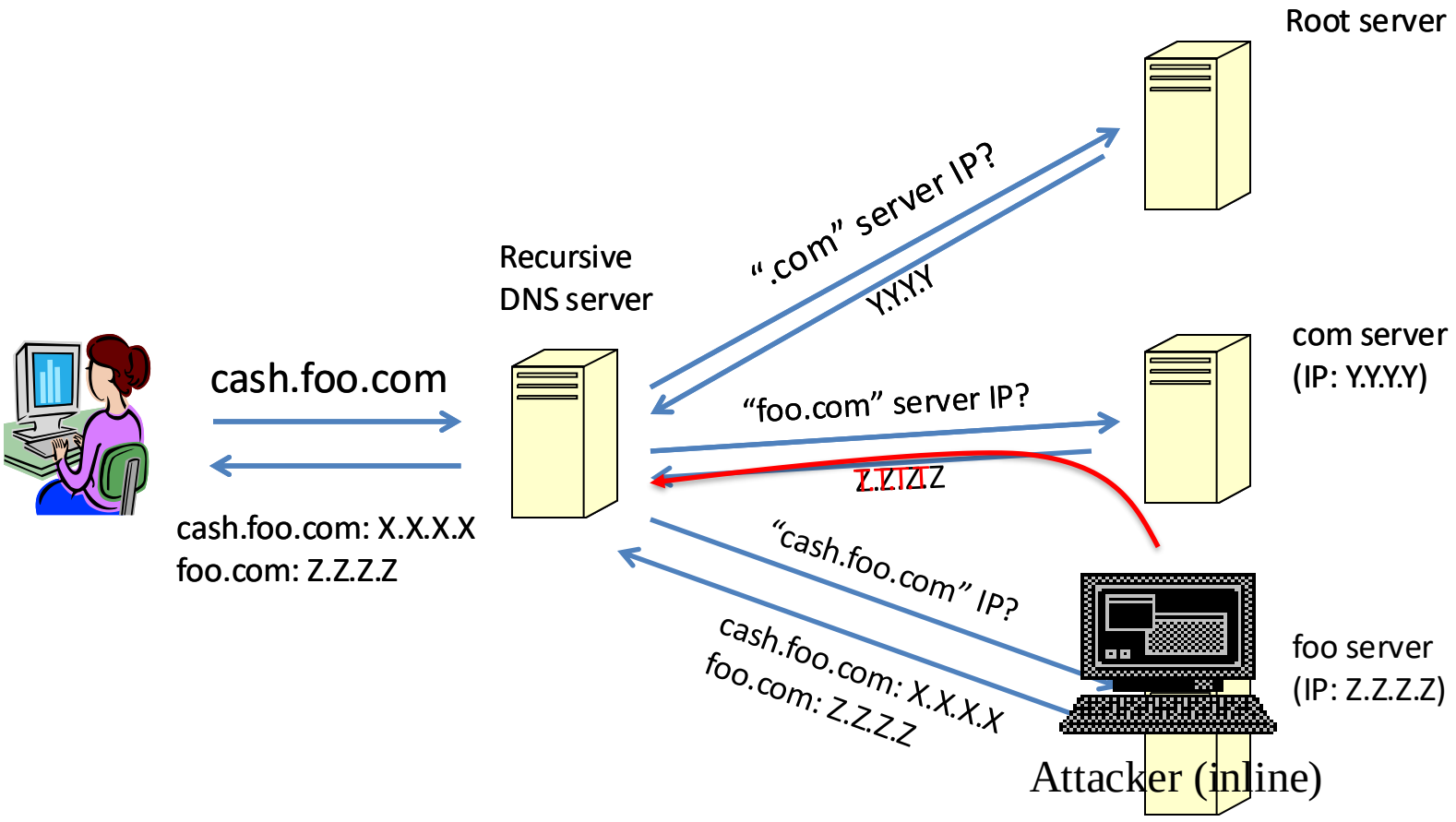
- “The Collateral Damage of Internet Censorship by DNS Injection”
  - Sparks, Neo, Tank, Smith, and Dozer, Sigcomm 2012

How DNS Works



Domain	IP
cash.foo.com	X.X.X.X

How DNS Injection Works



Domain	IP
cash.foo.com	X.X.X.X

Where does it start

- https://lists.dns-oarc.net/pipermail/dns-operations/2010-March/005260.html

[dns-operations] Odd behaviour on one node in I root-server

Mauricio Vergara Ereche mave at nic.cl
Wed Mar 24 18:22:40 UTC 2010

- Previous message: [dns-operations] k2.nap.k.ripe.net instance of K root server dropping IPv6 TCP connections?
- Next message: [dns-operations] Odd behaviour on one node in I root-server (facebook, youtube & twitter)
- **Messages sorted by:** [date] [thread] [subject] [author]

```
Hi there!

A local ISP has told us that there's some strange behavior with at least one
node in i.root-servers.net (traceroute shows mostly China)
It seems that when you ask A records for facebook, youtube or twitter, you get
an IP and not the referral for .com

It doesn't happen every time, but we have confirmed this on 4 different
connectivity places (3 in Chile, one in California)

This problem has been reported to Autonomica/Netnod but I don't know if anyone
else is seeing this issue.

This is an example of what are wee seeing:

$ dig @i.root-servers.net www.facebook.com A

; <<>> DiG 9.6.1-P3 <<>> @i.root-servers.net www.facebook.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7448
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.facebook.com.              IN      A

;; ANSWER SECTION:
www.facebook.com.       86400   IN      A       8.7.198.45

;; Query time: 444 msec
;; SERVER: 192.36.148.17#53(192.36.148.17)
;; WHEN: Wed Mar 24 14:21:54 2010
;; MSG SIZE  rcvd: 66



--
Mauricio Vergara Ereche                 User #188365 counter.li.org
DNS Admin NIC Chile                             mave [@] nic [.] cl
Miraflores 222 piso 14, Santiago CHILE               +56 2 9407710
Codigo Postal: 832-0198                        http://www.nic.cl
```

Collateral Damage

- Collateral damage occurs when a DNS query from a recursive resolver enters a censored network, causing the censorship mechanism to react.

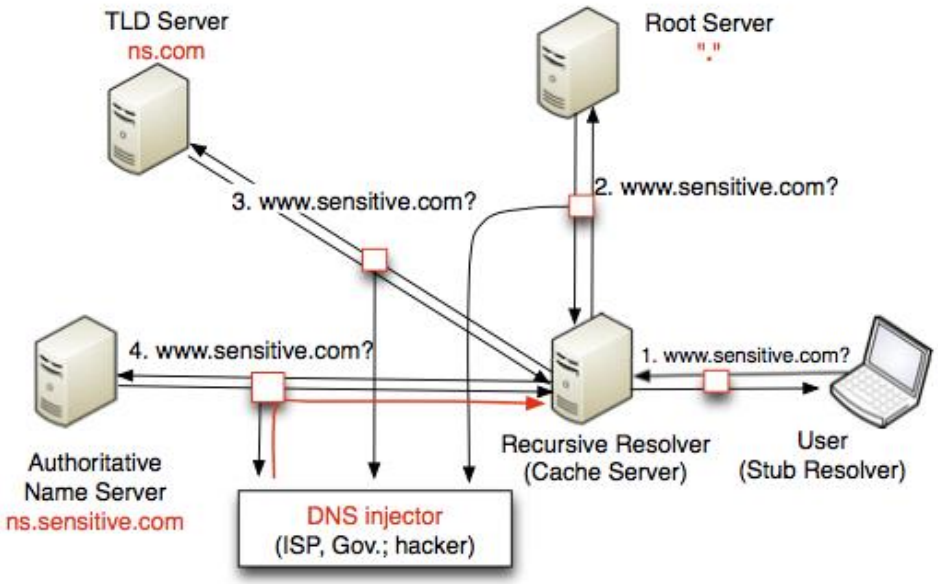
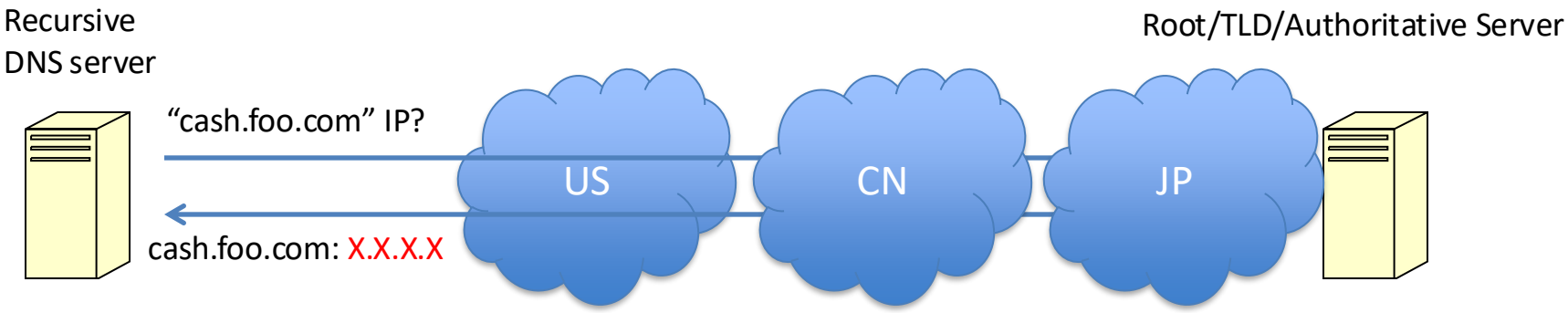


Figure 1: DNS query process and DNS injection

Collateral Damage

- All networks along the path of the query are suspicious



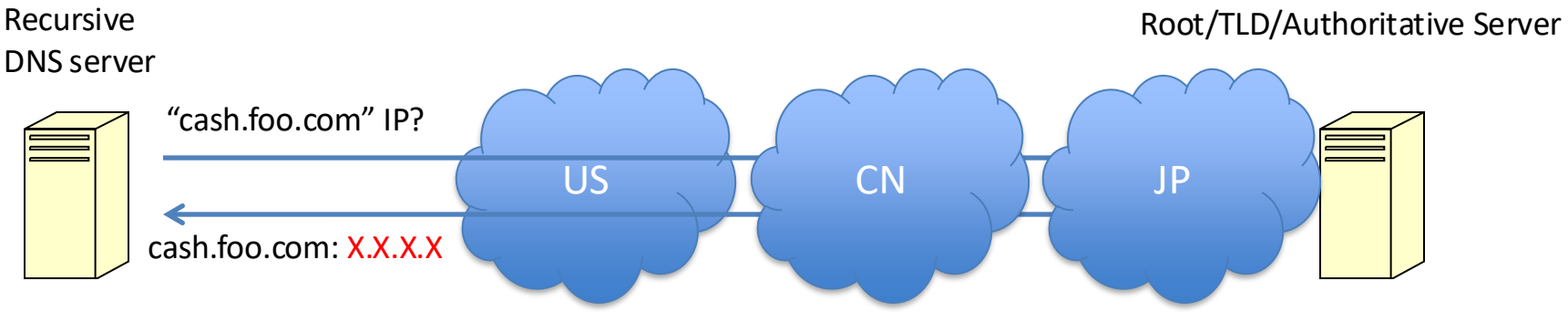
A Network?

- An organization can have a collection of IP addresses
  - E.g., corresponding to a subnet
- An IP address can be attributed to an organization
  - 130.108.224.196
  - whois 130.108.224.196
  - whois -h whois.cymru.com " -v 130.108.224.196"

Example

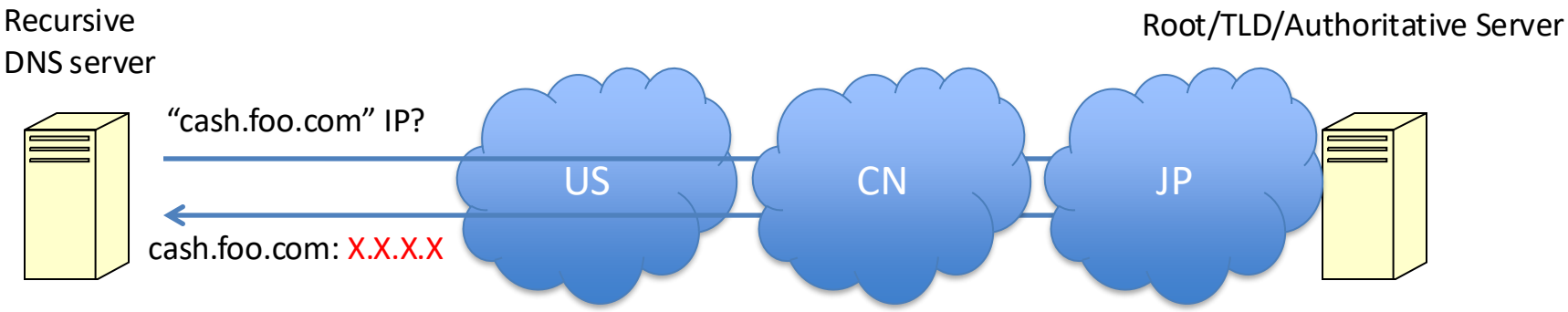
- Traceroute
- Mapping the IP of an router into its ASN/organization

Search for Injected Paths: Honey-Query



Fields	Values
Destination IP	?
Domain name	?

Search for Injected Paths: Honey-Query



Fields	Values
Destination IP	• Pick up an address from /24 network. (how many /24 different networks?) • This address does not run DNS service. (WHY?)
Domain name	• Domains that are commonly considered as “sensitive”

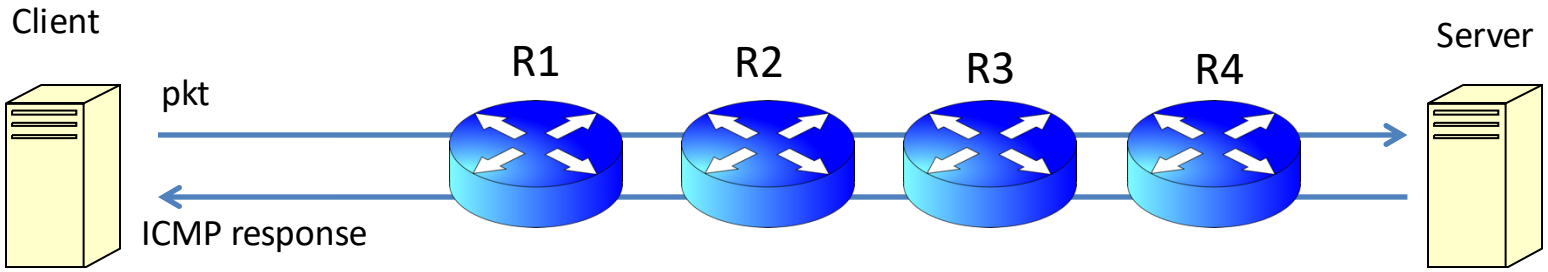
Honey-Query

- What do you expect after you send out the honey-query?
  - Not censored?
  - Censored?

Honey-Query

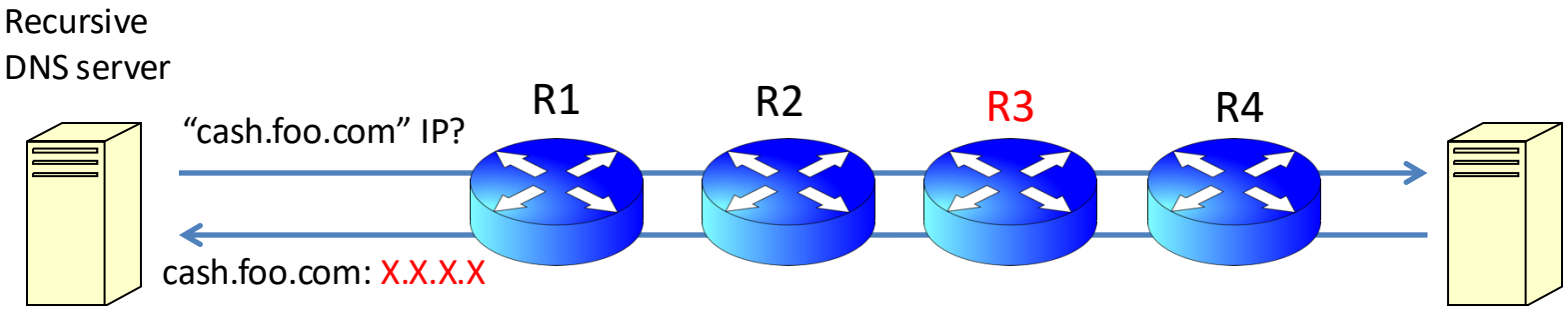
- What do you expect after you send out the honey-query?
  - Not censored?
    - No DNS response at all.
  - Censored?
    - A DNS response
    - Is the IP address in the response trustable?

Identify the Injector



TTL Value	Source IP address of the ICMP packet
1	R1
2	R2
3	R3
4	R4

Identify the Injector



TTL Value	Source IP address of the ICMP packet
1	R1
2	R2
3	R3
4	R4 + (A DNS response)

Some Statistics

AS Number	AS Name	Router IPs
4134	Chinanet	1952
4837	CNCGROUP China169 Backbone	489
4812	China Telecom (Group)	289
9394	CHINA RAILWAY Internet(CRNET)	78
9929	China Netcom Corp.	67
4808	CNCGROUP IP network China169 Beijing Province Network	55
9808	Guangdong Mobile Communication Co.Ltd.	38
17633	ASN for Shandong Provincial Net of CT	25
4538	China Education and Research Network Center	22
17816	China Unicom IP network China169 Guangdong province	19
Total 39 ASes		

Table 3: Information of top 10 injecting ASes.

Do not forget

- All honey queries are sent from real IP addresses controlled by authors
- These IP addresses are unlikely to reside in the censored networks
- Censors should actually not censor these IP addresses
- But they inject fake DNS responses anyway
  - “the DNS injector does not consider packet origin when injecting packets”.
  - Why?