Network Security Part I

Kevin Scrivnor

COMP 429

Fall 2022

What is network security?

- Specifically, security that involves communication
- Hacking has been around for a long time
- John Draper aka Captain Crunch
  - Phone Phreaker
  - Used whistle from the cereal box to hack phones

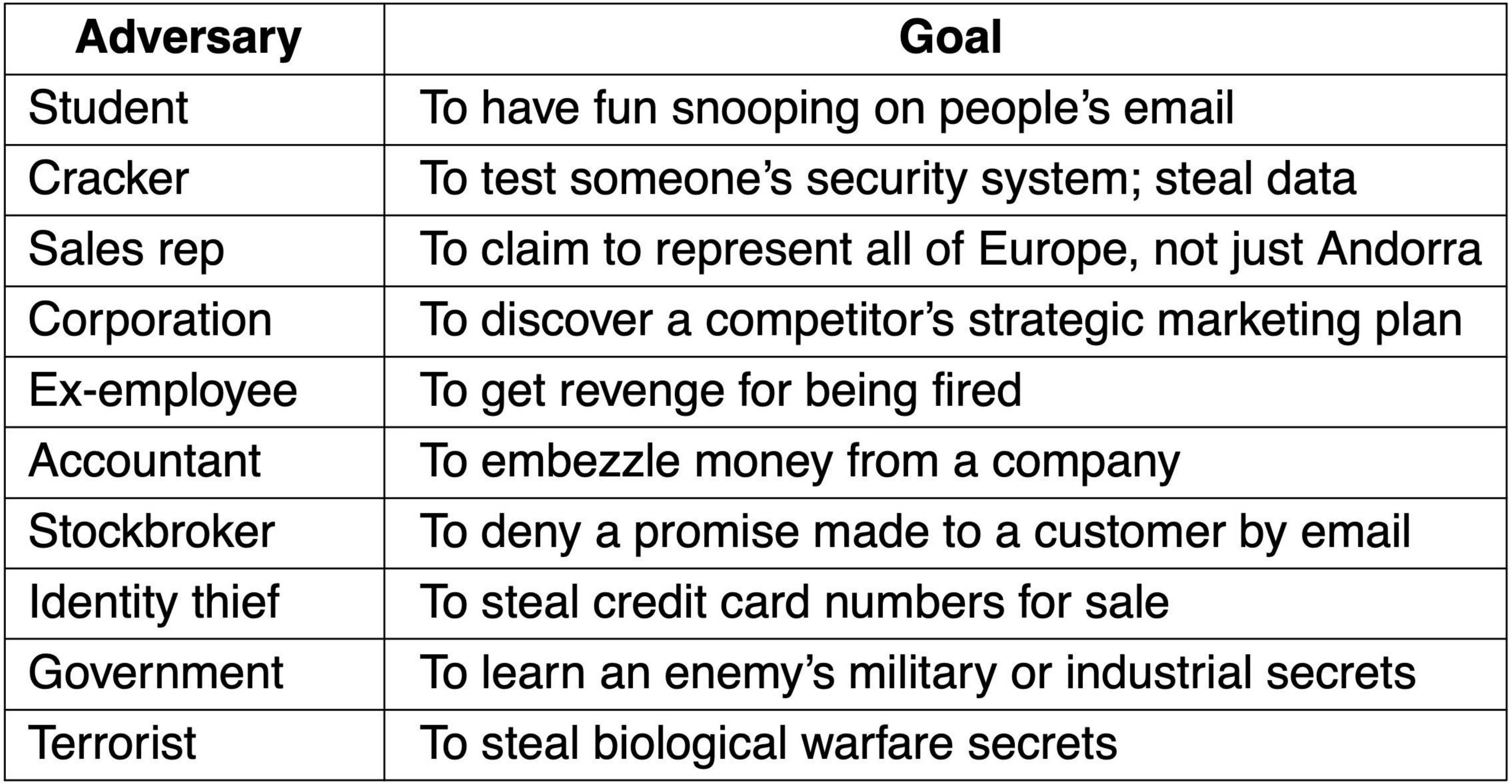
- Phone Network Communication
  - Done through signaling at specific frequencies
  - Turns out the captain crunch whistle frequency is the same as the code to make a free long distance call

Hackers Inspire

- Captain Crunch was eventually arrested and sent to jail
  - 4 months in Lompoc
- He inspired two other hackers:

- They eventually started a company called Apple

Hackers Cause Problems



Adversary	Goal
Student	To have fun snooping on people’s email
Cracker	To test someone’s security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Corporation	To discover a competitor’s strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Identity thief	To steal credit card numbers for sale
Government	To learn an enemy’s military or industrial secrets
Terrorist	To steal biological warfare secrets

We Shouldn’t Worry Too Much

- Well, depending on where you work
- If you’re a small tech company in Ventura
    - Your adversary is ex-employees, current employees, and maybe some automated foreign hacks
- If you’re a hosting government secrets
    - Your adversary is foreign intelligence agencies with infinite resources

- Don’t need to live life in fear, but you still need to take security as seriously as it needs to be taken
- https://www.usenix.org/system/files/1401_08-12_mickens.pdf
- Intelligence agencies will always get what they want:
- https://www.theguardian.com/world/2020/apr/02/global-battle-coronavirus-equipment-masks-tests

Fundamental Security Principles

- Created in 1975 by Jerome Saltzer and Michael Schoeder
- http://web.mit.edu/Saltzer/www/publications/protection/Basic.html
- These come from an academic paper in 1975, I will translate them for you one by one

Principle of economy of mechanism

- Academic speak for “simple is better than complex”
- Simple systems are easier to protect
- Goal is to minimize the attack surface

- Does the server run HTTP and the database? One server has to protect two complex entities
  - Separate the entities
  - Attack surface for each is smaller

Principle of Fail-Safe Defaults

- Default lack of permission is always safer

- Allow list
  - List of allowed IP addresses or programs a computer can run
  - Deny everything else by default

- Deny list
  - List of banned IP addresses or programs a computer can run
  - New malware that hasn’t made the list yet can still execute!

- We once had a meeting arguing with someone that the lists are mutually exclusive

Principle of Complete Mediation

- This will eventually be the future of security
- The idea of zero-trust
  - You literally trust nothing and must authenticate at every level

- Every access to every resource should be checked for authority
- Determine the source of the requester

- Coming soon™

Principle of Least Authority

- This is why we can’t have nice things
  - sudo privileges in the lab
  - local admin for maintenance

- Always run at user level
- When elevating privileges, log it

Principle of Least Common Mechanism

- If you run a DNS server, HTTP server, and Database all on a single machine, then only one of those services needs to be exploited for a hacker to gain access to everything

- If they are on separate servers, it becomes more difficult
  - DNS/HTTP are public facing
  - While a database is typically hidden in the private network

Principle of Open Design

- The algorithms for RSA and SHA hashes are open and well known
- The output of the algorithms is also available
- However, without the key, an attack cannot figure out what the plaintext is

- Versus, Physical Locks
  - It is publicly known how the lock works
  - Locksmiths can pick the locks without the key
  - This is bad security

Principle of Psychological Acceptability

- If it sucks to use, no one will use it

- More importantly
- It needs to be clear why the rules are there to begin with
  - Why do we have passwords? Prevent unauthorized access
  - Why do we have DUO? Incase someone steals your password

  - Why do we not have admin on the university computers? So students don’t look at other students work
  - And so they don’t install LoL

A Bit About Ethical Hacking

- Understanding how to hack is different than hacking organizations for fun
  - If you hack a hospital, you might kill someone
  - If you hack a university, you might waste resources and time

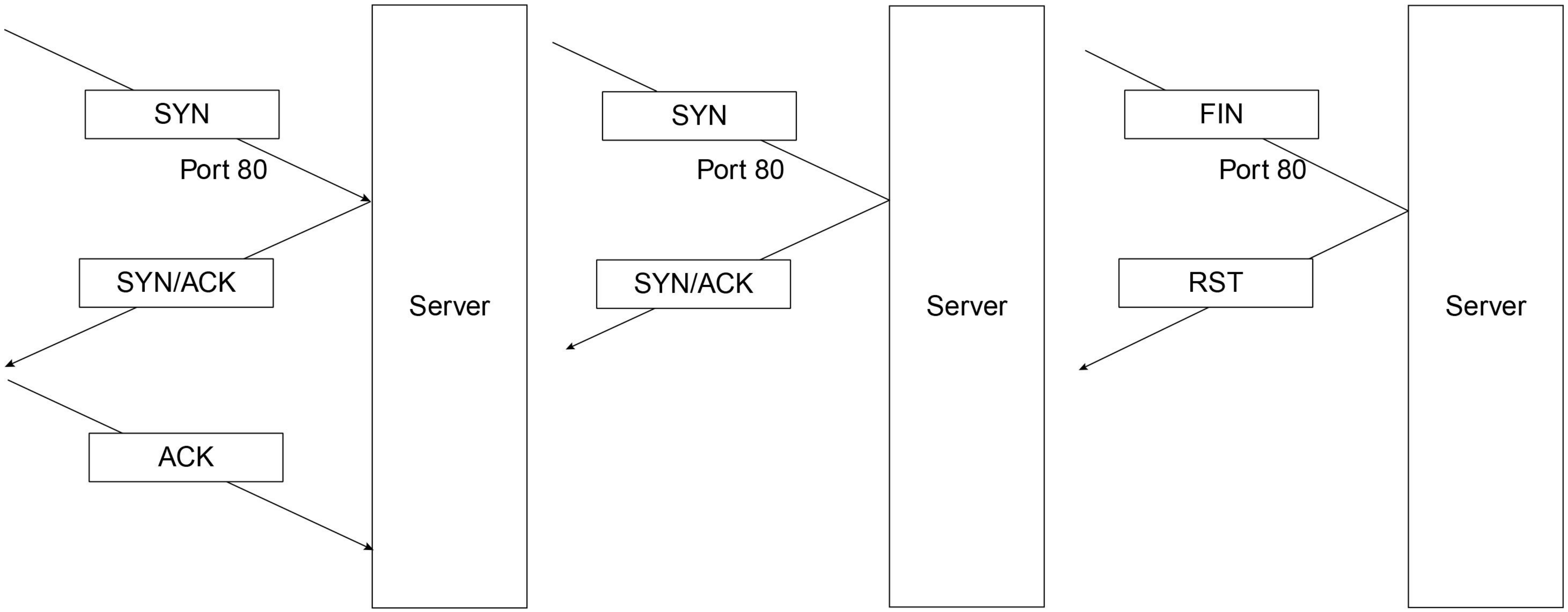
- Consider this, you want to be a fire fighter. Do you…
  - will the fire department want to hire an arsonist or…
  - someone who has studied how fire spreads in a safe/ethical way

Fundamental Attack Principles

- Reconnaissance
  - Enumeration
  - Discovery of services
  - Reachable machines, protocols used, services, etc
- Sniffing and Snooping
  - How to sniff traffic not on your own network?
- Spoofing
  - Pretending to be someone else (or something else)
  - IP spoofing
- Disruption
  - Denial of Service
  - Ransomware

Reconnaissance: port scanning

- Port Scanning



(a) Connect scan: connection established implies port is open

(b) Half open scan: SYN/ACK reply implies port open

(c) FIN scan: RST reply implies port is closed

Reconnaissance: fingerprinting

- Once a portscan is complete, the next step is to figure out more details about the system

- Say port 8080 is open on TCP
  - Likely a web server
  - Is it nginx, apache, tomcat, etc.?
  - Running Windows, Linux, MacOS X Server, etc.

- Every system implements things slightly differently, can you tell by the subtle differences which system it is?
  - nmap can

Sniffing and Snooping

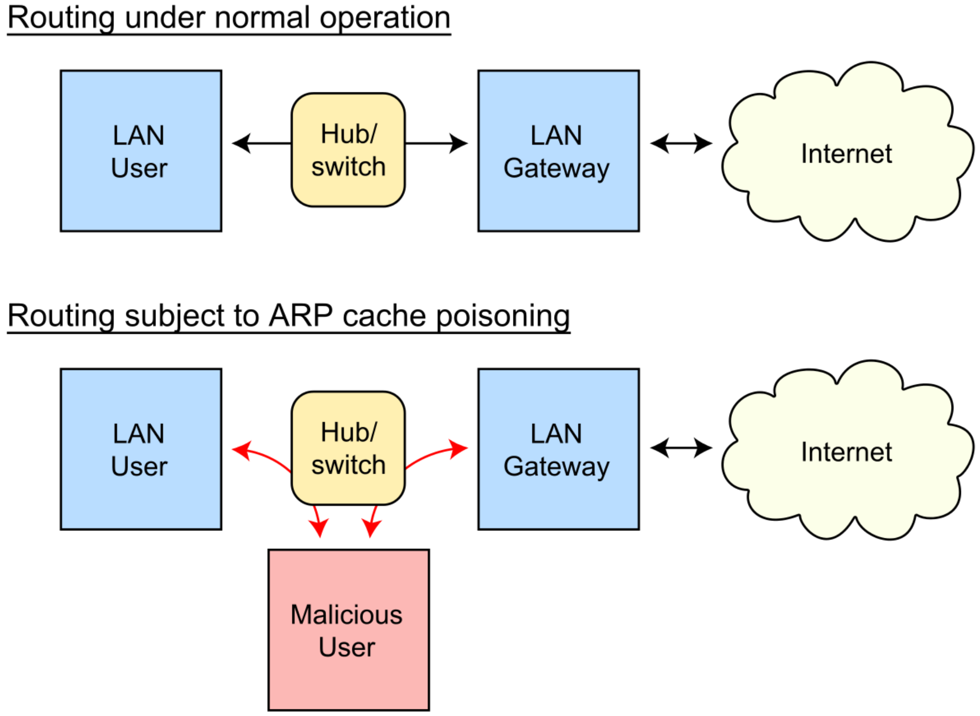
- Assumption: attacker has presence on the network now

- Broadcast Network vs. Switched Network
  - Broadcast networks like wifi broadcast every packet to every computer
  - A wifi card set to promiscuous mode can show all the data in the air
  - Switched networks only forward packets to the host, so even if a NIC is set to promiscuous mode, it will not see every packet

- How to snoop on a switched network?
  - Trick the switch

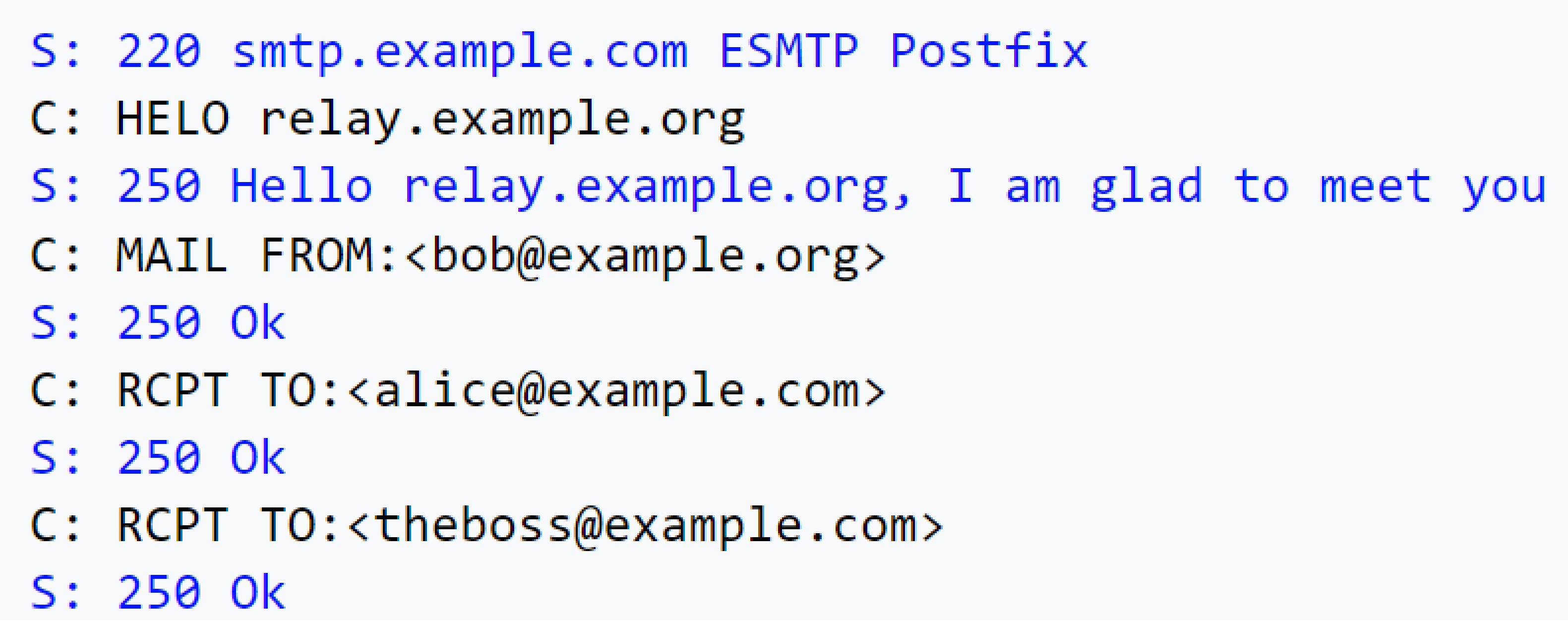
ARP Poisoning

- Recall in the ARP lab we saw a broadcast protocol ARP that asks who has a particular IP address?
  - An attacker can take advantage of this protocol by pretending to be a different host
  - Flood the network with ARP responses to trick the switch into routing through the attacker first
  - MITM Attack



Spoofing (Email)

- SMTP (Simple Mail Transfer Protocol)
- An SMTP server let's you decide where the mail comes from



```
S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok
C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
```

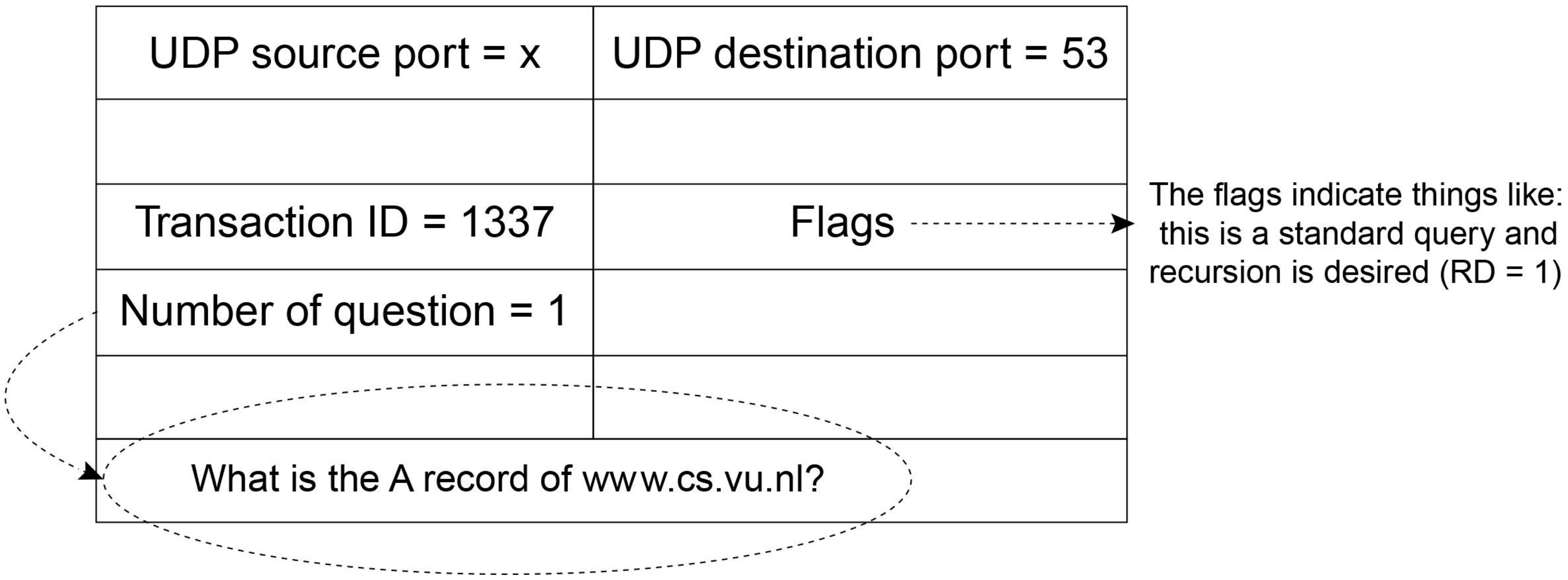
- X-Original-Authentication-Results: mx.google.com; spf=**softfail** (google.com: domain of transitioning kevin.scrivnor988@myci.csuci.edu **does not designate 114.130.184.93 as permitted sender**) smtp.mailfrom=kevin.scrivnor988@myci.csuci.edu;

Most Mail Servers Would Ignore This Email

- But it showed up in my inbox anyway
- Looking up the IP address, it was sent through an SMTP server through Bangladesh
- What examples of spoofing have you seen recently?
    - Texts
    - Emails
    - Calls
    - Mail
    - Etc.

DNS Spoofing

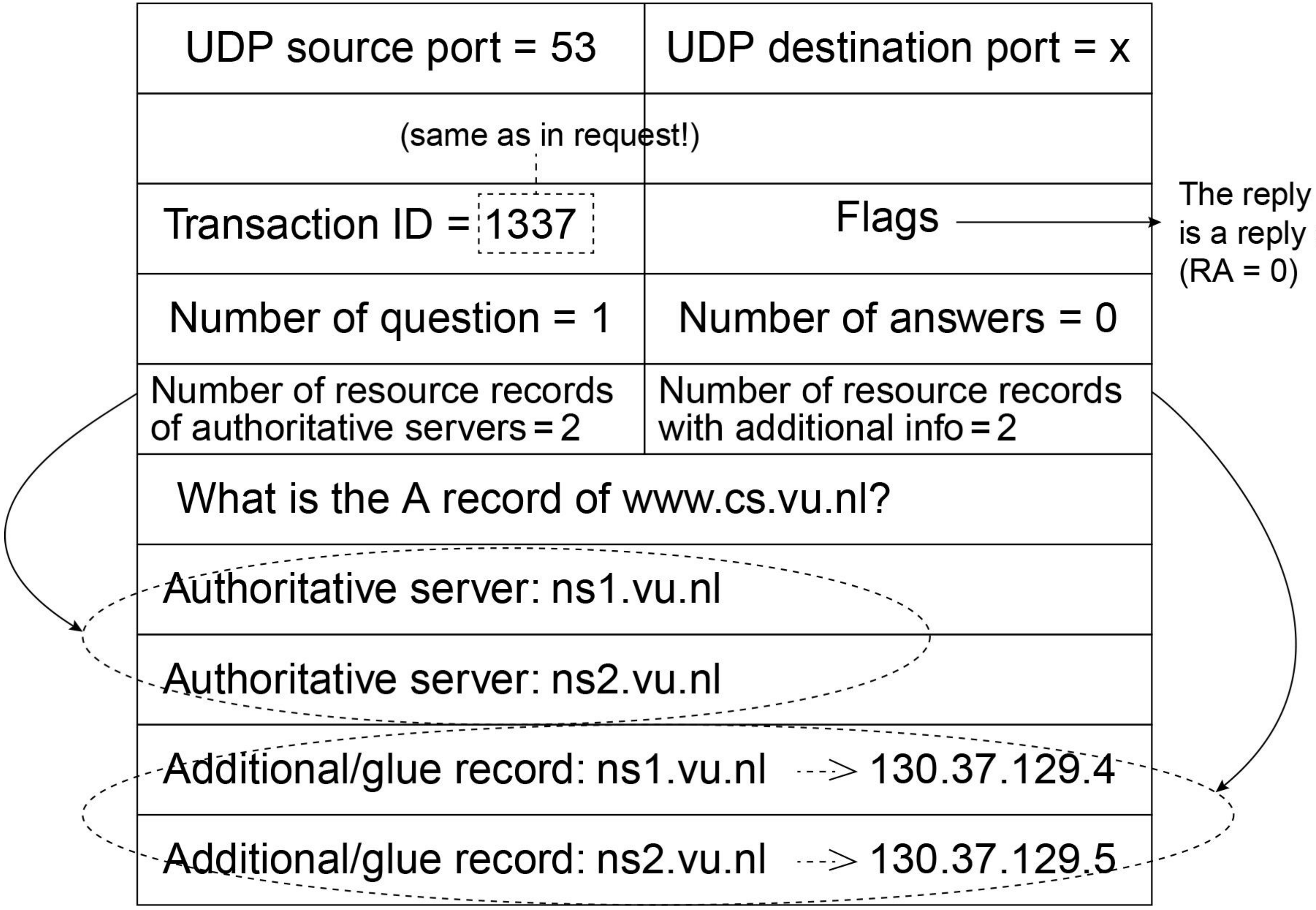
- How can you sniff traffic if you’re not on the network?
- You can trick DNS to report back a different IP address and just have the victim send you their traffic



UDP source port = x	UDP destination port = 53
Transaction ID = 1337	Flags
Number of question = 1	
What is the A record of www.cs.vu.nl?	

The flags indicate things like: this is a standard query and recursion is desired (RD = 1)

DNS Spoofing, the problem/solution



UDP source port = 53	UDP destination port = x
Transaction ID = 1337	Flags
Number of question = 1	Number of answers = 0
Number of resource records of authoritative servers = 2	Number of resource records with additional info = 2
What is the A record of www.cs.vu.nl?	
Authoritative server: ns1.vu.nl	
Authoritative server: ns2.vu.nl	
Additional/glue record: ns1.vu.nl --> 130.37.129.4	
Additional/glue record: ns2.vu.nl --> 130.37.129.5	

(same as in request!)

The reply flags may indicate that this is a reply and recursion is not possible (RA = 0)

Disruption is Easy

- Disruption of services is generally caused by three types of attacks:
  - Crashes
  - Algorithmic Complexity
  - Flooding

- Crashing
  - Attacker sends content that causes the victim to crash/hang
  - https://thehackernews.com/2018/02/crash-iphone-text.html
- Algorithmic Complexity
  - Attacker sends content that is crafted to cause a lot of overhead
  - Send an inefficient regex to a server to cause it to infinitely backtrack
- Flooding
  - Attack sends massive flood of requests, typically a server will become unresponsive

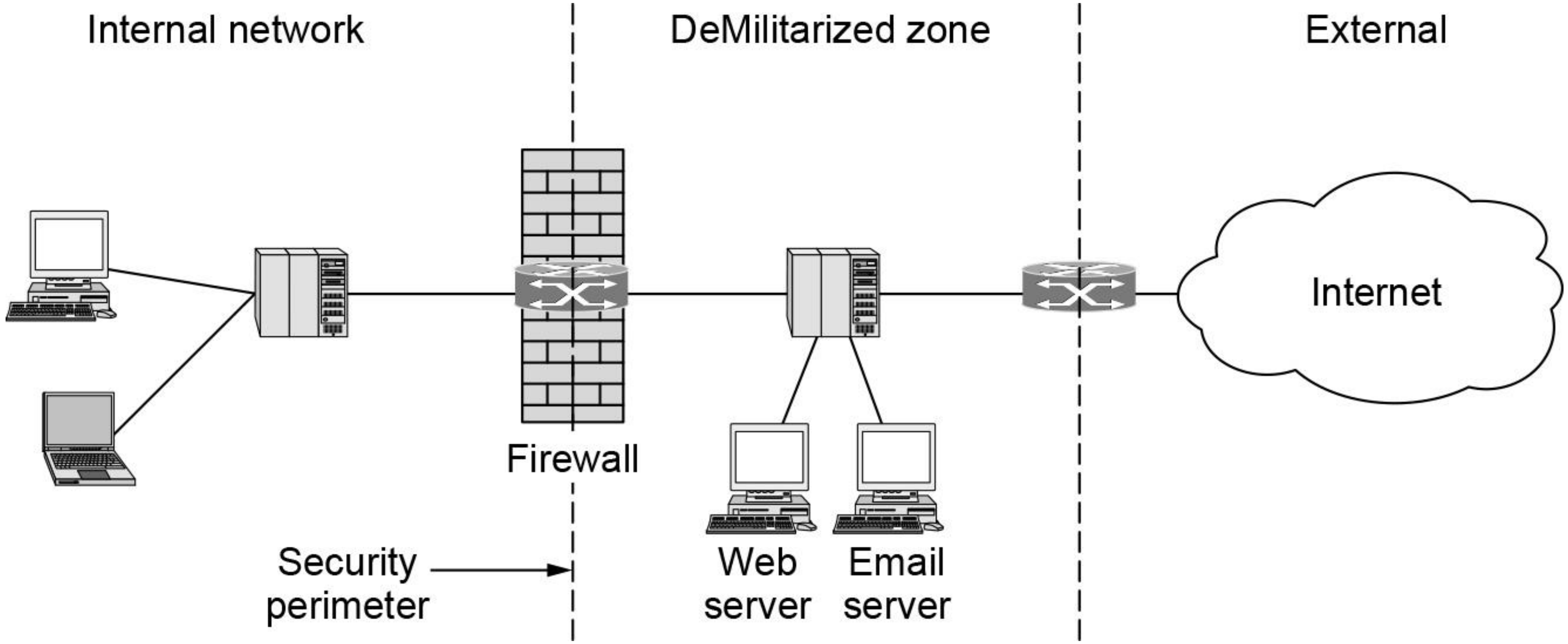
DDoS (Distributed Denial of Service)

- Botnets
    - A program that is running on a victims machine
    - Connects to an IRC server and awaits commands from hacker
    - The largest botnets may have infected millions of users

- How does a botnet flood?
    - SYN Floods
    - Send TCP SYN but then never send the ACK
    - Thus leaving the connection open and hanging (using up resources)

- How to fight a botnet?
    - Send all traffic to a cloud WAF (Web Application Firewall)
    - Scrubs the data and *tries* to not allow any malicious packets to hit your server

Firewall and DMZs



Selected Recent Breaches (Fall 2022)

- October 2022: MediBank
  - Health insurer lost 4 million customer’s data
  - Name, address, DoB, and insurance card numbers
  - Cost: 25-35 Million
- September 2022: Uber
- August 2022: Plex
  - Personal encrypted data
  - Usernames, passwords, emails
- January 2022: Crypto.com
  - 18 million in bitcoin
  - 15 million in Ethereum

Selected Recent Breaches (Spring 2023)

- American Bar Association
  - Credentials leaked for 1.4 million members
  - April 21
- MSI
  - Unknown what exactly was stolen
  - Gang requests $4,000,000 or will release data
  - MSI confirmed a breach has happened
  - April 7
- KFC/Pizza Hut/Taco Bell/Habit (Yum! Brands)
  - Ransomware
  - 300 restaurants closed for one day in the UK
  - Jan 18

Enumeration Demo

- Finding API keys

- Finding machines
- Finding services
- Service information
- Lucky guess?

- Then what?