# Security Engineering

Network security: integrating threat hunting, firewalls, intrusion detection, network logging and supporting services.

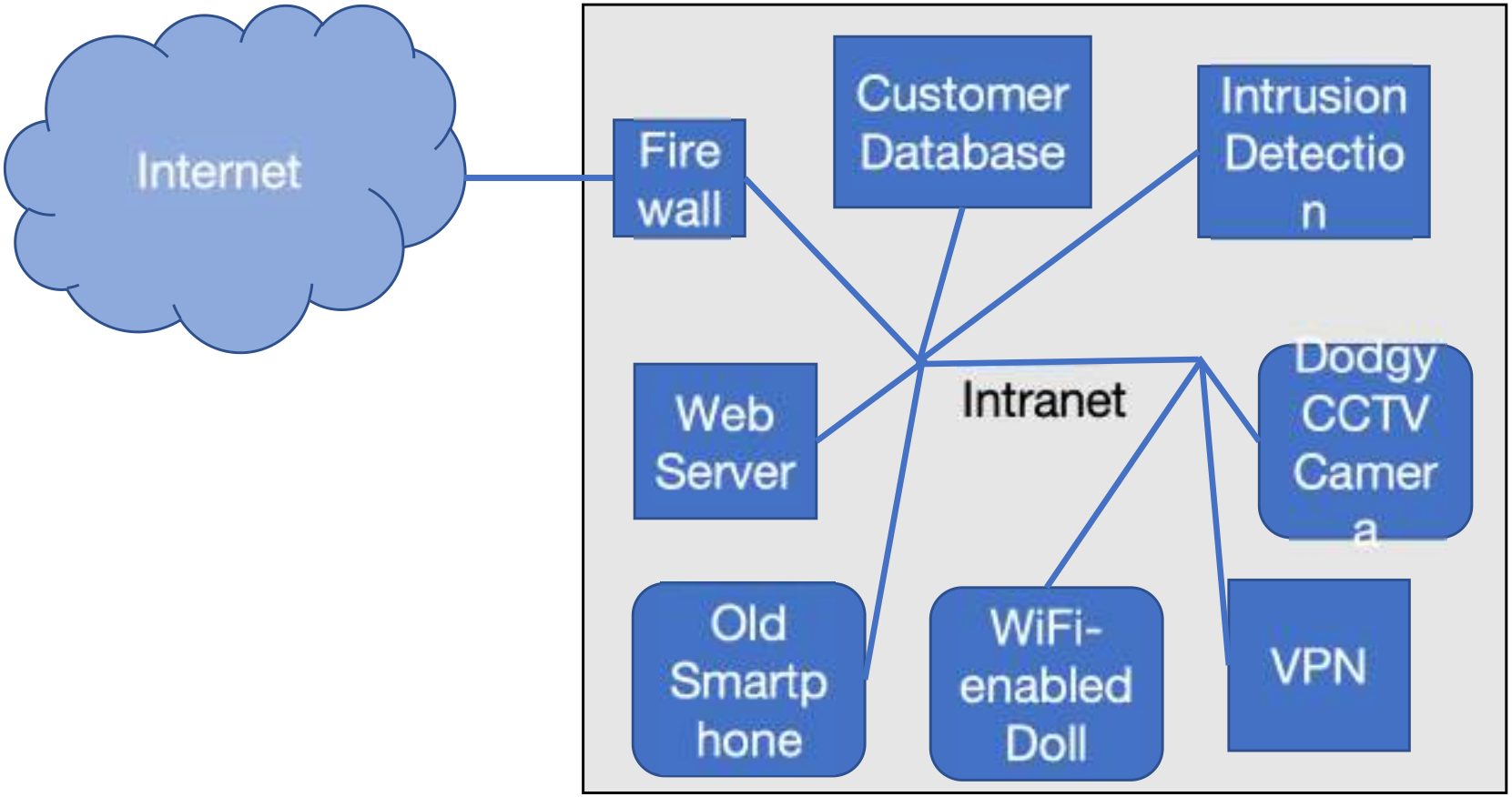
Lecturer: **Jingjie Li** & Daniel Woods

Acknowledgement: Ross Anderson & Sam Ainsworth

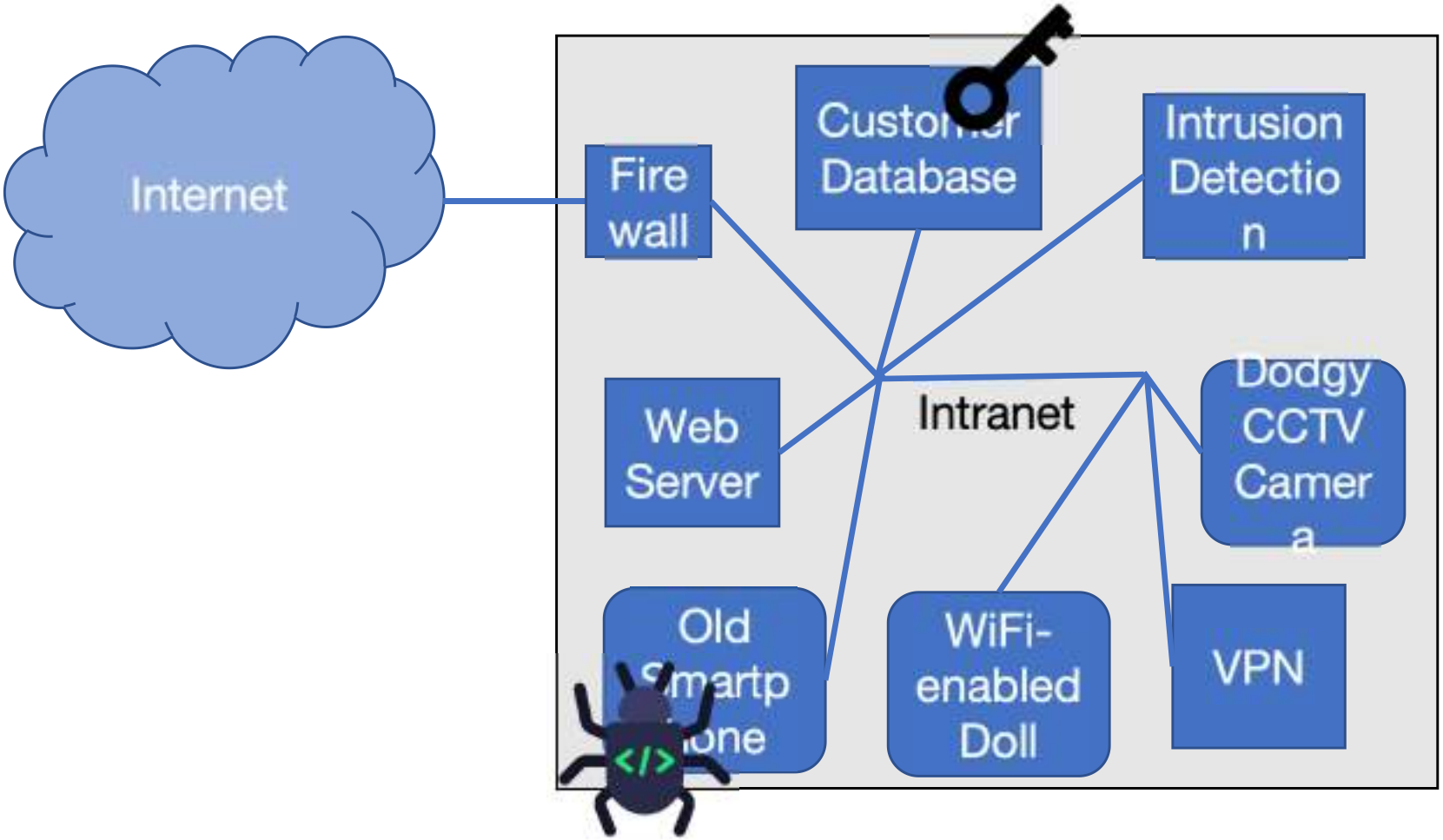
# Think and Discuss

- What is Internet?
- What are connected on Internet?
  - Your phone?
  - Your laptop?
  - Our school's GPU cluster?
  - A website?
- Who can we trust?

# Perimeterisation

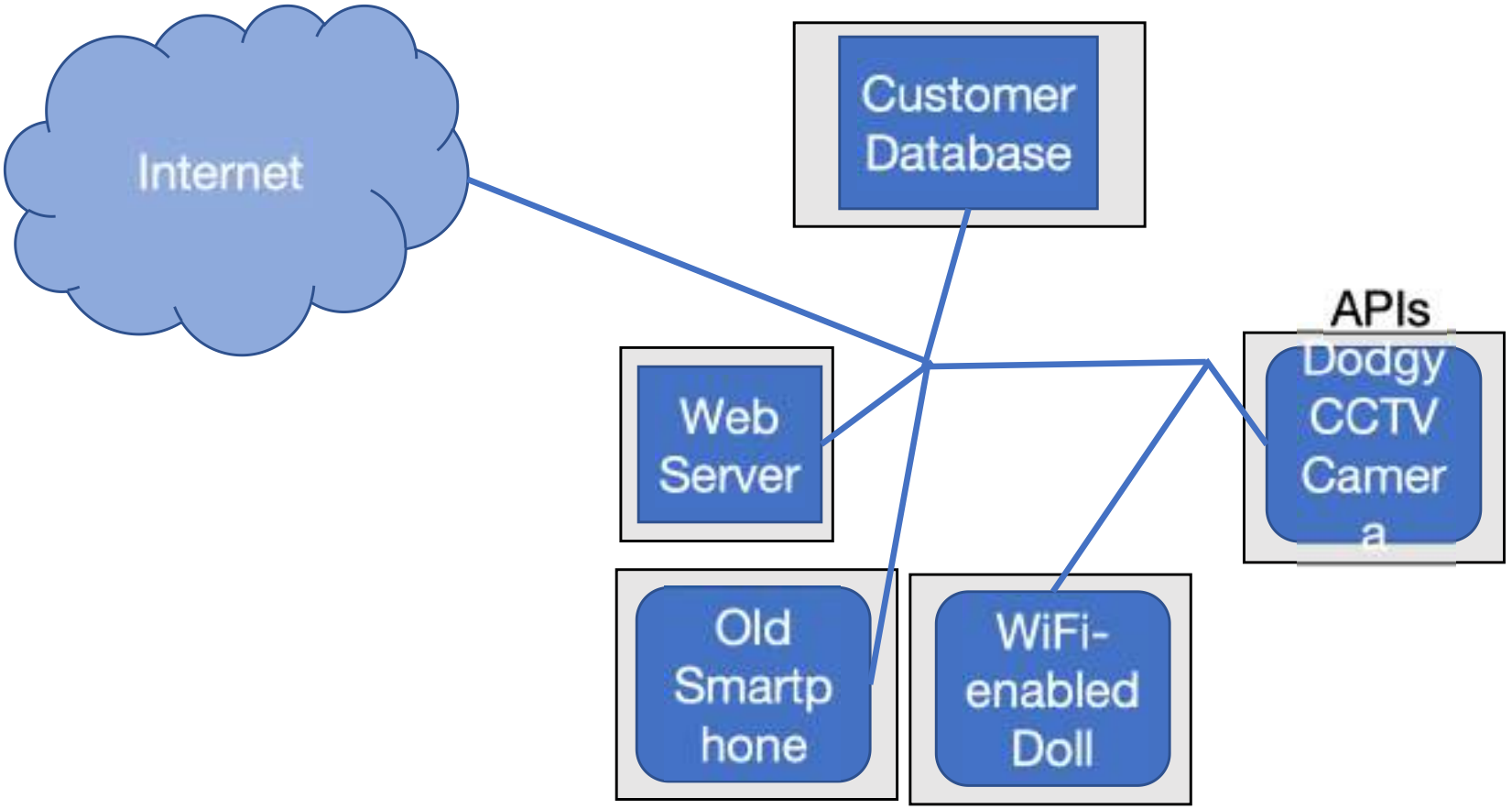


# Perimeterisation



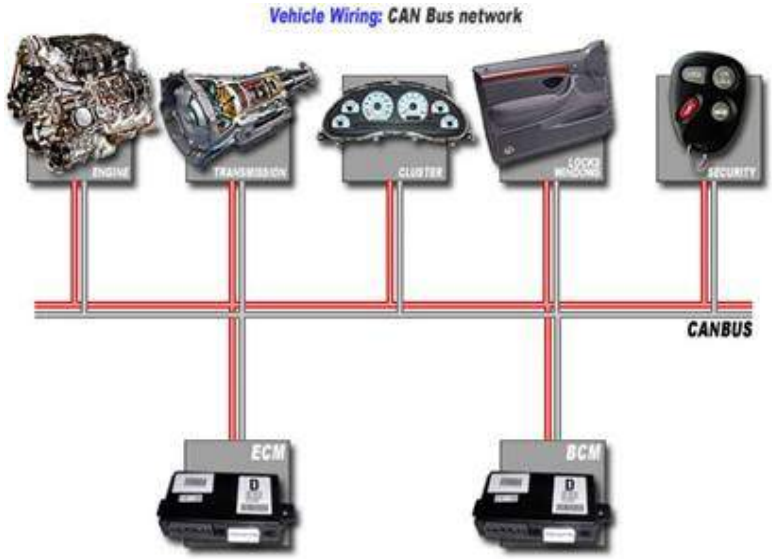
# (De)perimeterisation (Zero-trust networking)

e.g. Google's BeyondCorp




Shifting access control from network perimeter to individual user and devices

# What should be isolated in a smart car, and how?

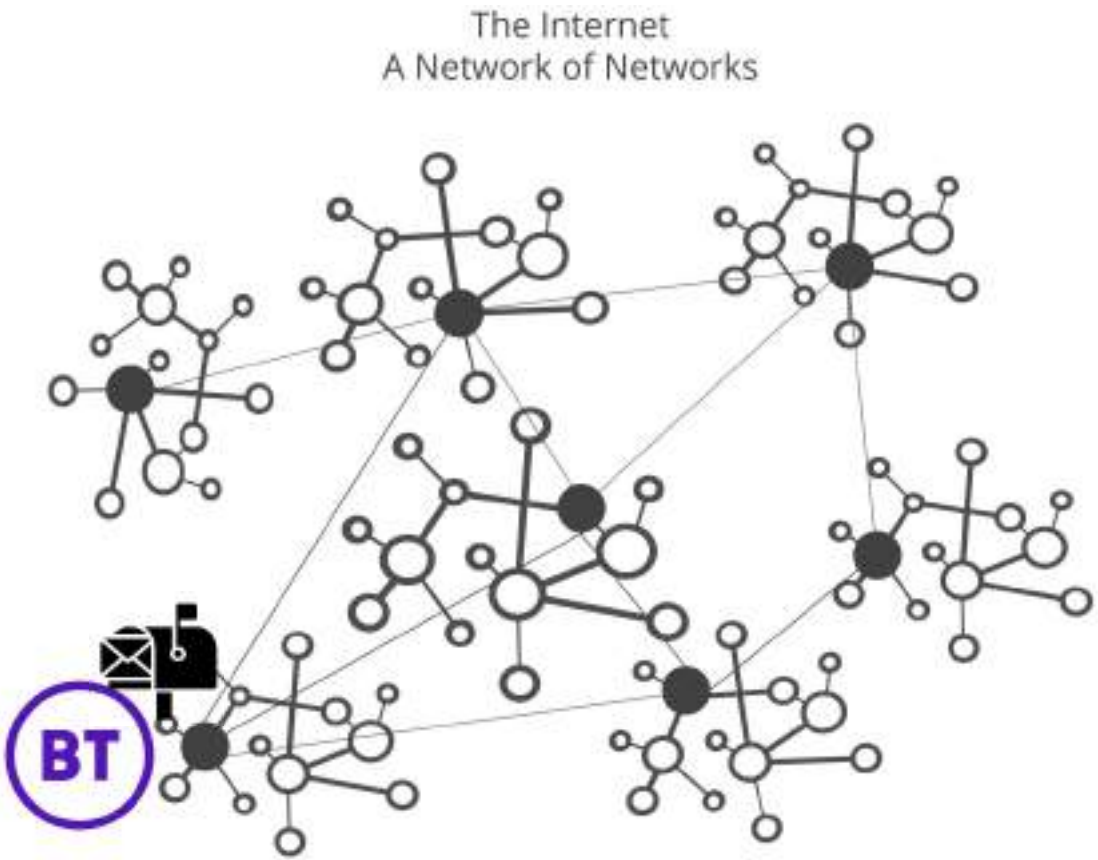



https://nvidianews.nvidia.com/news/nvidia-powers-digital-dashboard-in-new-tesla-motors-electric-sedan
https://autoditex.com/page/can-bus--controller-area-network-34-1.html

# Think and Discuss

- So...are we secure enough?
- Why?

# BGP




- Used for networking between Autonomous Systems in the internet (e.g. ISPs, telcos, large organisations)

https://www.cloudflare.com/zh-cn/learning/security/glossary/what-is-bgp/

# BGP

- Used for networking between Autonomous Systems in the internet (e.g. ISPs, telcos, large organisations)
- No intrinsic security – so lots of examples of **false routes**
- National state actors censor or DDoS through false routes
- Various instances of intelligence collection via MITM
- ->Some "adversaries" are more powerful than the others!

# BGP Attacks: countermeasures

- Accept a limited number of routes from each peer
- Internet Routing Registries: at least there's a log, but it's filled with known incorrect data.
- Cloudflare: monitoring routing via BGP collectors
- **Resource Public Key Infrastructure**: "*Autonomous system X announces IP address range Y*"
  - But do public keys really make things more robust? Who will hold the private keys?
  - And how do you get widespread deployment?

# Think and Discuss

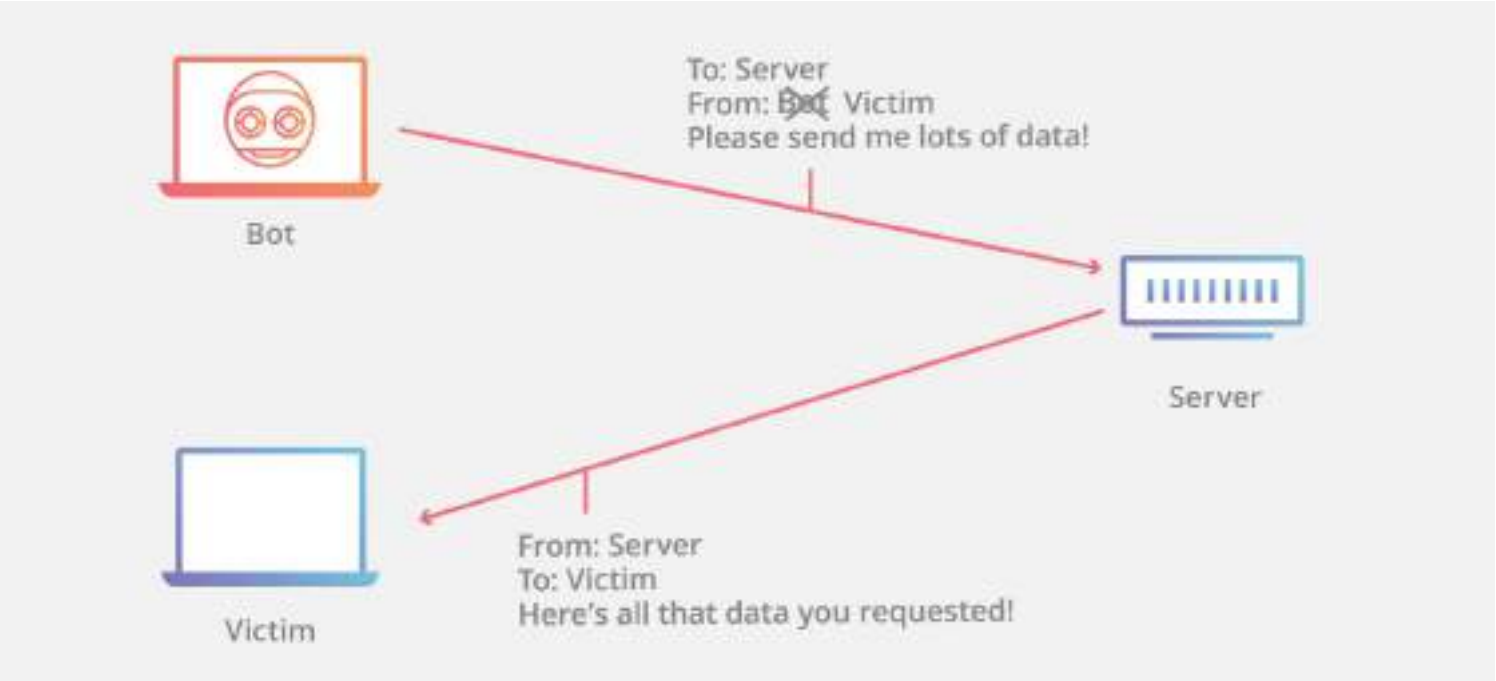
- What could a less resourced attacker do?

# Denial of Service

- Take out your rivals' service
- Country? Company? Video-game player?

# IP Spoofing

- Hiding/impersonating sender's identity/IP




DoS by IP spoofing

https://www.cloudflare.com/learning/ddos/glossary/ip-spoofing/

# Denial of Service

- How to save bandwidths of the attacker?
- Amplifier attacks

A -> B: SYN; my number is X
B -> A: ACK; now X+1
SYN; my number is Y
A -> B: ACK; now Y+1
(start talking)

TCP/IP handshake

# Denial of Service

- TCP is stateful -> Amplifier attacks

Spoofed IP**"C"** -> B: SYN; my number is X
B -> C: **ACK**; now X+1
SYN; my number is Y
B -> C: **ACK**; now X+1
SYN; my number is Y
B -> C: **ACK**; now X+1
SYN; my number is Y
…

TCP Syn Reflection

# Denial of Service

- TCP is stateful -> Amplifier attacks

**"C"** -> B: SYN; my number is X

B -> C: **ACK**; now X+1

SYN; my number is Y_cookie  Not stored

(until a correct copy is received)

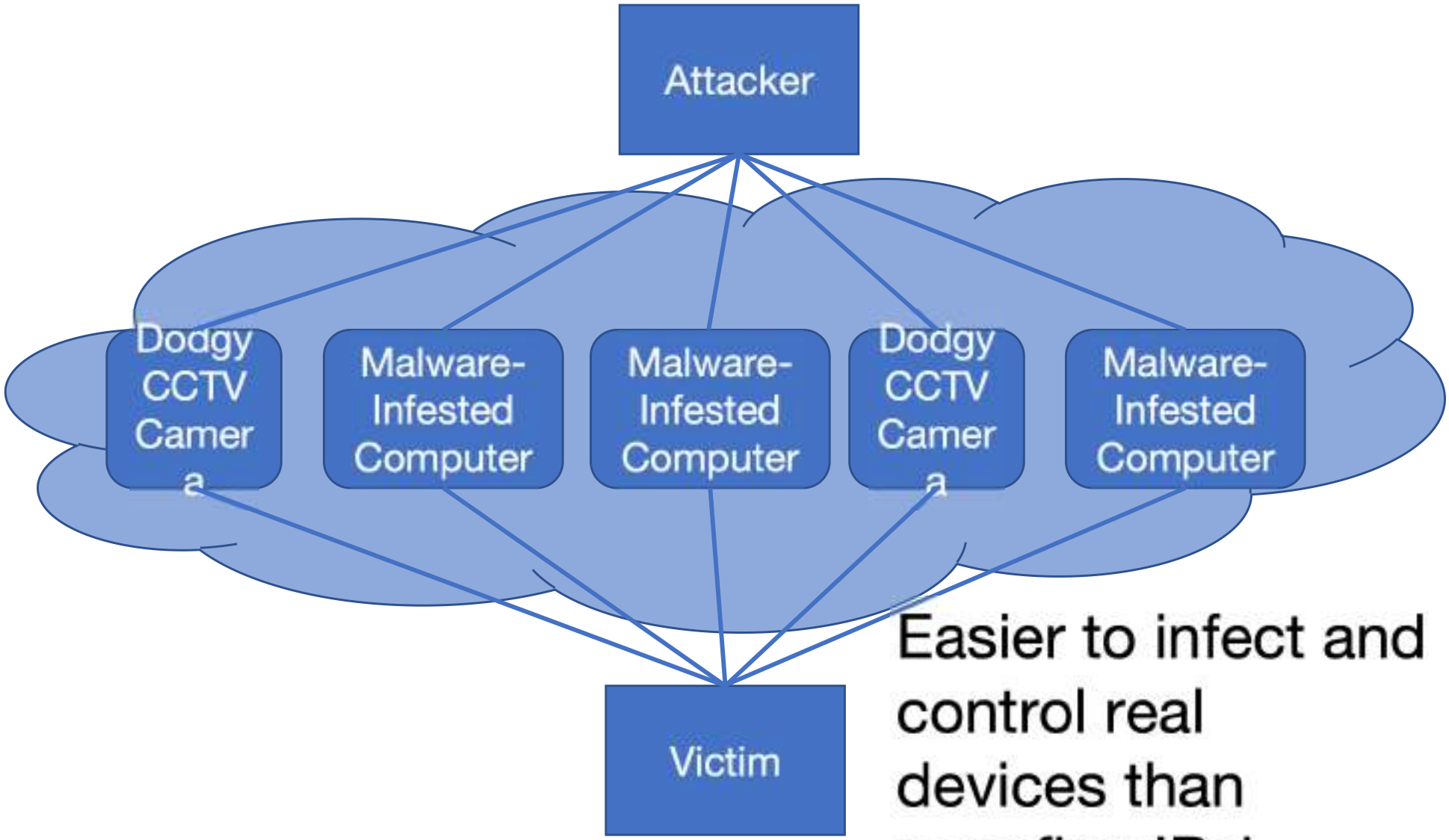
TCP SYNcookie

- What is the cost of a SYNcookie?

# Think and Discuss

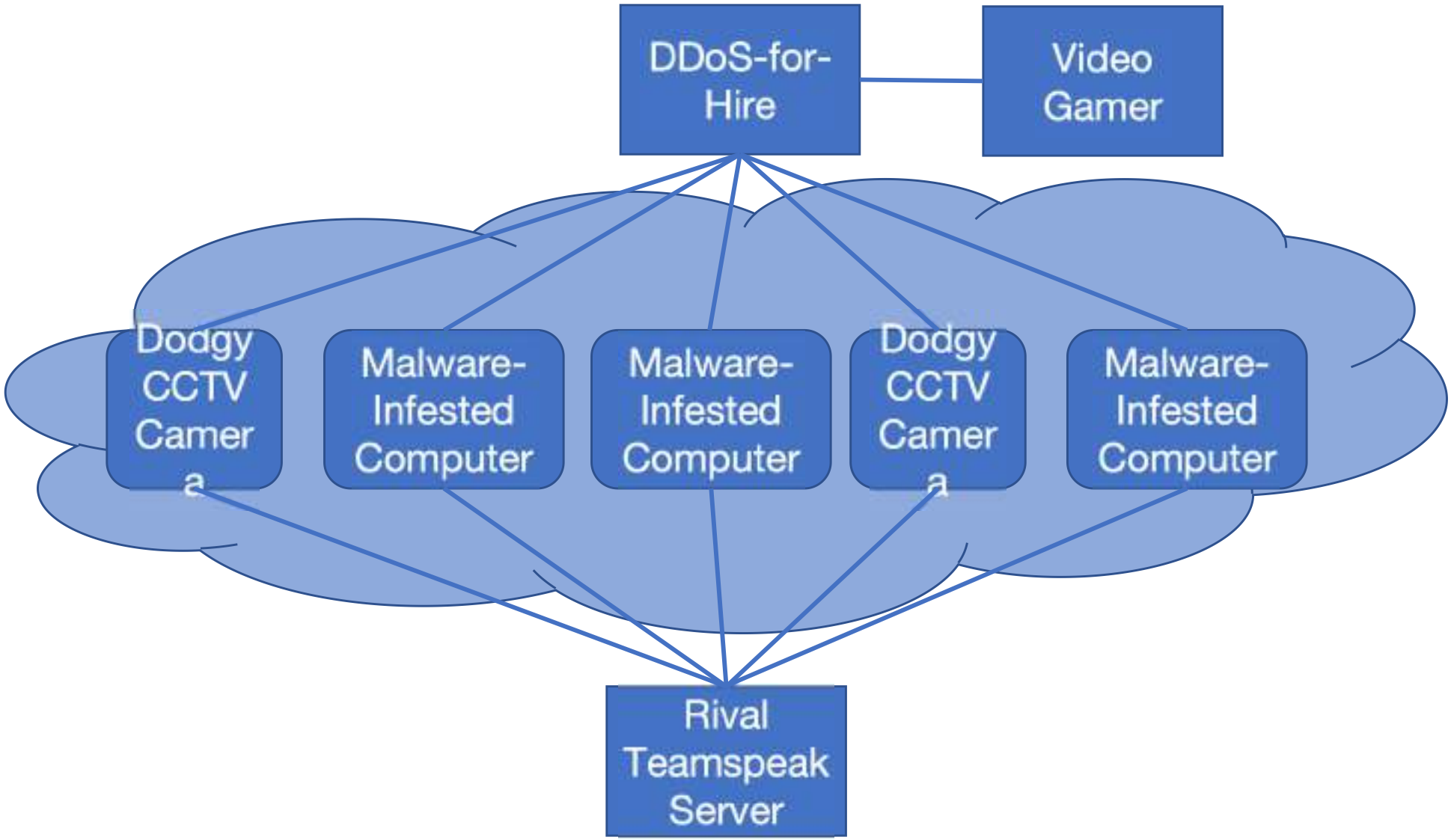
- What other ways we can defend against DoS by SYNC flood?

# Distributed Denial of Service

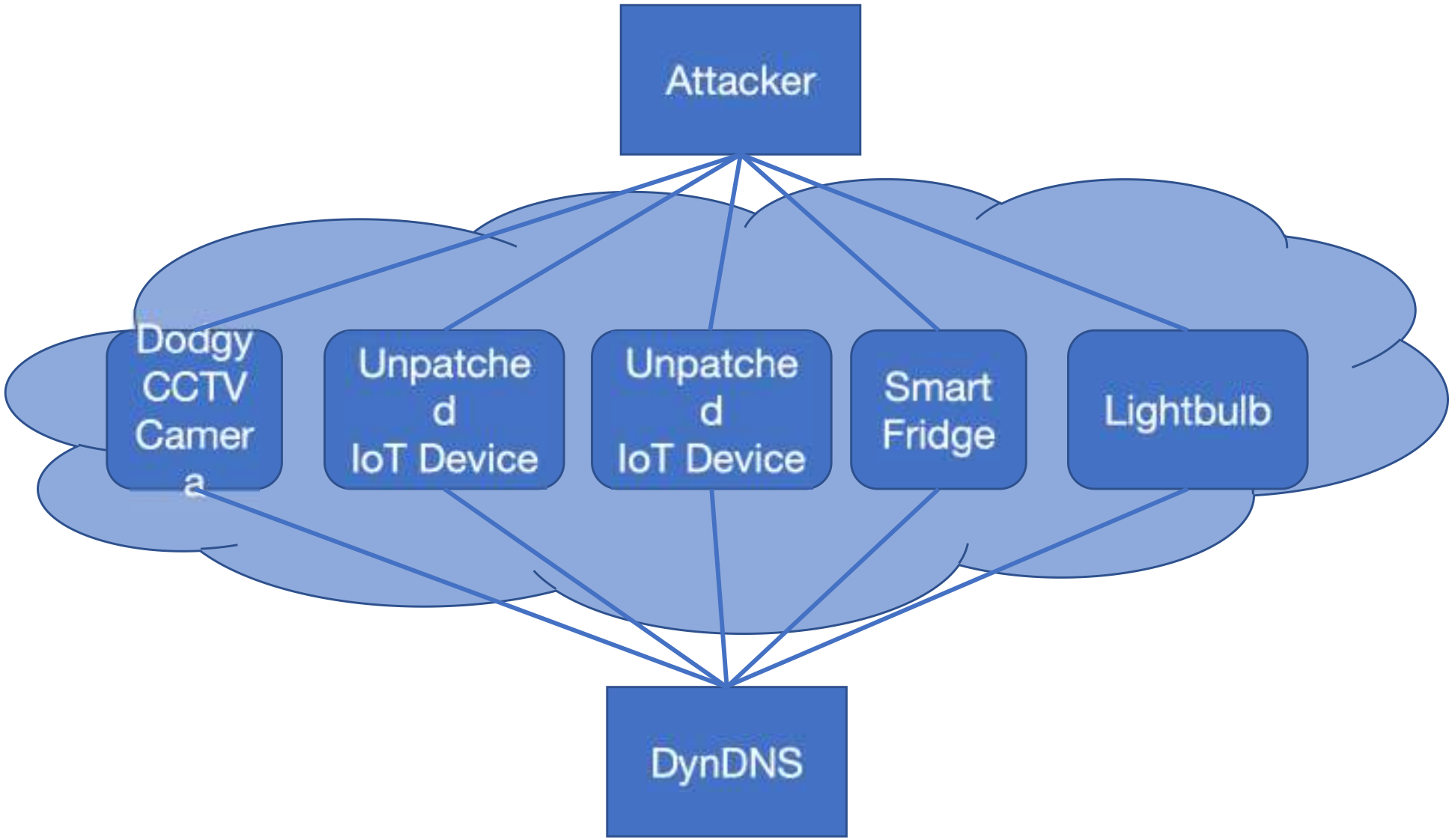



Easier to infect and control real devices than spoofing IPs!

# Distributed Denial of Service



# Mirai Botnet (2016)



# Even more today!

## The biggest DDoS attack ever has been detected - but fortunately you probably barely noticed it

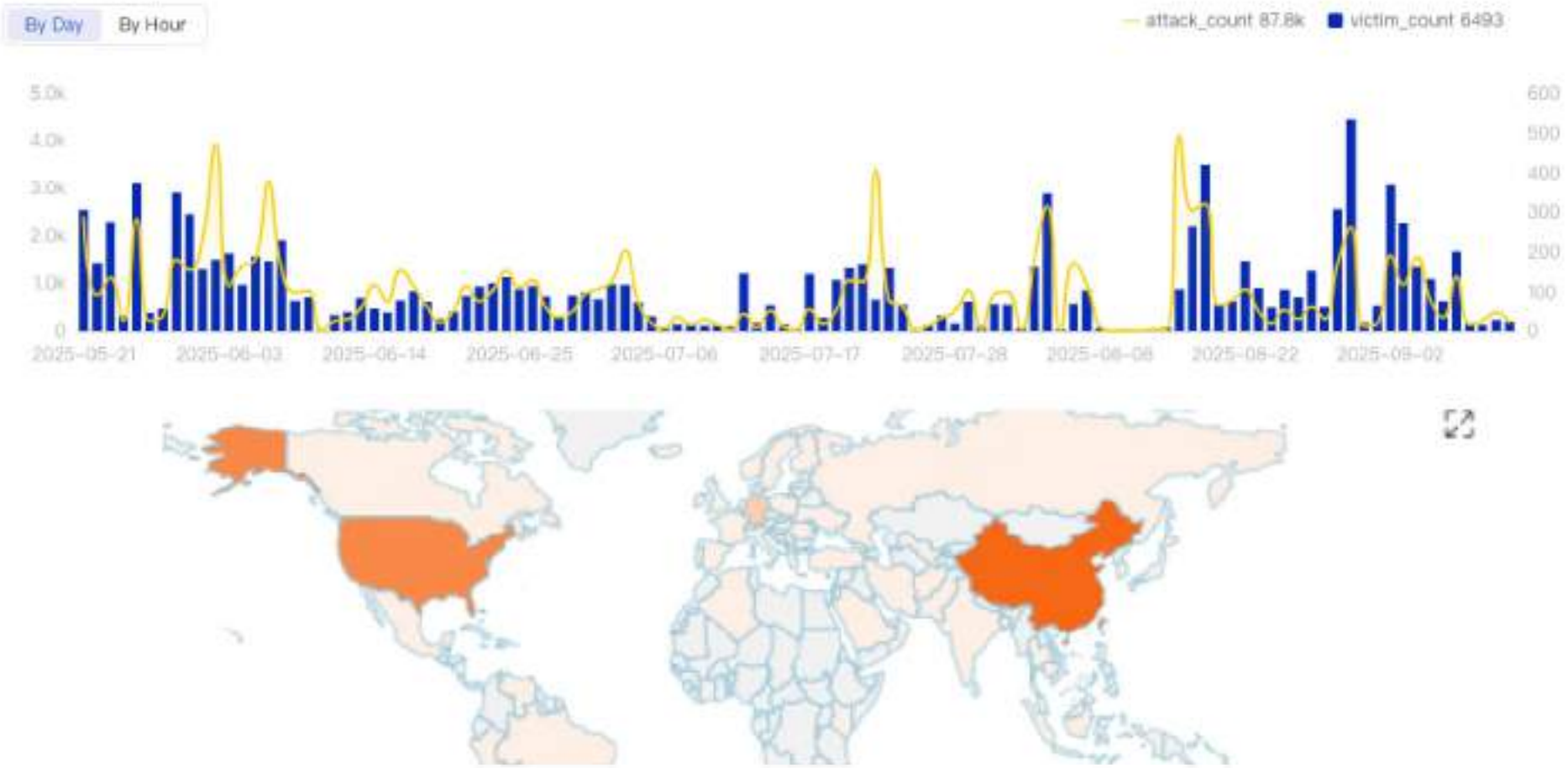
News By Sead Fadilpašić published 3 days ago

Cloudflare mitigated a major attack by Aisuru botnet


(Image credit: FrameStockFootages / Shutterstock)

https://www.techradar.com/pro/security/the-biggest-ddos-attack-ever-has-been-detected-but-fortunately-you-probably-barely-noticed-it

# Aisuru botnet




https://blog.xlab.qianxin.com/super-large-scale-botnet-aisuru-en/#:~:text=rampant%20cybercriminal%20activity.-,Anonymous%20Source%20&%20XLab%20Visibility,Forky:%20responsible%20for%20botnet%20sales

# Think

- How to control these machines?

# Malware

- Viruses, changing exes to run themselves
- Worms, spreading themselves over network
- Trojans, hiding themselves among legitimate programs
- Remote Access Trojans, allowing remote maclious access

# Malware

- Viruses
- Worms
- Trojans
- Remote Access Trojans
- Rootkits
- Potentially Unwanted Software
- Stalkerware?
- Antivirus Software Itself???

# Intrusion Detection and Mitigation

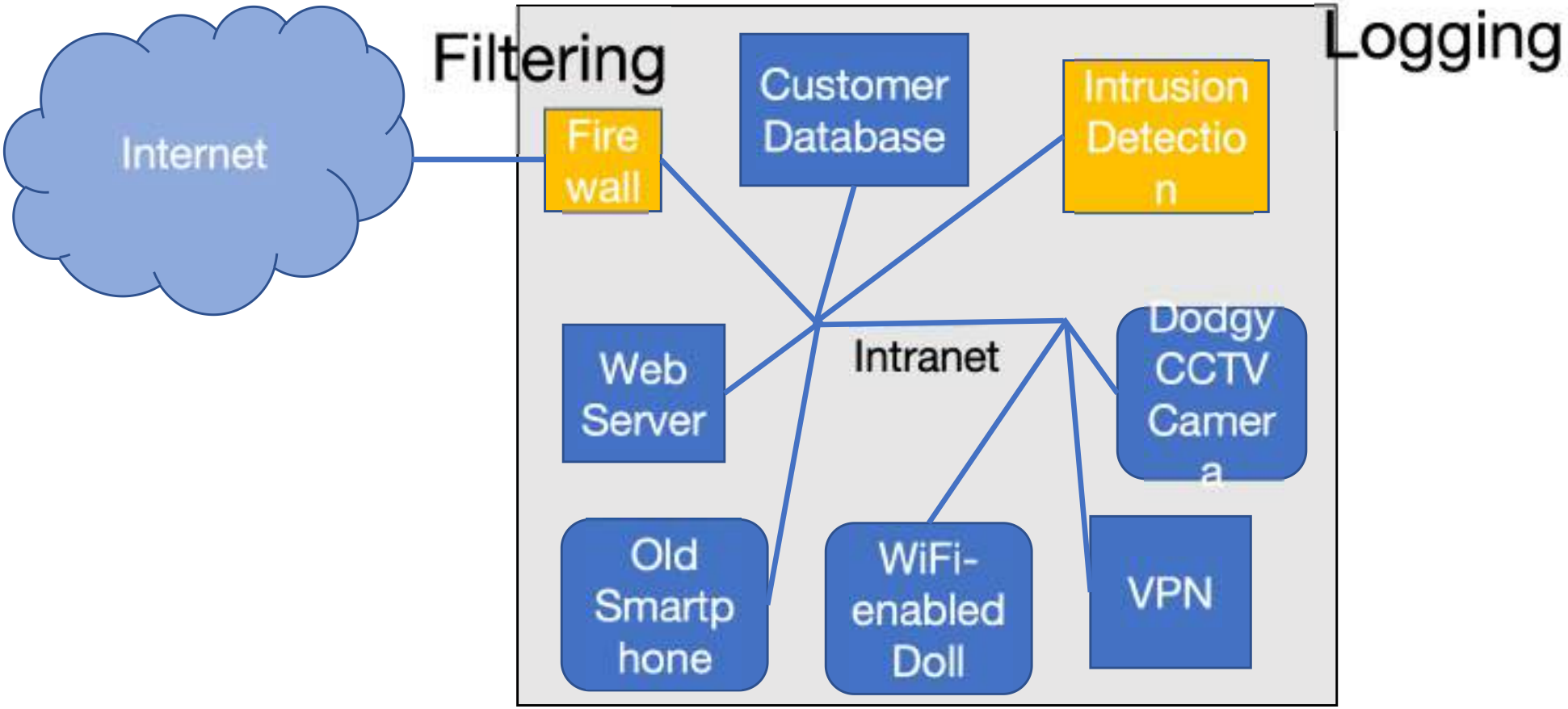
- Intranets of any reasonable size will get infected.
- What is the perimeter, really (VPN, BYOD)?
- Spearphishing: if YOUR sysadmin gets attacked, will you just “blame and train”?
- Adkins et al.: Make criminal adversaries’ attacks expensive (e.g. CAPTCHA) so they go after easier targets

# Insider Risk -- Defences

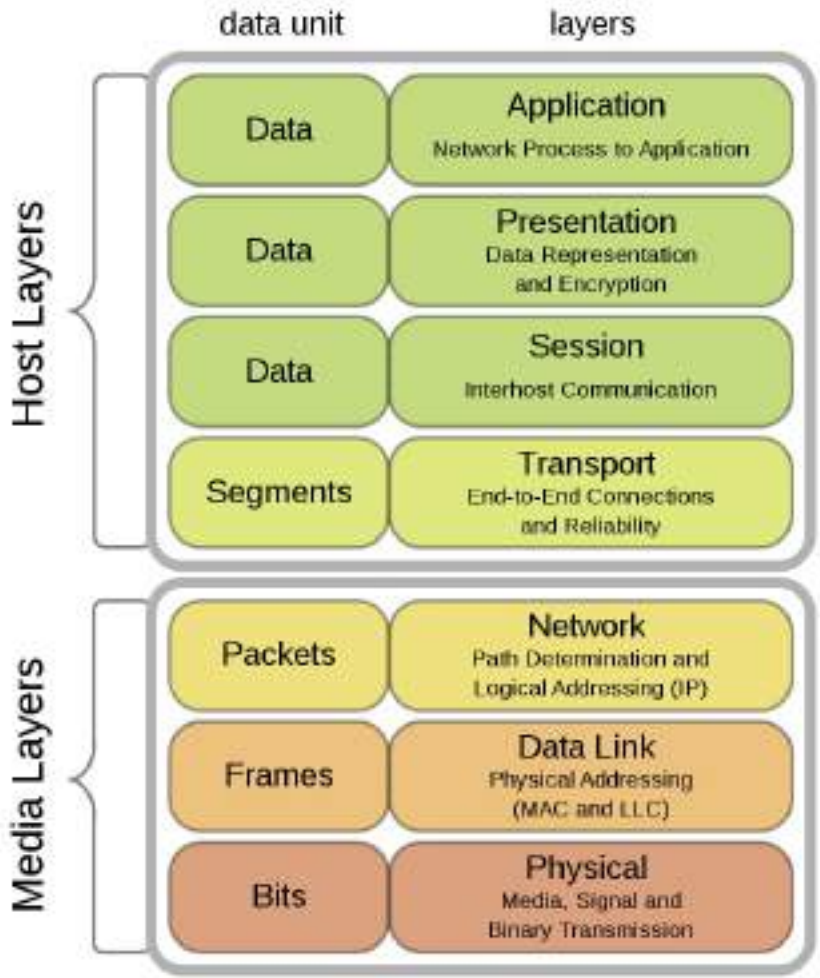
- Least Privilege
- Zero Trust
- Multi-party Authorisation
- Business Justifications
- Auditing and Detection
- Recoverability

From *Building Secure & Reliable Systems: Best Practices for Designing, Implementing and Maintaining Systems*, Heather Adkins, Betsy Beyer, Paul Blankinship, Piotr Lewandowski, Ana Oprea & Adam Stubblefield

# Intrusion Detection and Mitigation



# Filtering: Firewalls

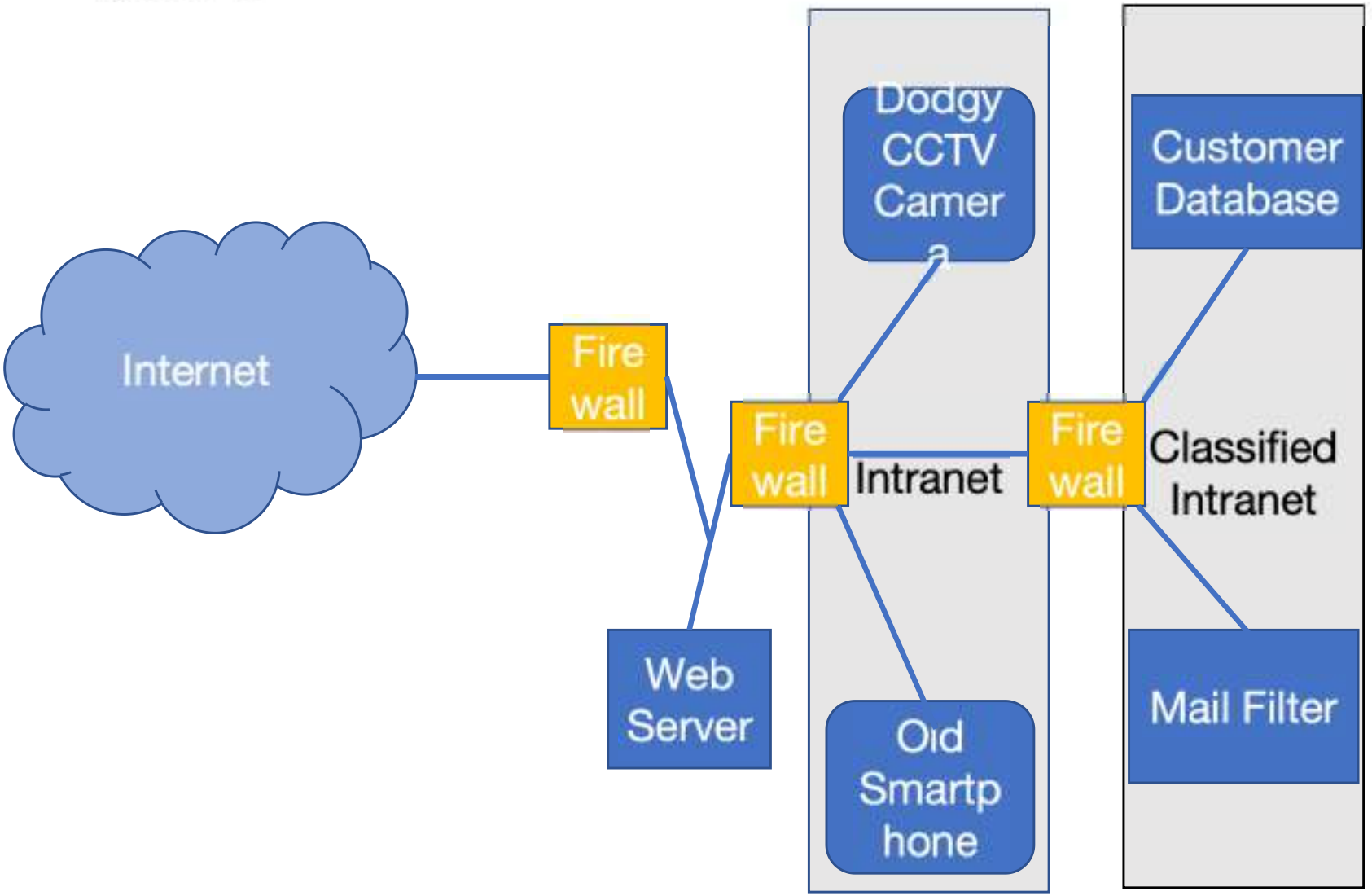



Content Filtering: Application Layer

Circuit Gateways: Full TCP sessions.

Packet Filtering: IP-address spoofing, IP deny lists, port blocking

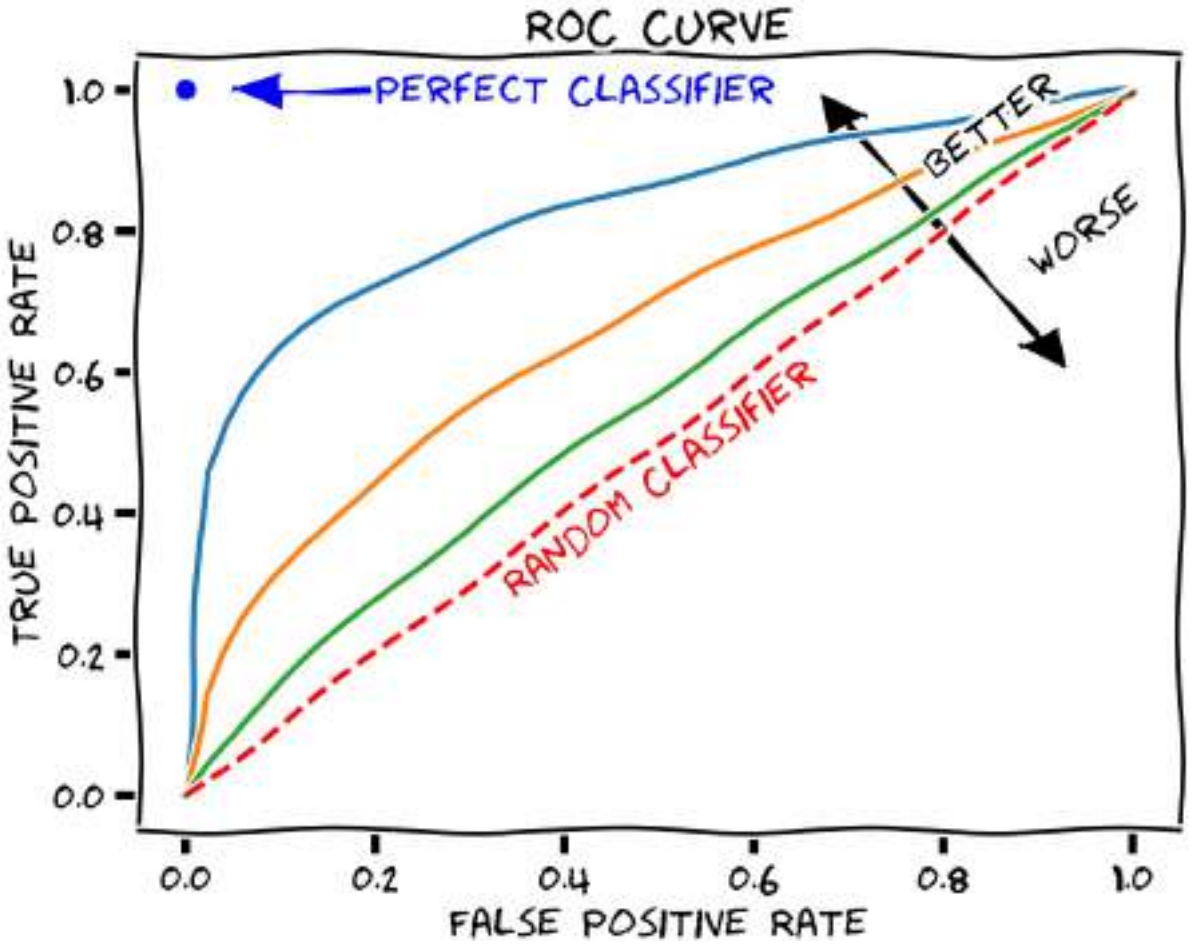
# Where should your protections be?



# Intrusion Detection Systems

- Monitoring and Logging: Don't block, just sound and alarm or forward on.
- Misuse Detection: known bad things
- Anomaly Detection: unusual things?

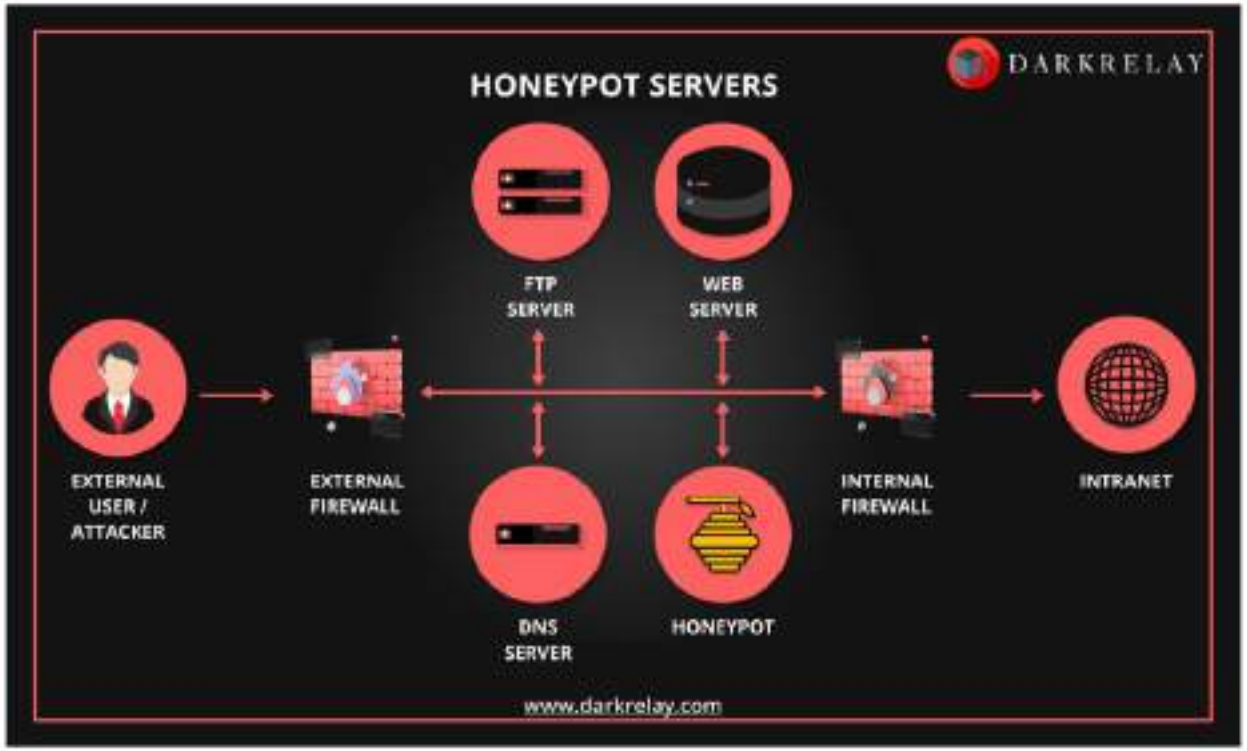
# ROC Curve


ROC CURVE
PERFECT CLASSIFIER
BETTER
WORSE
RANDOM CLASSIFIER
TRUE POSITIVE RATE
FALSE POSITIVE RATE
0.0
0.2
0.4
0.6
0.8
1.0

# Challenges in Intrusion Detection

- The internet is noisy: malice or error?
- Signal-to-noise ratios
- We should always be wary of machine learning
  - Generalization issues and limited quality data
- Audit trails (or lack thereof)
- Compliance vs real defence under cat and mouse games
- Global vs Local detection issues (wrt deperimeterisation)

# Honeypots




- Pros: low cost,  legitimate information, low false positive
- Cons: distinguishability, security risks to the owner, somewhat limited information

# Networks and Cryptography

- WiFi: WEP was weak, but WPA2 supported widely, and uses AES
- Is WiFi a “perimeter”? Issues around trust (default router passwords, IoT devices, unpatched devices)
- VPNs: Funnel packets over untrusted internet into trusted perimeters. It's protocol's IPSec's key exchange probably weak by default ☹

# Networks and Cryptography: HTTPS

- HTTPS (via TLS) now on >60% of connections
- Exchange session keys based on public-key infrastructure
- How do you identify who you're talking to? Certificating Authorities (CA).
- Are CAs trustworthy?
- False positives: ROC curves again
- LetsEncrypt was a real game-changer – any websites  get certificates for free

# Email Security

- Why we care about emails?

## Hillary Clinton emails - what's it all about?

6 November 2016

**Amazon's closely guarded "Project Dawn" redundancies were accidentally exposed when a draft email from a senior AWS executive was mistakenly sent to staff**

## Coinbase phishing email warning

The scam uses convincing emails and login pages

04 Aug 2025


https://www.cgsinc.com/blog/how-to-identify-a-malicious-email-6-tips

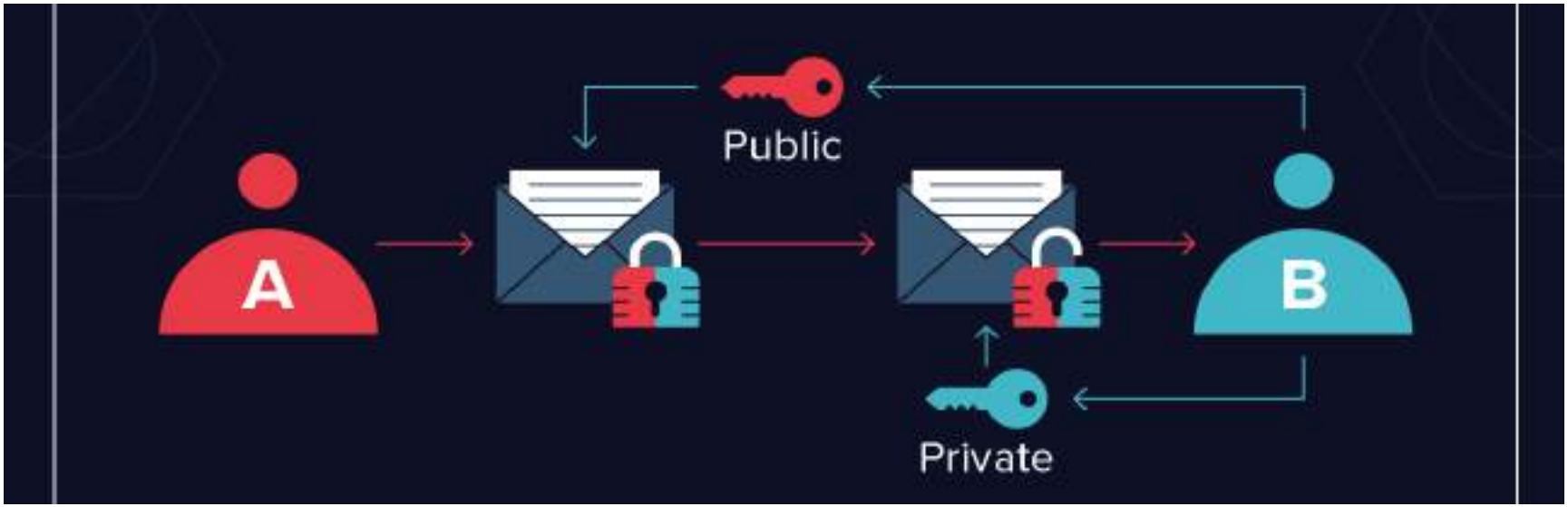
# Email Security

- Simple Mail Transfer Protocol (SMTP)
- Emails are not encrypted by users by default
- Vulnerable to bulk interception and spam
- Types of attacks enabled (categorized by Cloudflare)
  - Fraud
  - Phishing
  - Malware
  - Account takeover
  - Email interception

# Email Security - Defenses

- Confidentiality: 95% of emails are with 5 big webmail providers, providing Transport Layer Security
- Unwanted emails
  - Legitimate sources: blocking / marking spams
  - Against DDoS-like campaign
    - Domain keys identification mail, signing the email with key in domains' public record
    - Sender policy framework, tracing mail to source IP, does not allow forwarding
    - Domain-based Message Authentication, Reporting and Conformance, telling what recipient should do when authentication fails
    - Machine learning based systems

# Email Security - Defenses

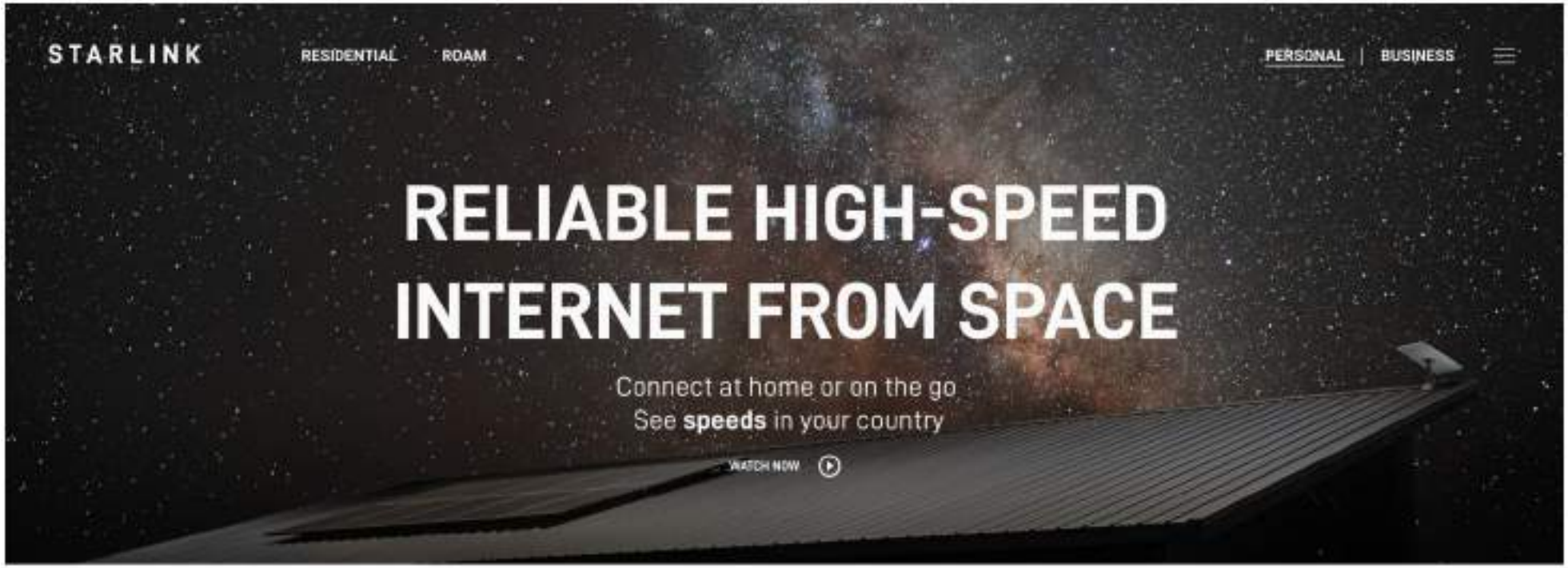



PGP (Pretty Good Privacy): Why Johnny Can't Encrypt

# Email Security - Defenses


How do people recognize scam / spam / phishing emails?

# Bonus: Is Starlink more secure or less? What are the challenges?



# Is Starlink more secure or less? What are the challenges?

- Limited bandwith for public key infrastructure
- Users' physical location privacy
- Jamming is easier
- A more central control (good or bad?)

https://www.usenix.org/conference/usenixsecurity24/presentation/koisser

# Extras

# Tools of Attack/Defence

```
$ nmap -A scanme.nmap.org

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-29 20:02 CET
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.16s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 5.3p1 Debian 3ubuntu7.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_  2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp   open  http       Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
9929/tcp open  nping-echo Nping echo
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|storage-misc|WAP
Running (JUST GUESSING): Linux 2.6.X|3.X|2.4.X (94%), Netgear RAIDiator 4.X (86%)
```

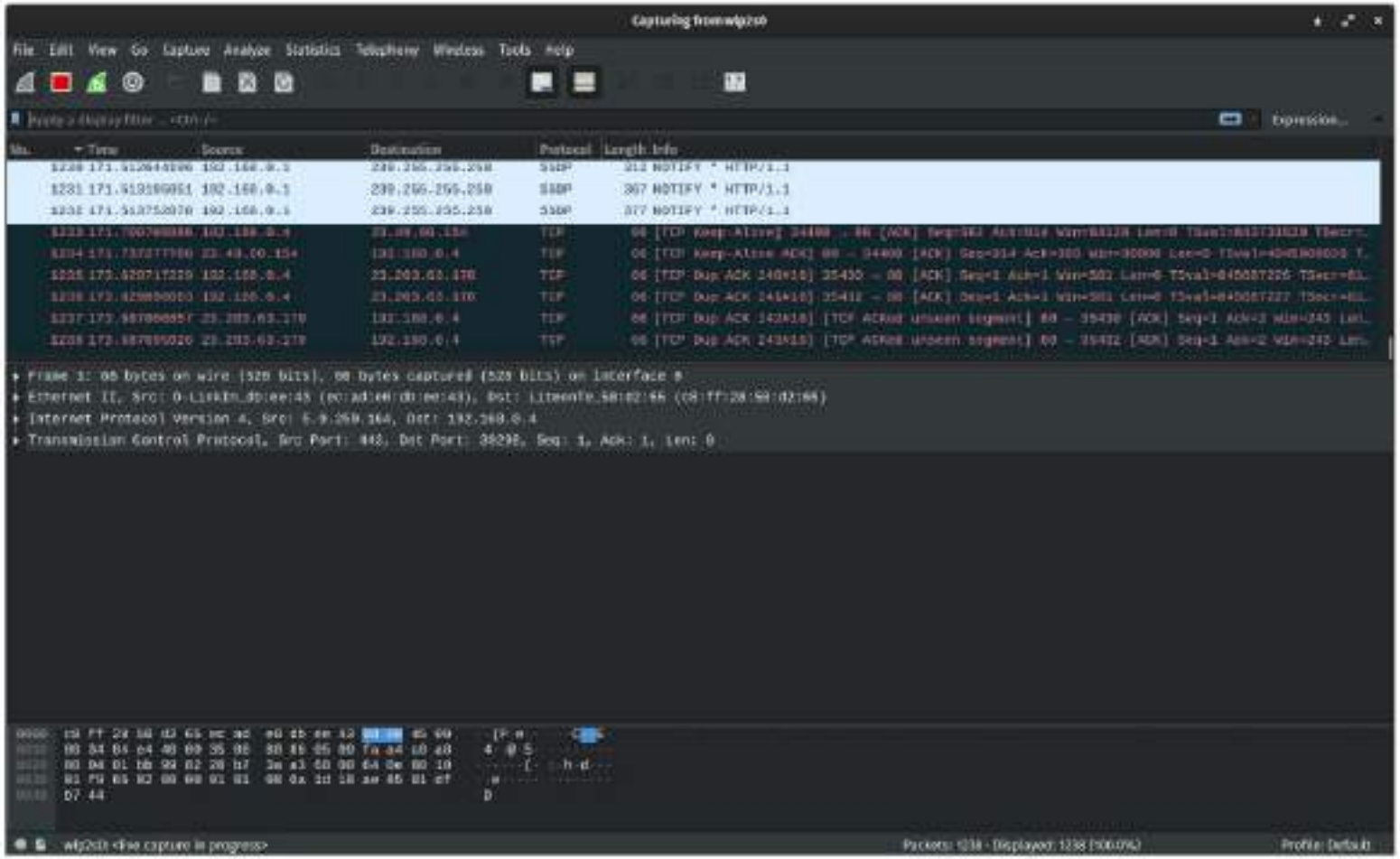
## Nmap: Port scanning

# Tools of Attack/Defence

```
% echo "GET / HTTP/1.0\n" | netcat localhost 80

HTTP/1.1 200 OK
Date: Sat, 07 Jan 2006 08:43:27 GMT
Server: Apache
Last-Modified: Wed, 28 Dec 2005 08:09:31 GMT
ETag: "13c6e-14-1ea644c0"
Accept-Ranges: bytes
Content-Length: 20
Connection: close
Content-Type: text/html

nothing to see here

%
```

Netcat: Port Scanning / Listening (of specific ports)

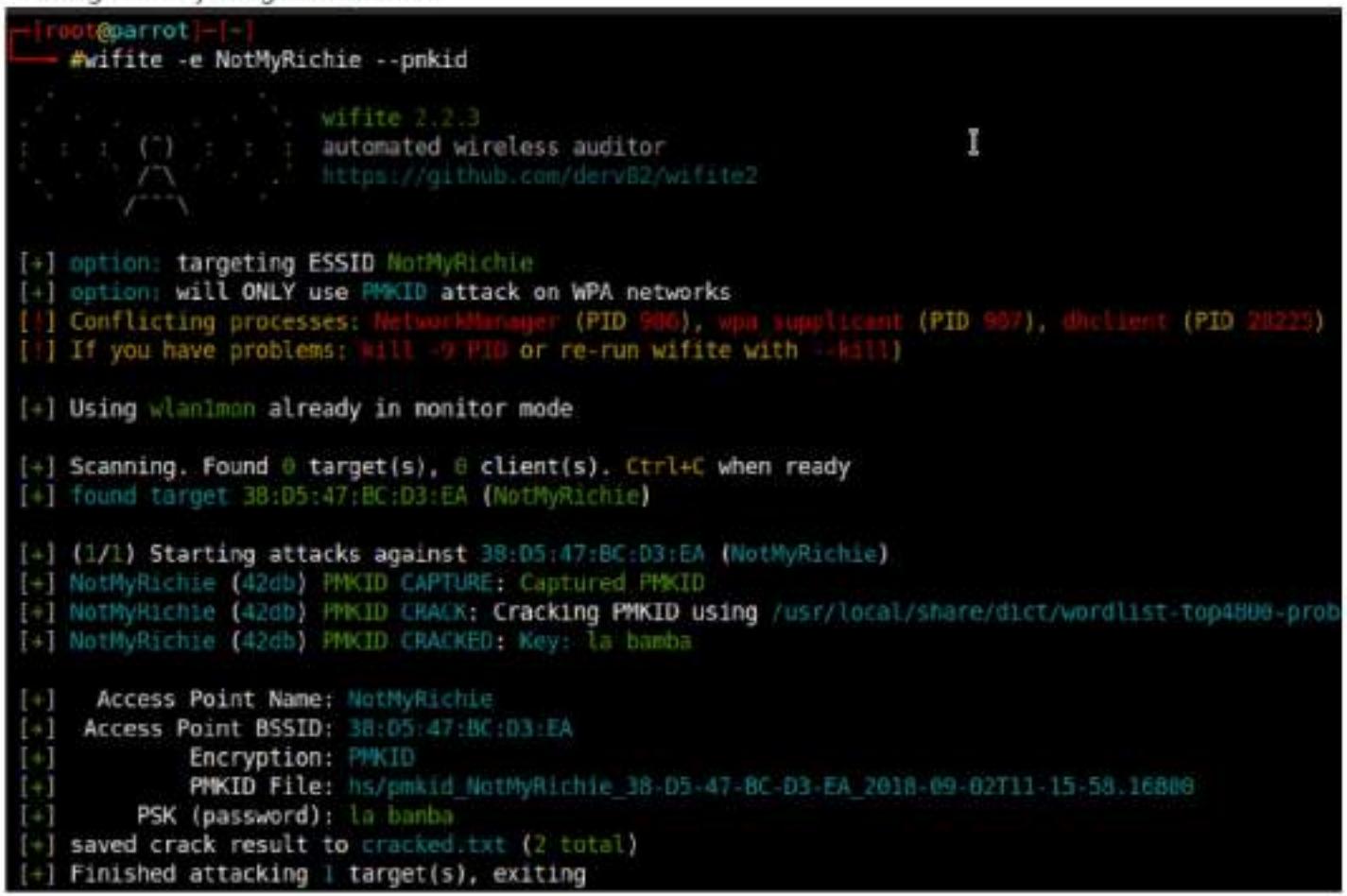
# Tools of Attack/Defence




Wireshark: Packet Sniffing

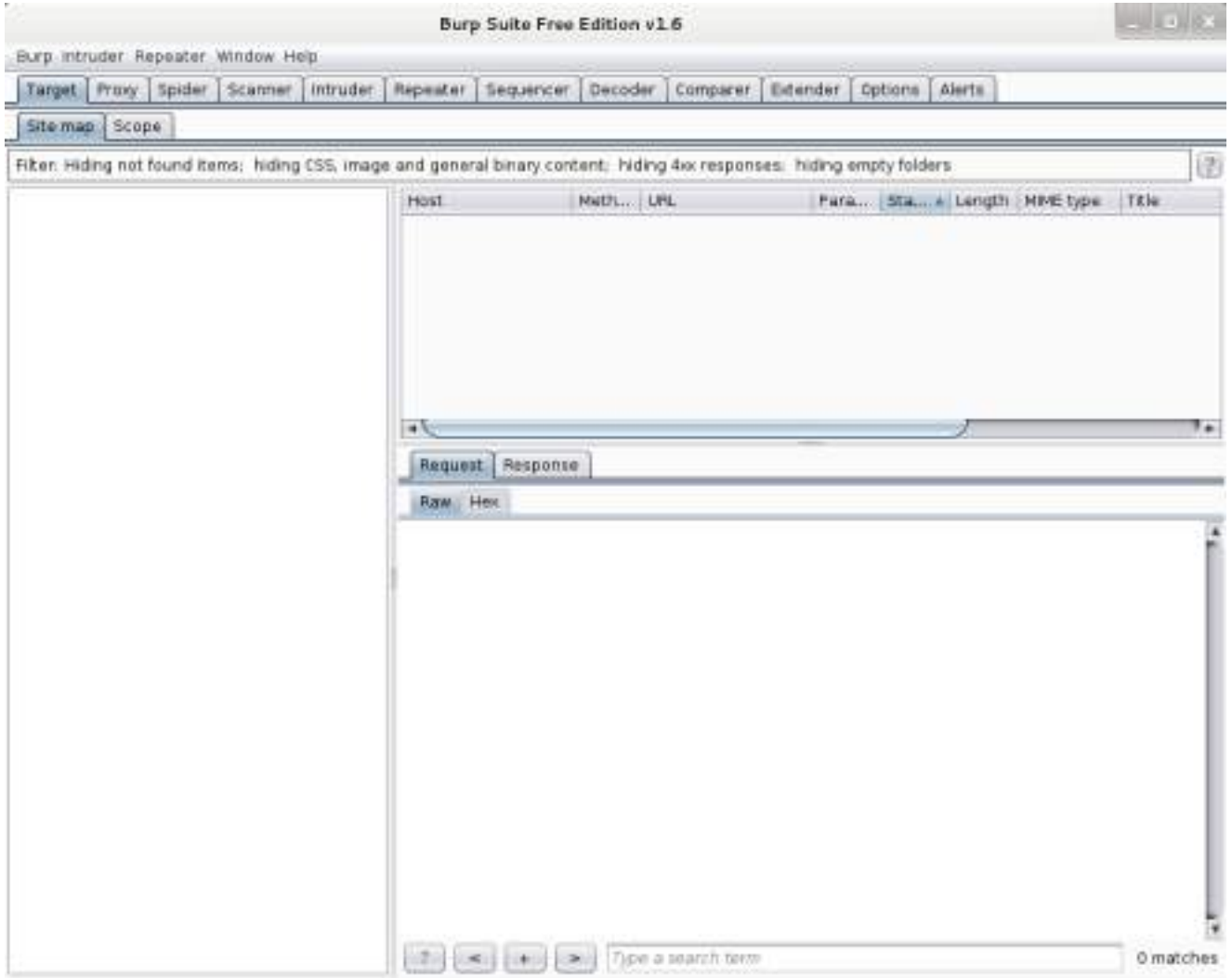
# Tools of Attack/Defence

Cracking WPA key using PMKID attack:




WiFite: WiFi hacking

# Tools of Attack/Defence




Burp Suite: Attack and Defend Web *Applications*