Διάλεξη #20 - Network Security

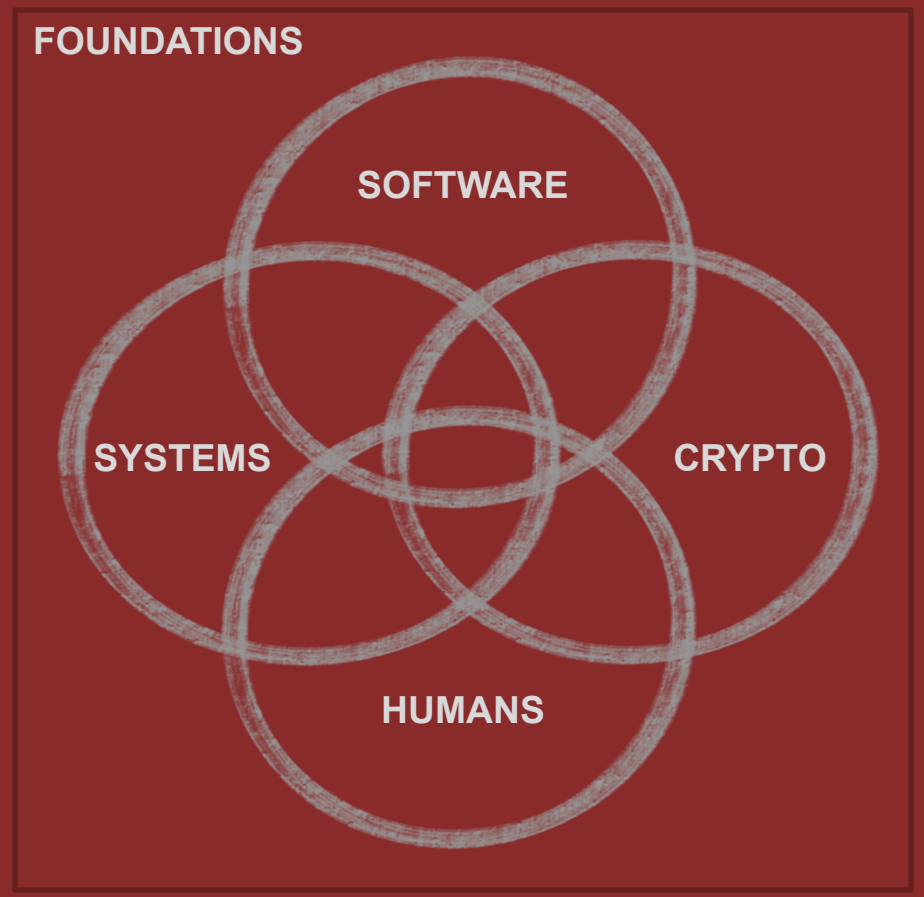
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Εισαγωγή στην Ασφάλεια

Θανάσης Αυγερινός

THIS ISN'T WHAT I MEANT WHEN I SAID I WAS CONCERNED ABOUT LATERAL MOVEMENT RISK.

Huge thank you to David Brumley from Carnegie Mellon University for the guidance and content input while developing this class!



Ανακοινώσεις / Διευκρινίσεις

- Υπενθύμιση Εργασία #3 - Προθεσμία: 15 Ιουνίου, 23:59
- Ο νέος διαγωνισμός "Special Guests" είναι για δικά σας challenges - λίγη υπομονή όσο λύνουμε κάποια προβληματάκια
- 2η ημερομηνία διαγωνίσματος: 6-9μμ, 10 Ιουλίου 2024.
  - Μπορείτε να προσέλθετε μόνο σε μια από τις δύο εξετάσεις (doh!)

Την προηγούμενη φορά

- Web Security
- Web App Background
- Broken access control
- Injection
  - XSS
  - Command
  - SQL
- CSRF

Σήμερα

- Networks 101
- Scanning
- Firewalls

Server Side Request Forgery (SSRF)

Server Side Requests

Modern websites are composed of several smaller services.

Frontend

API

```
POST /product/stock HTTP/1.0
Content-Type:
application/x-www-form-urlencoded
Content-Length: 118

stockApi=http://stock.weliketoshop.net:8080
/product/item/12345
```

1

```
GET
stockApi=http://stock.weliketoshop.net:8080
/product/item/12345
```

2

3

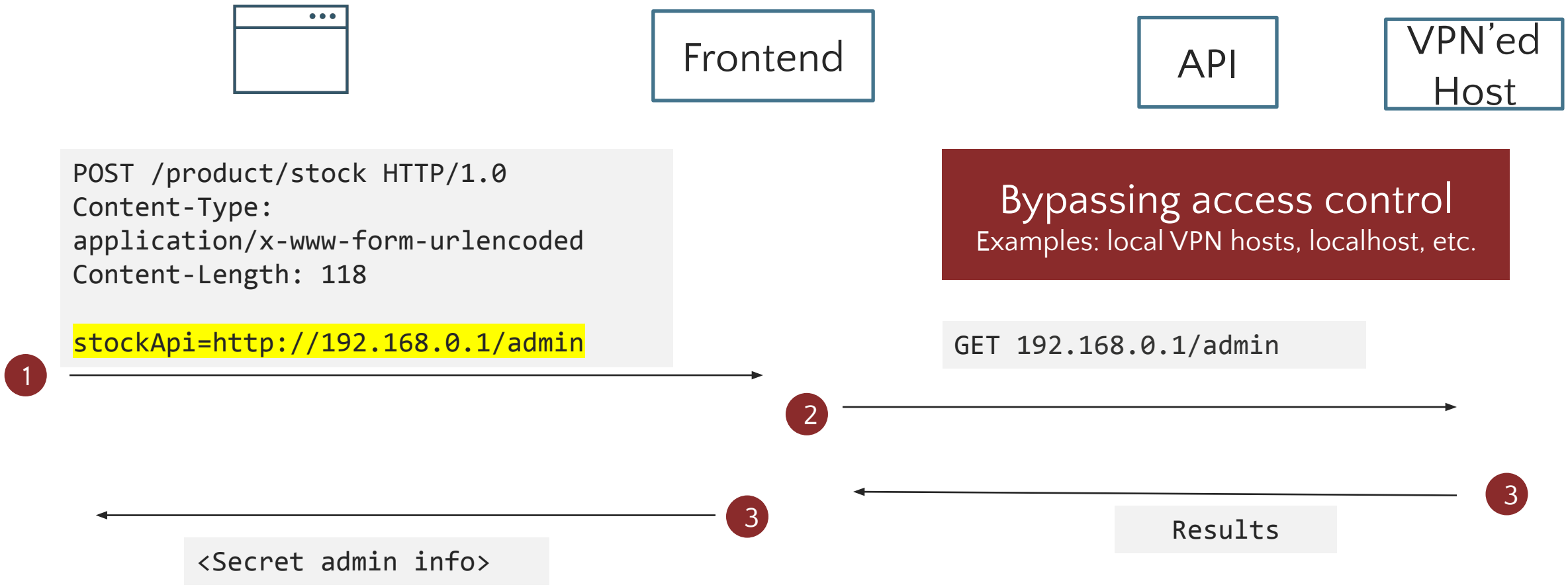
```
<API Result>
```

4

```
<Next Page>
```

Server Side Requests

SSRF: attacker induces the application to make an HTTP request back to the hosting server



Networks 101

Five Key Aspects of Networking

Data communications: bits over signals

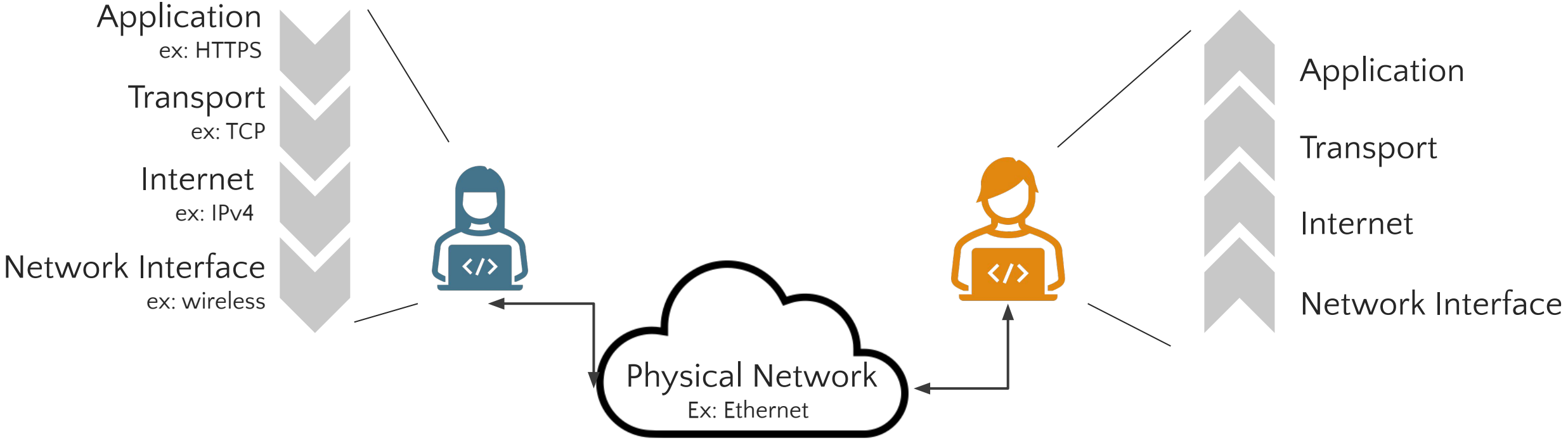
Networks: Packets over bits

Internets: Datagrams over packets

Network programming: Application data over the Internet

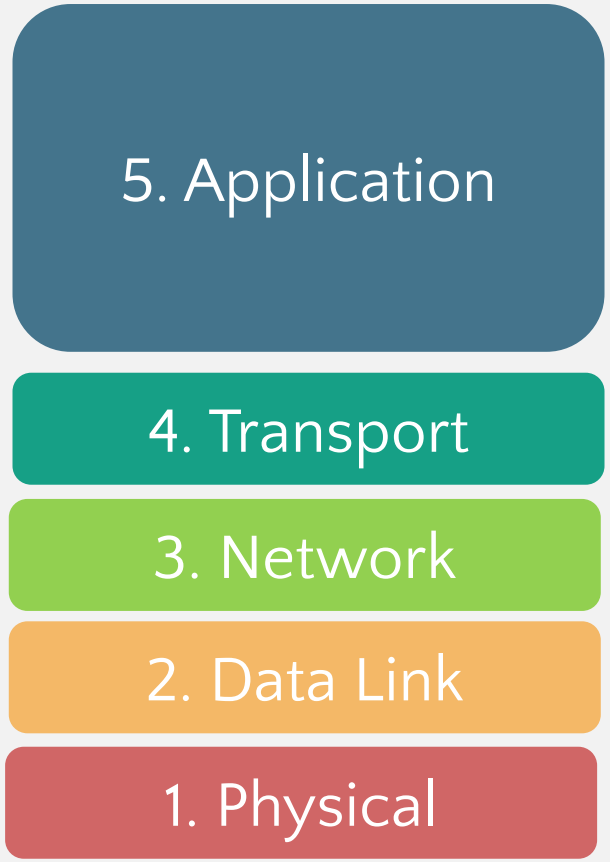
Cross-functional concepts: network configuration, control, and management

Network Layers



OSI Model

Internet reference model



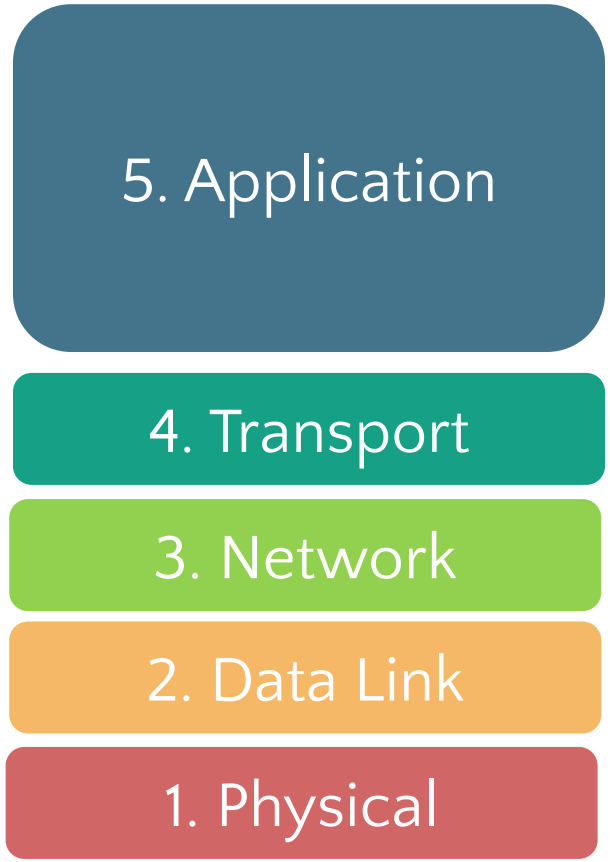
- Session, Presentation, and Application layers combined
- ISO 7-layer model created by committee vote
- "All 7 layers" used in marketing

Warning! Layering model is an abstraction!

In real life there are inter-layer dependencies.

Image from bmc.com

Protocol Example: BGP



BGP (Border Gateway Protocol) is the protocol underlying the global routing system of the internet. It manages how packets get routed from network to network through the exchange of routing and reachability information among edge routers.

Operates at: Transport layer

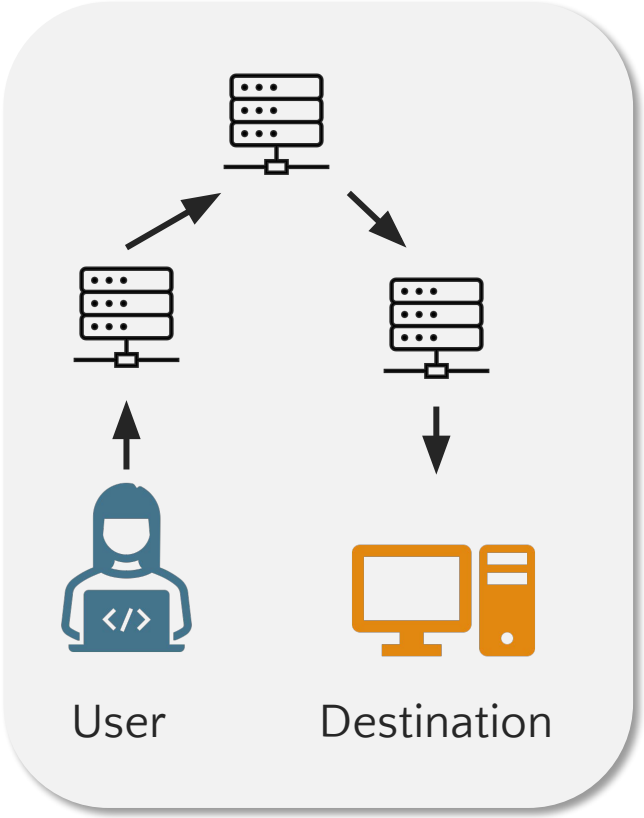
Controls: Network layer

Crypto Exchange KLAYswap Loses $1.9M After BGP Hijack

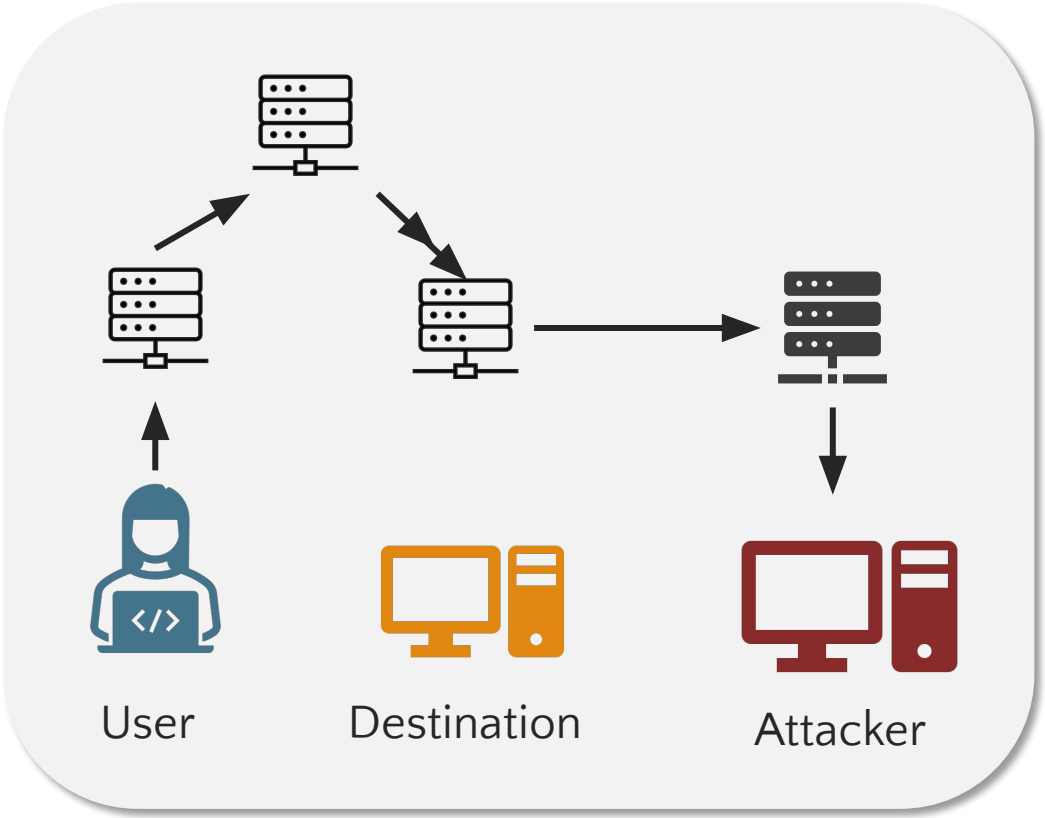
Hackers Performed Border Gateway Protocol Hack to Conduct Illegal Transactions

Prajeet Nair (@prajeetspeaks) • February 16, 2022

Attackers manipulated the network flow and configured it so that the users connected to KLAYswap could download malicious code from the server sent by the attacker rather than the normal Software Development Kit file or KakaoTalk, a popular South Korean application used by the cryptocurrency exchange platform.

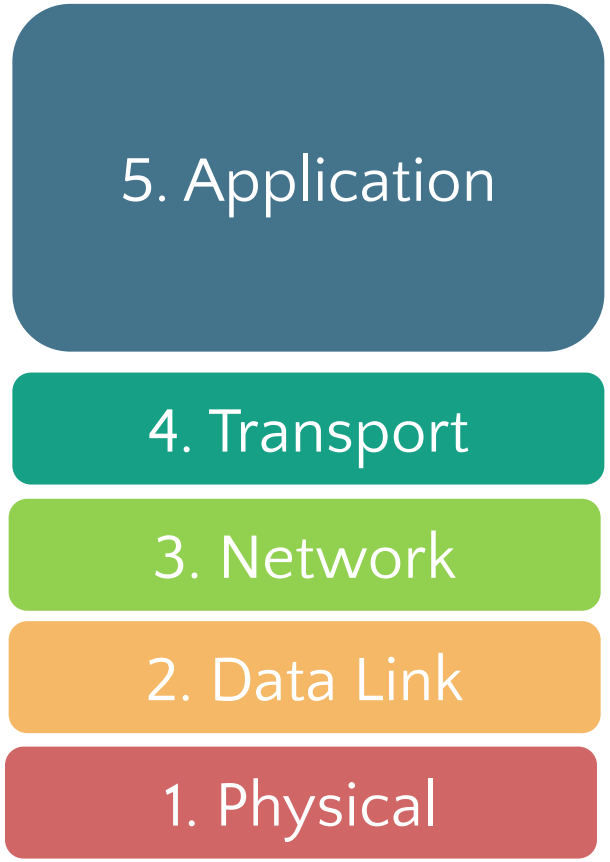


Normal BGP Routing



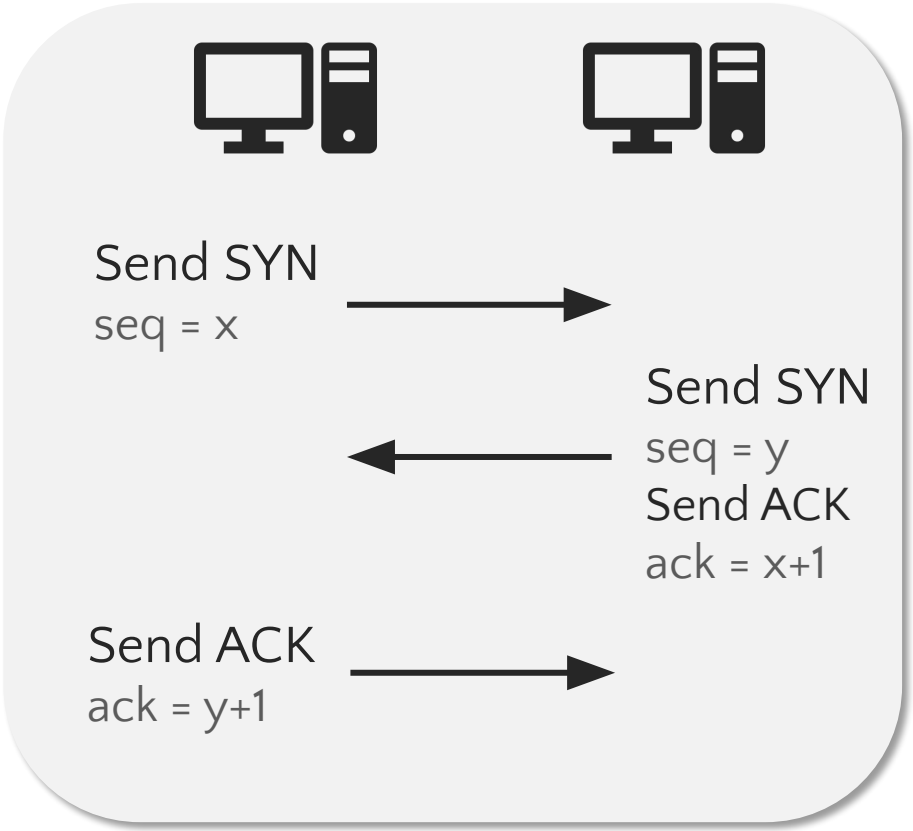
Attacker disrupted routing

Protocol Example: TCP



TCP (Transmission Control Protocol) is a reliable stream delivery service operating over IP. It provides host-to-host connectivity.

Operates at: Transport layer

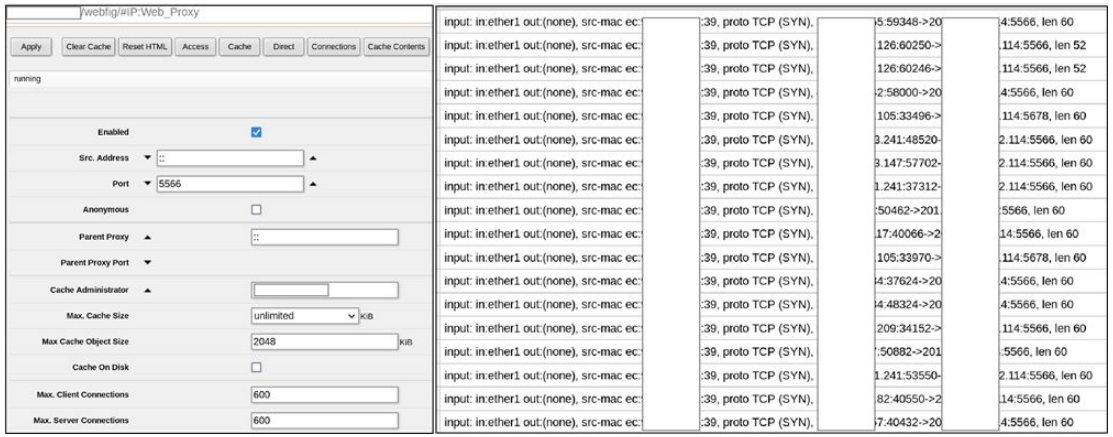


3 Way TCP Handshake

Distributed Denial of Service Attacks

Cyberattack hits Ukrainian banks and government websites

PUBLISHED WED, FEB 23 2022•11:08 AM EST UPDATED WED, FEB 23 2022•6:15 PM EST



[Mirai](#) and [Meris](#) Botnet Syn Flood Attack

Meris Botnet:

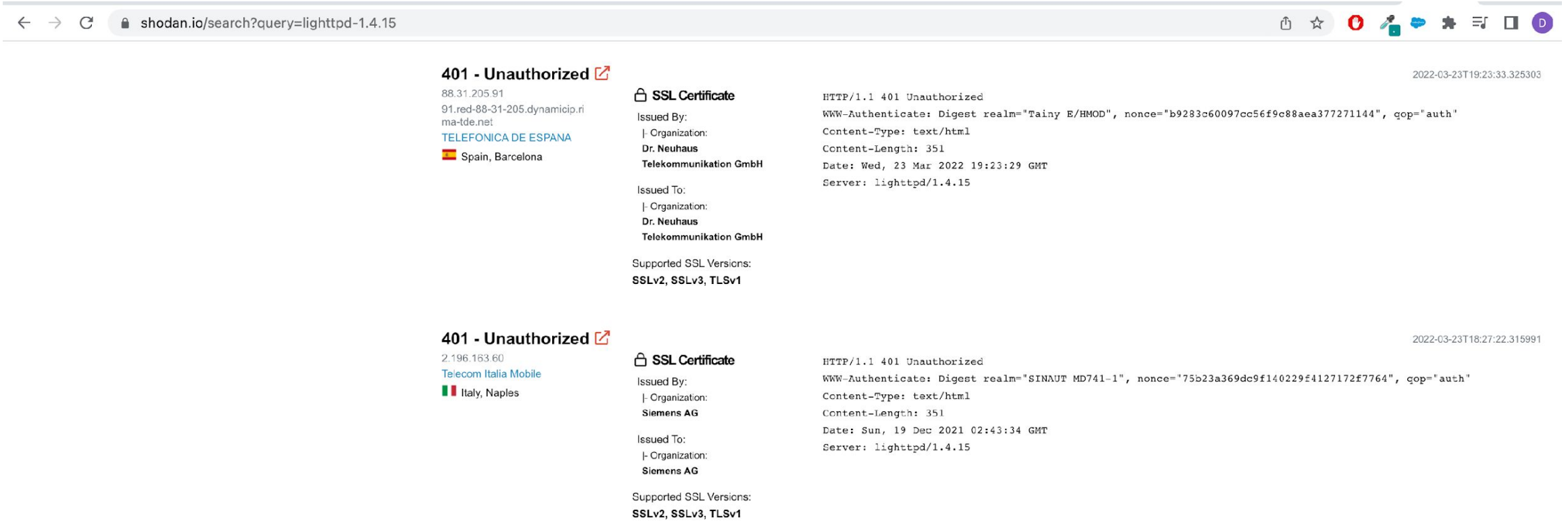
- Infected routers and networking hardware manufactured by the Latvian company MikroTik
- Approximately 250k compromised devices

Mirai Botnet:

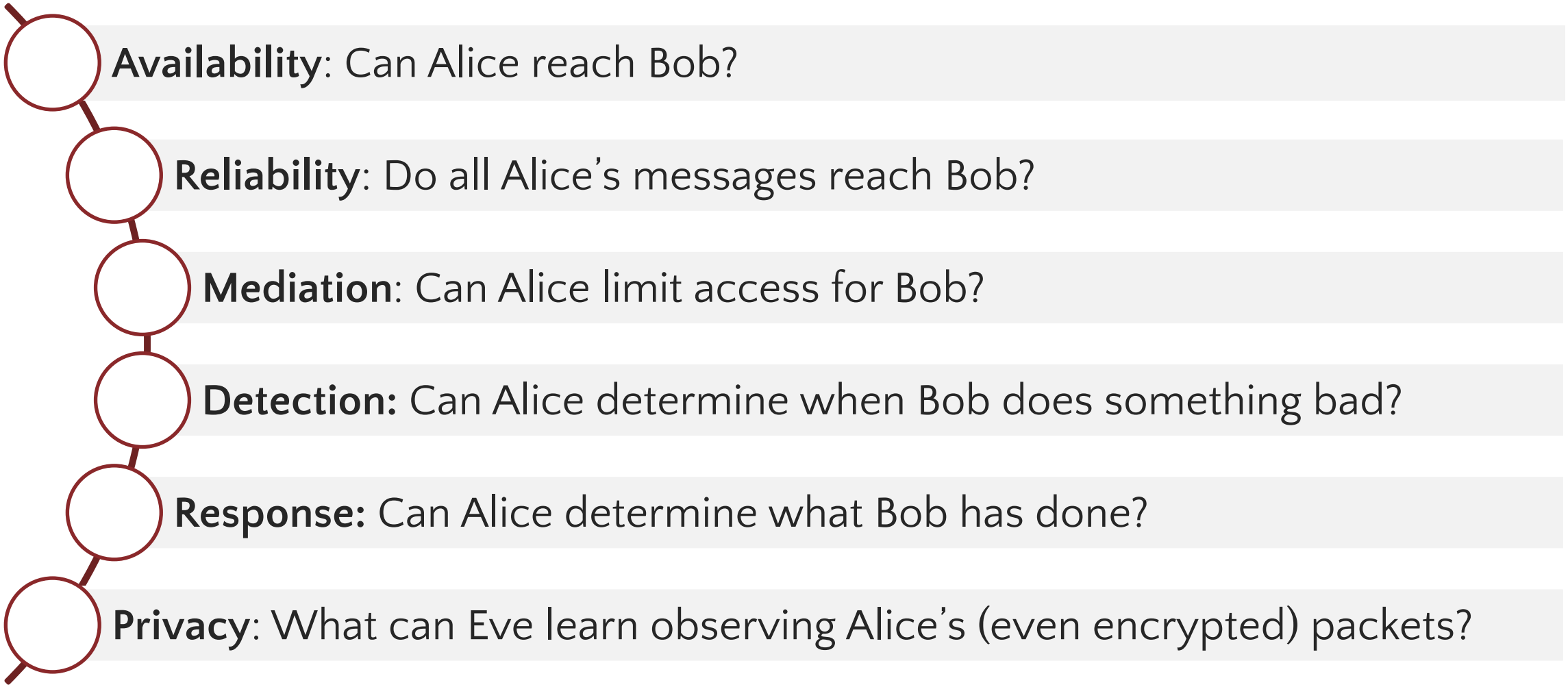
- IOT compromise, often through default username/password w/ phishing
- Est 800k–2.5 million infected devices
- Approximately 250k compromised devices

Source:
https://www.cnbc.com/2022/02/23/cyberattack-hits-ukrainian-banks-and-government-websites.html
https://cert.gov.ua/article/37139

Do I even need to mention scanning?



Example Network Security Goals



- **Availability**: Can Alice reach Bob?
- **Reliability**: Do all Alice's messages reach Bob?
- **Mediation**: Can Alice limit access for Bob?
- **Detection:** Can Alice determine when Bob does something bad?
- **Response:** Can Alice determine what Bob has done?
- **Privacy**: What can Eve learn observing Alice's (even encrypted) packets?

Availability & Reliability

Denial of Service Mitigation

Definition: Denial of Service

A denial-of-service attack is a cyber-attack where the attacker attempts to deny or degrade the availability of a (network) resource. Distributed DoS is coordinating multiple hosts against a single target.

Volume Attacks

Overwhelm server with requests

State-holding attacks

Exhaust server memory/disk/etc.

Computation Attacks

Trigger slow execution paths

Layer Examples

Application-Level

HTTP{S} flood,

Transport

Syn flooding, UDP flooding

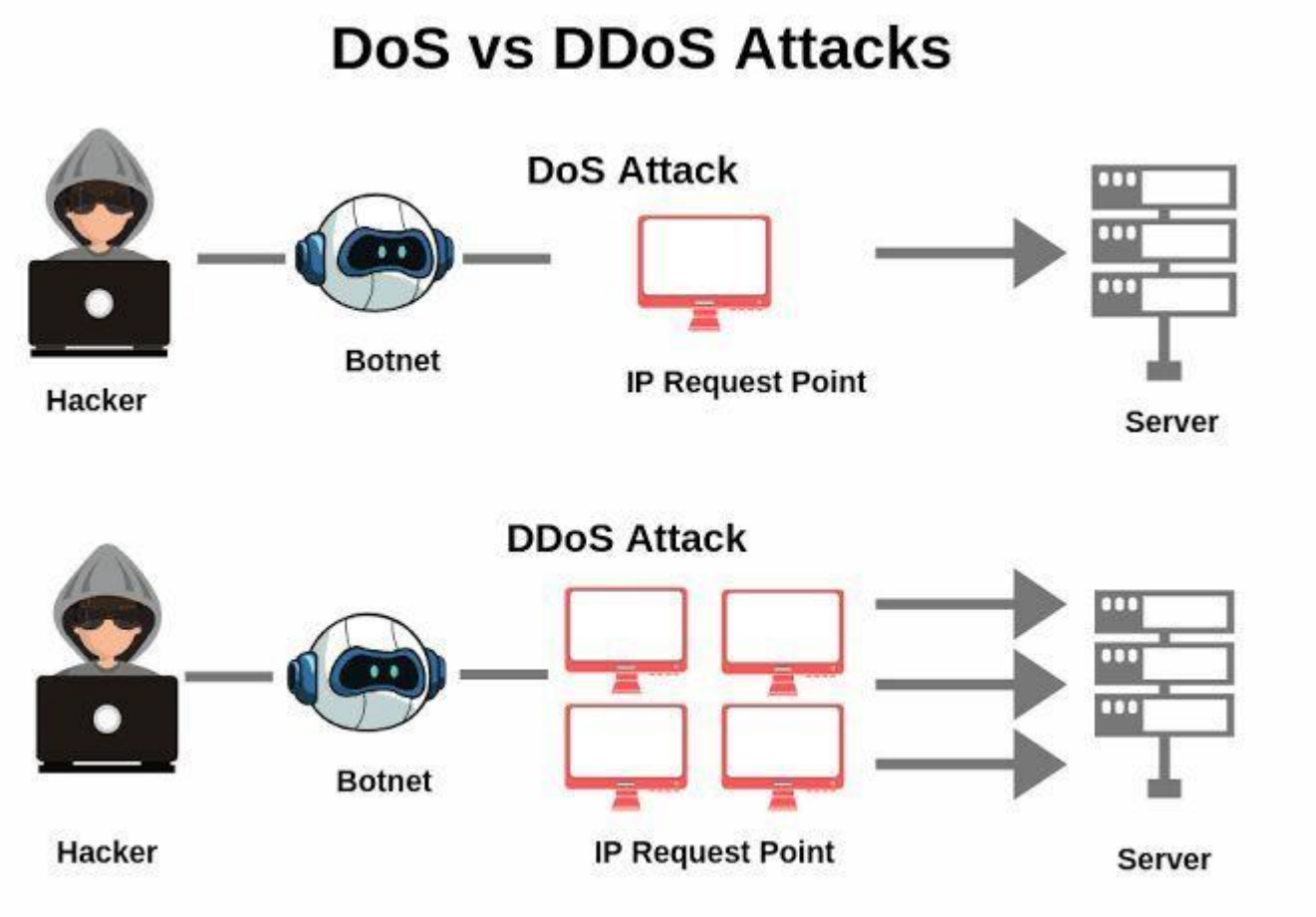
Network

ICMP “ping” flood, "smurf attack", ”ping-of-death”

Data link

Ethernet exponential backoff attacks, WEP disassociation attacks

DOS vs DDOS


DoS vs DDoS Attacks
DoS Attack
Hacker
Botnet
IP Request Point
Server
DDoS Attack
Hacker
Botnet
IP Request Point
Server

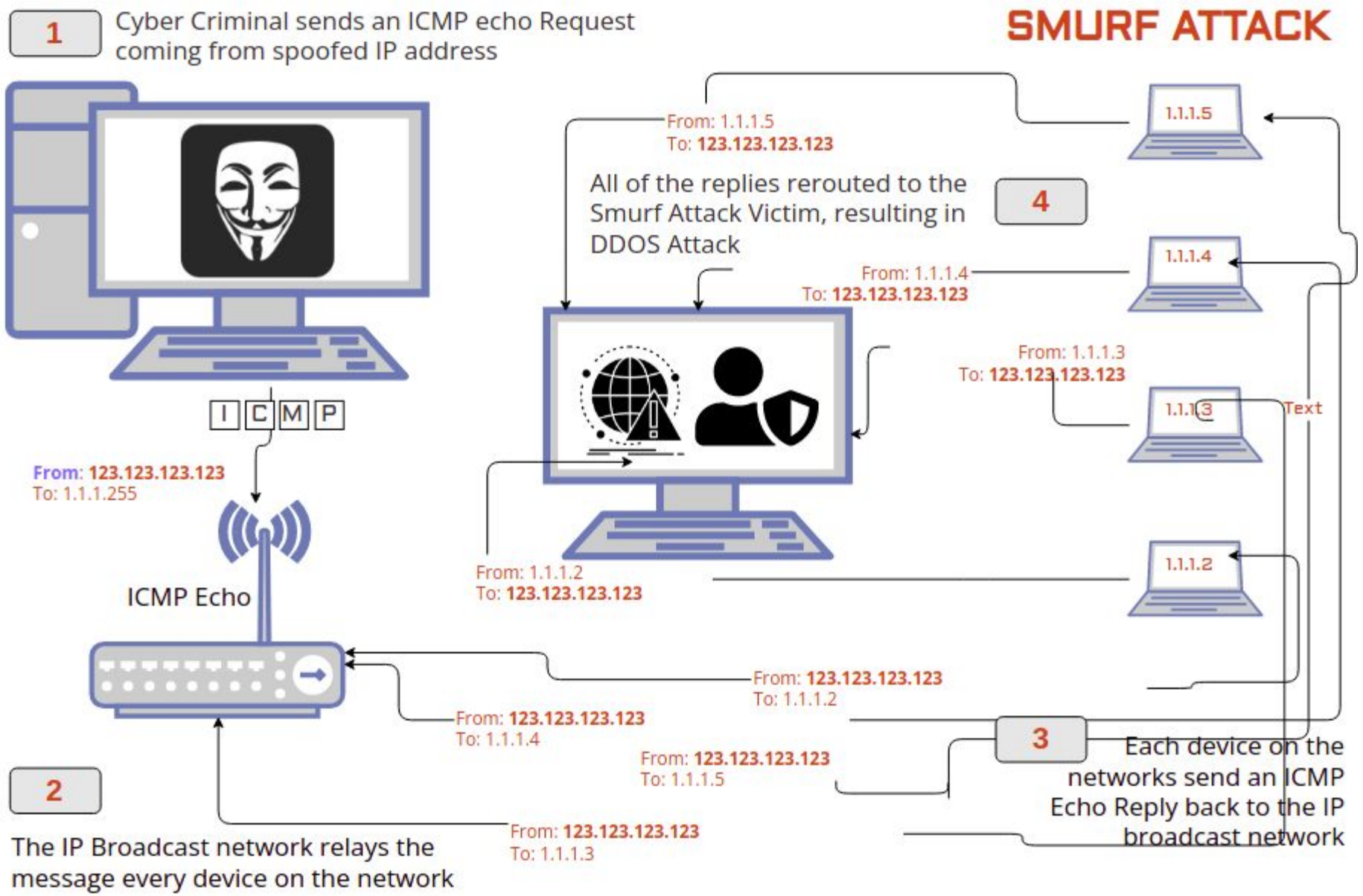
Important DoS Concepts: Amplification and Spoofing

In DDoS, ***amplification*** is the degree of bandwidth enhancement that an original attack traffic undergoes during its transmission towards the victim computer.

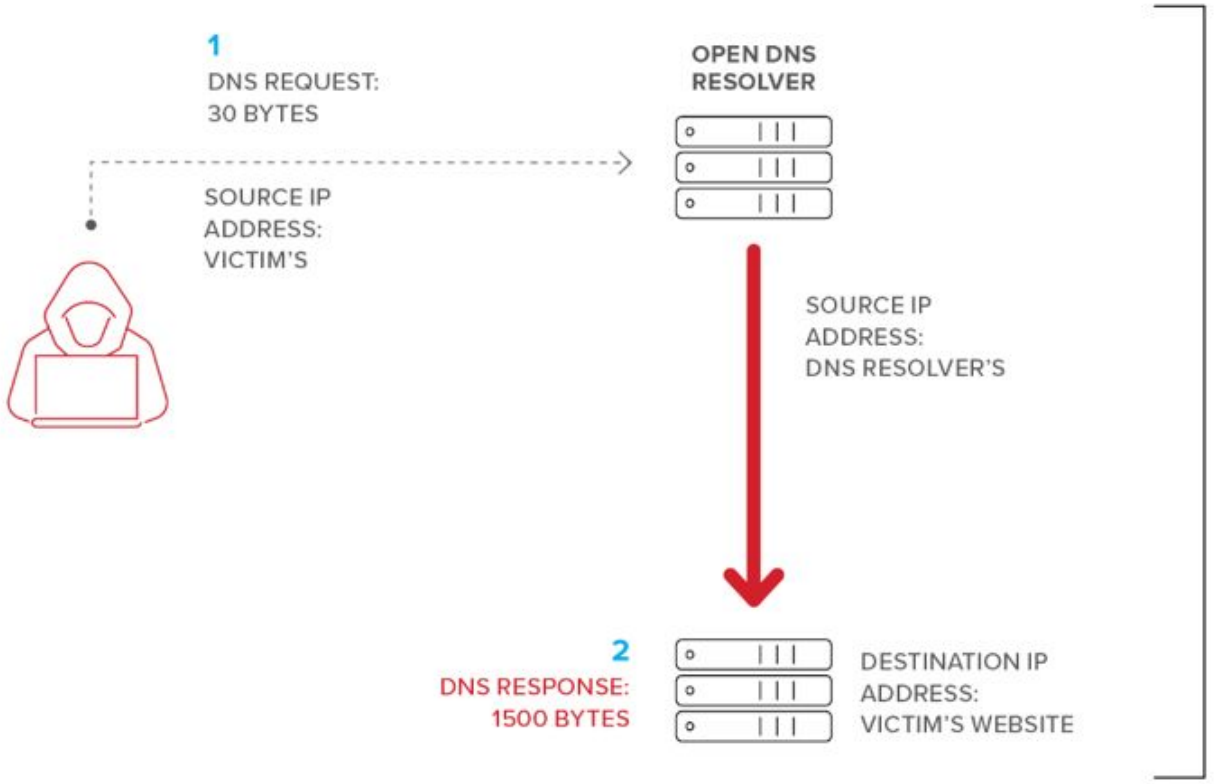
An amplification factor of 100, for example, means that an attacker could manage to create 100 Mb/s of traffic using just 1 Mb/s of its own bandwidth.

A spoofing attack is a situation in which a person or program successfully identifies as another by falsifying data, to gain an illegitimate advantage, e.g., IP spoofing.

An Oldie: The Smurf Attack



The Traditional: DNS Resolution Amplification



AMPLIFICATION FACTOR

50x

x1,000,000
(Botnet size)

The Modern - CVE-2022-26143

A zero-day vulnerability in the Mitel MiCollab business phone system has recently been discovered (CVE-2022-26143). This vulnerability, called TP240PhoneHome, which Cloudflare customers are already protected against, can be used to launch UDP amplification attacks. This type of attack reflects traffic off vulnerable servers to victims, amplifying the amount of traffic sent in the process **by an amplification factor of 220 billion percent** in this specific case.

https://blog.cloudflare.com/cve-2022-26143-amplification-attack/

Example Mitigation: Content distribution network (CDN)

Volume Attack Mitigation

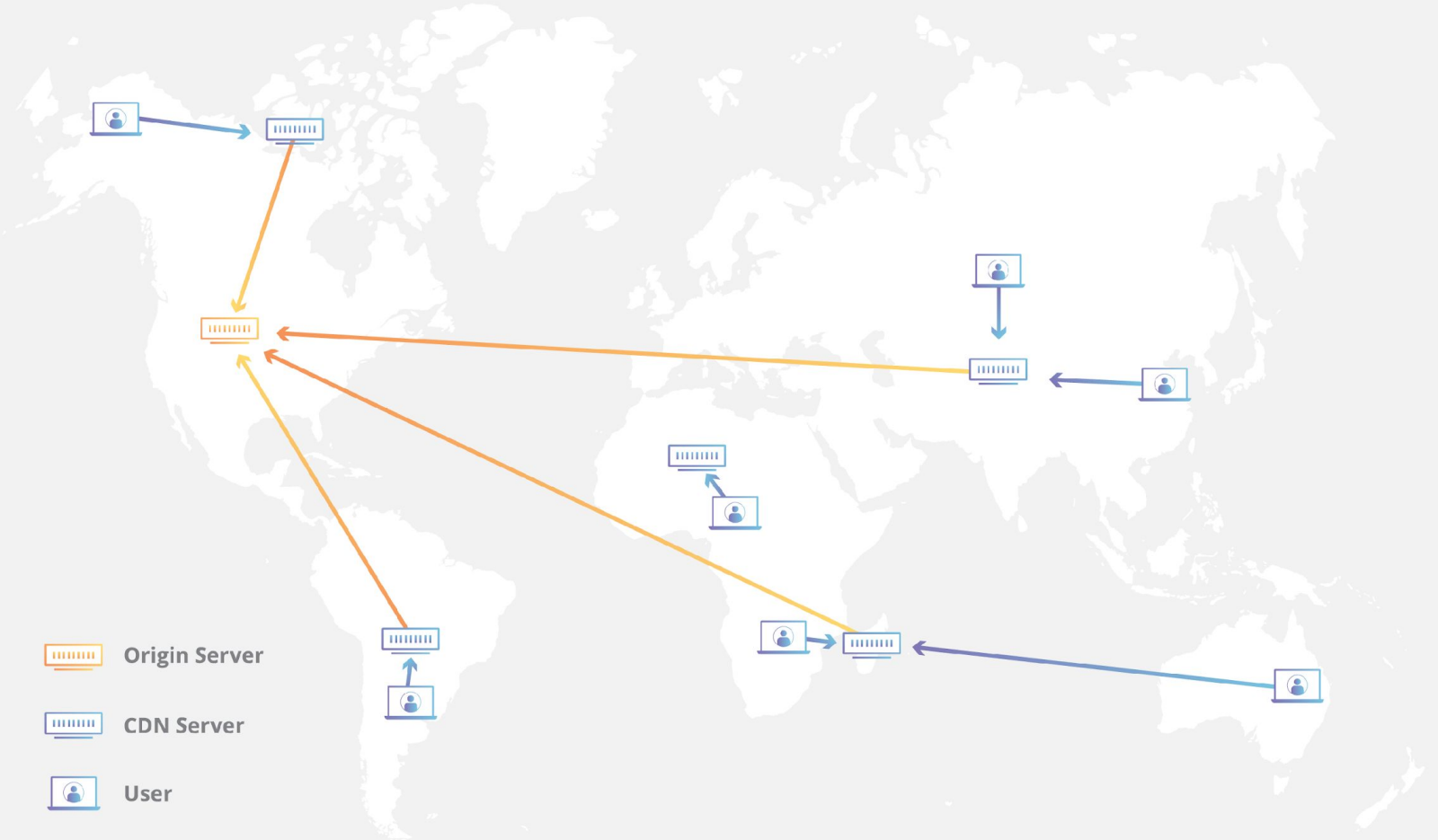
Distribute resources

State-holding attacks

Cleverly reduce state

Computation Attacks

Optimize/disable algorithms



Credit: https://www.cloudflare.com/learning/cdn/what-is-a-cdn/

Volume Attack Mitigation

Distribute resources

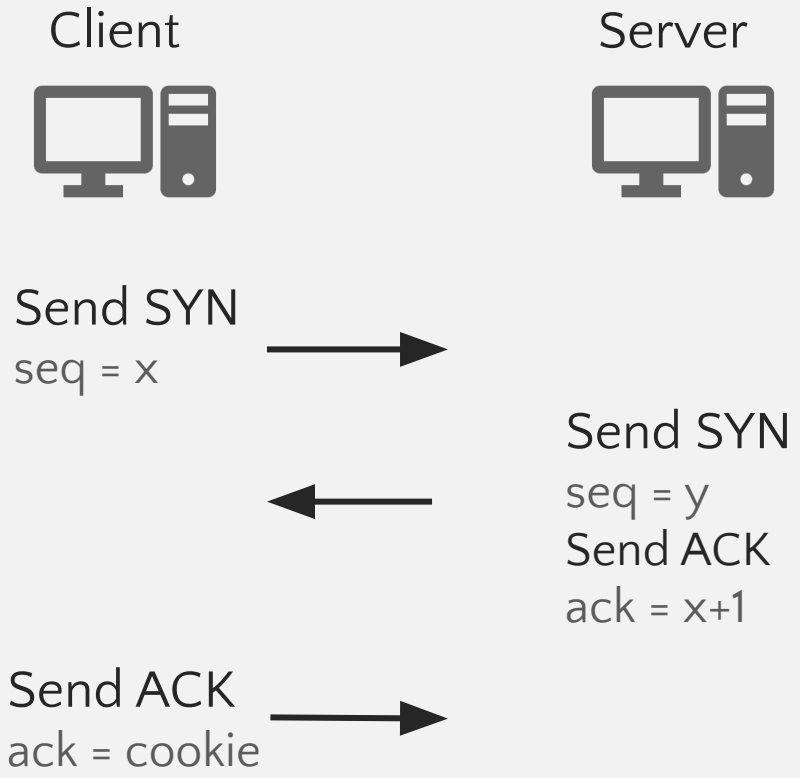
State-holding attacks

Cleverly reduce state

Computation Attacks

Optimize/disable algorithms

Example Mitigation: Syn Cookies Remove State



Syncookie inventor – Dan Bernstein

Syn floods target server keeping state for each SYN.

SYN Cookies replace keeping ACK number state with an encoding of client info

Volume Attack Mitigation

Distribute resources

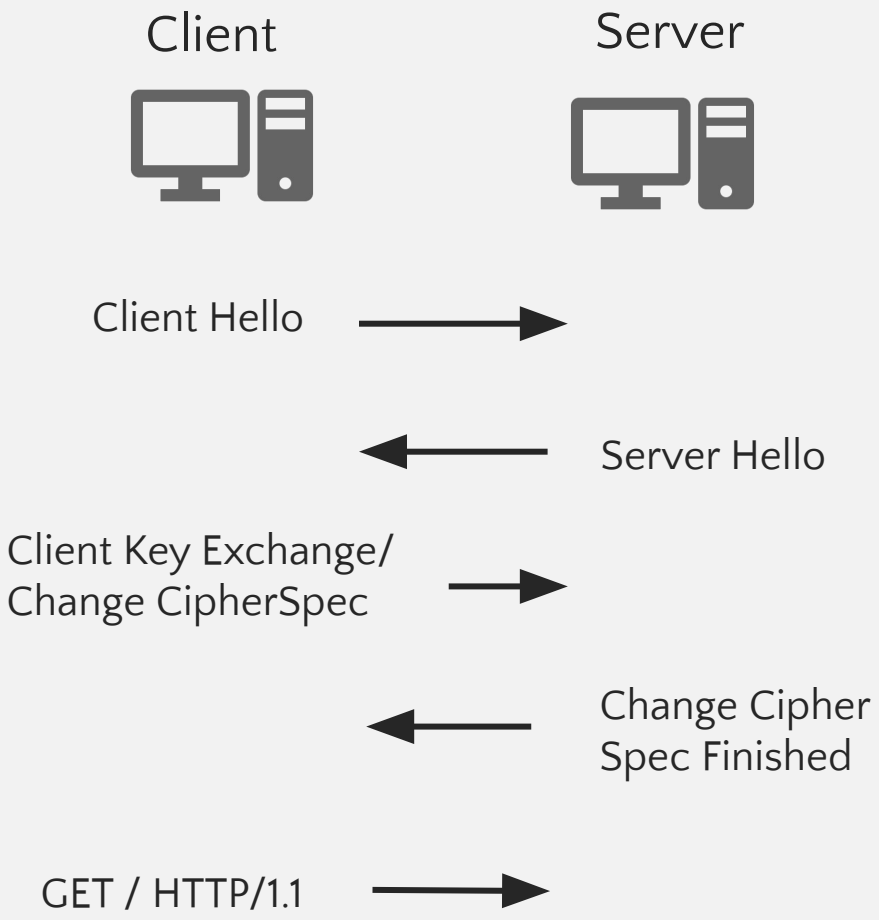
State-holding attacks

Cleverly reduce state

Computation Attacks

Optimize/disable algorithms

Example Mitigation: Disable TLS Renegotiation



Normal SSL/TLS

Fact: RSA Asymmetry

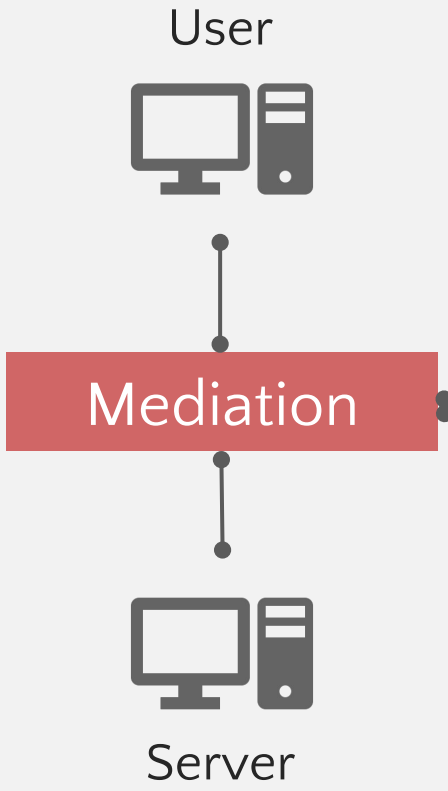
- Public key is 17 bits (65537)
- Secret key is thousands of bits

Attack: TLS allows client to initiate renegotiation, causing huge server computation.

Defense: disable TLS renegotiation, use elliptic curves, etc.

Mediation & Detection

Firewalls & IDS



Types of Mediation

Firewall

Enforce pre-configured access policy

Intrusion Detection System

Passive monitor for violation

Intrusion Prevention System

Block detected violations

Desired Properties

Expressiveness: What kinds of policies can we write?

Effectiveness: How well does it detect attacks while avoiding false positives?

Efficiency: How many resources does it take, and how quickly does it decide?

Ease of use: How much training is necessary? Can a non-security expert use it?

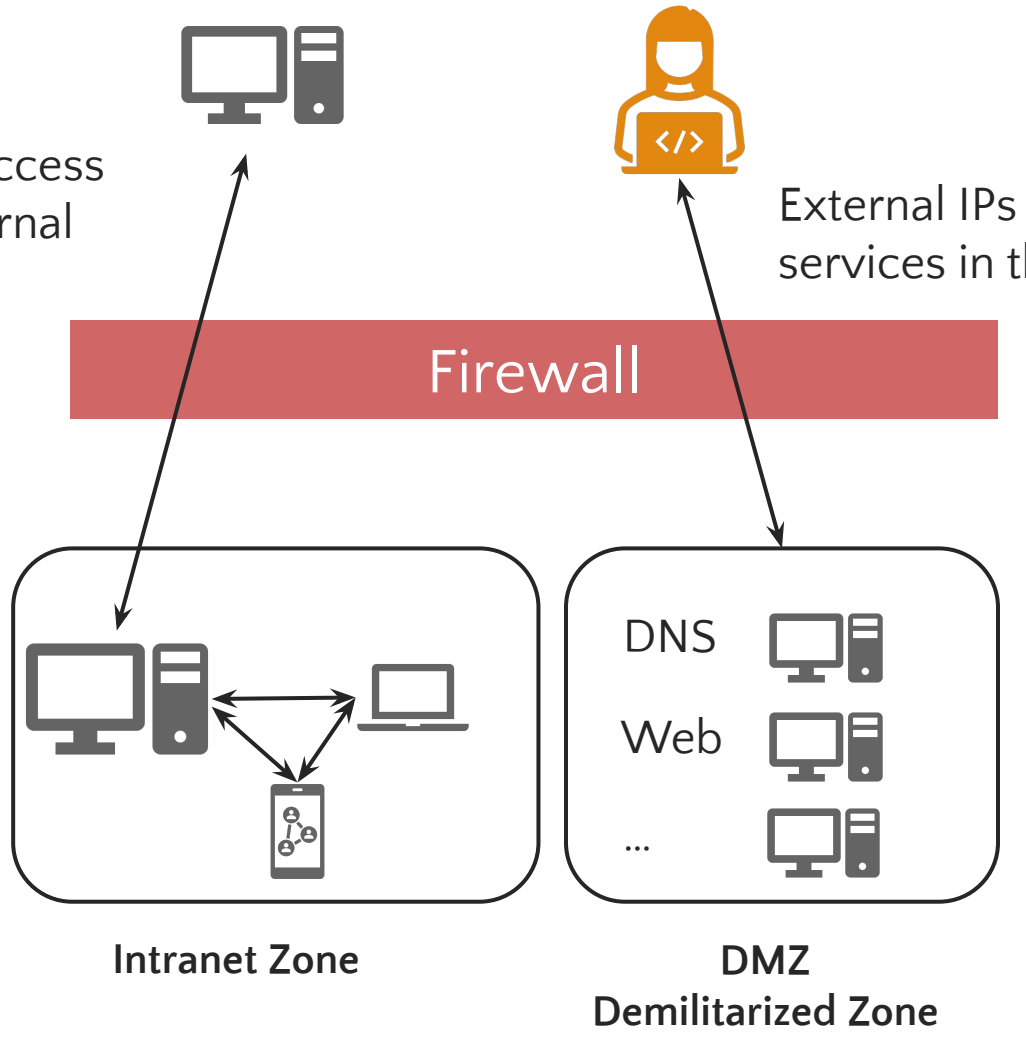
Security: Can the system itself be attacked?

Transparency: How intrusive is it to use?

Trust Zones: Traditional Network Security

Internal devices can access both internal and external resources

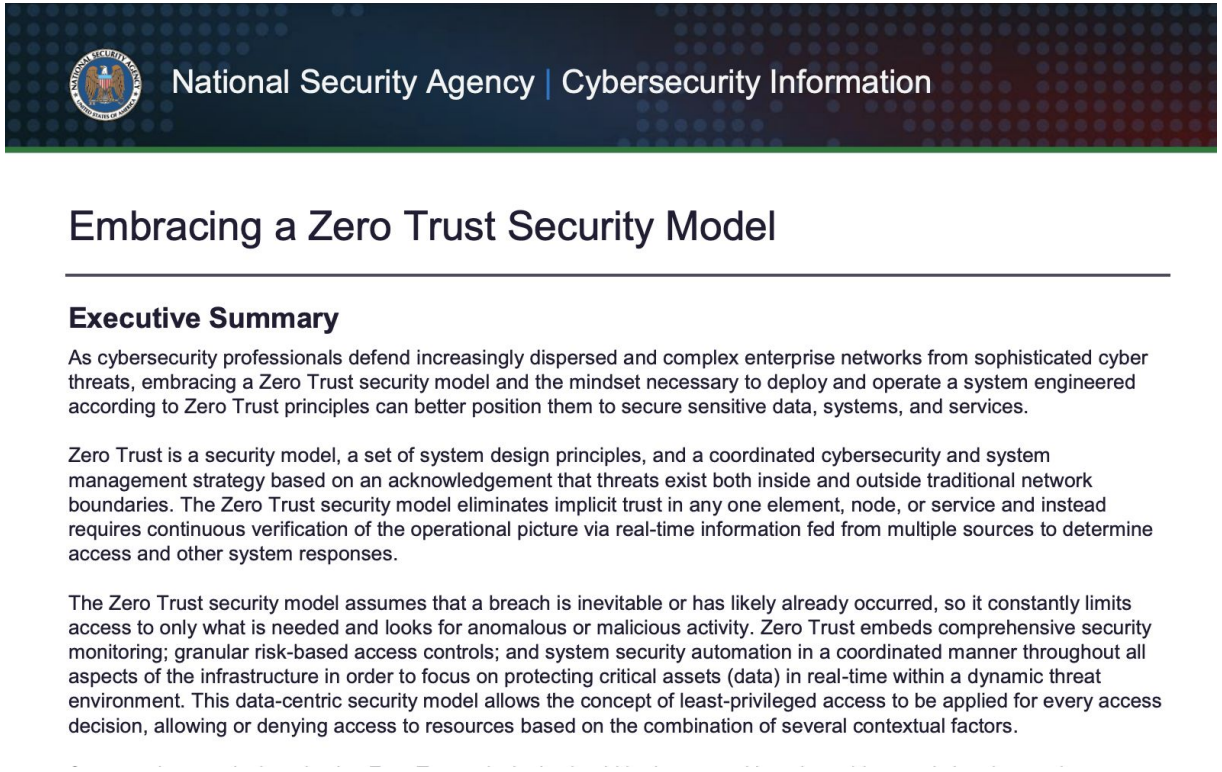
External IPs can only access services in the DMZ



Concept can be extended to any number of trust zones

Zero Trust

[Aka Defense in Depth for networks]



National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

The Zero Trust security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting critical assets (data) in real-time within a dynamic threat environment. This data-centric security model allows the concept of least-privileged access to be applied for every access decision, allowing or denying access to resources based on the combination of several contextual factors.

Zero Trust is a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information fed from multiple sources to determine access and other system responses.

https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Guiding Principles

Always Verify

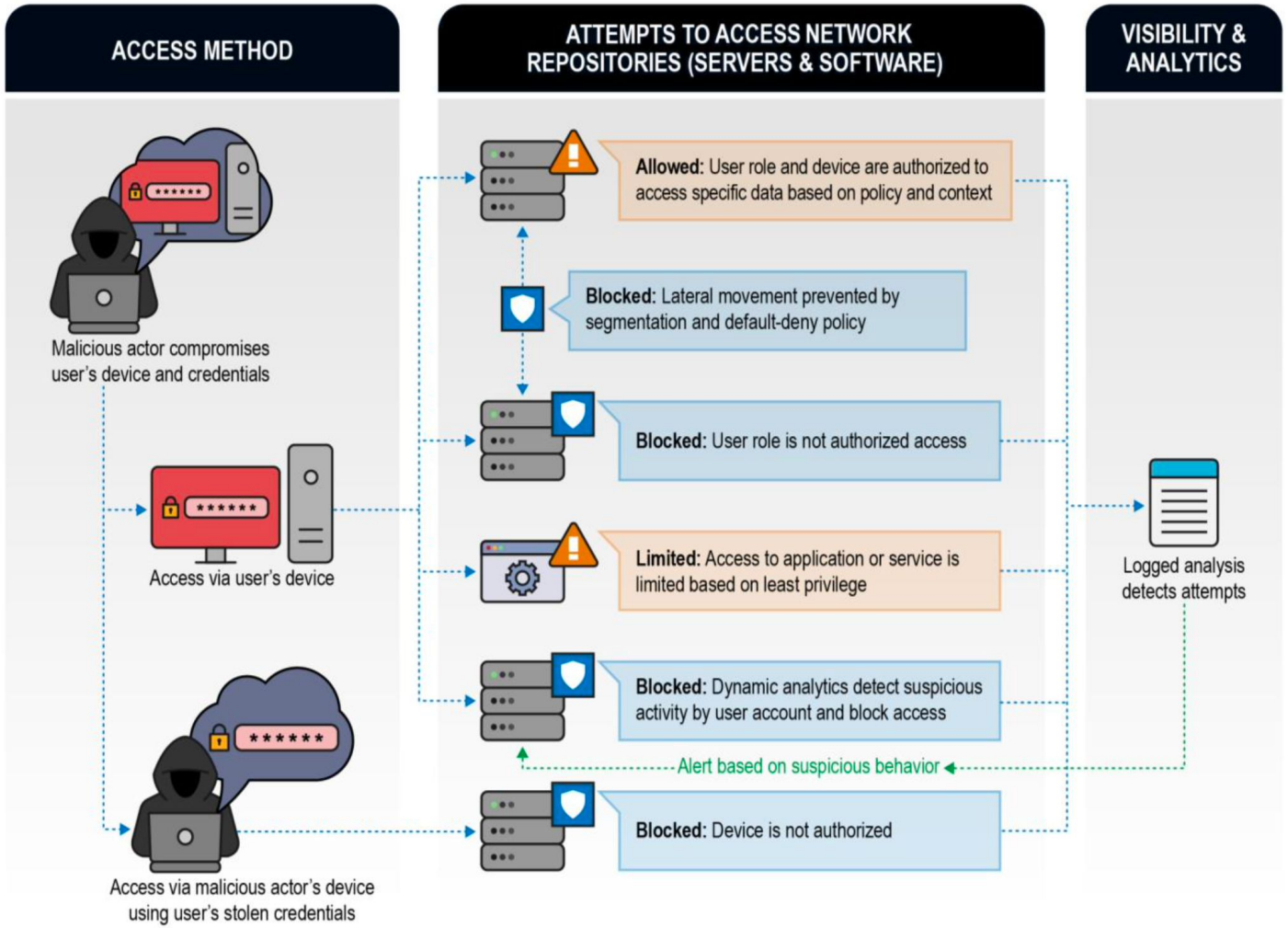
Treat every user, device, application, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege dynamically.

Assume Breach

Assume adversary already inside the network. Deny by default and heavily scrutinize all users for acess. Log, inspect, and monitor for suspicious activity

Verify Explicitly

Access to all resources using multiple attributes (dynamic and static) to derive confidence levels for contextual decisions.



Example of Zero Trust remote exploitation scenarios where most attempts would have been successful in non-Zero Trust environments. Source: NSA Embracing a Zero Trust Security Model

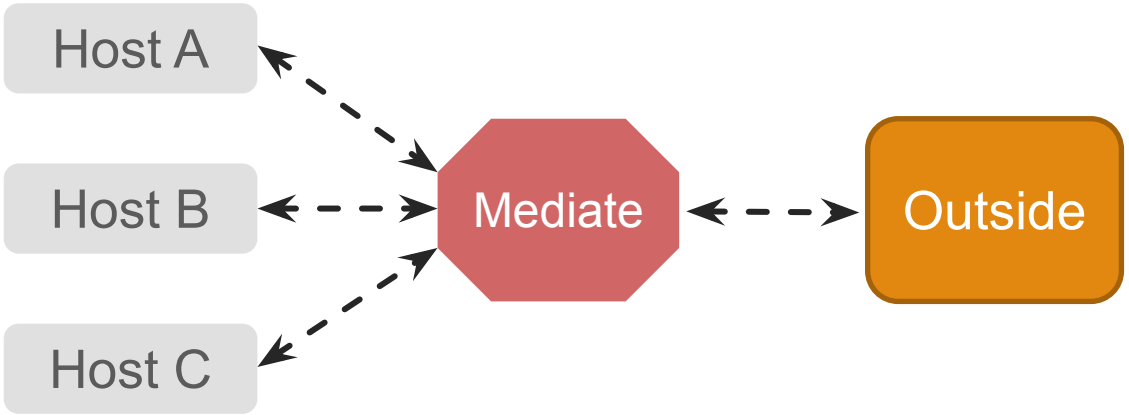
Mediation Placement

Host-based Mediation

Pros:
- Faithful to host state
- Faithful to local config
- Travels with you

Cons:
- No network correlation
- Must be installed, configured, maintained on every host

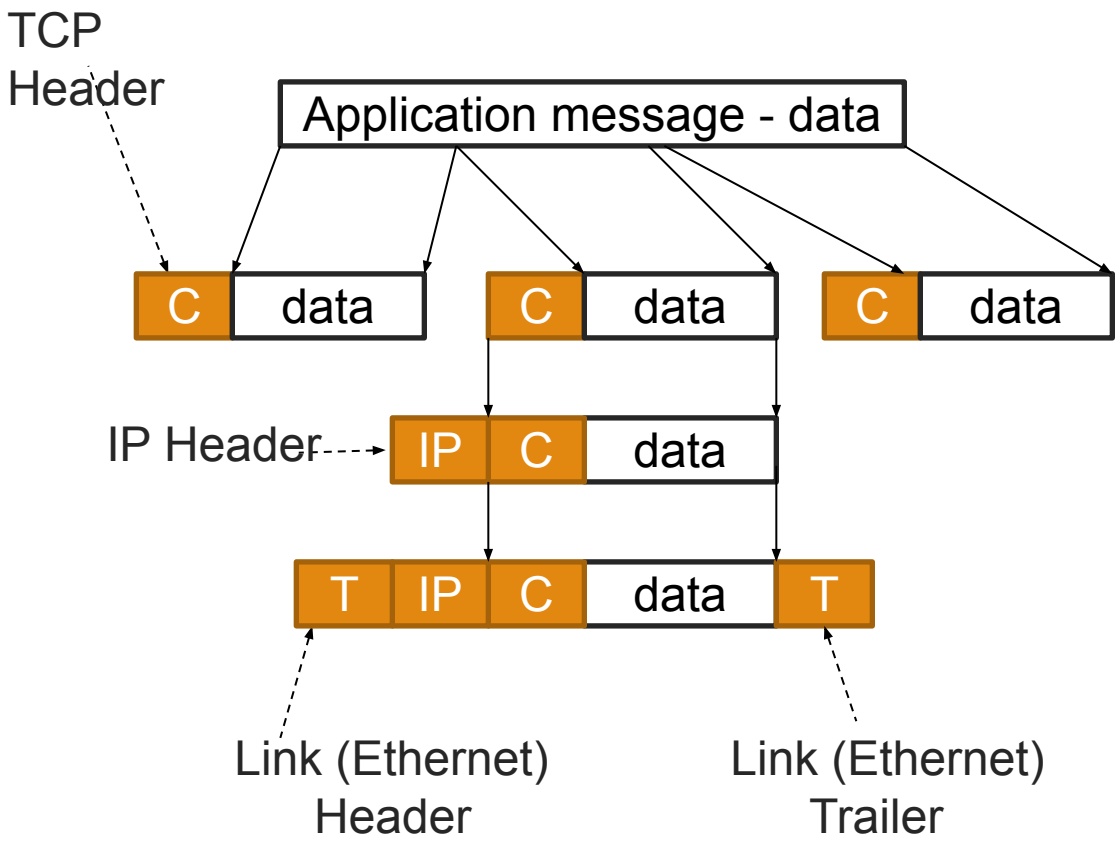
Network-Based Firewall



Pros:
- Correlate among nodes
- Protect every host

Cons:
- Unknown host app state
- Replicate host network state

Mediation State



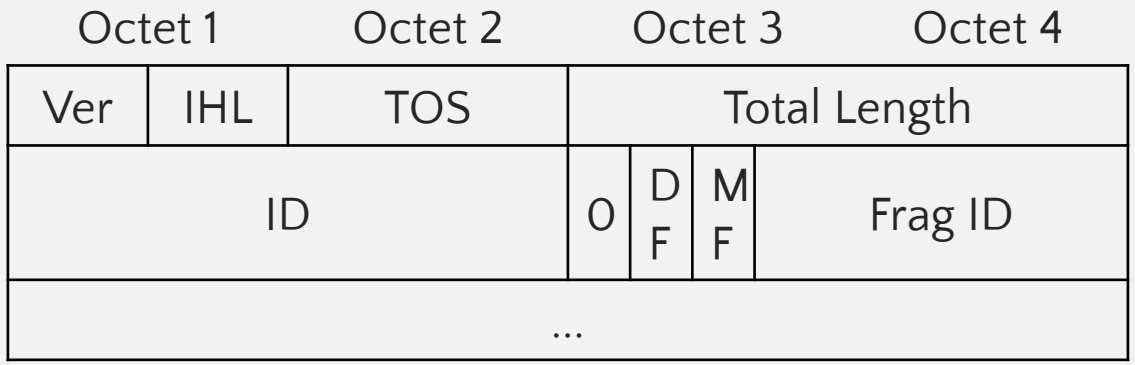
Filter by packet fields. Less expensive, lower fidelity

- IP (src, dst)
- Protocol (tcp, udp)
- Flags (SYN, ACK)
- Payload up to a single packet

Add storage across packets. More expensive, higher fidelity

- Replicate host sessions
- Sessions
- Session data

Example State: IP Fragments



DF : Don't fragment (0 = May, 1 = Don't)
MF: More fragments (0 = Last, 1 = More)
Frag ID = Octet number

IP Hdr	DF=0	MF=1	ID=0	Frag 1	Data chunk 1
IP Hdr	DF=0	MF=1	ID=n	Frag 2	Data chunk 2
IP Hdr	DF=1	MF=0	ID=2n	Frag 3	Data chunk 3

Mediate

Network-based mediator needs to reconstruct data from chunks. Difficult to be faithful to hosts behavior.

Quiz Question

What is one ***ADVANTAGE*** of a network protocol-layer firewall ***OVER*** an application firewall?

A. Protocol-layer firewalls can protect traffic for many different applications

B. Protocol-layer firewalls operate at a higher layer in the network stack

C. Protocol-layer firewalls never need to keep state

D. Protocol layer firewalls have cooler names

Quiz Question

What is one ***ADVANTAGE*** of an application protocol-layer firewall ***OVER*** a network firewall?

A. Application layer firewalls can correlate among hosts on the network

B. Application layer do not need to replicate network state

C. Application layer can see full TCP/IP information

D. Application layer firewalls are easier to keep up to date

A tool worth knowing: Wireshark

https://www.wireshark.org/

Other handy tools: nmap, traceroute, tcpdump, snort etc

Rule vs. Anomaly Detection

Rule-based

Pre-configured rules determine malice.

Examples: regular expressions of known exploits,

Cryptographic hash of malware

Detect any fragments less than 256 bytes
alert tcp any any -> any any (minfrag: 256; msg:
"Tiny fragments detected, possible hostile activity";)
Detect IMAP buffer overflow
alert tcp any any -> 192.168.1.0/24 143
(content: "|90C8 C0FF FFFF|/bin/sh";
msg: "IMAP buffer overflow!";)

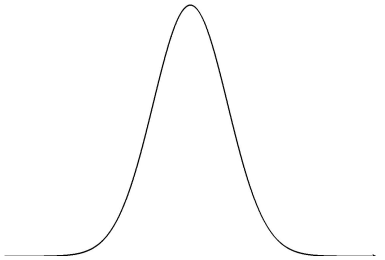
Snort Rule Example

Anomaly

Alert on deviations from the norm

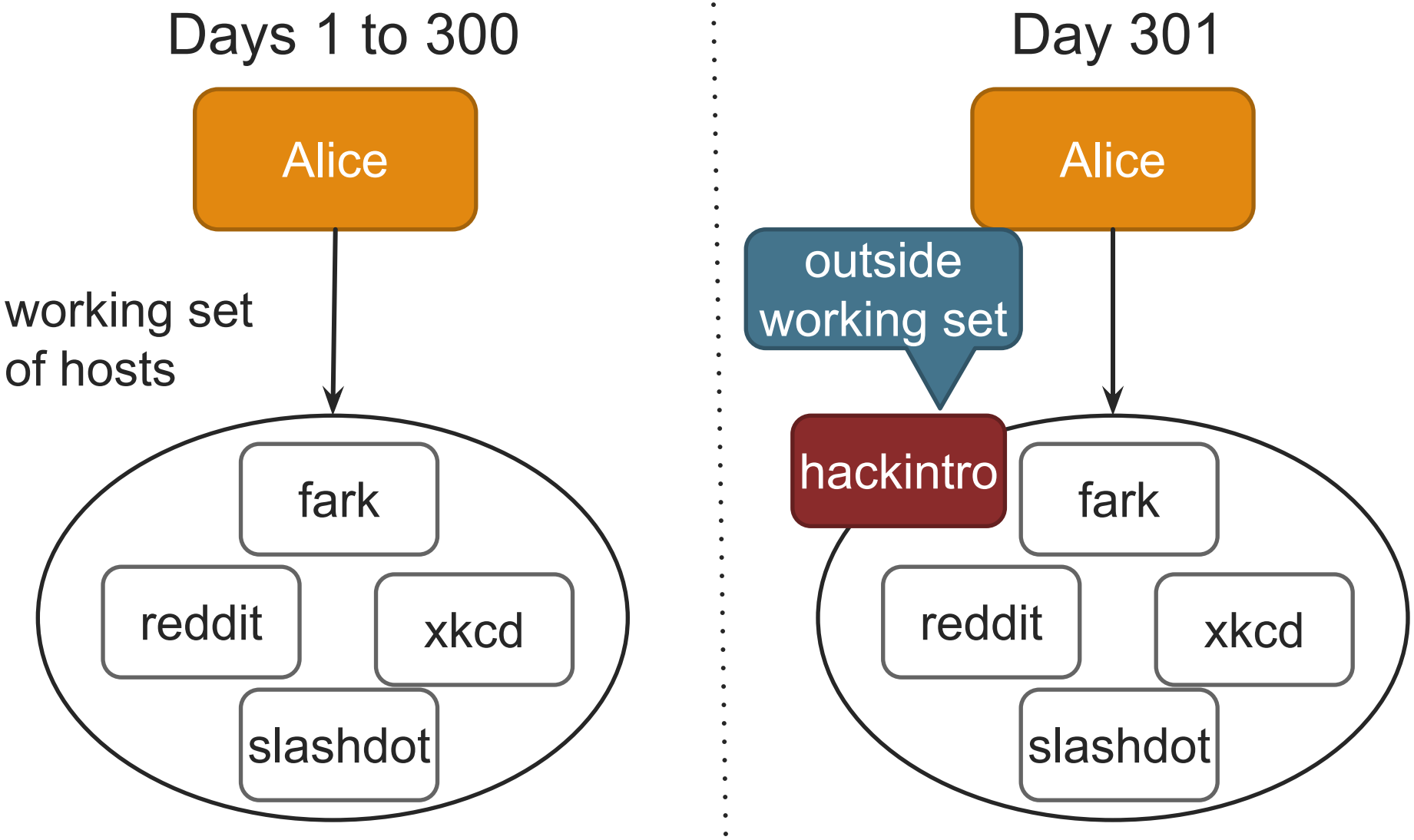
Examples: usual host connections,

unusual packet size, unusual packet data



Normal distribution of events

Anomaly Example: Working Sets



Ευχαριστώ και καλή μέρα εύχομαι!

Keep hacking!