

Διάλεξη #21 - Network Security

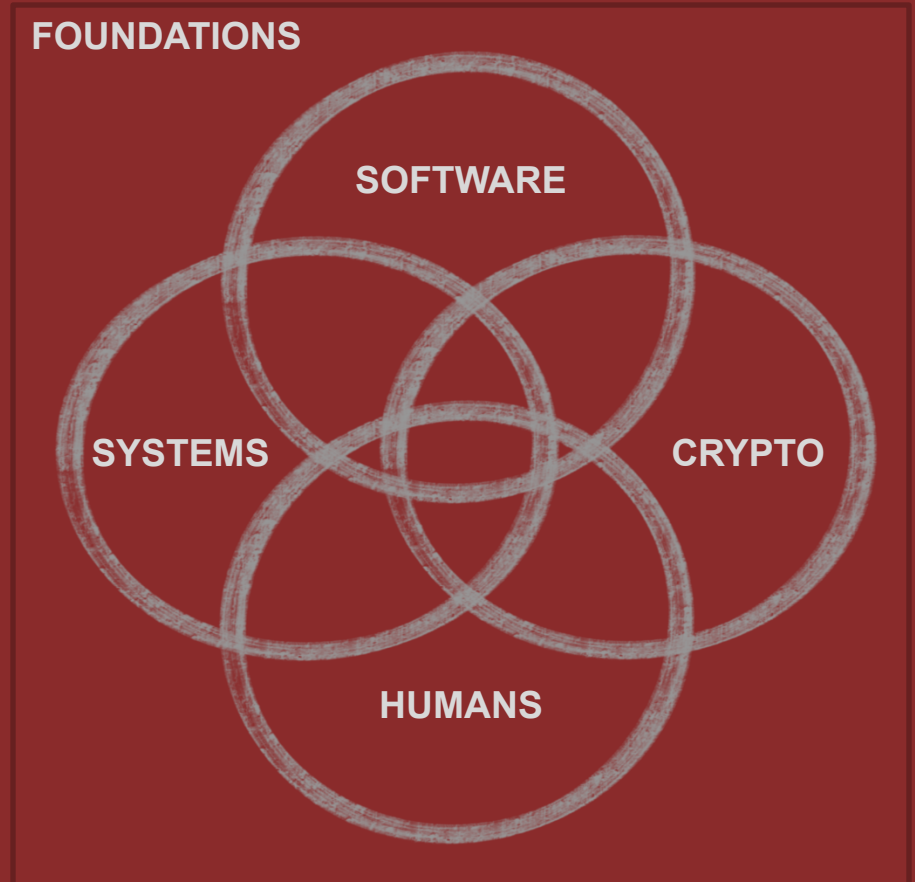
Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών

Εισαγωγή στην Ασφάλεια

Θανάσης Αυγερινός



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



Ανακοινώσεις / Διευκρινίσεις

- Attack Defense competition:
 - what to expect?

Την προηγούμενη φορά

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



Σήμερα

- Networks 101
- Scanning
- Firewalls
- Base Rate Fallacy

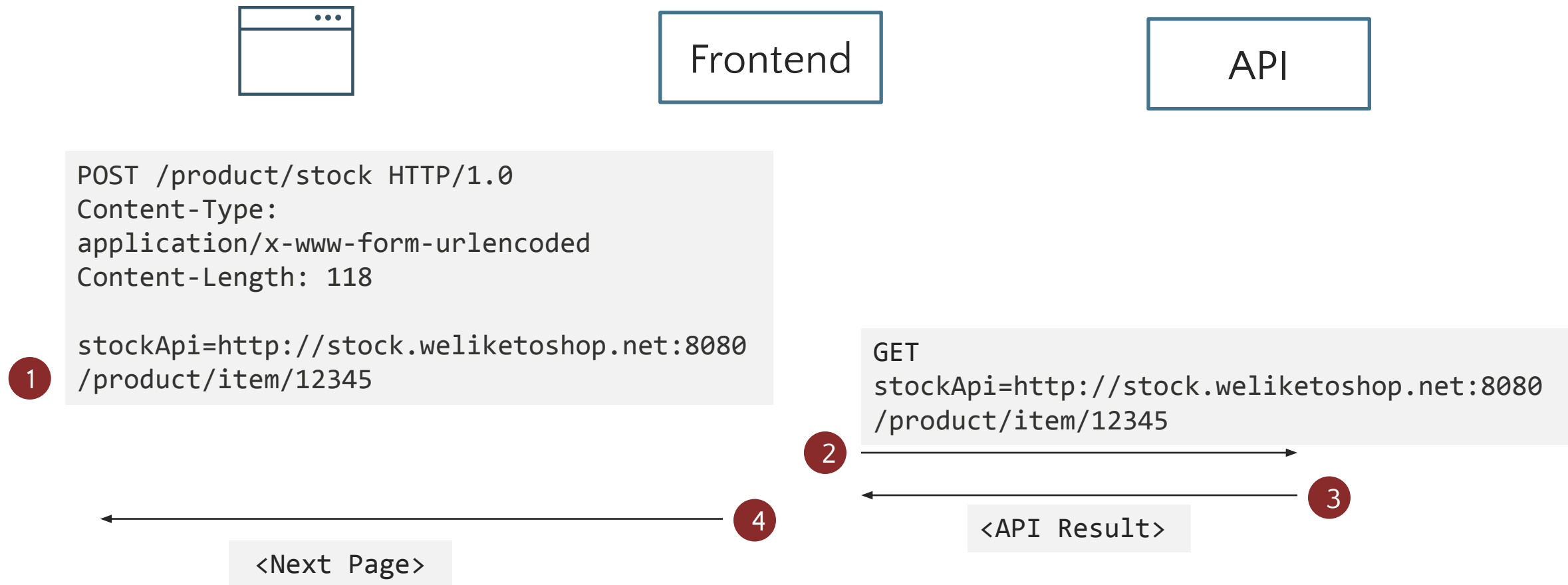




Server Side Request Forgery (SSRF)

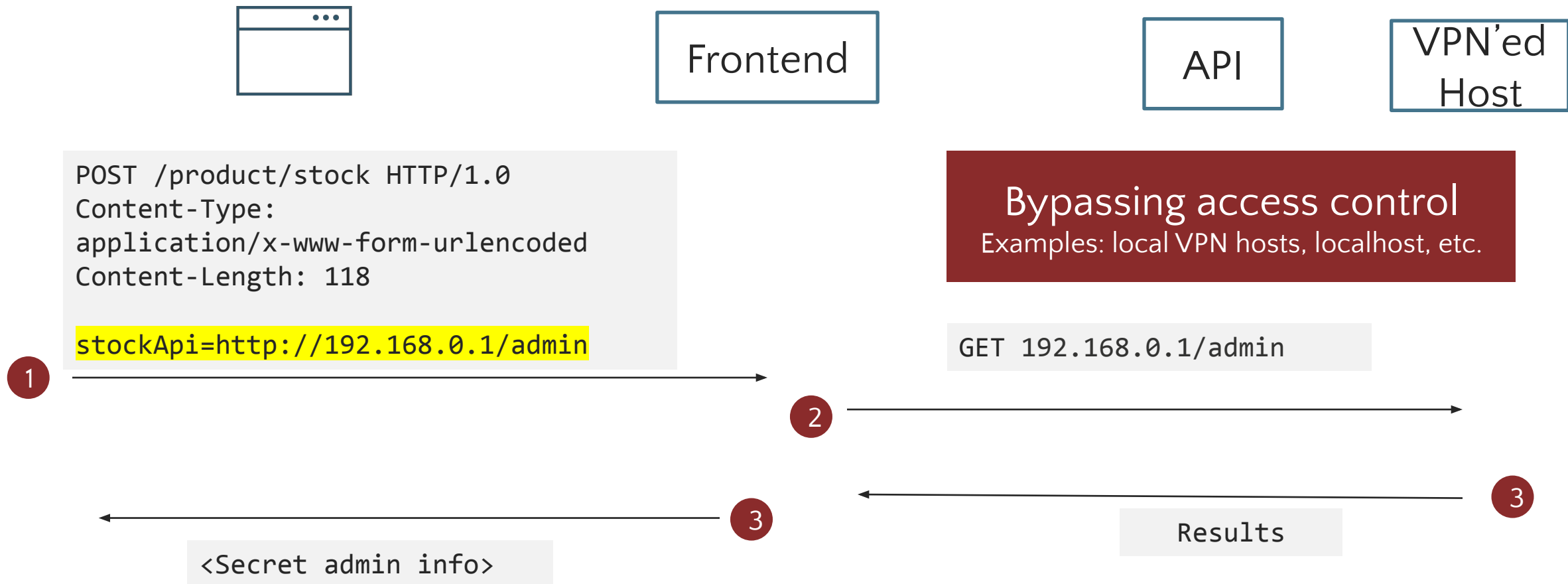
Server Side Requests

Modern websites are composed of several smaller services.



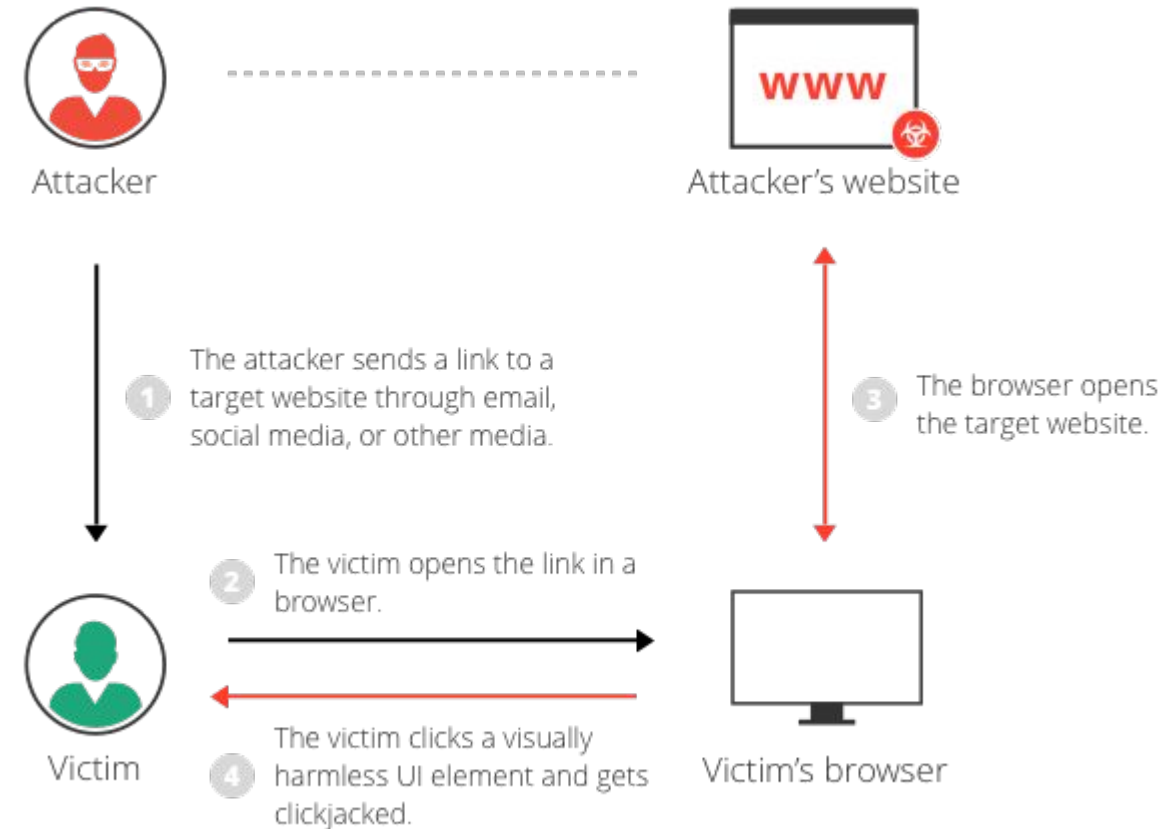
Server Side Requests

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



More Popular Web Attacks

- Insecure Direct Object References (IDOR)
 - Predictable URLs allow unauthorized access to data. Example:
 - http://example.com/user/42/credit_card_info
- Insecure Deserialization
 - Malicious serialized input triggers remote code execution.
- Clickjacking
 - Trick users into clicking UI elements
- And many more, misconfiguration, XXE, etc





Networks 101

Five Key Aspects of Networking



Data communications: bits over signals



Networks: Packets over bits



Internets: Datagrams over packets

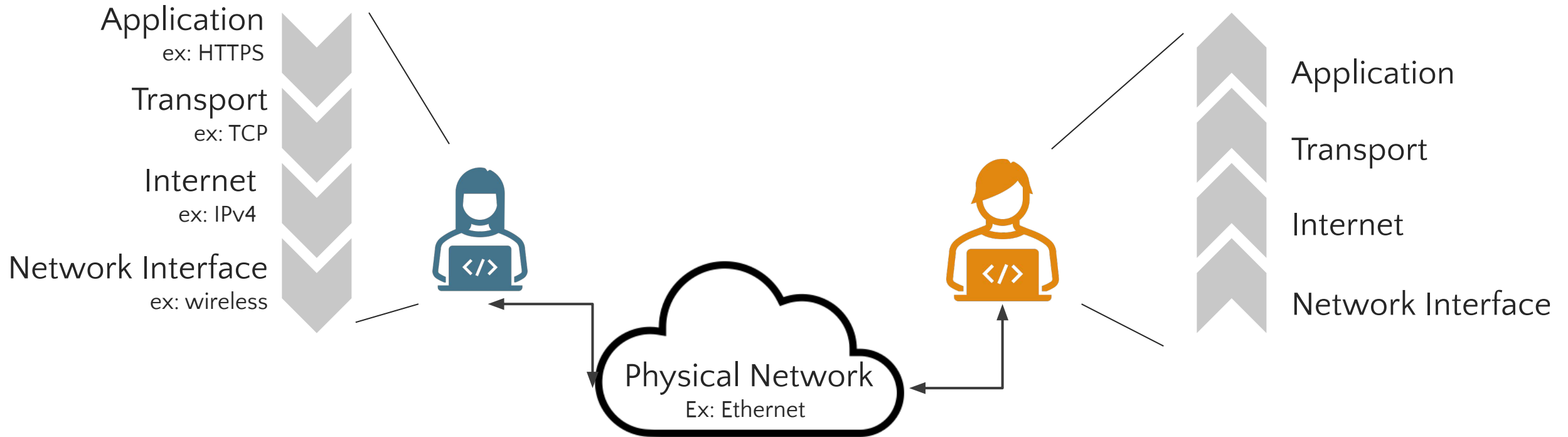


Network programming: Application data over the Internet



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

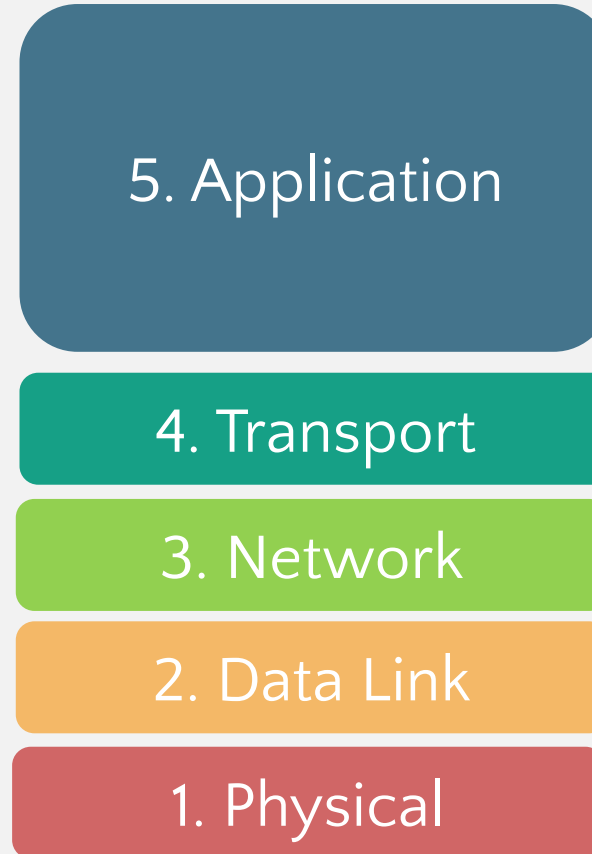
Network Layers



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.

Protocol Example: BGP

5. Application

4. Transport

3. Network

2. Data Link

1. Physical

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.

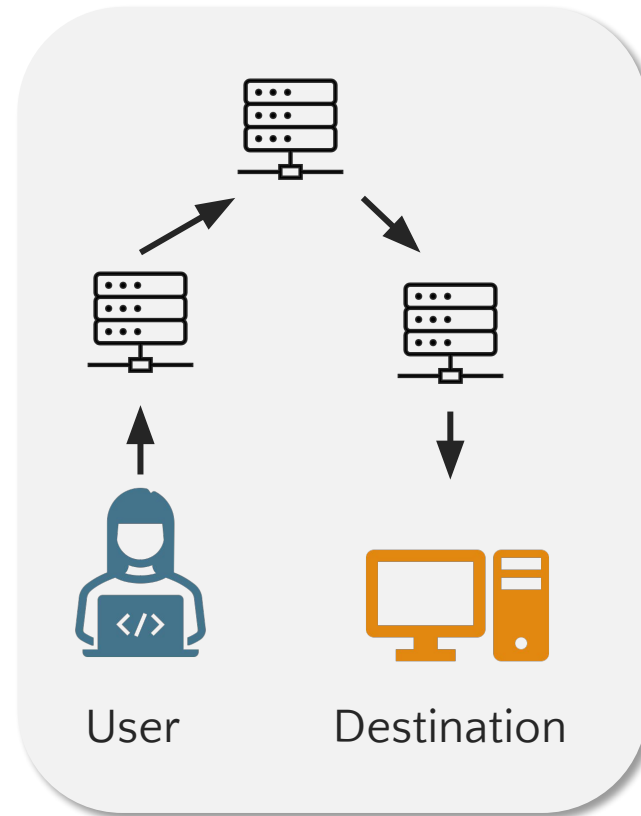
Operates at: Transport layer
Controls: Network layer

Crypto Exchange KLAYswap Loses \$1.9M After BGP Hijack

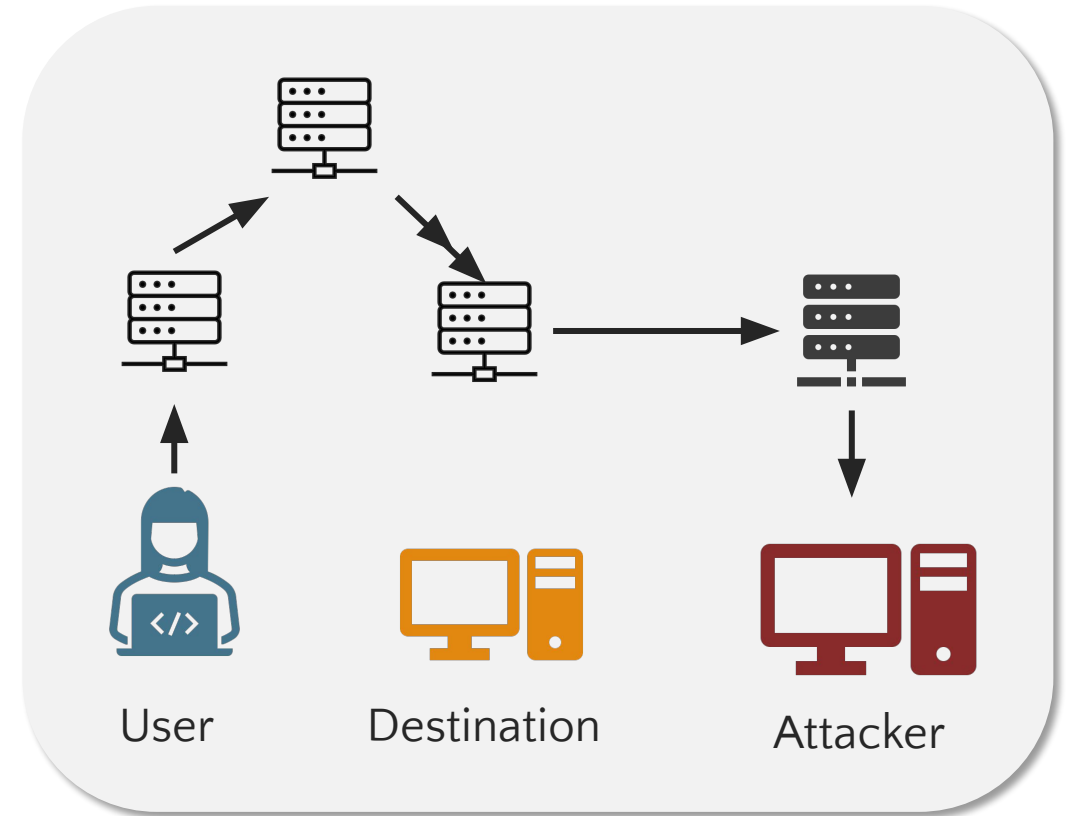
Hackers Performed Border Gateway Protocol Hack to Conduct Illegal Transactions

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

5. Application

4. Transport

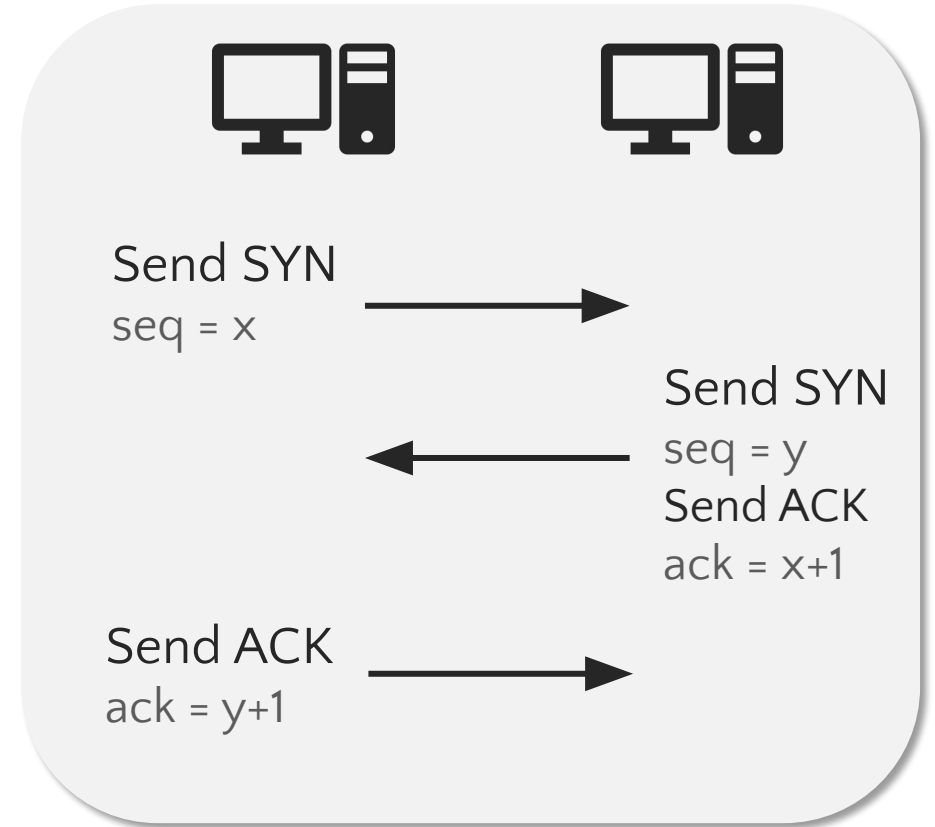
3. Network

2. Data Link

1. Physical

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

webfig@iP:Web_Proxy	
Apply Clear Cache Reset HTML Access Cache Direct Connections Cache Contents	
running	
Enabled <input checked="" type="checkbox"/>	
Src. Address	::
Port	5566
Anonymous	<input type="checkbox"/>
Parent Proxy	::
Parent Proxy Port	
Cache Administrator	
Max. Cache Size	unlimited
Max Cache Object Size	2048
Cache On Disk	<input type="checkbox"/>
Max. Client Connections	600
Max. Server Connections	600

input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	5.59348->20	4:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	126:60250->	114:5566, len 52
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	126:60246->	114:5566, len 52
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	2:58000->20	4:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	105:33496->	114:5678, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	3.241:48520-	2.114:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	3.147:57702-	2.114:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	1.241:37312-	2.114:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	:50462->201	5:566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	17:40066->2	14:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	105:33970->	114:5678, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	4:37624->20	4:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	4:48324->20	4:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	209:34152->	114:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	:50882->201	:5:566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	1.241:53550-	2.114:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	82:40550->2	14:5566, len 60
input: in.ether1 out:(none), src-mac ec:	:39, proto TCP (SYN),	7:40432->20	4:5566, len 60

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.cnn.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?

←

→

↺

shodan.io/search?query=lighttpd-1.4.15

🔗

☆

🔴

🔧

☁

⚙

📄


👤

401 - Unauthorized

88.31.205.91

91.red-88-31-205.dynamicip.rima-tde.net

TELEFONICA DE ESPANA

 Spain, Barcelona

🔒 **SSL Certificate**

Issued By:
|- Organization:
Dr. Neuhaus
Telekommunikation GmbH

Issued To:
|- Organization:
Dr. Neuhaus
Telekommunikation GmbH

Supported SSL Versions:
SSLv2, SSLv3, TLSv1

HTTP/1.1 401 Unauthorized

WWW-Authenticate: Digest realm="Tainy E/HMOD", nonce="b9283c60097cc56f9c88aea377271144", qop="auth"

Content-Type: text/html

Content-Length: 351

Date: Wed, 23 Mar 2022 19:23:29 GMT


Server: lighttpd/1.4.15

2022-03-23T19:23:33.325303

401 - Unauthorized

2.196.163.60

Telecom Italia Mobile

 Italy, Naples

🔒 **SSL Certificate**

Issued By:
|- Organization:
Siemens AG

Issued To:
|- Organization:
Siemens AG

Supported SSL Versions:
SSLv2, SSLv3, TLSv1

HTTP/1.1 401 Unauthorized

WWW-Authenticate: Digest realm="SINAUT MD741-1", nonce="75b23a369dc9f140229f4127172f7764", qop="auth"

Content-Type: text/html


Content-Length: 351

Date: Sun, 19 Dec 2021 02:43:34 GMT

Server: lighttpd/1.4.15

2022-03-23T18:27:22.315991

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

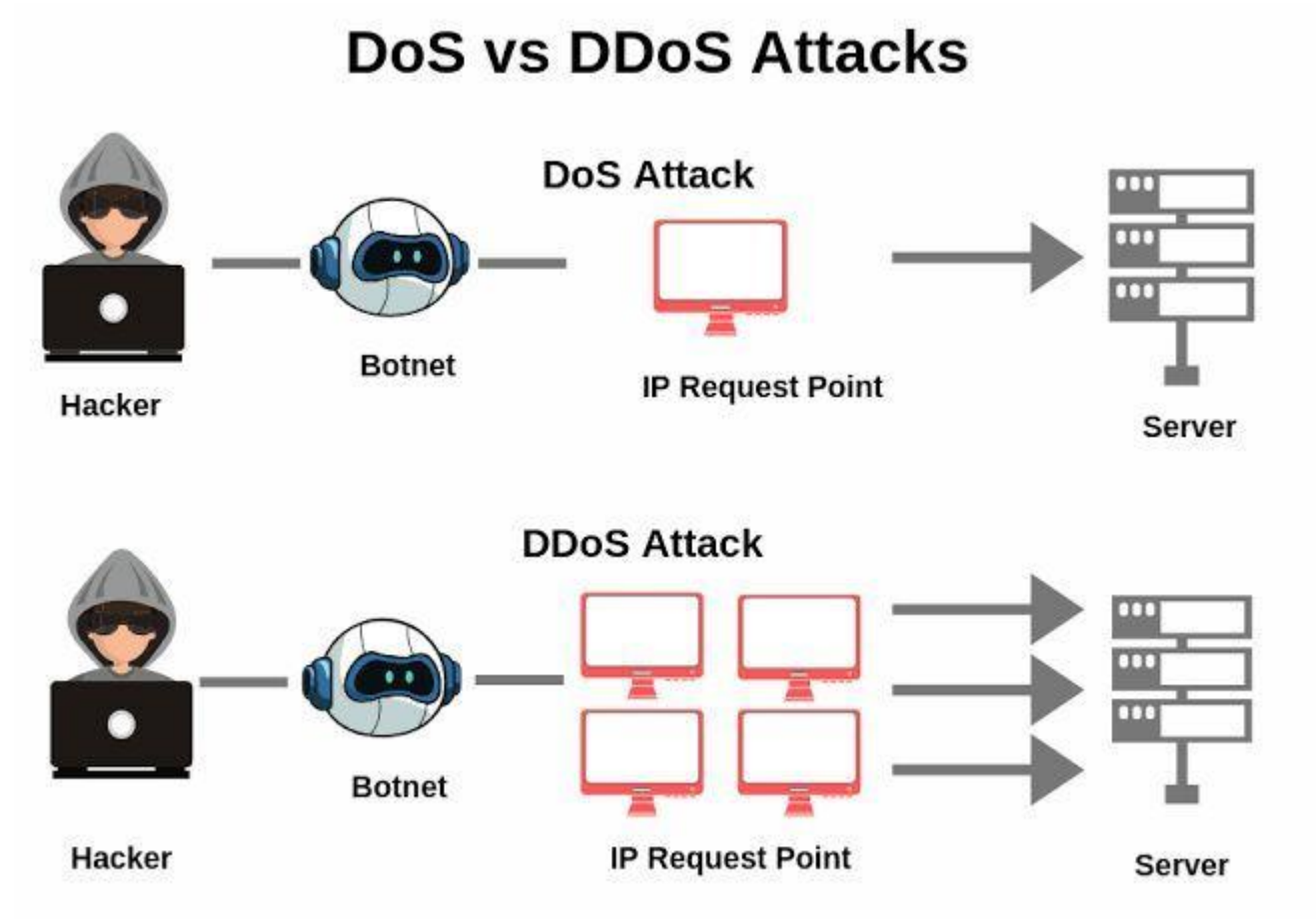


Network
ICMP “ping” flood, “smurf attack”,
“ping-of-death”



Data link
Ethernet exponential backoff attacks,
WEP disassociation attacks

DOS vs DDOS



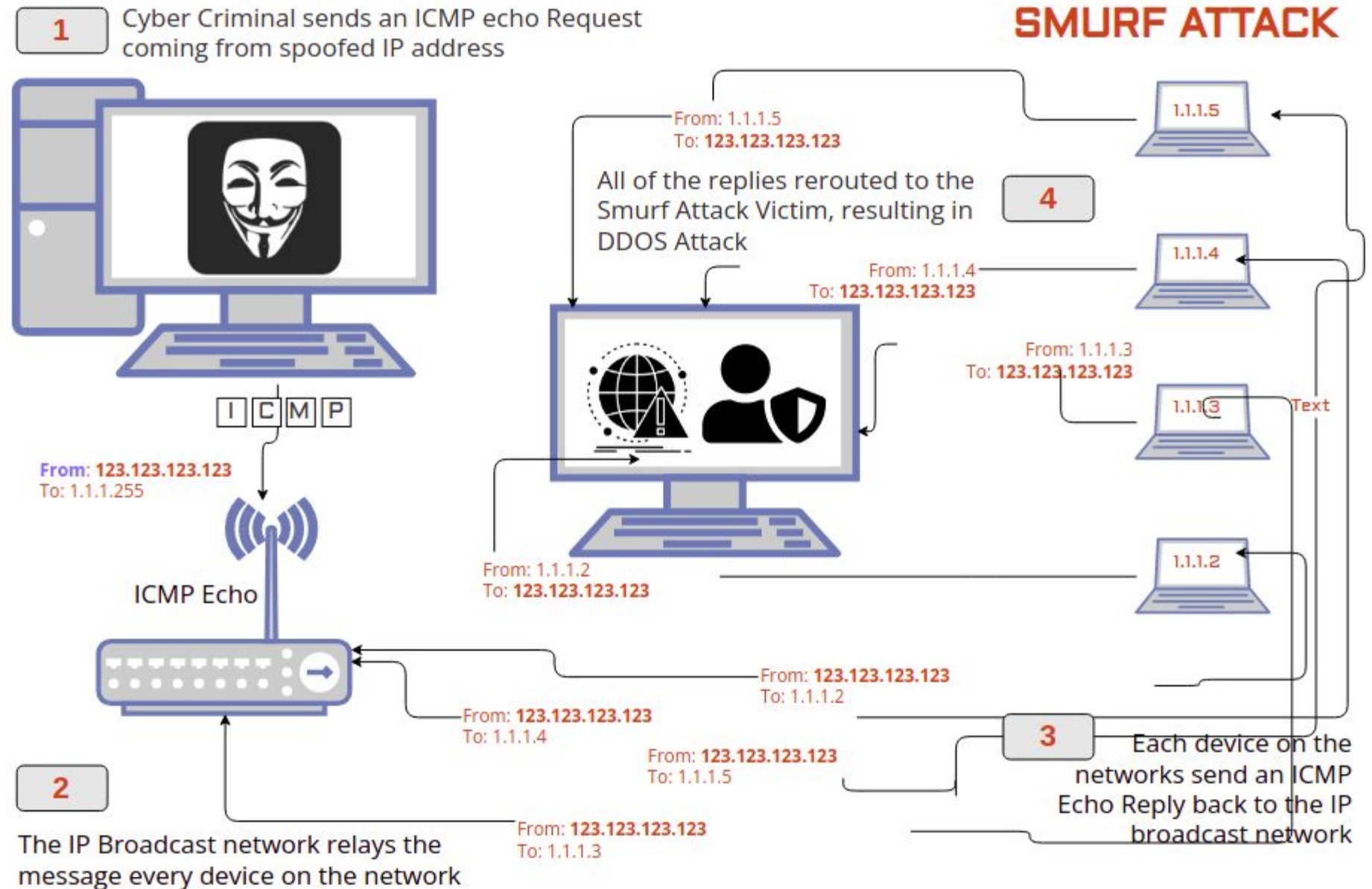
Important DoS Concepts: Amplification and Spoofing

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

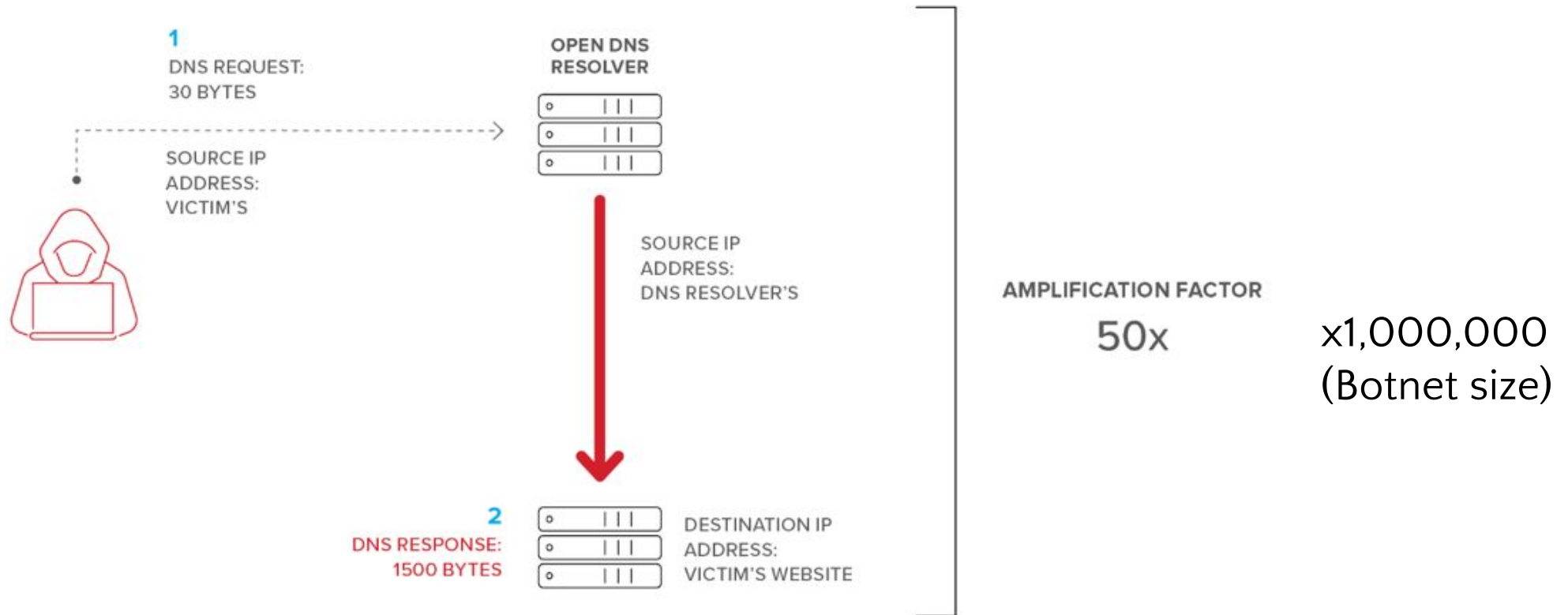
An amplification factor of 100, for example, means that an attacker could manage to create 100 Mb/s of traffic using just 1 Mb/s of its own bandwidth.

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



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.

Example Mitigation: Content distribution network (CDN)

Volume Attack Mitigation

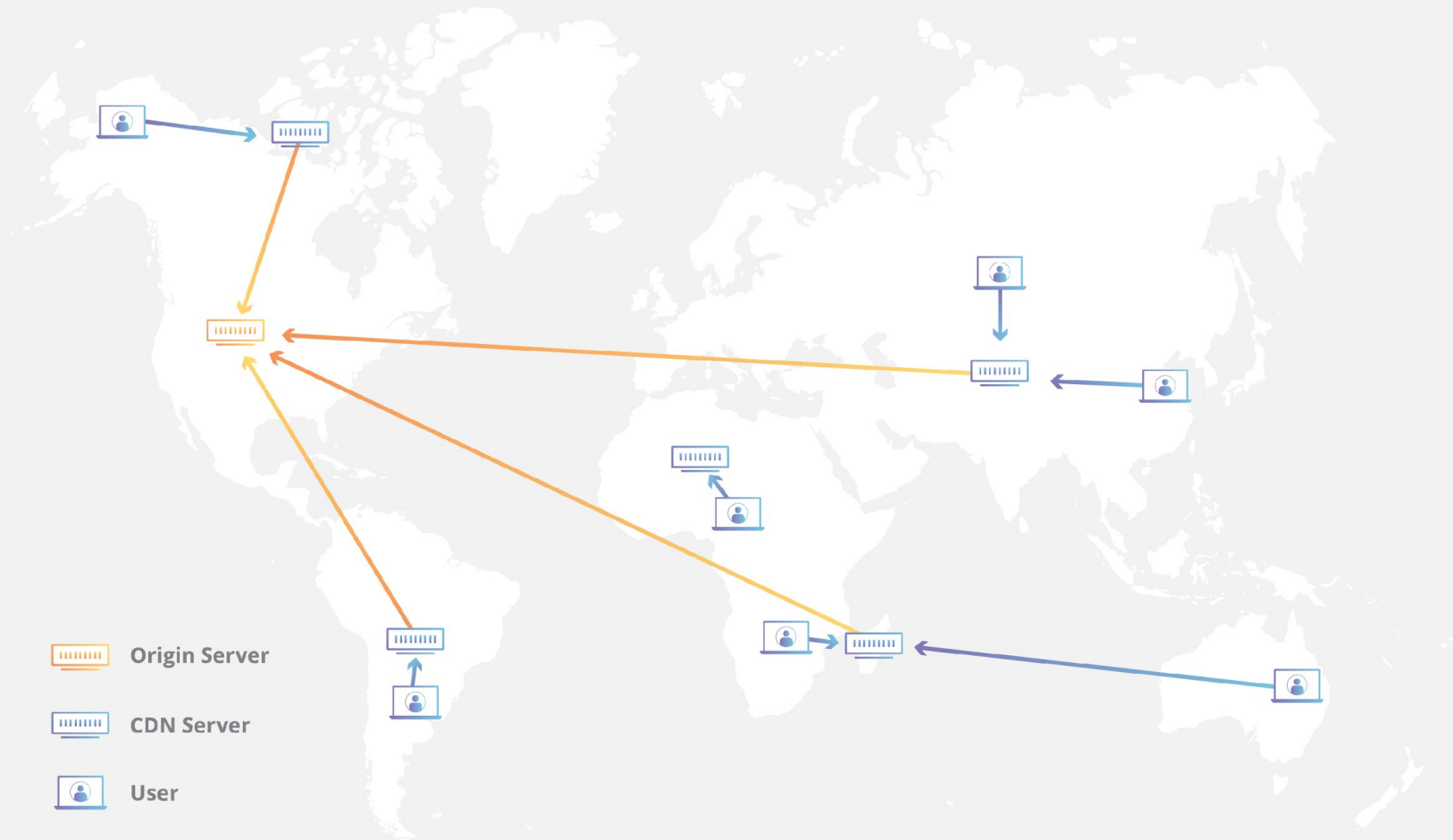
Distribute resources

State-holding attacks

Cleverly reduce state

Computation Attacks

Optimize/disable algorithms



Example Mitigation: Syn Cookies Remove State

Volume Attack Mitigation

Distribute resources

State-holding attacks

Cleverly reduce state

Computation Attacks

Optimize/disable algorithms

Client



Send SYN
seq = x

Server



Send SYN
seq = y
Send ACK
ack = x+1

Send ACK
ack = cookie

Syn floods target server keeping state for each SYN.

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

Example Mitigation: Disable TLS Renegotiation

Volume Attack Mitigation

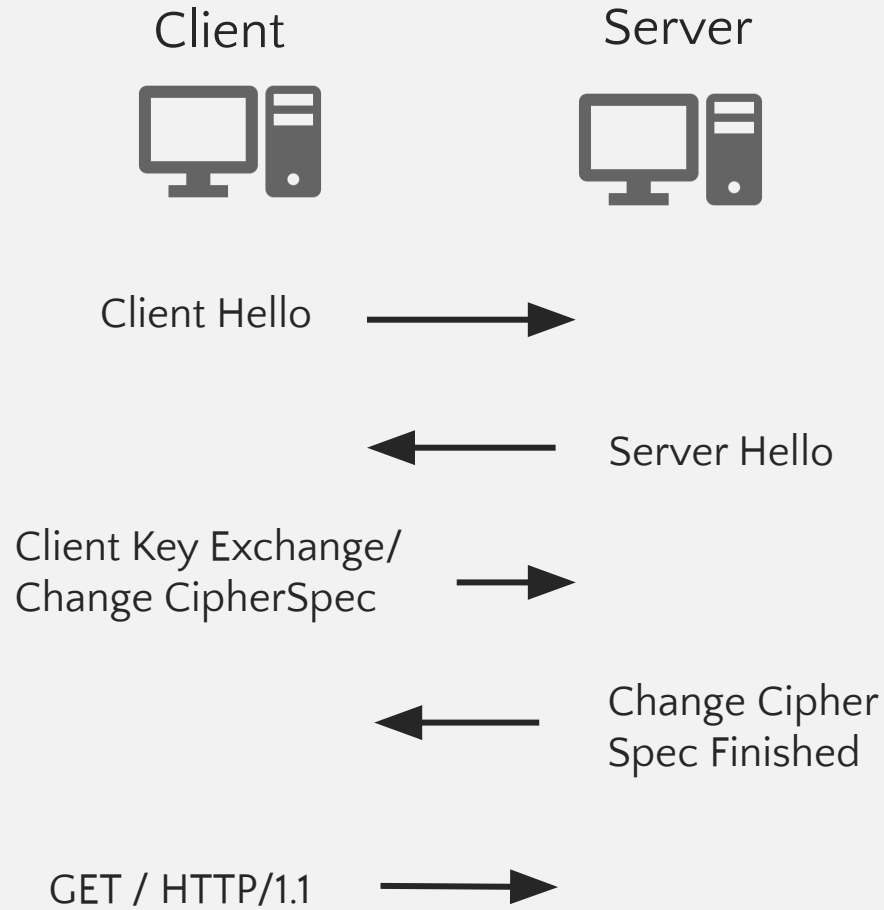
Distribute resources

State-holding attacks

Cleverly reduce state

Computation Attacks

Optimize/disable algorithms



Normal SSL/TLS

Fact: RSA Asymmetry

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

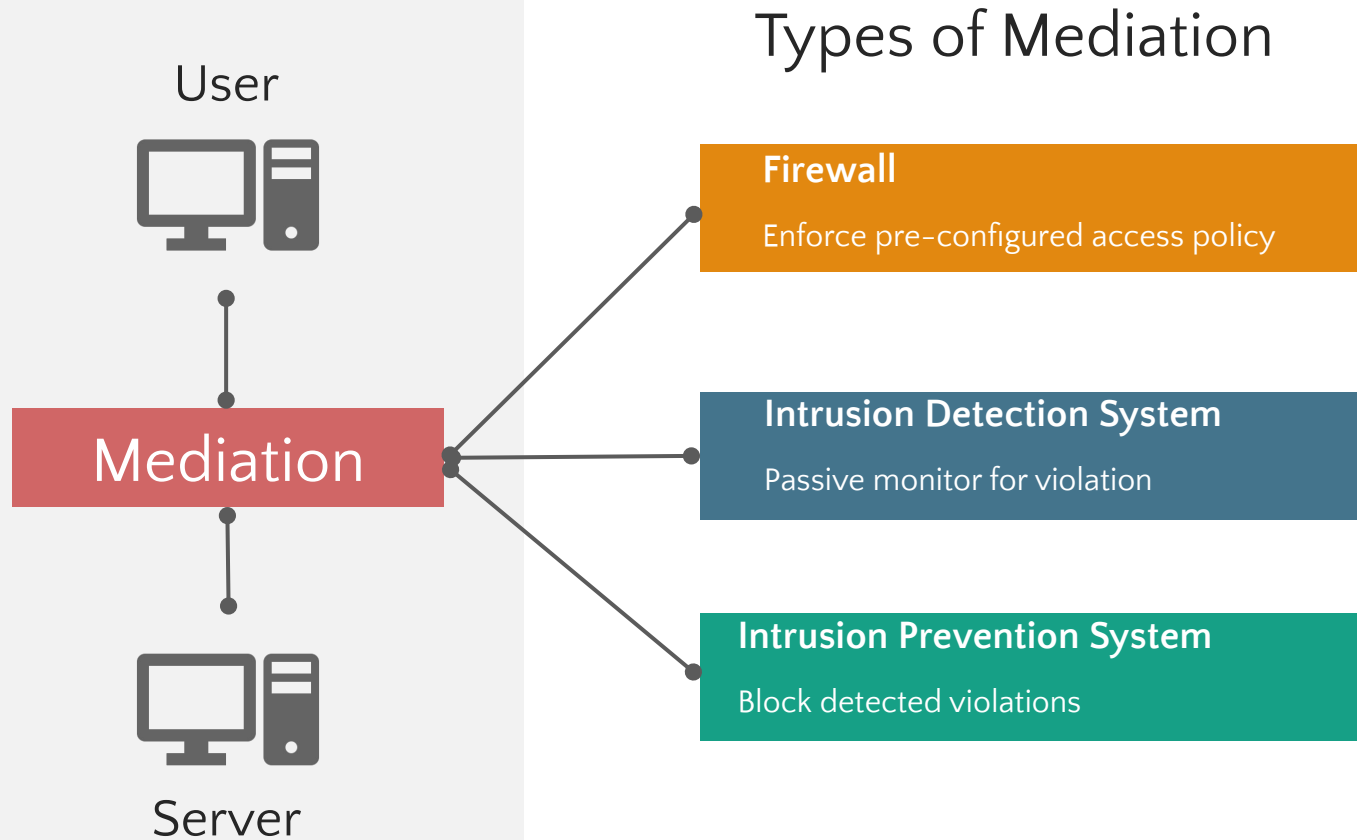
Attack: TLS allows client to initiate renegotiation, causing huge server computation.

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



Mediation & Detection

Firewalls & IDS



Desired Properties

Expressiveness: What kinds of policies can we write?

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

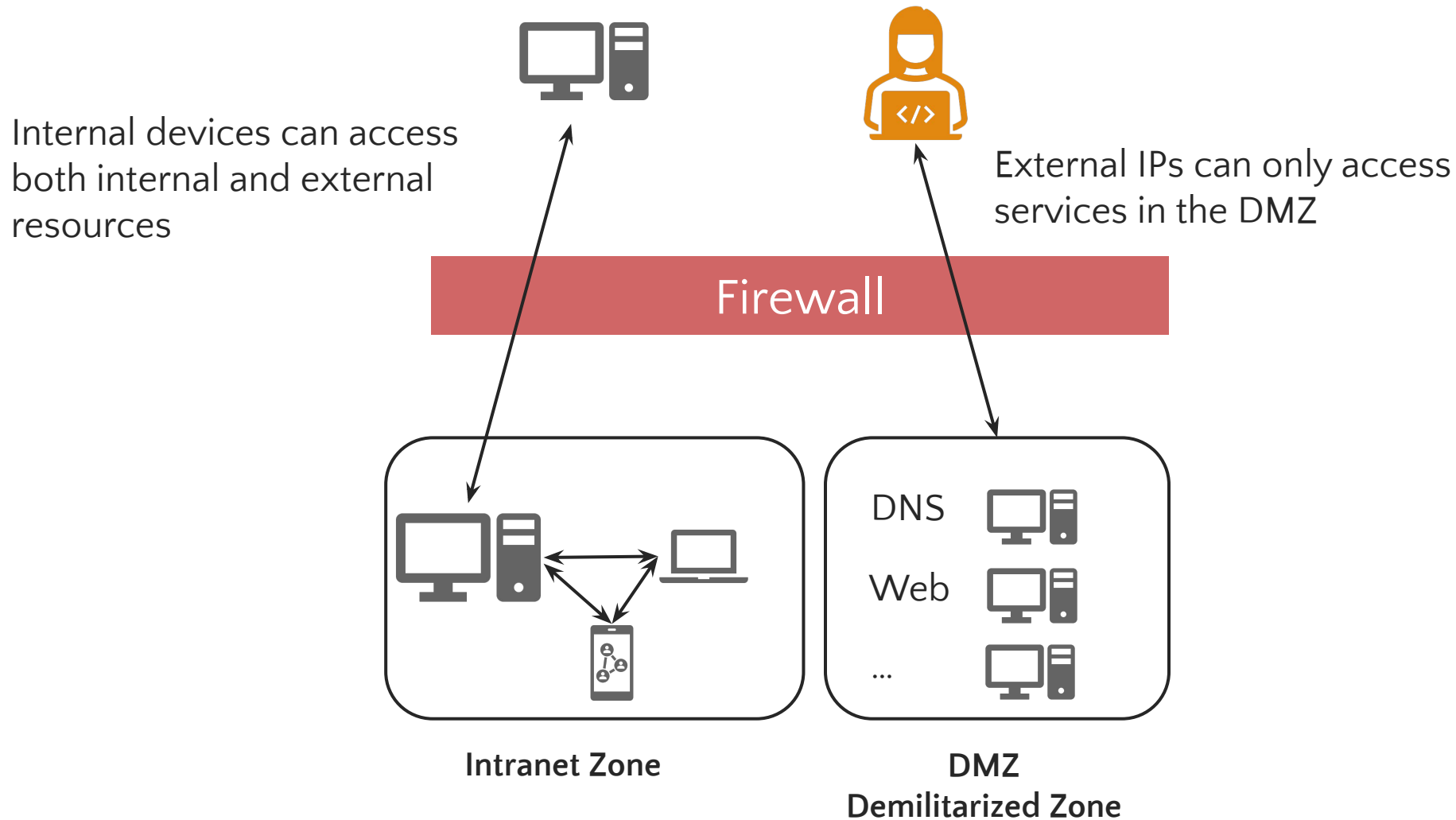
Efficiency: How many resources does it take, and how quickly does it decide?

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



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

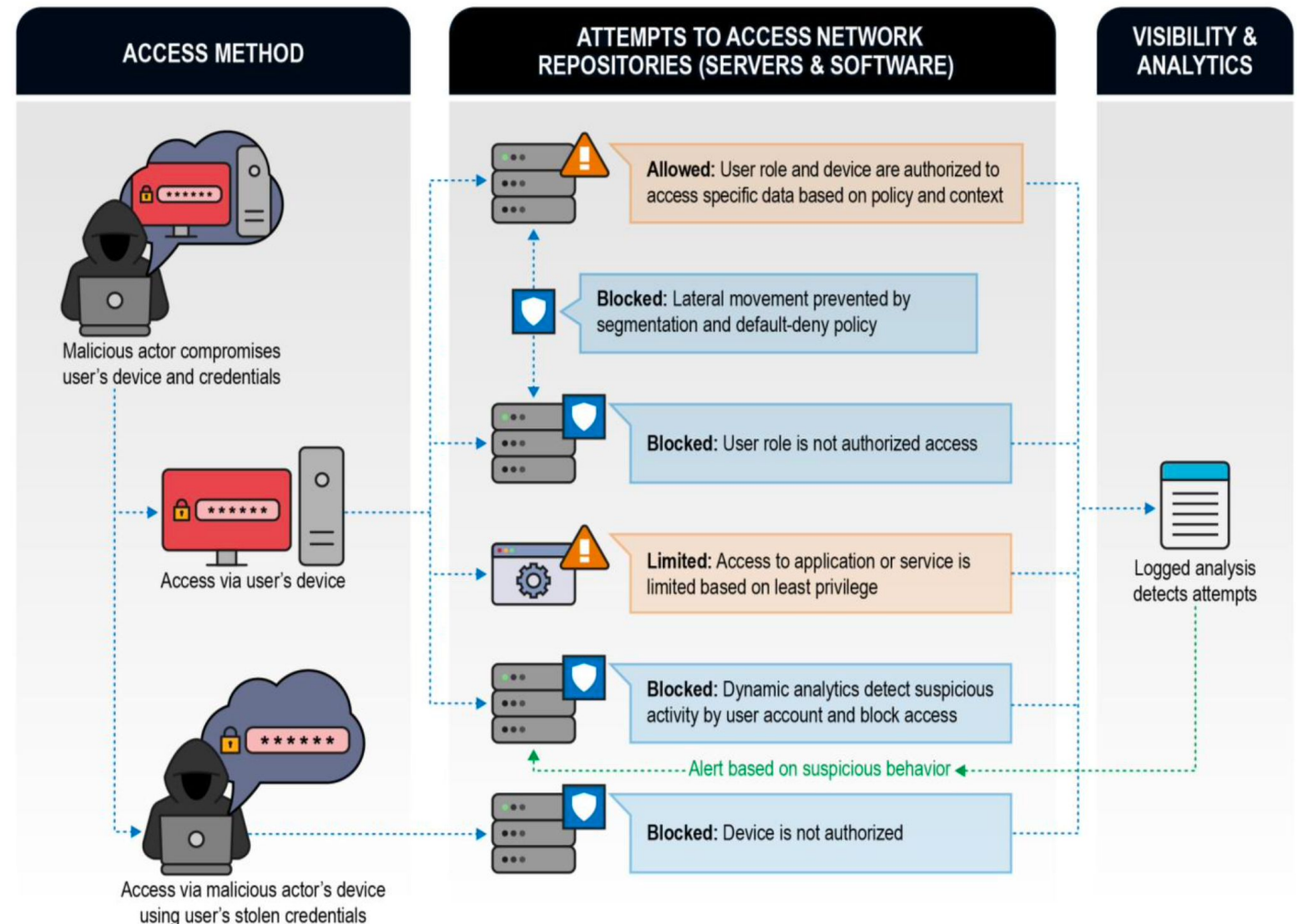
Treat every user, device, application, and data flow as untrusted. Authenticate and explicitly authorize each to the least privilege dynamically.

Assume Breach

Assume adversary already inside the network. Deny by default and heavily scrutinize all users for access. 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



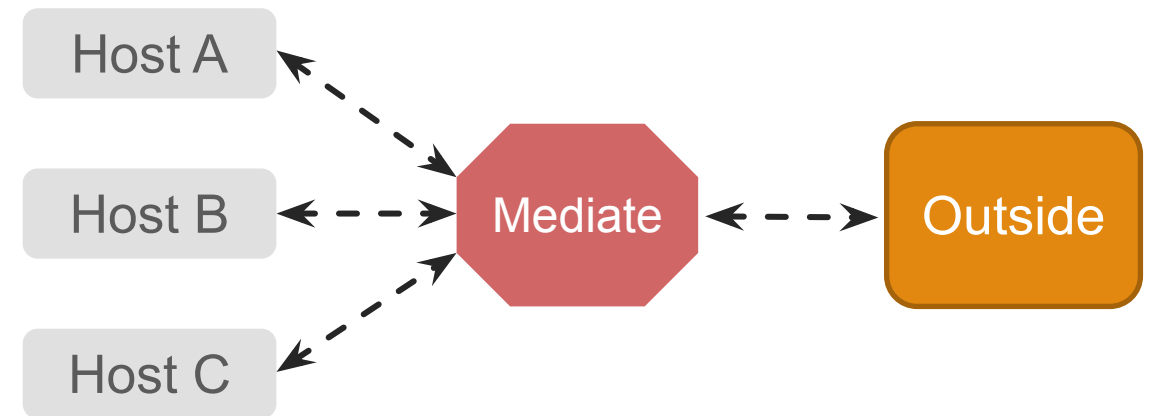
Pros:

- 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



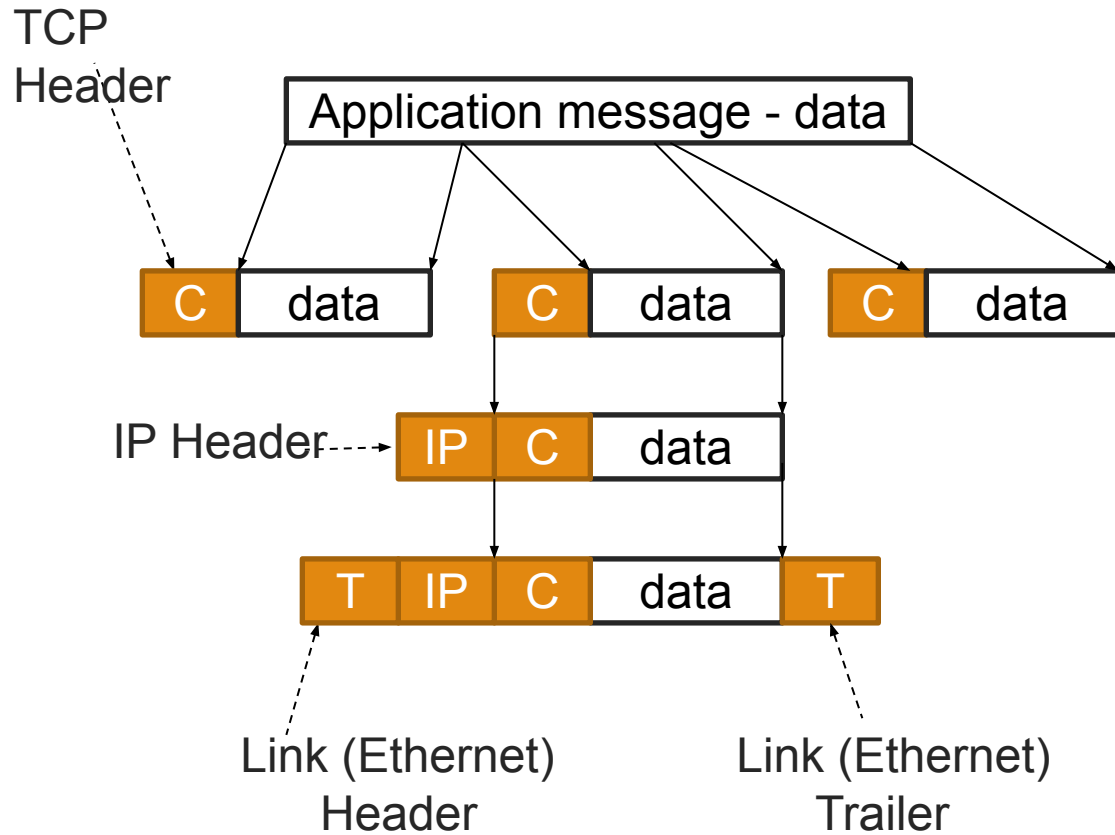
Pros:

- 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

Octet 1		Octet 2		Octet 3		Octet 4	
Ver	IHL	TOS		Total Length			
ID				0	D F	M F	Frag ID
...							

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



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

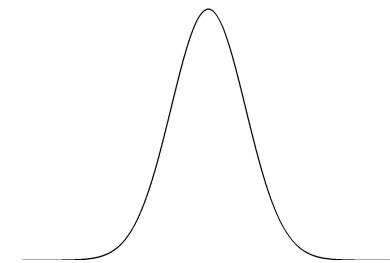
Detect any fragments less than 256 bytes
alert tcp any any -> any any (minfrag: 256; msg:
"Tiny fragments detected, possible hostile activity";)
Detect IMAP buffer overflow
alert tcp any any -> 192.168.1.0/24 143
(content: "|90C8 COFF FFFF|/bin/sh";
msg: "IMAP buffer overflow!";)

Snort Rule Example

Anomaly

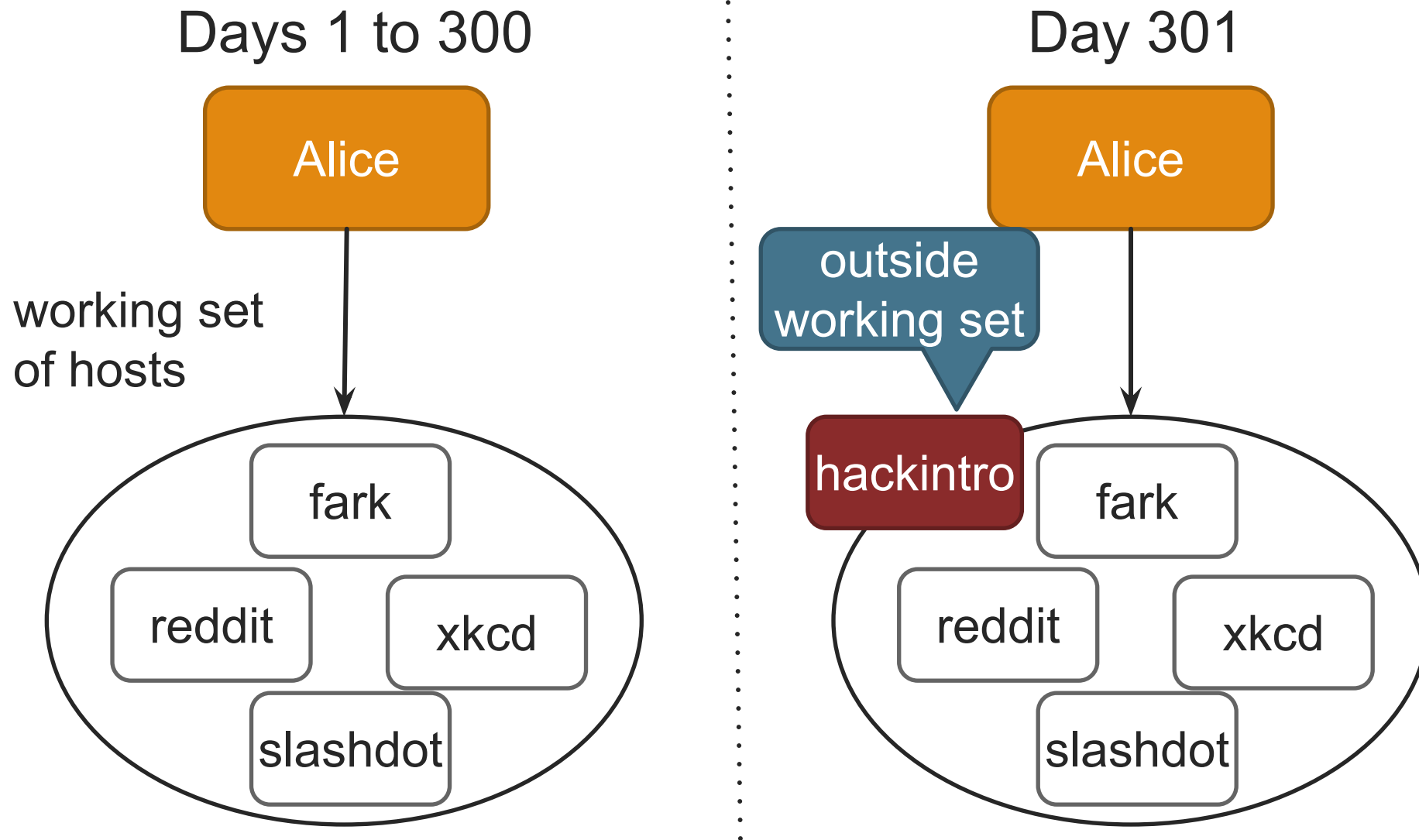
Alert on deviations from the norm

Examples: usual host connections,
unusual packet size, unusual packet data



Normal distribution of events

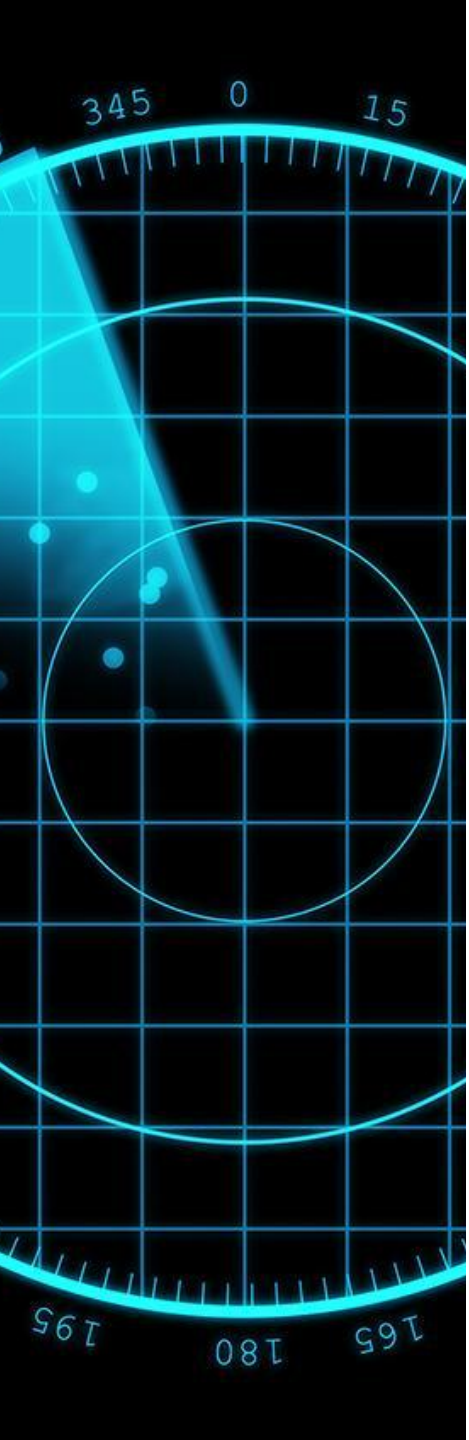
Anomaly Example: Working Sets





Detection Theory

Lies, Damn Lies, and Statistics



Detection theory or **signal detection theory** is a means to measure the ability to differentiate between information-bearing patterns and random patterns that distract from the information (called noise). In the field of electronics, the separation of such patterns from a disguising background is referred to as ***signal recovery***.

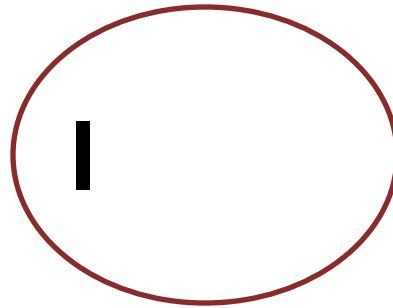
Ω

Let Ω be the set of all possible events.
For example:

- Audit records produced on a host
- Network packets seen

Ω

Example: IDS Received 1,000,000 packets.
20 of them corresponded to an intrusion
The intrusion rate $\Pr[I]$ is:
 $\Pr[I] = 20/1,000,000 = .00002$



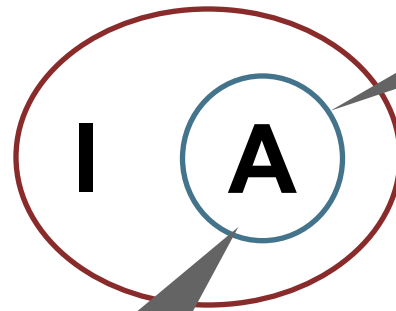
Set of intrusion
events I

Intrusion Rate:

$$\Pr[I] = \frac{|I|}{|\Omega|}$$

Ω

Legend:
 Ω = Events
 I = Intrusion
 A = Alarm



Defn: Sound
 $A \subset I$

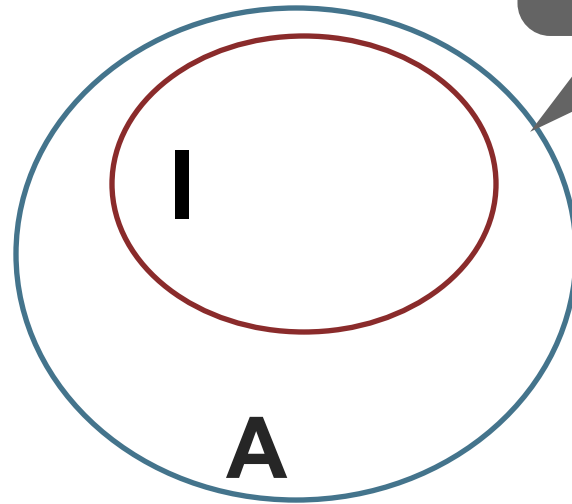
Set of alerts **A**

Alert Rate:

$$\Pr[A] = \frac{|A|}{|\Omega|}$$

Ω

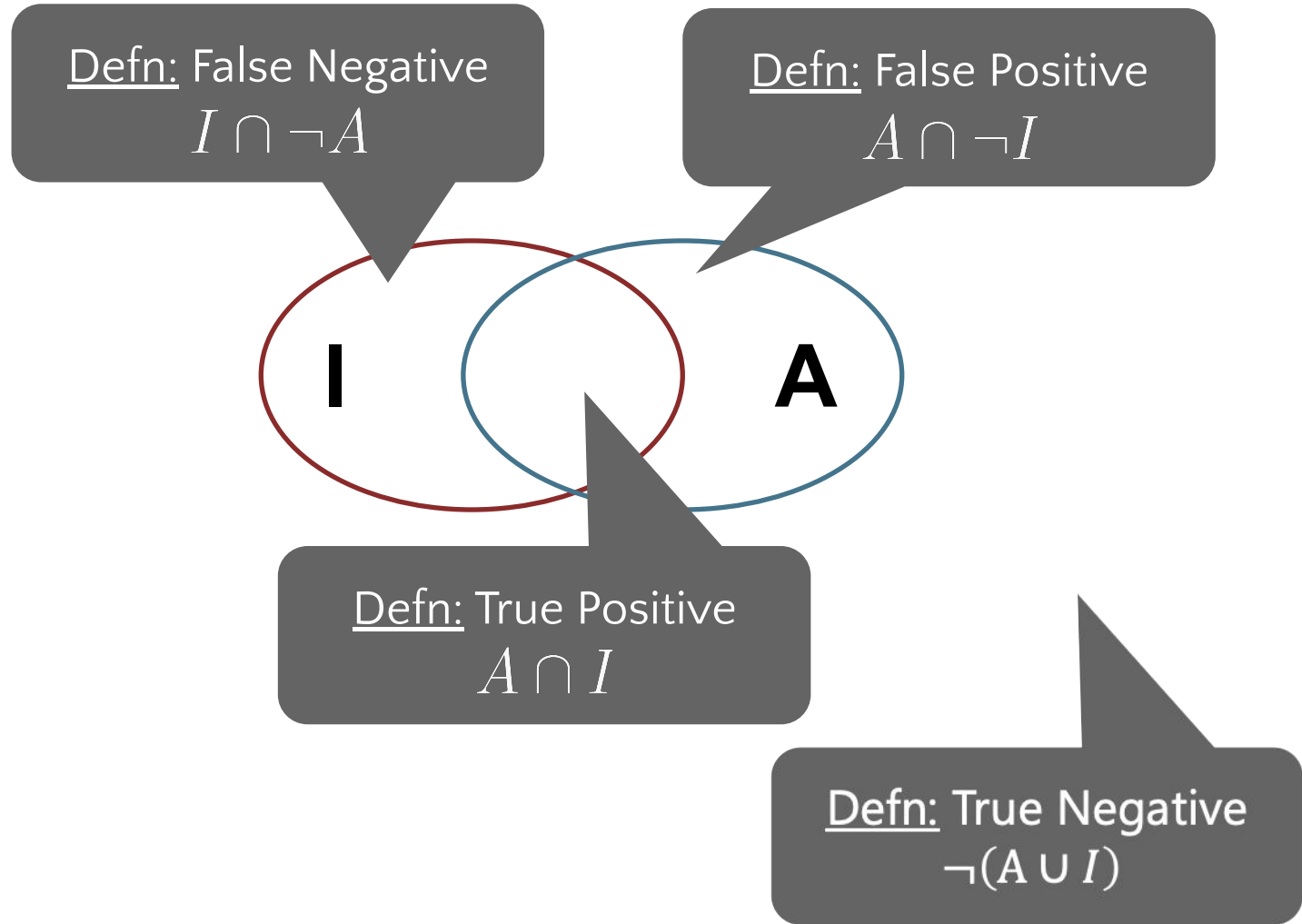
Legend:
 Ω = Events
 I = Intrusion
 A = Alarm



Defn: Complete
 $I \subset A$

Ω

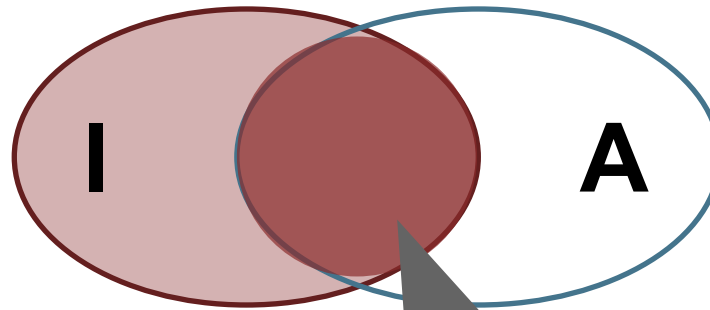
Legend:
 Ω = Events
 I = Intrusion
 A = Alarm



Ω

Think of the detection rate as the set of intrusions raising an alert normalized by the set of all intrusions

Legend:
 Ω = Events
 I = Intrusion
 A = Alarm



Defn: Detection rate

$$\Pr[A|I] = \frac{\Pr[A \cap I]}{\Pr[I]}$$

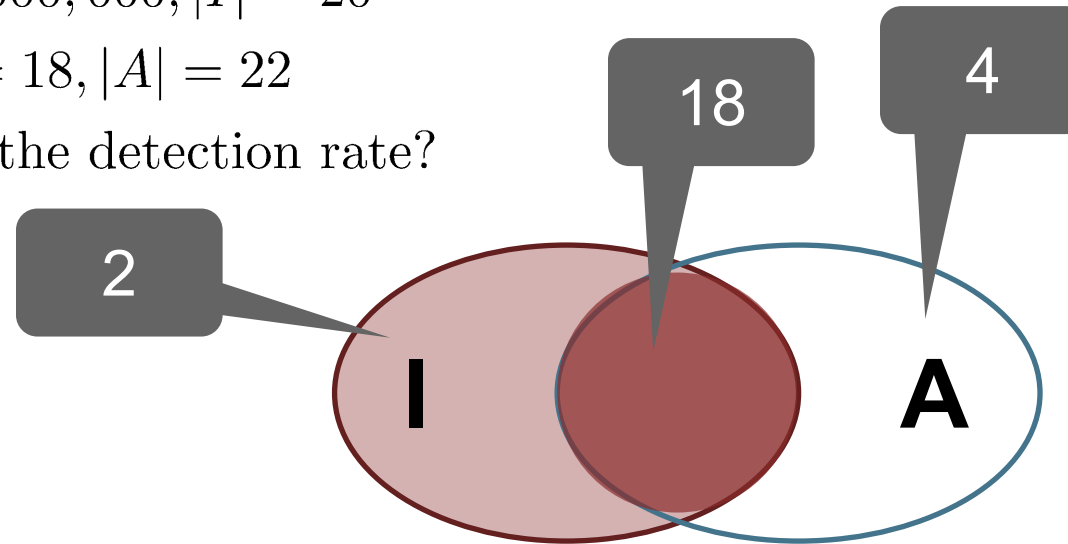
Ω

Suppose:

$$|\Omega| = 1,000,000, |I| = 20$$

$$|I \cap A| = 18, |A| = 22$$

What is the detection rate?



Quiz Question

$$\Pr[A|I] = \frac{\Pr[A \cap I]}{\Pr[I]}$$

- A. 10%
- B. 20%
- C. 50%
- D. 90%

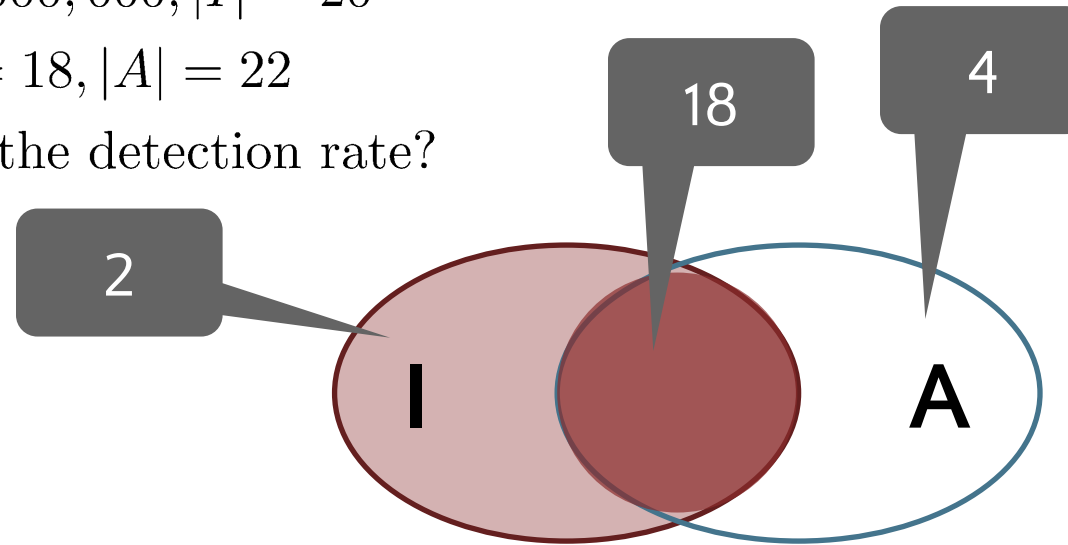
Ω

Suppose:

$$|\Omega| = 1,000,000, |I| = 20$$

$$|I \cap A| = 18, |A| = 22$$

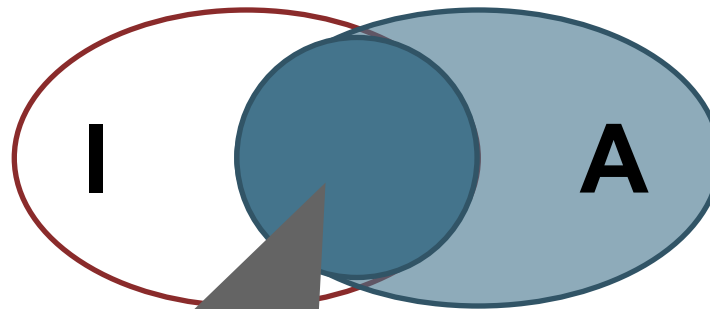
What is the detection rate?



$$Pr[A|I] = \frac{Pr[A \cap I]}{Pr[I]} = 18/20 = .90 = 90$$

Ω

Think of the Bayesian detection rate as the set of *intrusions raising an alert* normalized by the *set of all alerts* (vs detection rate, which normalizes on intrusions)



Defn: Bayesian detection rate

$$\Pr[I|A] = \frac{\Pr[A \cap I]}{\Pr[A]}$$

Crux of ID usefulness!

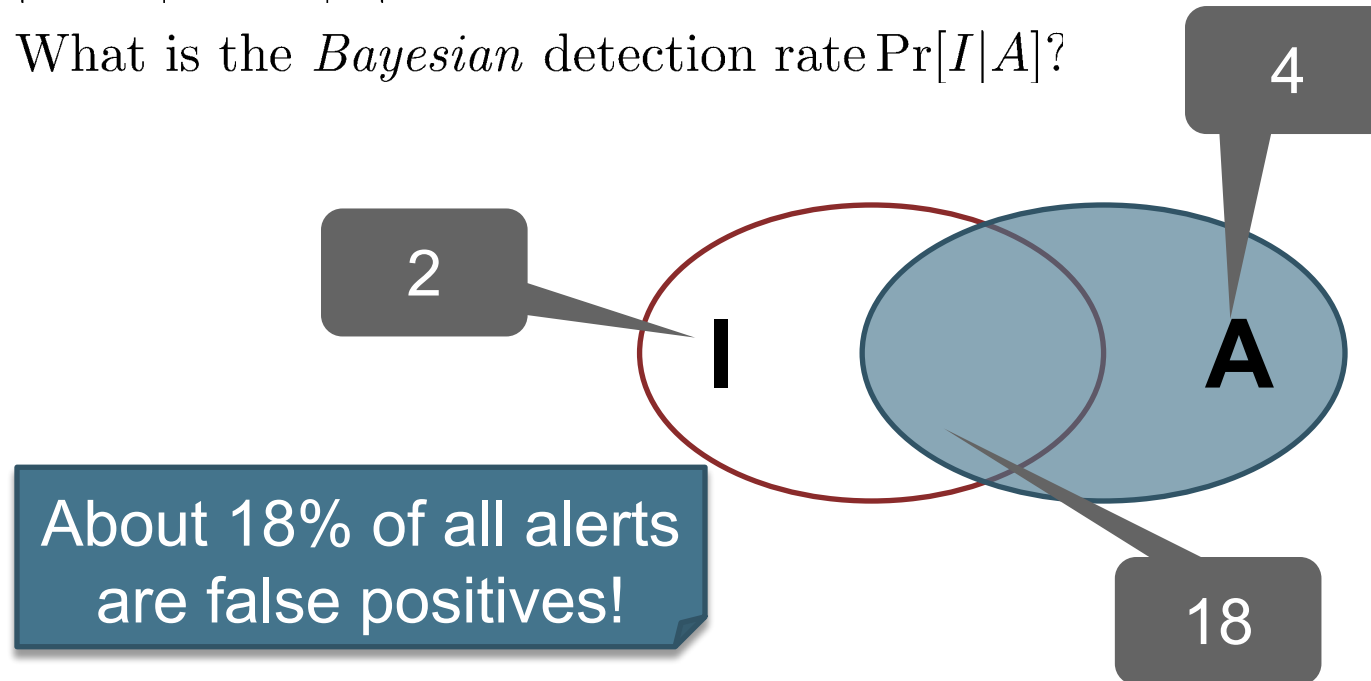
Ω

Suppose:

$$|\Omega| = 1,000,000, |I| = 20$$

$$|I \cap A| = 18, |A| = 22$$

What is the *Bayesian* detection rate $\Pr[I|A]$?



$$\Pr[I|A] = \frac{\Pr[A \cap I]}{\Pr[A]} = 18/22 = .81 \approx 82\%$$

Challenge

We're often given the detection rate and can estimate the intrusion rate, and want to calculate the Bayesian detection rate

- 99% accurate medical test
- 99% accurate IDS
- 99% accurate test for deception
- ...

Calculating Bayesian Detection Rate

Fact:

$$\Pr[A] = \Pr[I] * \Pr[A|I] + \Pr[\neg I] * \Pr[A|\neg I]$$

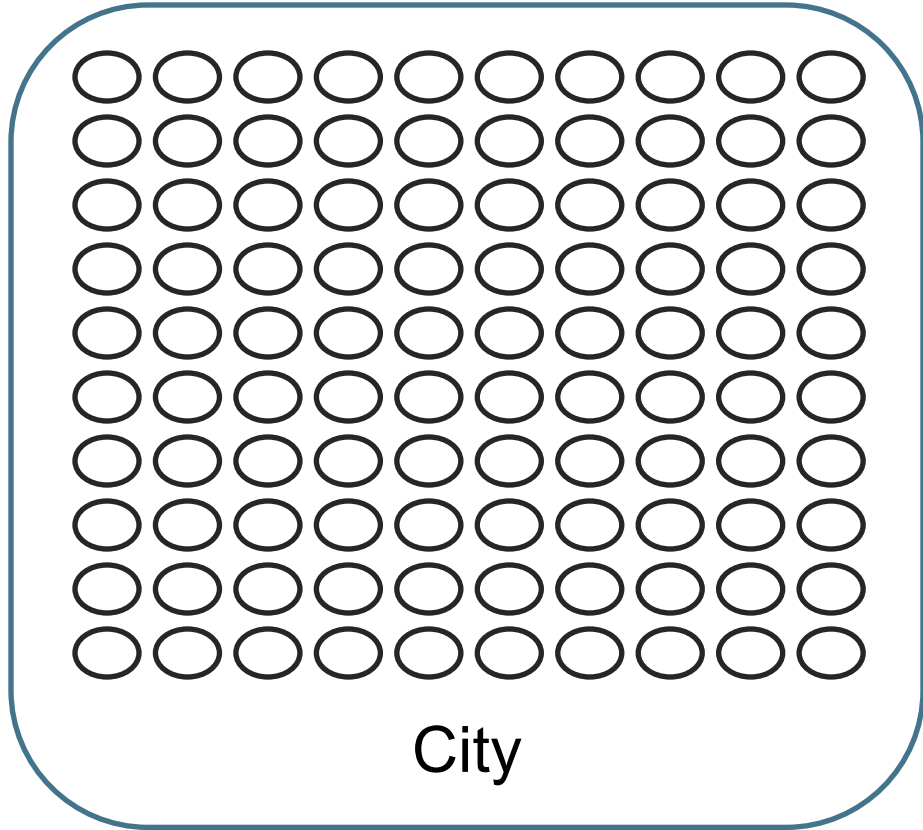
So to calculate the Bayesian detection rate:

$$\Pr[I|A] = \frac{\Pr[A \cap I]}{\Pr[A]}$$

One way is to compute this when $\Pr[A]$ but the base rate $\Pr[I]$ is:

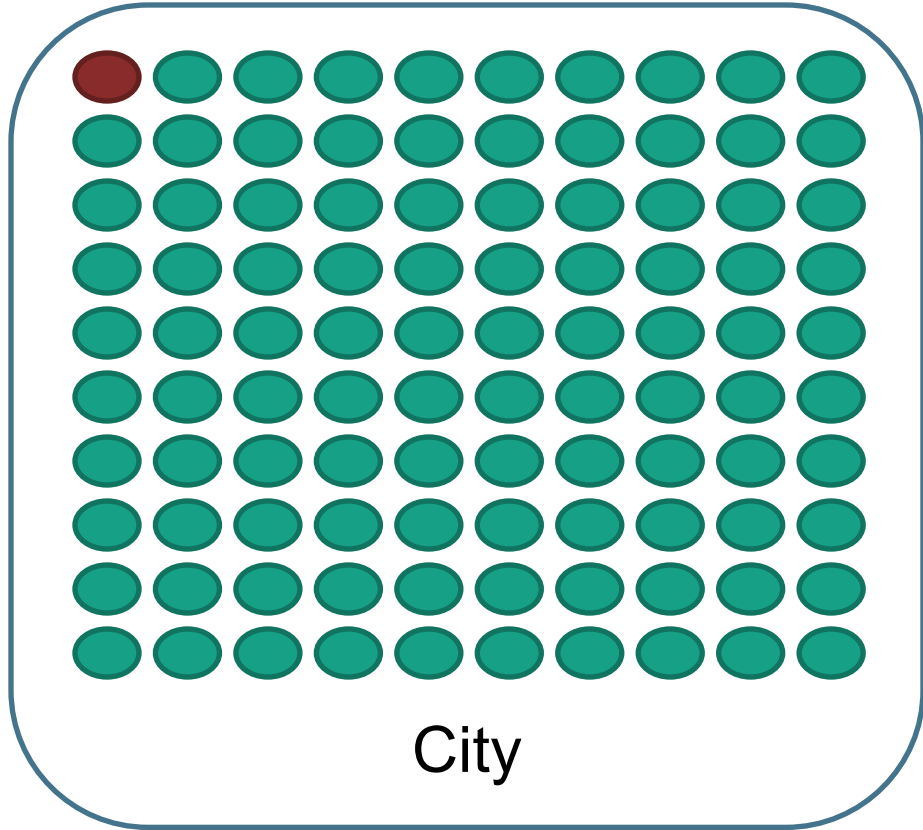
$$\Pr[I|A] = \frac{\Pr[A \cap I]}{\Pr[I] * \Pr[A|I] + \Pr[\neg I] * \Pr[A|\neg I]}$$

Example



- 100 people in the city
- 1 is a terrorist
 - Thus, the base rate of terrorists is 1/100
- Suppose we have a new terrorist facial recognition system that is 99% accurate
 - 99/100 times when someone is a terrorist there is an alarm
 - For every 100 good guys, the alarm only goes off once
- An alarm went off; is the suspect really a terrorist?

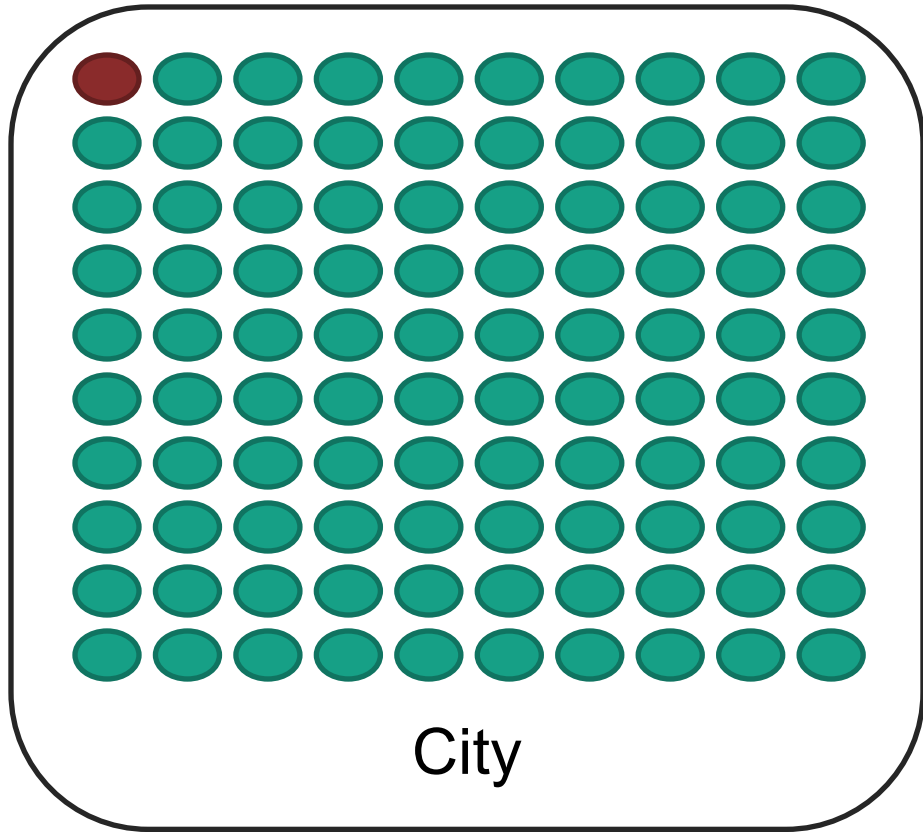
Example



Answer: The facial recognition system is 99% accurate. That means there is only a 1% chance the guy is not the terrorist.

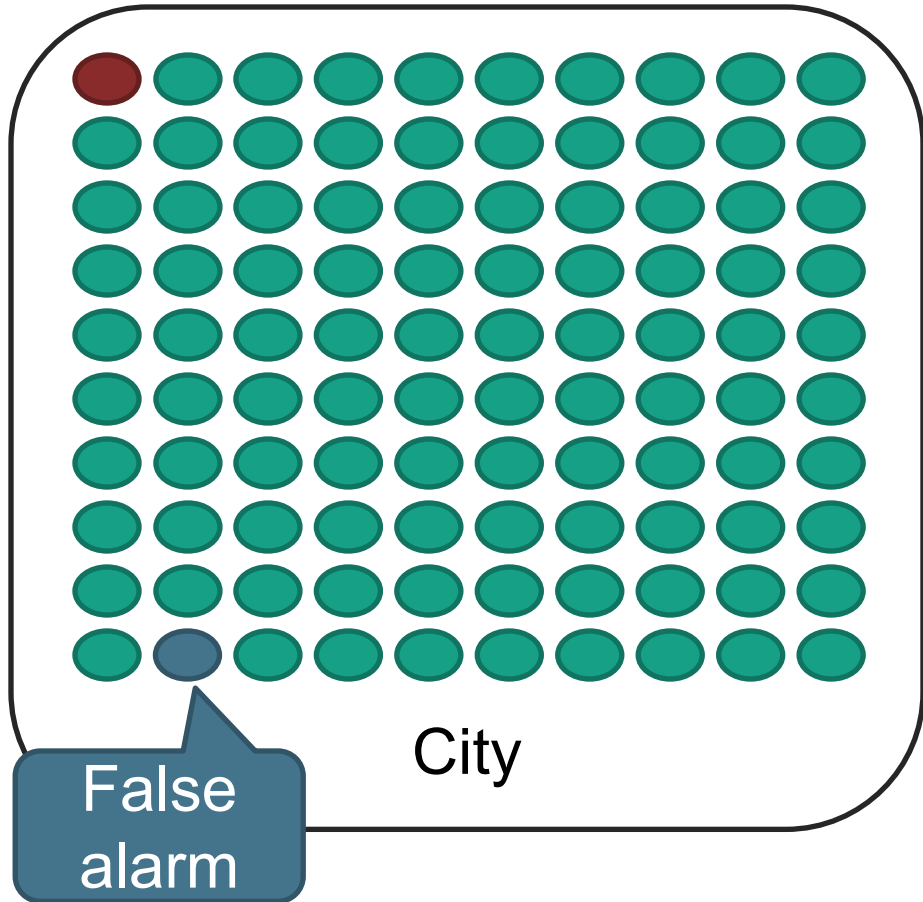
Wrong!

Formalization



- 1 is a terrorist, and we have their picture
 - Thus, the base rate of terrorists is 1/100
 $P[T] = 0.01$
- 99/100 times when someone is a terrorist there is an alarm
 $P[A|T] = .99$
- For every 100 good guys, the alarm only goes off once
 $P[A | \text{not } T] = .01$
- Want to know $P[T|A]$

Intuition: Given 99 good guys, we have $99 \cdot .01 \approx 1$ false alarm



- 1 is a terrorist, and we have their picture
 - Thus, the base rate of terrorists is $1/100$
 $P[T] = 0.01$
- 99/100 times when someone is a terrorist there is an alarm
 $P[A|T] = .99$
- For every 100 good guys, the alarm only goes off once
 $P[A | \text{not } T] = .01$
- Want to know $P[T|A]$

Have: $\Pr[T] = 0.01$

$\Pr[A|T] = .99, \Pr[A|\neg T] = .01$

Want to calculate: $\Pr[T|A] = \frac{\Pr[T \cap A]}{\Pr[A]}$

Unknown

Unknown

Mathematically..

$$\Pr[A \cap I] = \Pr[A|I] * \Pr[I]$$

$$\Pr[A] = \Pr[I] * \Pr[A|I] + \Pr[\neg I] * \Pr[A|\neg I]$$

$$\text{Have: } \Pr[T] = 0.01$$

$$\Pr[A|T] = .99, \Pr[A|\neg T] = .01$$

$$\text{Want to calculate: } \Pr[T|A] = \frac{\Pr[T \cap A]}{\Pr[A]}$$

$$= \frac{\Pr[T \cap A]}{\Pr[T] * \Pr[A|T] + \Pr[\neg T] * \Pr[A|\neg T]}$$

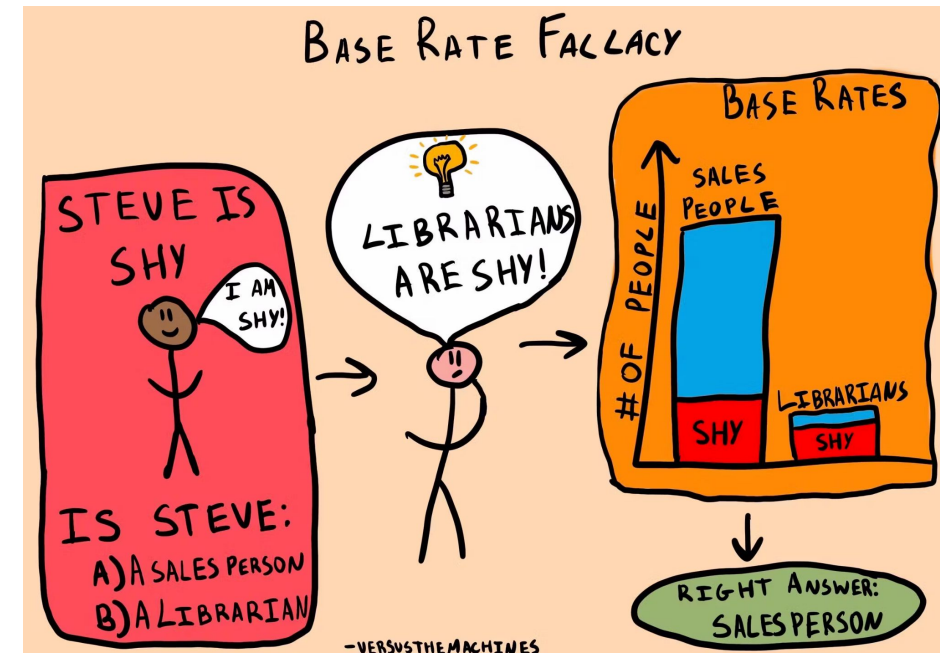
$$= \frac{\Pr[A|T] * \Pr[T]}{\Pr[T] * \Pr[A|T] + \Pr[\neg T] * \Pr[A|\neg T]} = \frac{.99 * .01}{.01 * .99 + .99 * .01}$$

*99% accuracy + this specific dataset
= wrong predictions 50% of the time!*

= 50%

Base Rate Fallacy


- Base rate fallacy = focusing purely on “accuracy” (or similar) and ignoring the base rate
 - Even very high accuracy + very low base rate = potentially very high false positive rate
- Implications for anomaly detection:
 - *Rare anomalies very hard to detect without high false positives*



Let's Test Ourselves

<https://www.omnicalculator.com/statistics/false-positive-paradox>

Network Security is a Large Field

- 
- 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?

Ευχαριστώ και καλή μέρα εύχομαι!

Keep hacking!