CYBER 100

27TH DECEMBER 2023

Cyber Security & Infrastructure: Concepts, Threats and Best Practices

Speakers:

Chaoyi Lu *(Tsinghua University)*

Mingming Zhang *(Zhongguancun Laboratory)*

December 27, 2023

Contents

Part I: Introduction to cyber security

- What is “security”?
- Cyber security and concepts
- Internet infrastructure

What is “security”?

- “Security” in literal terms
  - State of being proteted from unauthorized access and other risks

I.2.e. With reference to encryption, or telecommunications or computer systems: the state of being protected from unauthorized access; freedom from the risk of being intercepted, decoded, tapped, etc. **1955–**

1955 In many ciphers much additional security is gained by a second transposition.
L. D. Smith, *Cryptography* iii. 56 ···

...

2006 Ethical hackers attempt to use the same methods criminal hackers would use to break into an organisation's systems to expose gaps in security, which can then be closed.
Computer Weekly 31 October 68/1 ···

Show more quotations

“Security” in Oxford English Dictionary

What is "cyber security"?

- "Cyber security" in literal terms
  - Security relating to computer systems or the internet

Security relating to computer systems or the internet, *esp.* that intended to protect against viruses or fraud. **1990–**

In earliest use with reference to computer-aided systems for securing property.

1990 Turns out the guy used to work cyber security for us downside... Used to make sure SPARTOS was up on his inoculations.
J. McKinney, *Kaduna Memories* ii. xi. 115 ···

1994 Currently, state laws guard the privacy of medical records. But their vast differences raise questions for cyber security.
Dispatch (Moline, Illinois) 10 April d5/2 ···

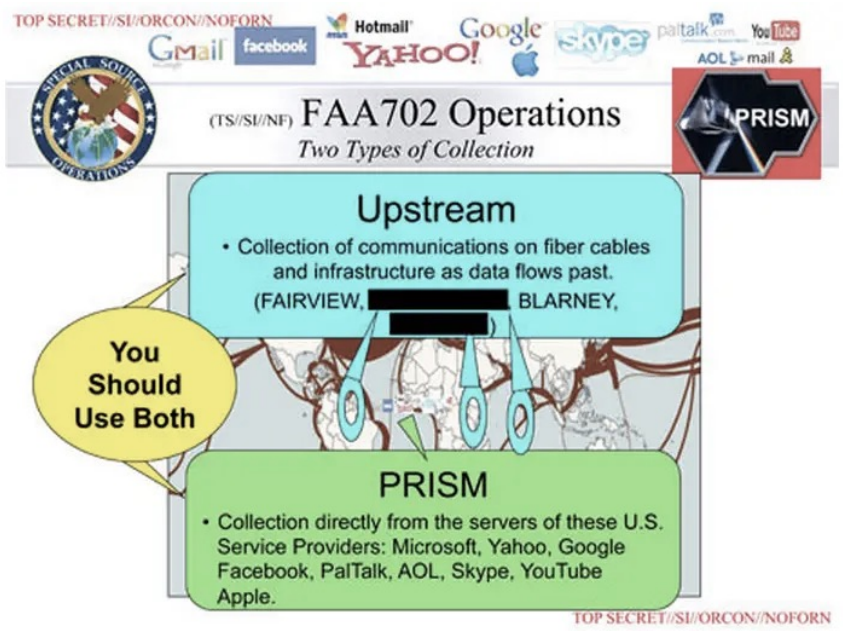
1995 One of the biggest challenges for strategic leaders in the 21st century will be cyber security —protecting computers and the links between them.
W. T. Johnsen et al., *Princ. War 21st Cent.* (Strategic Studies Inst. U.S. Army War College, Pennsylvania) 22

"Cyber security" in Oxford English Dictionary

What is "cyber security"?

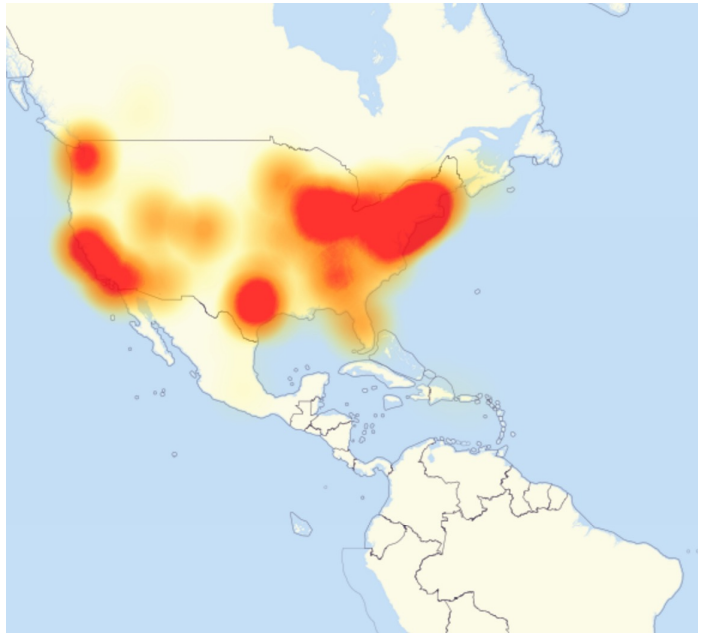
❑ Cyber security incidents - Examples

❑ Security incidents causing global impact and major loss



Data breach & sniffing
(e.g., Surveillance project)

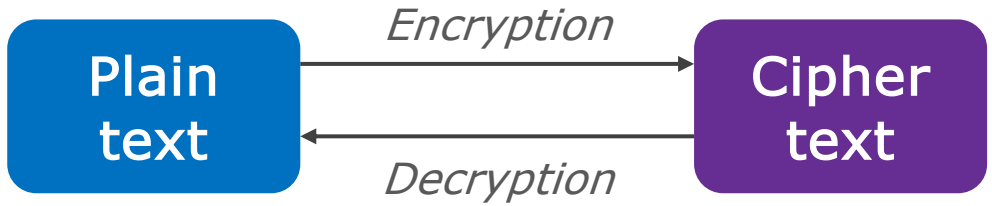
Computer virus
(e.g., WannaCry ransomeware)

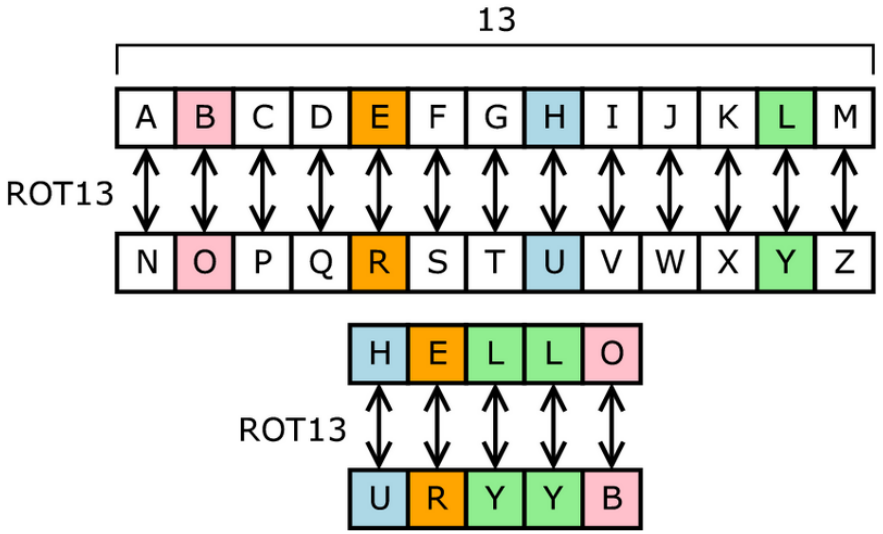


Global Internet attacks
(e.g., Dyn DoS outage)

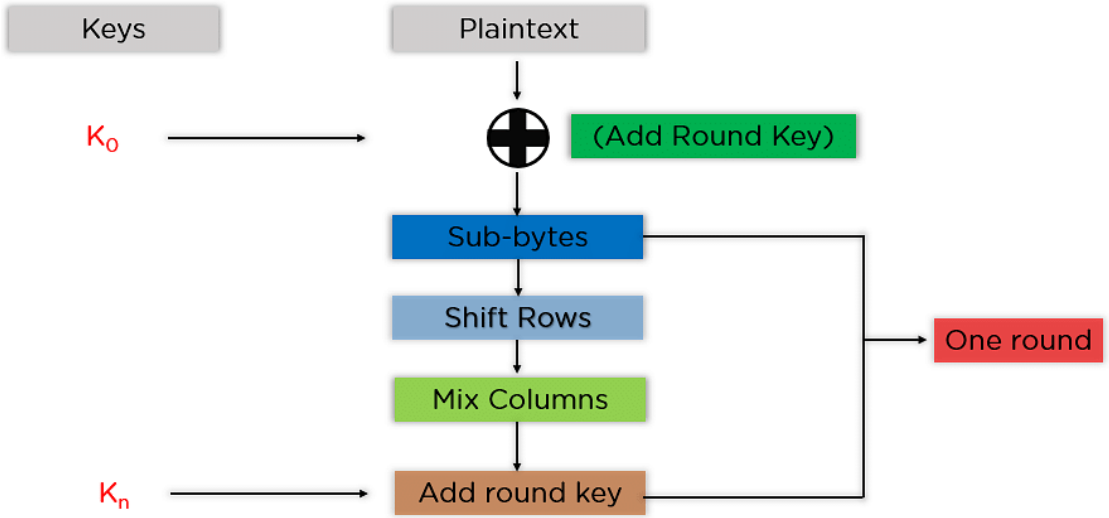
What falls within "cyber security"?

- **Cryptography**
  - **Encrypts** data into unreadable text
  - Dates back for thousands of years





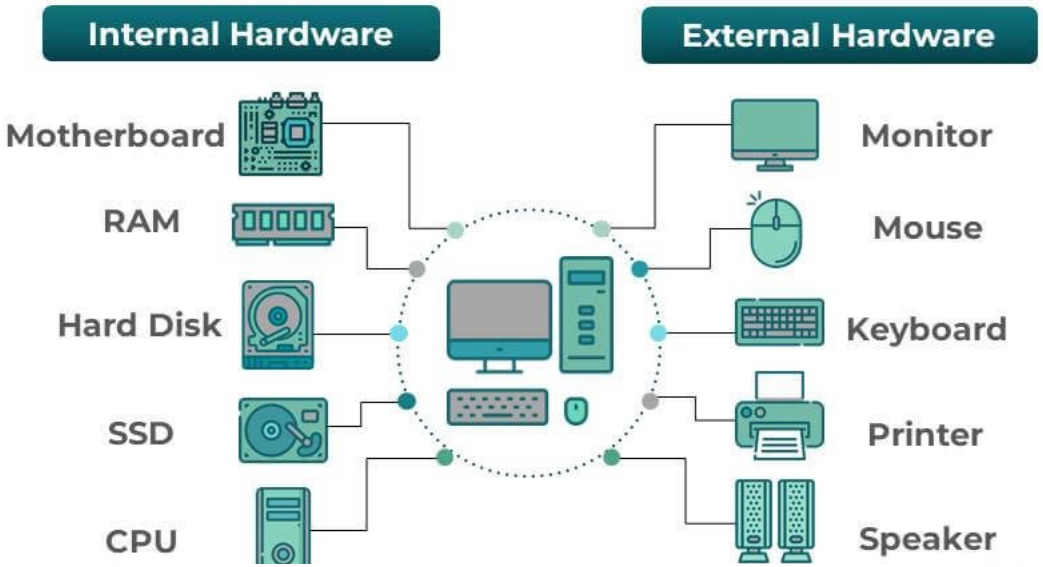
Classical cipher
(e.g., Caesar cipher, 58BC)



Symmetric cipher
(e.g., Advanced Encryption Standard, 2001)

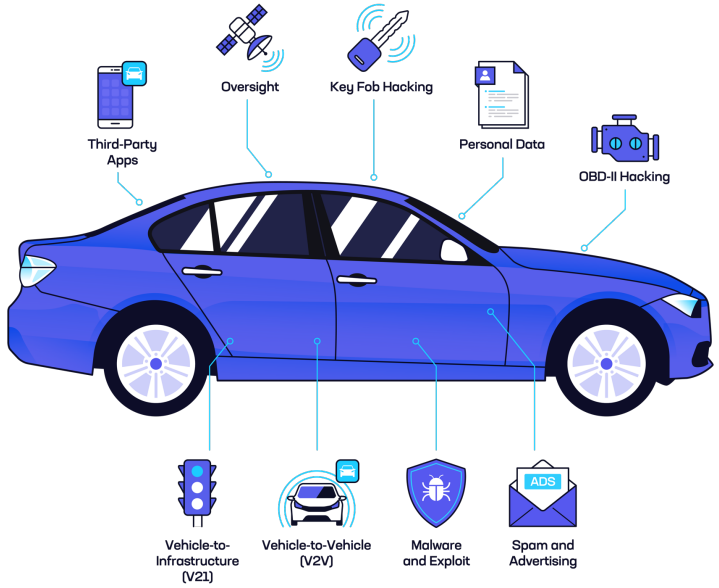
What falls within “cyber security”?

- **System security**
  - Hardware: computer hardware, IoT & embedded devices



Security of computer hardware
(e.g., unauthorized RAM access)

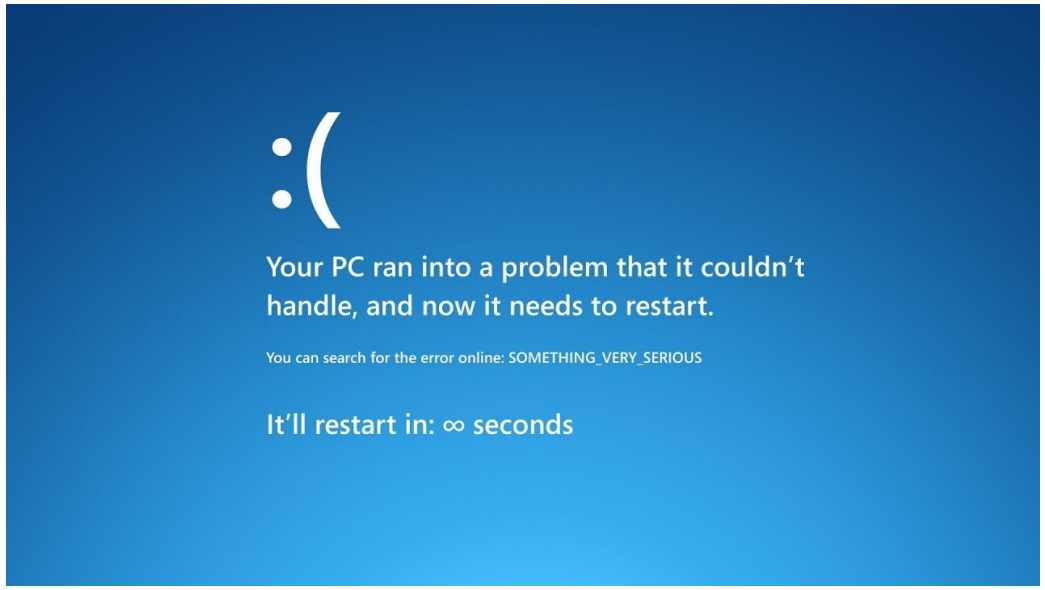
IoT security
(e.g., adversary signals)



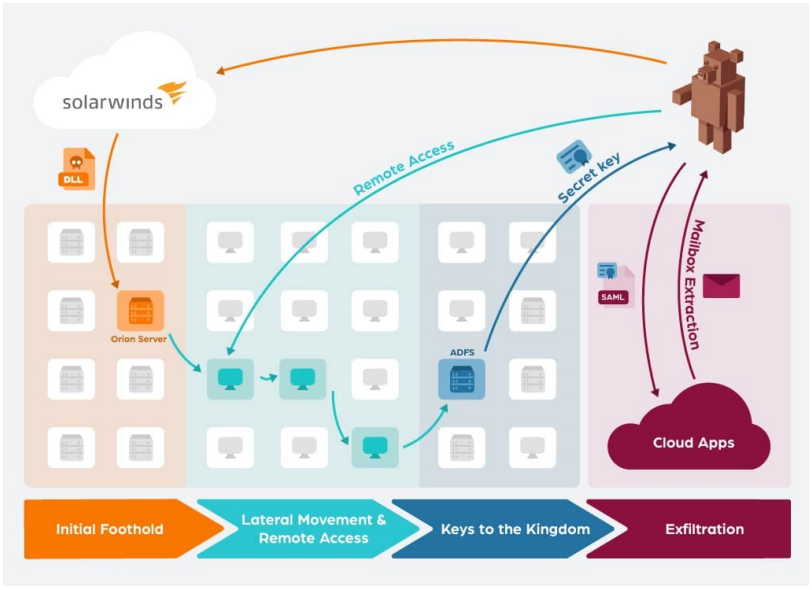
Automobile security
(e.g., lock picks)

What falls within "cyber security"?

- System security (contd.)
  - Hardware: computer hardware, IoT & embedded devices
  - Software: exploit of vulnerabilities, malware analysis, supply chains



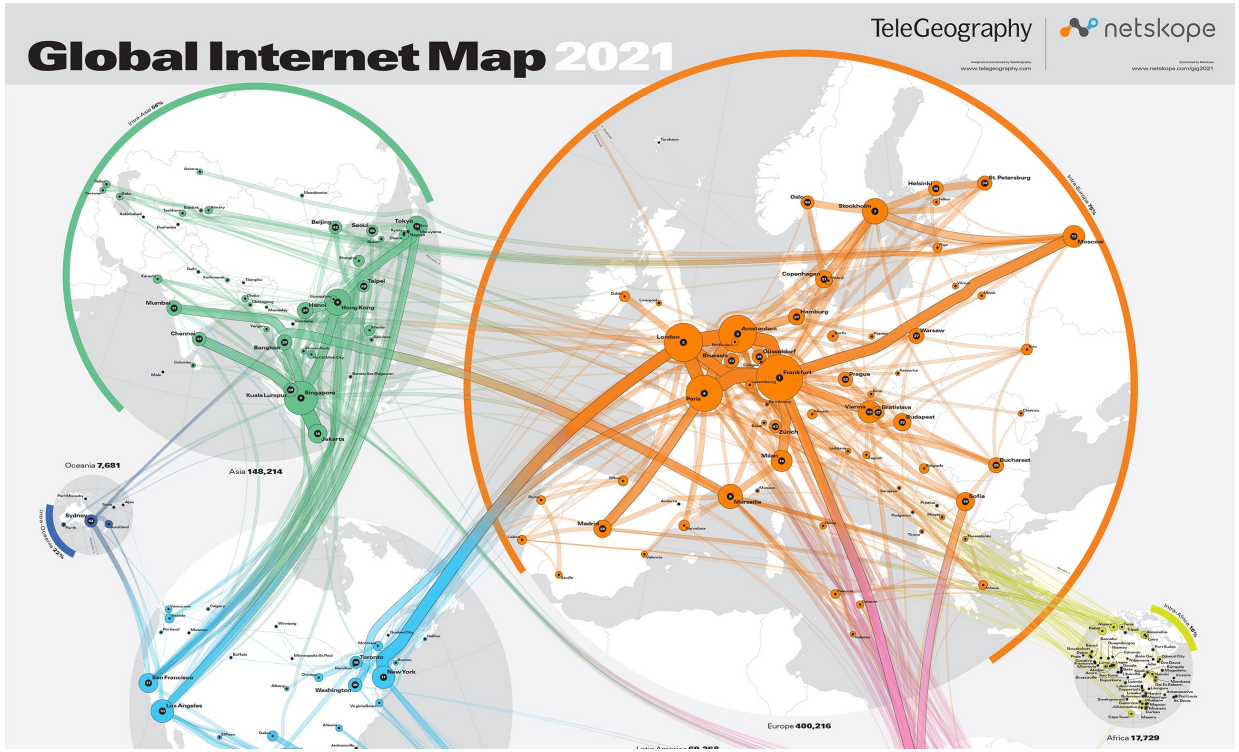
Unexpected run-time behaviors
(e.g., software crash / command execution)



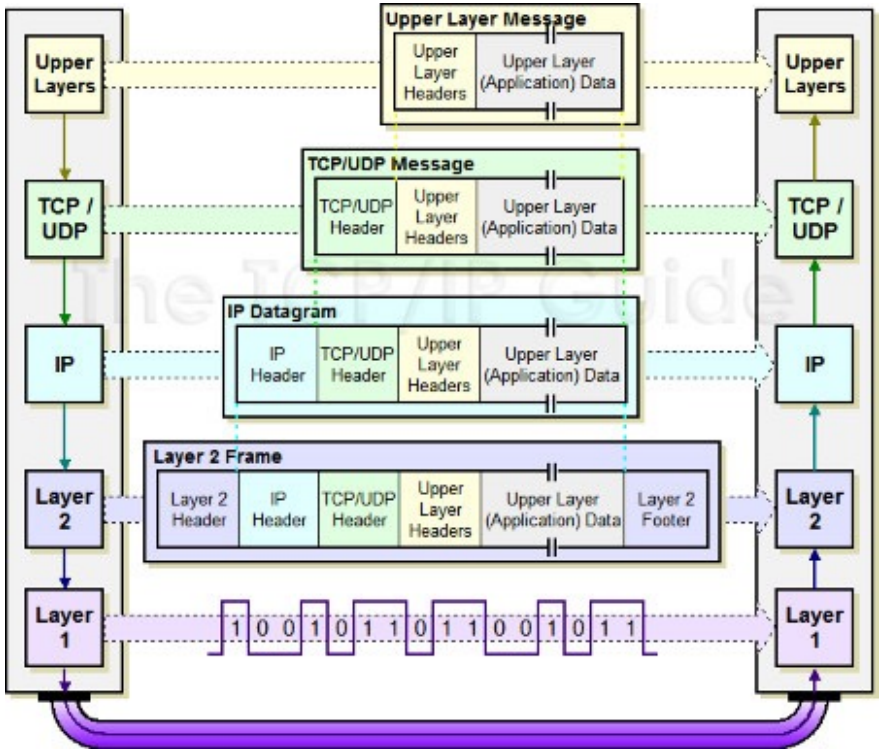
Compromised software & malware
(e.g., SolarWinds attack)

What falls within “cyber security”?

- Network security
  - Global Internet & TCP/IP protocol stack



How to hold together links across the globe?

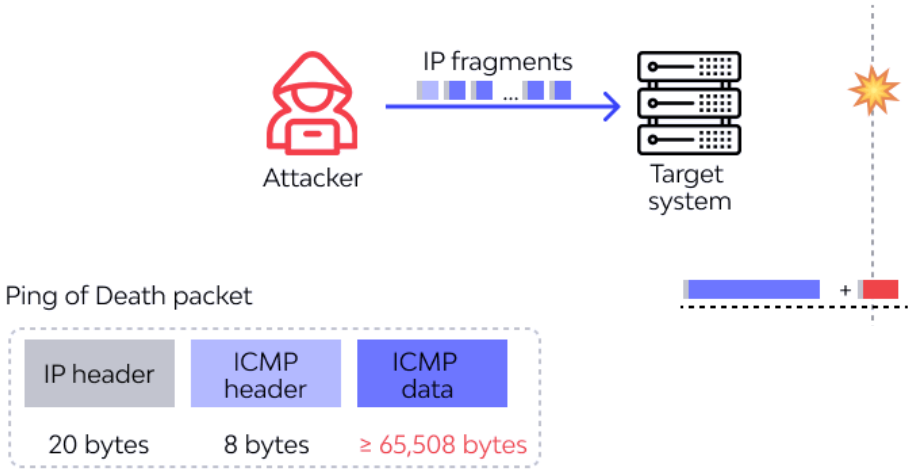


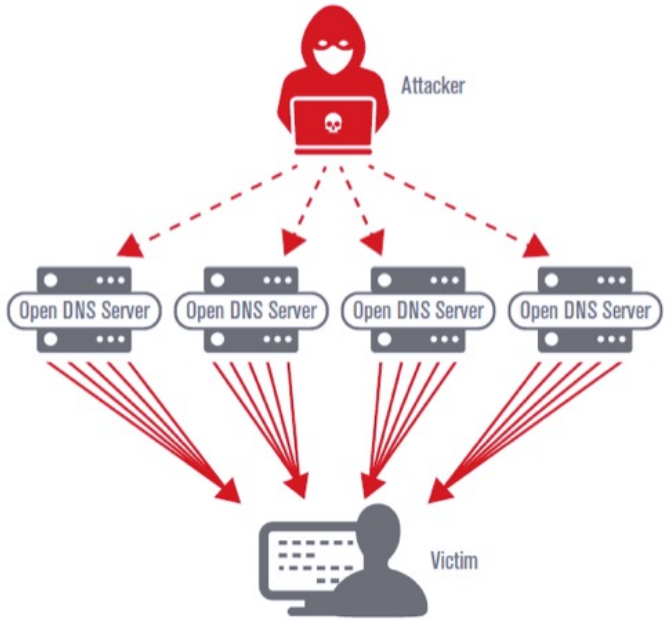
The Internet protocol stack

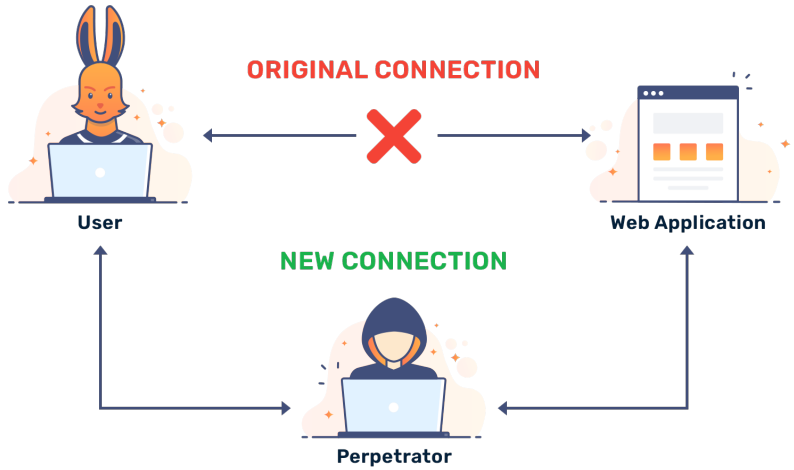
What falls within “cyber security”?

❑ Network security (contd.)

- ❑ Global Internet & TCP/IP protocol stack
- ❑ When Internet protocols are exploited…







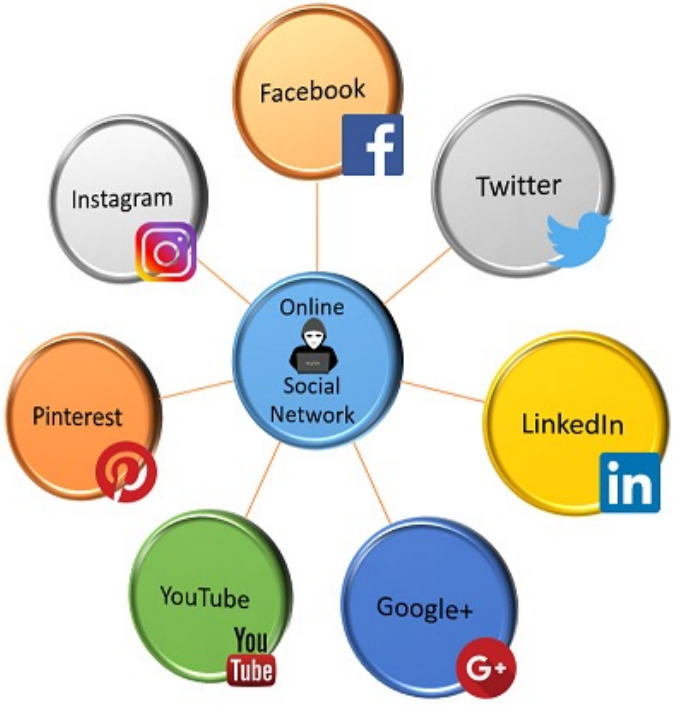
Crafted / malformed packets
(e.g., Ping of Death)

Denial-of-Service attacks
(e.g., Reflected amplification)

Link / data interception
(e.g., man-in-the-middle)

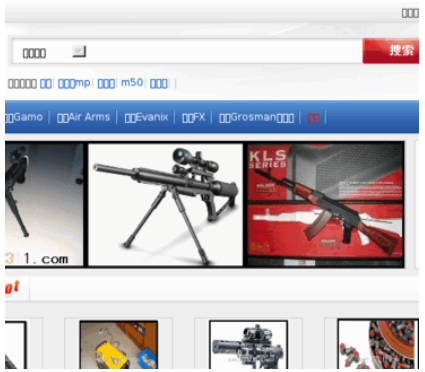
What falls within “cyber security”?

- Application security
  - Applications running on top of Internet & systems



Social networks, emails and instant messaging

Online payments



Underground activities

Internet infrastructure

- "Infrastructure" in literal terms
  - Foundational and base equipment

A collective term for the subordinate parts of an undertaking; substructure, foundation; *spec.* the permanent installations forming a basis for military operations, as airfields, naval bases, training establishments, etc. **1927–**

1927 The tunnels, bridges, culverts, and 'infrastructure' work generally of the Ax to Bourg-Madame line have been completed.
Chambers's Journal 14 May 374/2 ···

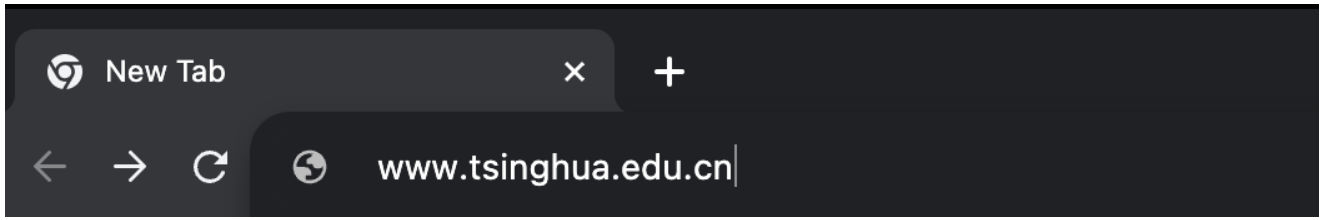
...

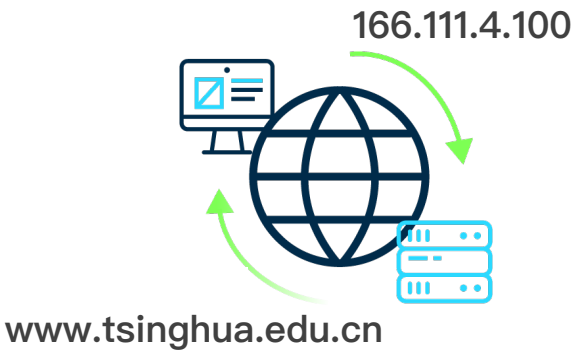
1971 A very complex infrastructure of scores of vernacular languages.
J. Spencer, *English Language in West Africa* 31 ···

"Infrastructure" in Oxford English Dictionary

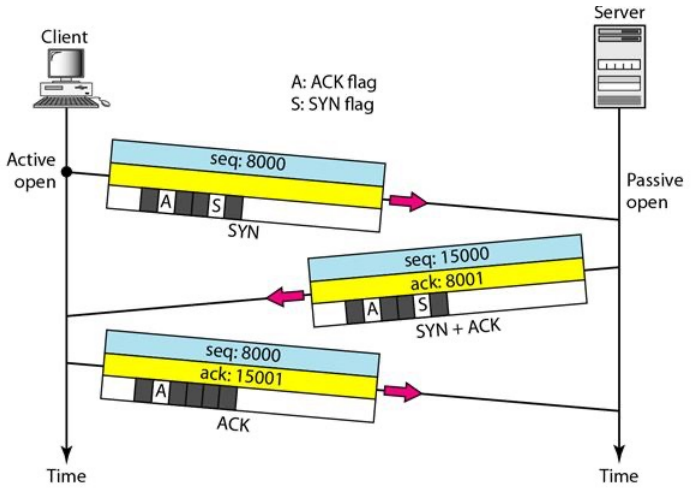
Internet infrastructure

- Let's start from opening a browser
  - What happens after we type in website name and press enter?

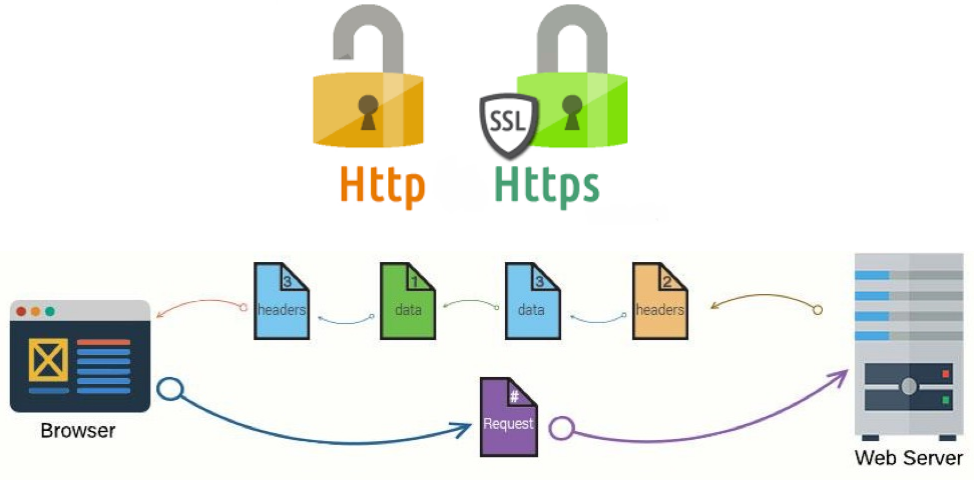




Name-address translation



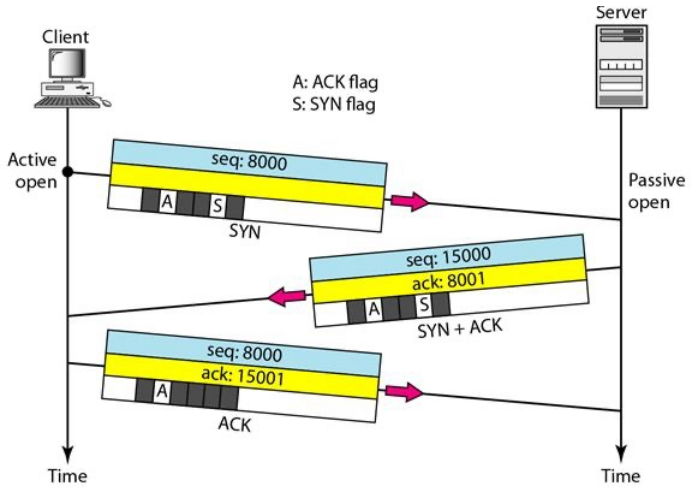
Route & connect to website server

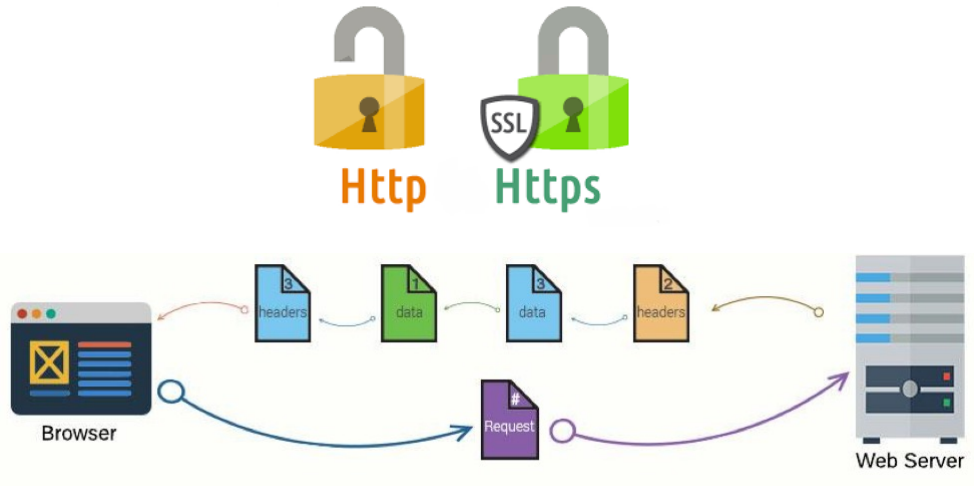


Security verification & data transmission

Internet infrastructure

❑ What are considered as infrastructure?





Name-address translation

Route & connect to website server

Security verification & data transmission

- Domain Name System (DNS)
- Links & cables
- Routing systems
- Cloud systems
- Public Key Infrastructure

Part II.1: Domain Name System & security

- Roles and concepts of DNS
- Common security risks
- Best security practices

Why do we need a naming system?

- IP addresses: identifier of Internet hosts
  - Not friendly to human users – too difficult to remember!

166.111.4.100

IPv4

2402:f000:1:404:166:111:4:100

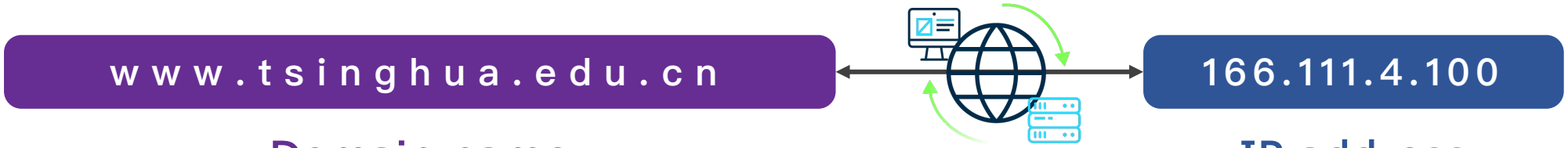
IPv6

- Domain names: another set of identifiers, but readable
  - Cannot be processed directly by machines

The web service of
Tsinghua University,
an educational institution
in China

Here it comes - DNS

- **Domain Name System (DNS)**
  - The "Phone Book" of Internet
  - Provides translation between names and addresses

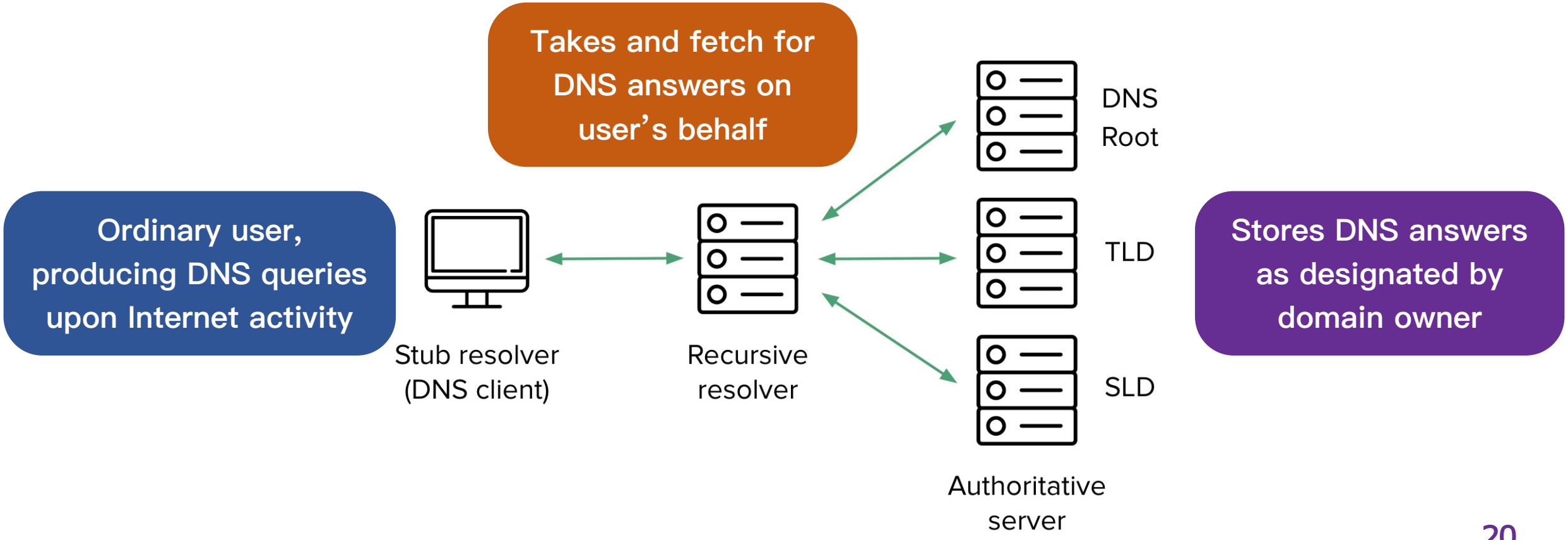


- **DNS precedes almost every Internet activity**
  - Without phone book, you may not know the numbers or make calls
  - **Without DNS, Internet uses are basically offline**

How does DNS work?

❑ Domain resolution model

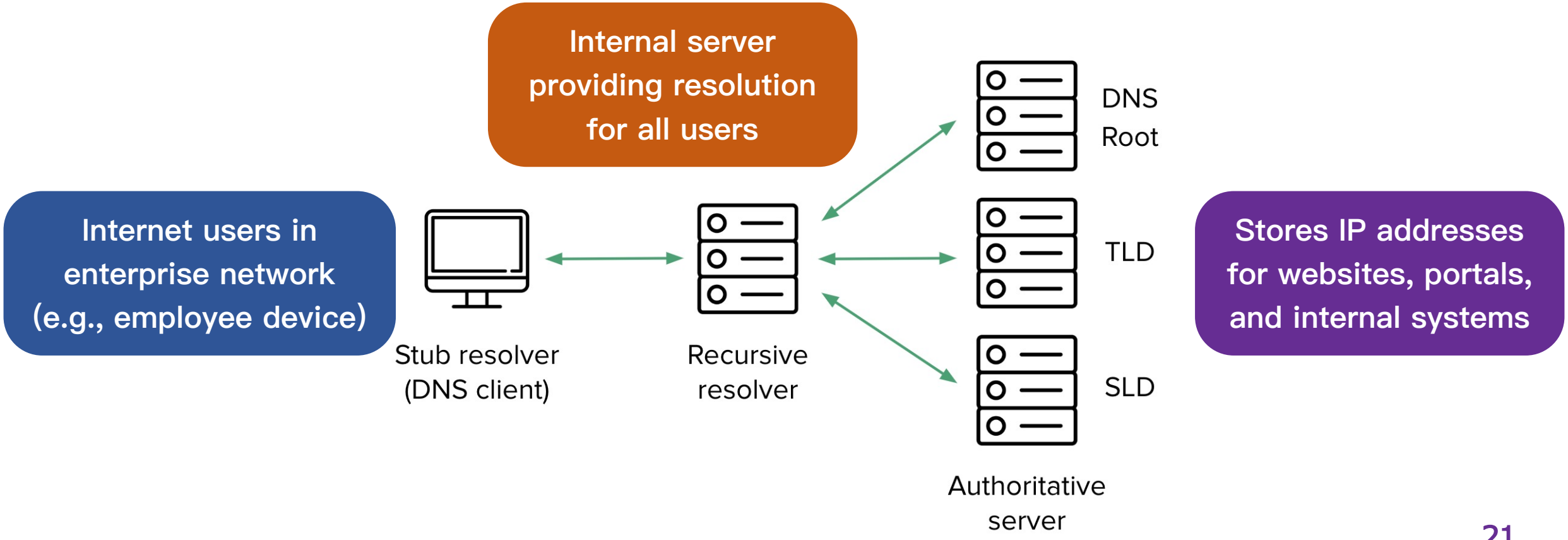
- ❑ 3 components: DNS client, recursive resolver, authoritative servers



How does DNS work?

❑ Why should enterprises care about DNS?

❑ Connection between DNS and enterprise networks

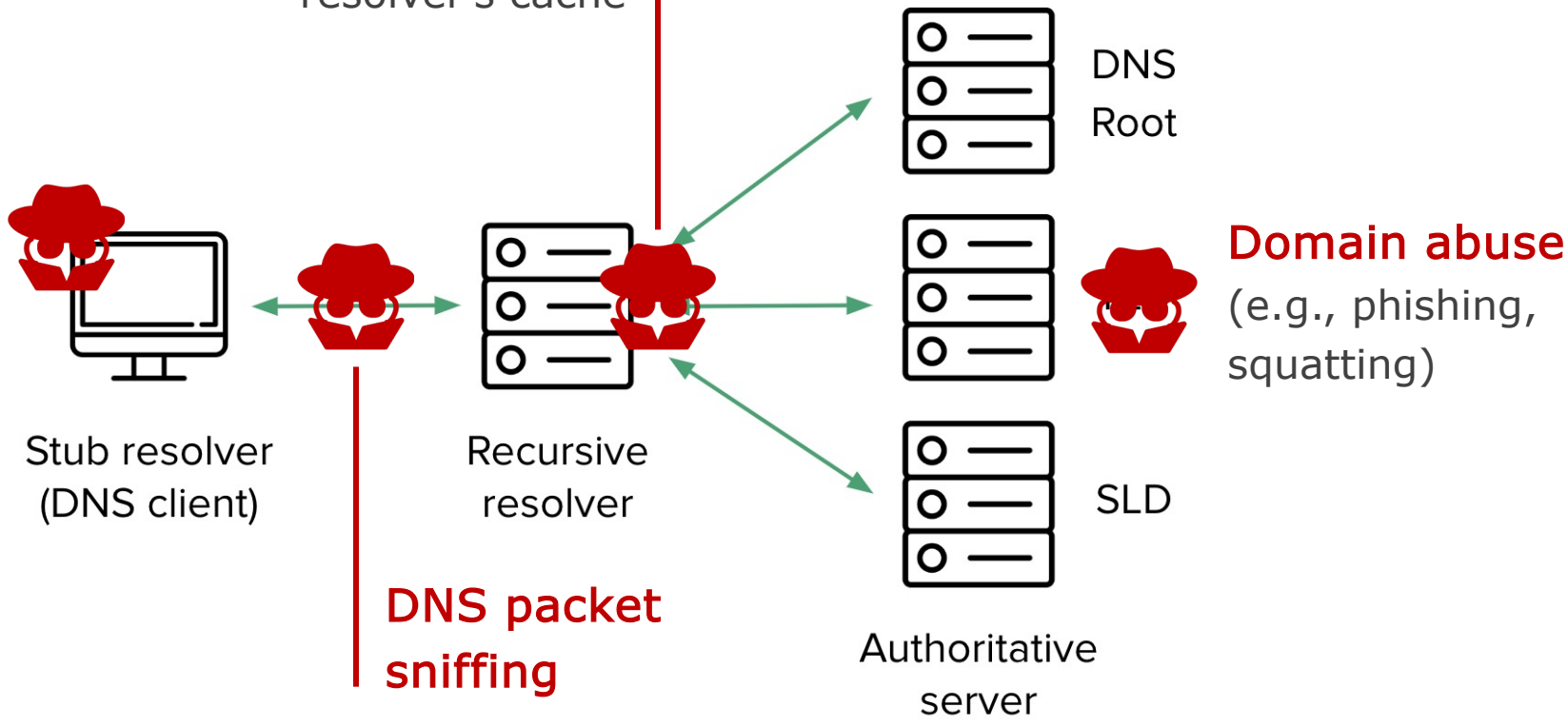


How may DNS go wrong?

❑ Typical security risks of the DNS

Tampering DNS resolver configuration
(e.g., by infected malware)

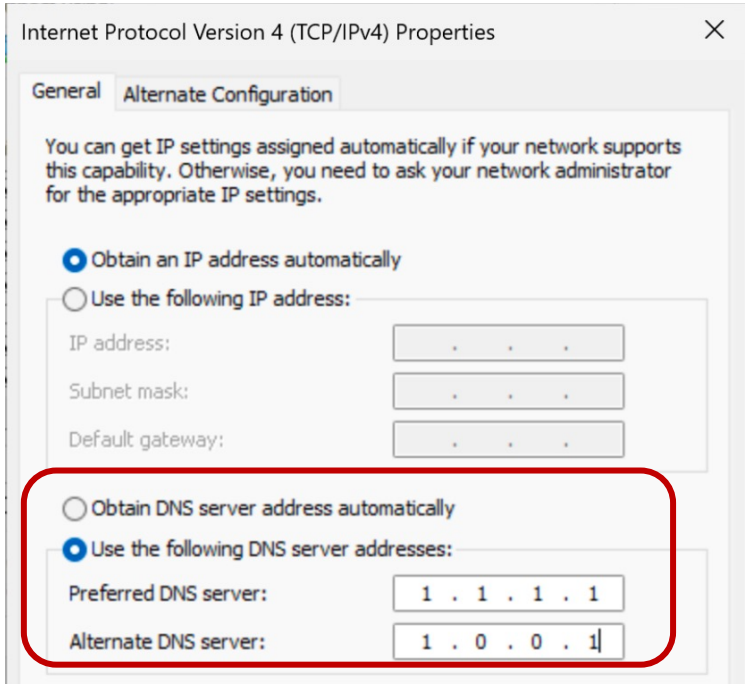
DNS cache poisoning
Writes rogue data into resolver's cache



Typical DNS threats

❑ I. Tampering with DNS configuration

- ❑ Malware changes user OS configurations
- ❑ "It's like forcing you to use attacker's phone book"



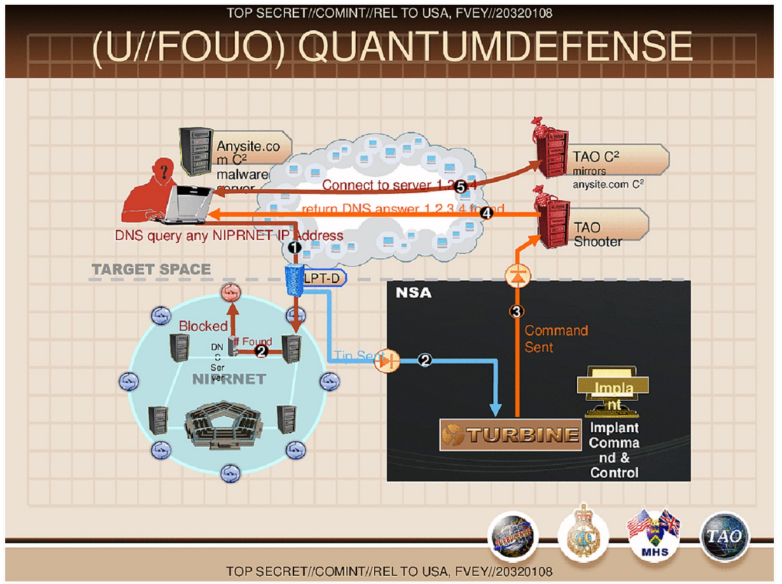
About which DNS resolver to use:

- ❑ By default, allocated automatically from network
- ❑ Users may **configure their preferred server** in OS settings
- ❑ **Malware may tamper with this setting**

Typical DNS threats

II. DNS packet sniffing

- DNS messages are transferred in **plain-text**
- **Everyone on the path may see who's querying what**
- May further build Internet user profile and invade privacy

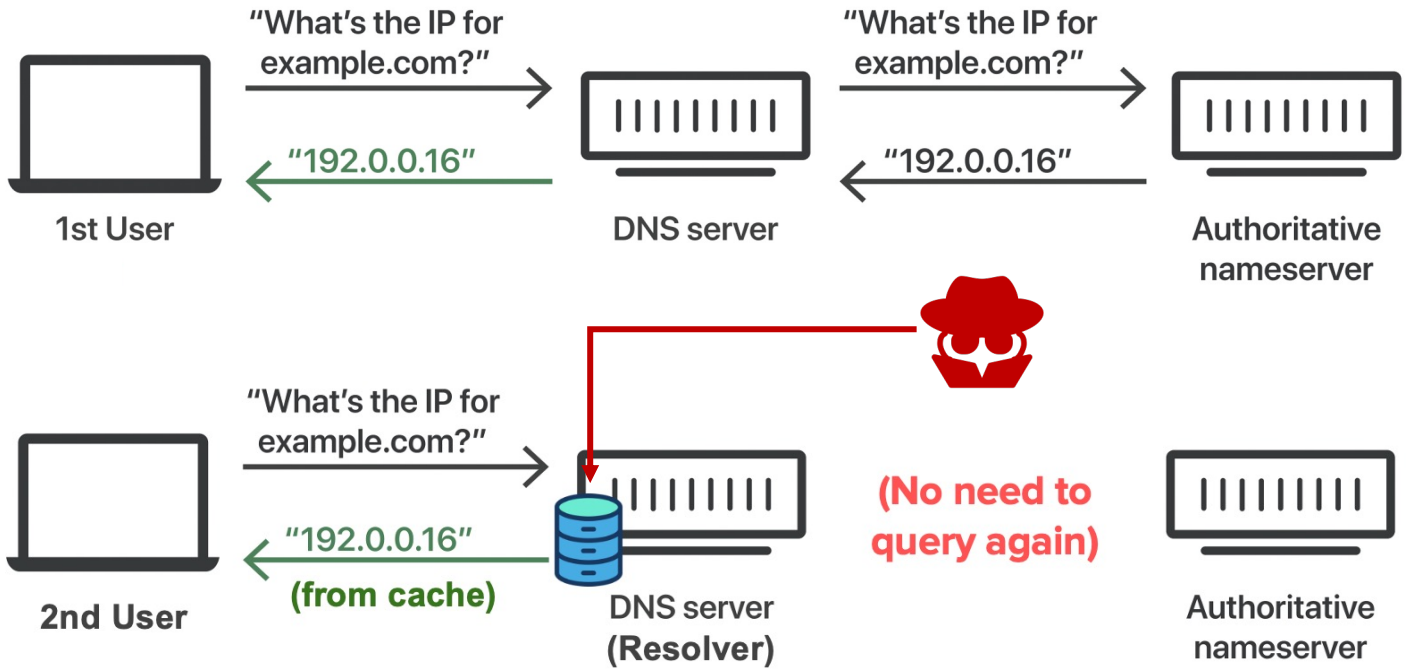


QUANTUM Project that sniffs DNS

Typical DNS threats

❑ III. DNS cache poisoning

- ❑ Recursive resolvers maintain cache to speed up query process



For the 1st user:

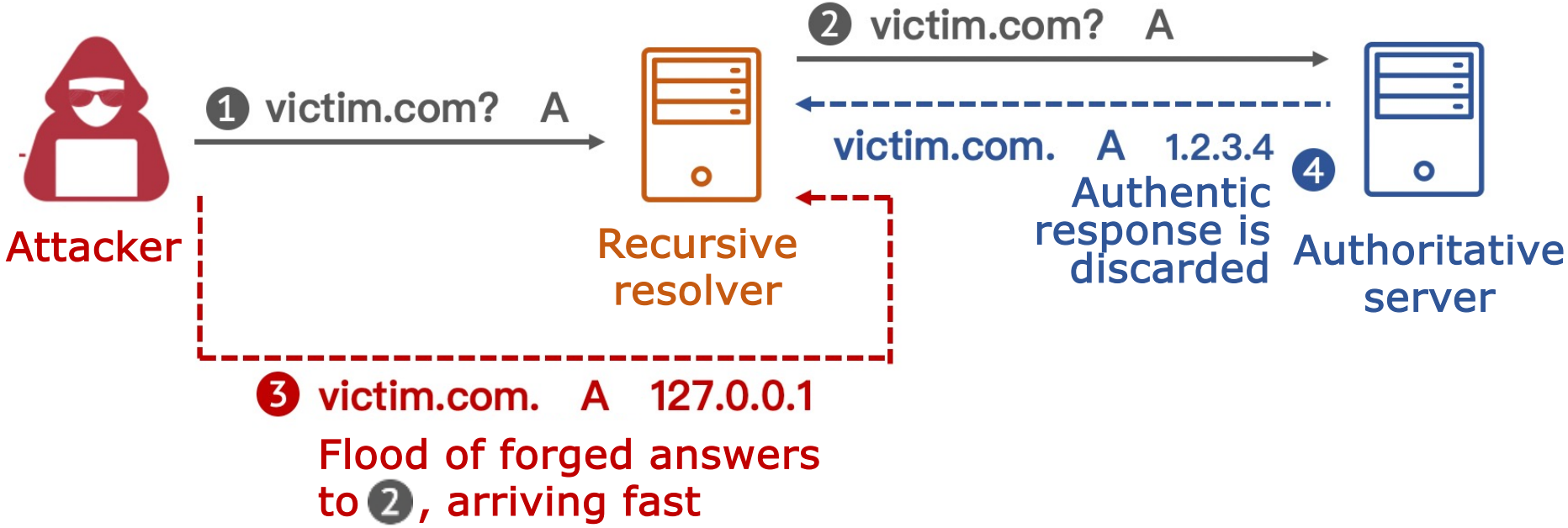
- ❑ DNS resolver queries authoritative servers to get answers.

For the 2nd user and beyond:

- ❑ Cache saves the resolver from repeatedly querying authoritative servers.

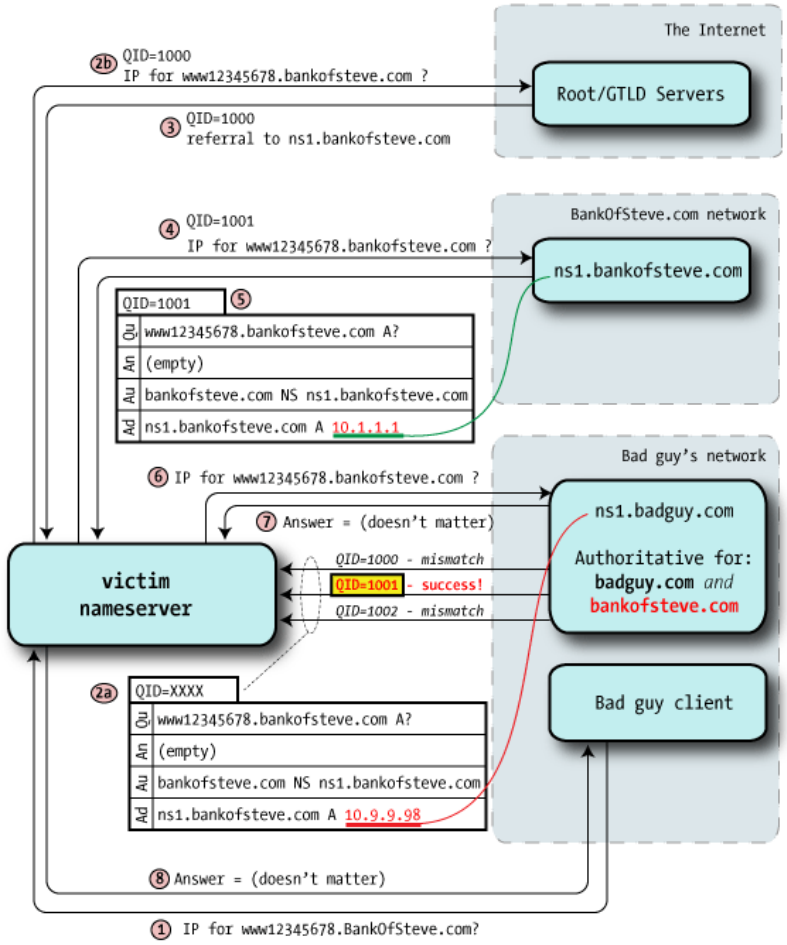
Typical DNS threats

- III. DNS cache poisoning (contd.)
  - Attackers trick resolver into accepting and caching rogue answers
  - Effect persists until cache expires



Typical DNS threats

❑ III. DNS cache poisoning (contd.)



The Kaminsky DNS vulnerability (2008):

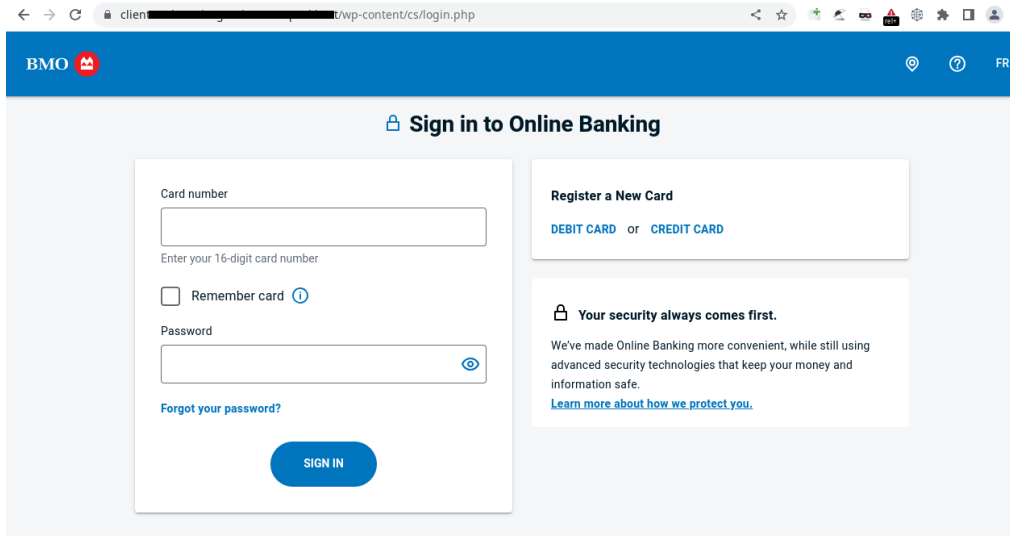
- ❑ Exploits lack of randomness in DNS packets
- ❑ Allows attackers to hijack entire domain zones
- ❑ **Led to DNS server patches world-wide**

Typical DNS threats

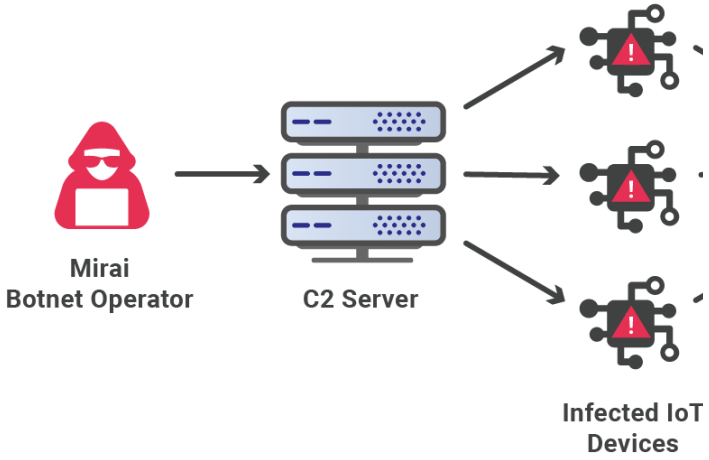
CYBER 100
27TH DECEMBER 2023

❑ IV. Domain abuse

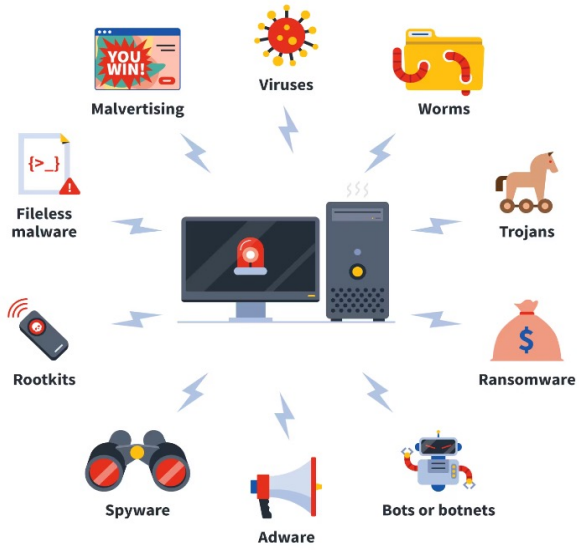
- ❑ Domains can be put into malignant acts!



Phishing websites impersonating brand domains



Botnet Command & Control

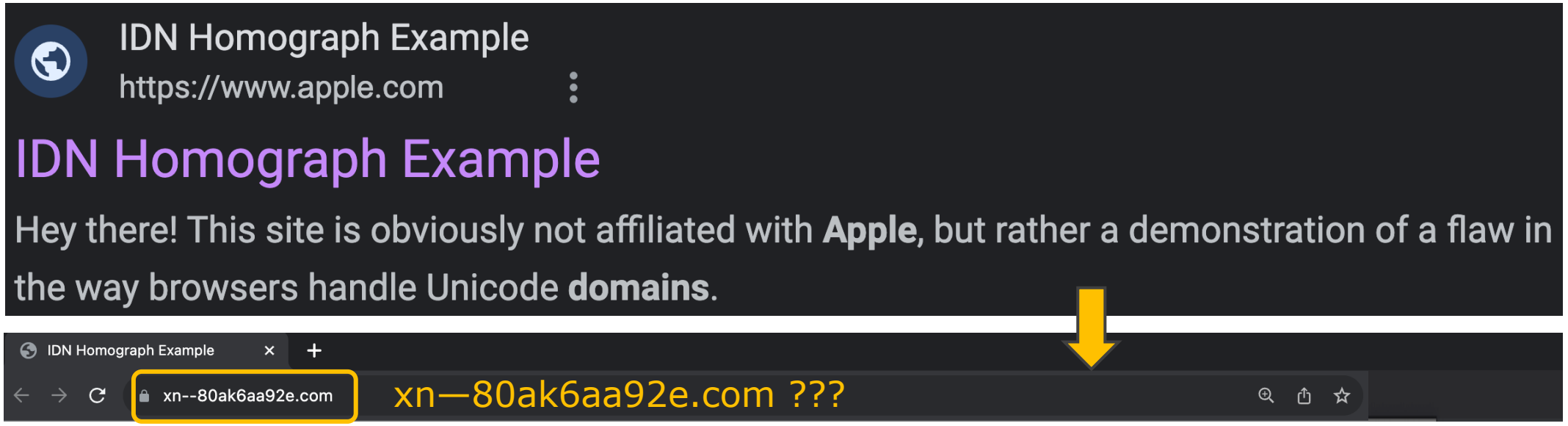


Malware distribution websites

Typical DNS threats

❑ IV. Domain abuse (squatting)

❑ Spot the difference!



Hey there!

This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way browsers handle Unicode domains. This is proof-of-concept works in Chrome 58 and earlier along with all versions of Firefox.

Typical DNS threats

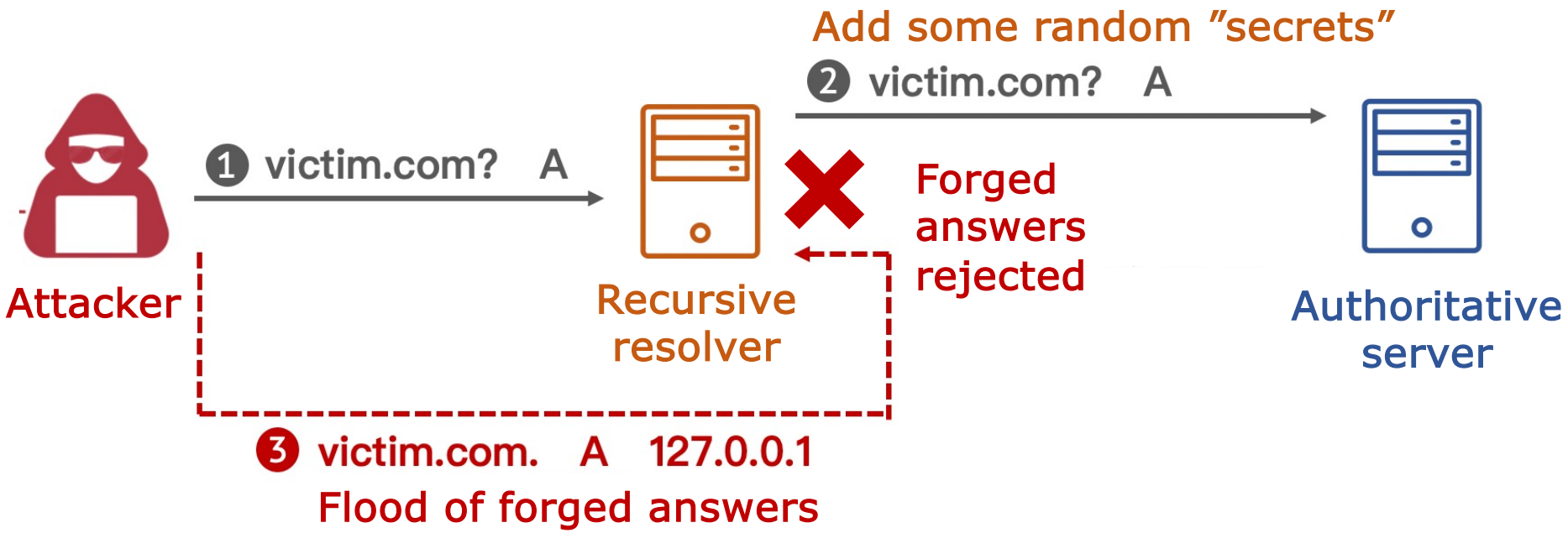
❑ IV. Domain abuse (squatting, contd.)

❑ Domain squatting: impersonating brand domains

Category	How to generate new domains	Examples (for youtube.com)
Typosquatting	Generate typos from keyboards	youtu**eb**.com (switch neighboring letters) y**i**utube.com (replace with neighboring letter on keyboard)
Bitsquatting	Flip binary bits within letters	youtub**u**.com
Combosquatting	Insert new parts into brands	youtube**-videos**.com youtube**customerservice**.com
Levelsquatting	Insert long levels after brands	youtube.com.**youtube-new.com**
Homographic	Use resembling letters	y**0**utube.com (replace with resembling ASCII letters) youtub**ė**.com (replace with resembling letters in other character sets)

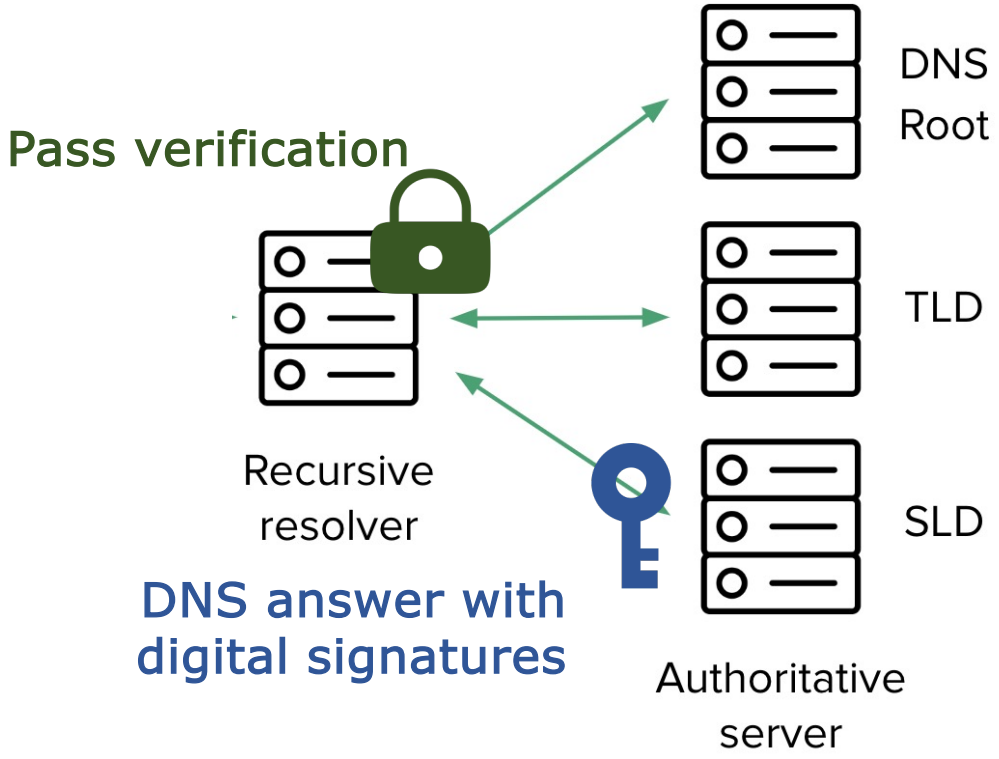
DNS security practices

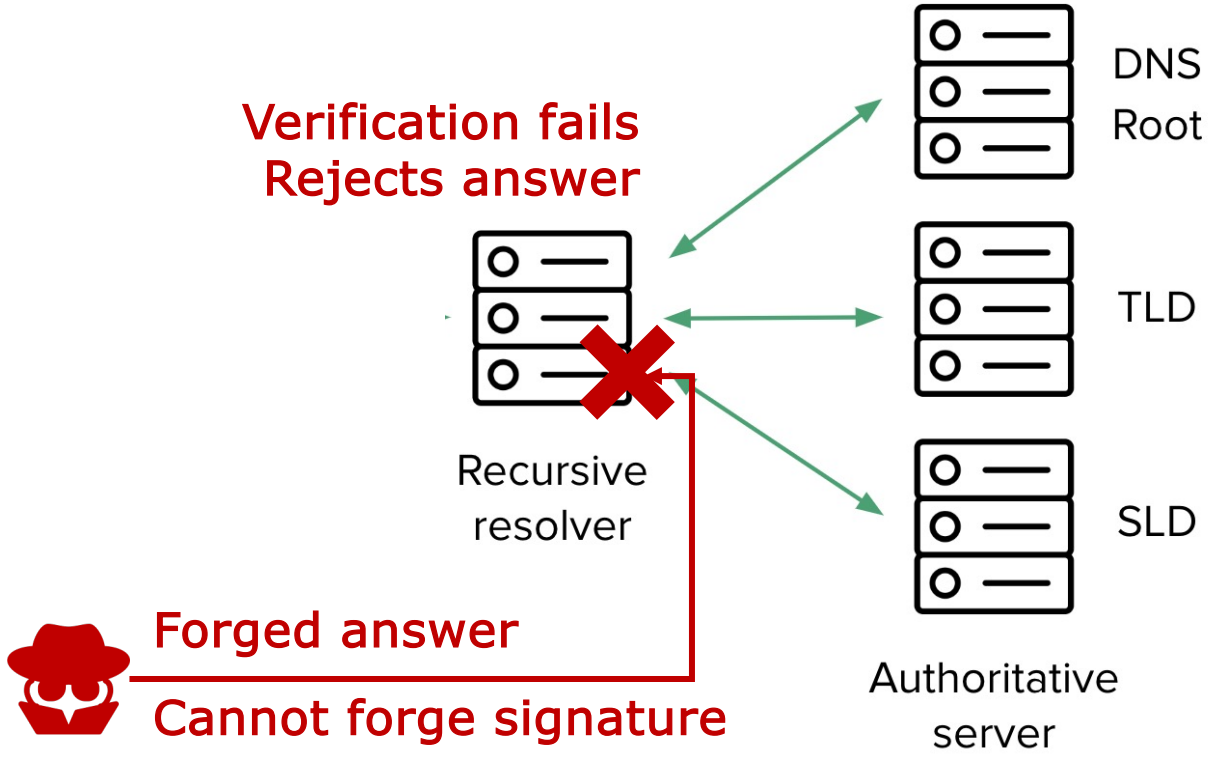
- I. Make resolvers more resilient to forged answers
  - Use latest DNS resolver software
  - Enable port & TXID randomization (by default)
  - Deploy DNS cookies



DNS security practices

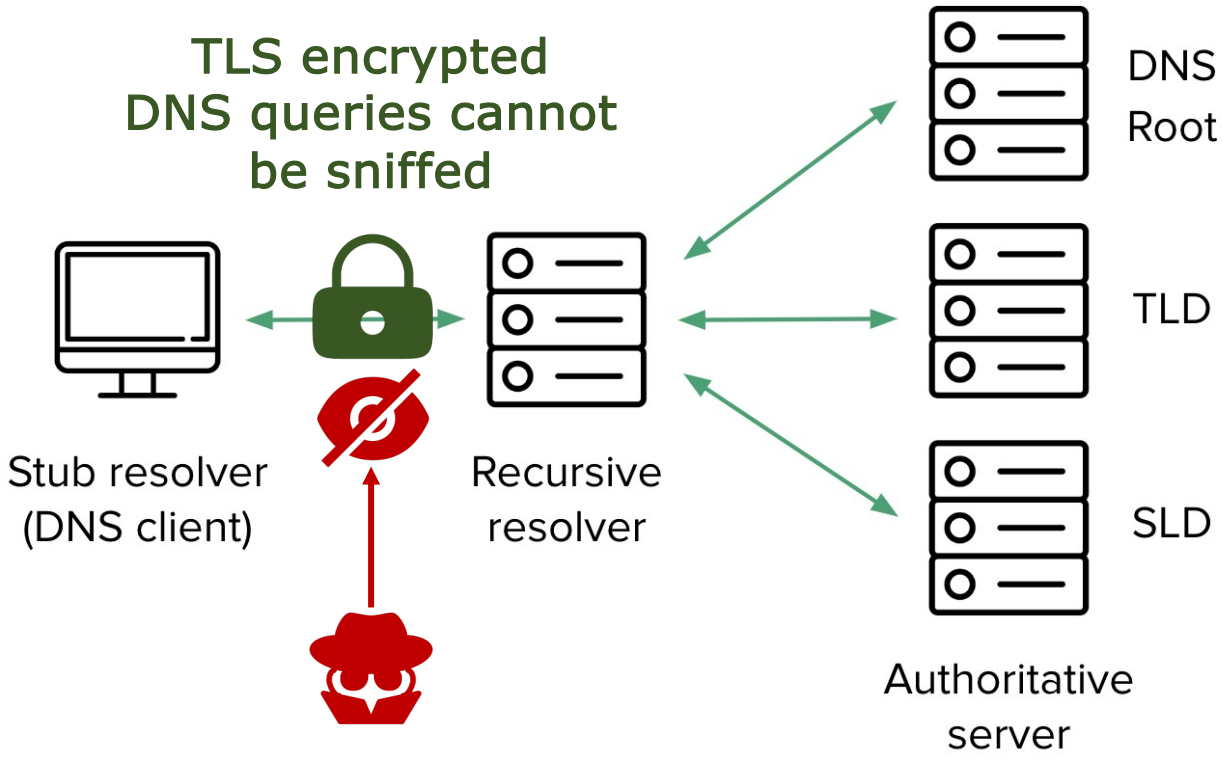
- II. DNSSEC – best practice for data origin authentication
  - Sign your own domains
  - Enable DNSSEC validation on your resolvers





DNS security practices

- III. Encrypted DNS – add confidentiality
  - DNS messages tunneled in encrypted TLS connections
  - Deployed on clients and recursive resolvers



Current protocols:

- DNS-over-TLS (DoT, 2016)
- DNS-over-HTTPS (DoH, 2018)
- DNS-over-QUIC (DOQ, 2022)

Part II.2: Cloud infrastructure & security

- 1 Cloud Hosting Infrastructure
- 2 Common Security Risks
- 3 Secure Practice Suggestions

Public Cloud Hosting Services

❑Concept

- ❑The platforms offering shared resources and infrastructure to customers for hosting their websites, applications, or other content.
- ❑A specialized middlebox between clients and servers.

❑Common types

- ❑Web Hosting, e.g., Cloudflare CDN, WordPress, Alibaba Cloud OSS.
- ❑DNS Hosting, e.g., Godaddy, NS1, UltraDNS, Amazon Route53

❑Advantages to deploy

- ❑Scalability, Reliability, and Security

CLOUDFLARE Alibaba Cloud duda JIMDO Microsoft Azure

Public Cloud Hosting Services

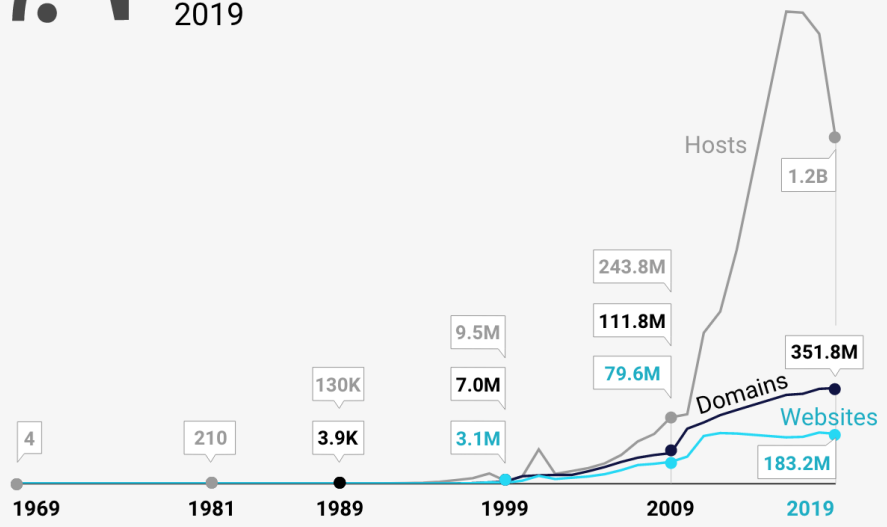
- **Example: Content Delivery Networks (CDNs)**
  - Globally Distributed: a large volume of servers on Internet backbone
  - Cache then Forward: act as the Reverse Proxy to the website
  - Proximity Service: redirect the user's request to the nearest server
  - DDoS Protection: off-load traffic from botnet-based DDoS attack

Public Cloud Hosting Services

- Public hosting services have emerged as popular choices for a majority of websites.

Web Hosting Statistics 2023: State of The Website Hosting Industry

The growth chart with number of web hosts, domain names, and websites from 1969 to 2019

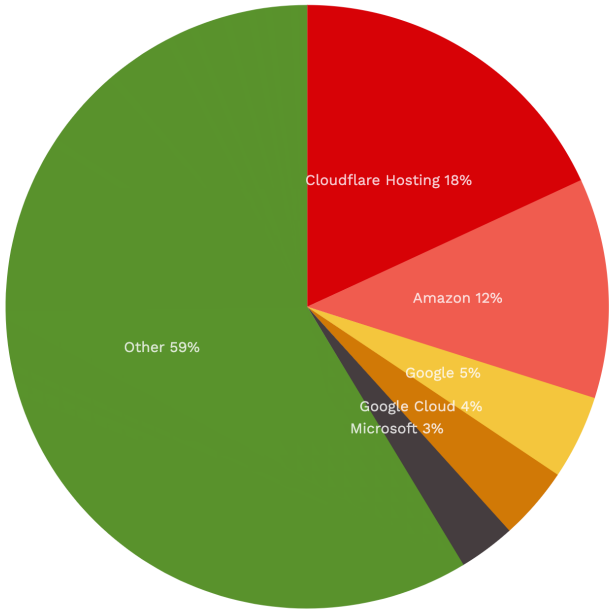


Source: netvalley .com, firstsitefuide.com

firstsiteguide.com

Web Hosting Usage Distribution in the Top 1 Million Sites

Distribution for websites using Web Hosting providers



2,626,349 Detections

of Web Hosting Providers in the Top 1 Million Sites. Last updated 19th Dec 2023.

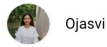
U.S. Server Location is currently the most popular technology in this category.

Top 1m Top 1,000,000 sites by traffic	2,626,349
Top 100k Top 100,000 sites by traffic	390,371
Top 10k Top 10,000 sites by traffic	47,698
Entire Internet	798,535,766
United States	138,658,943
United Kingdom	22,104,973
Germany	18,738,682
Russia	10,311,602
France	8,089,637
China	7,538,442
Netherlands	6,533,103

Significance of Security in Cloud Services

- Network failures and security flaws in public hosting platforms can result in widespread service interruptions, resource abuse, and data leaks.

AWS Outage: Facebook, Netflix, Ring & Disney Plus Among Affected Services



Ojasvi Nath Assistant Editor, Spiceworks Ziff Davis December 8, 2021

The service interruption resulted in longer loading times and disruptions for a large portion of the internet and has affected everything from Alexa, Prime Video, Netflix, Hulu, Roku, Facebook, and Ring security cameras to Disney Plus and League of Legends.

SOCRadar®
Extension to Your SOC Team!

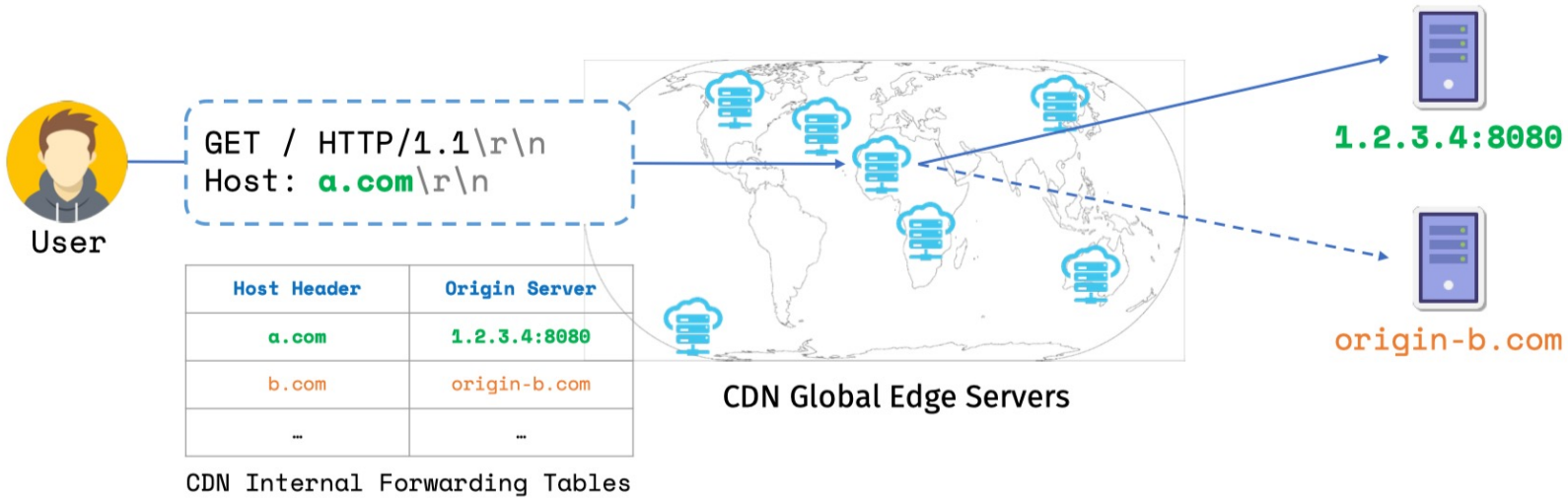
Sensitive Data of 65,000+ Entities in 111 Countries Leaked due to a Single Misconfigured Data Bucket

October 19, 2022

SOCRadar has detected that sensitive data of **65,000 entities became public** because of a misconfigured server. The leak includes **Proof-of-Execution (PoE)** and **Statement of Work (SoW)** documents, user information, product orders/offers, project details, **PII (Personally Identifiable Information)** data, and documents that may reveal intellectual property.

Common Network Security Risks

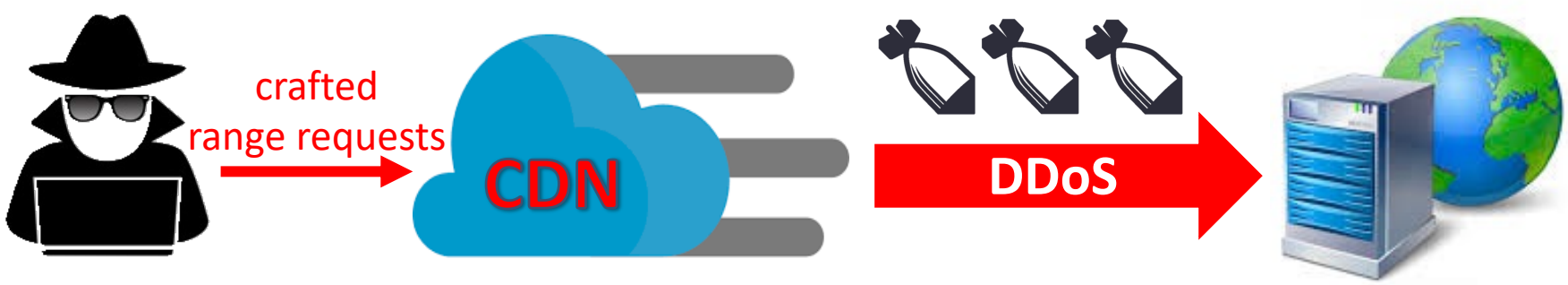
- CDN lacks of ownership verification for the Origin Server
  - CDN can be configured to fetch resource from any IP and any port



- Some CDNs lack of ownership verification for Deployed Custom Domains.
  - Anyone can deploy any domain names without authority to flawed hosting platforms.

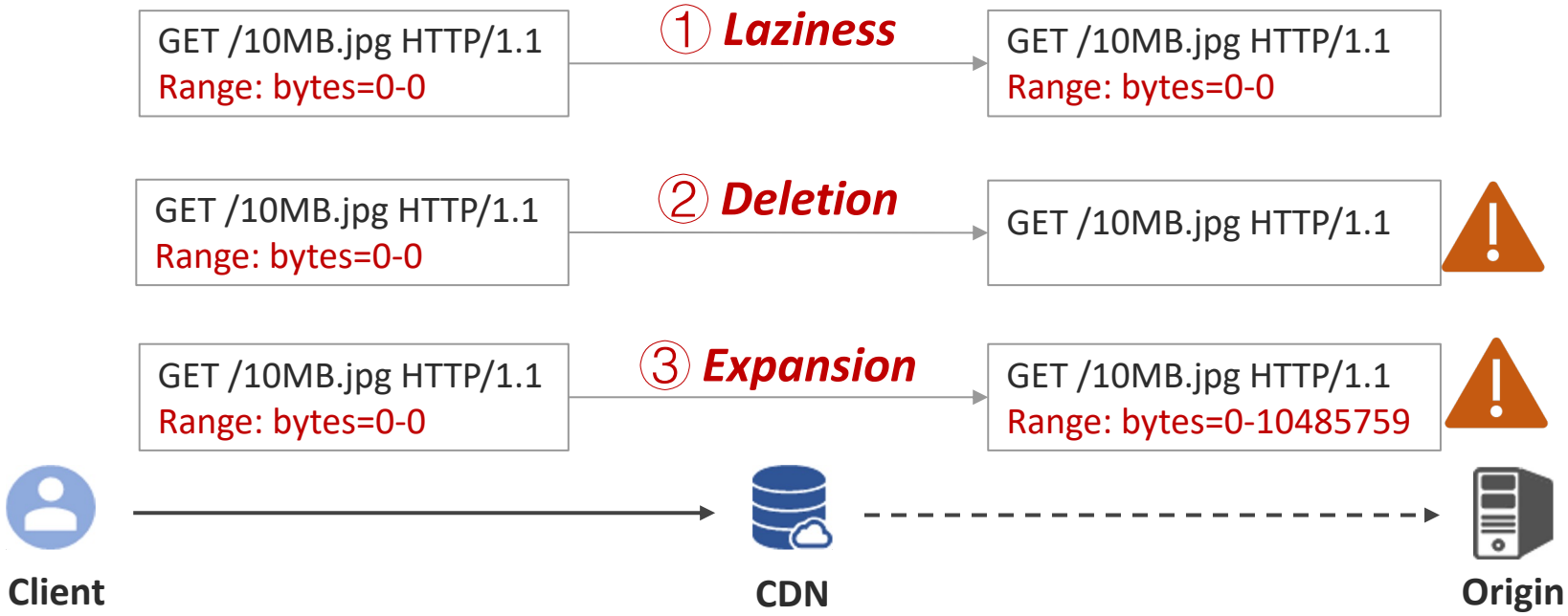
Common Network Security Risks

- Denial-of-service (DoS) attack
- Shared resources reuse and abuse
- Network sniffing and hijacking



Threat I: Range-based Amplification Attack

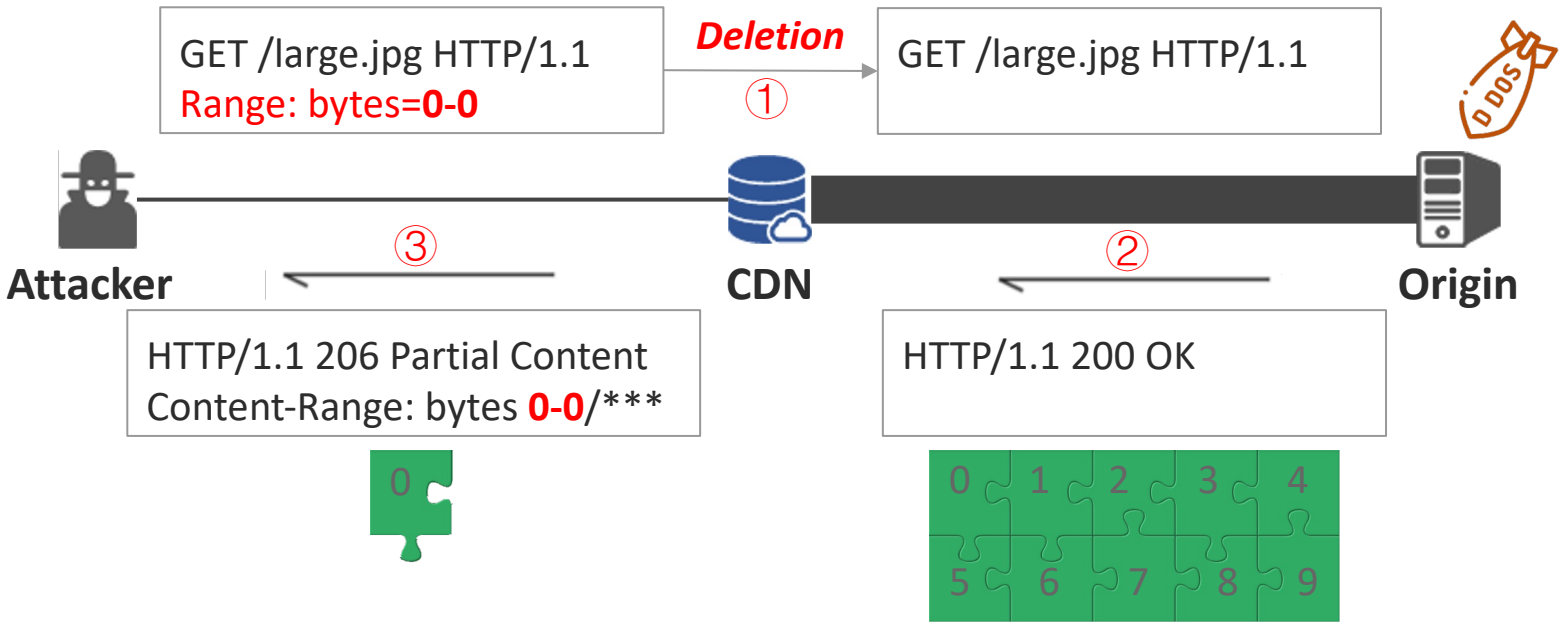
- HTTP Range Header: allow clients to indicate byte ranges; only the desired part is transferred
- Different CDN vendors adopt various Range policies:



[DSN 2020, Best Paper Award] CDN Backfired: Amplification Attacks Based on HTTP Range Requests

Threat I: Range-based Amplification Attack

- A CDN platform may increase the requested bytes from origin servers, leading to DDoS attacks toward the back-end websites.



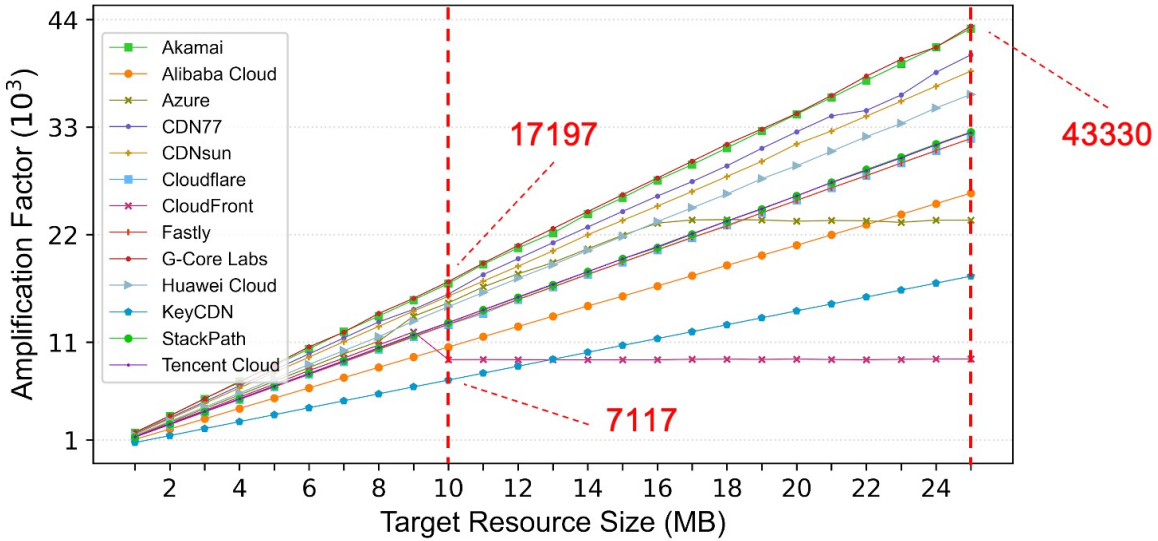
[DSN 2020, Best Paper Award] CDN Backfired: Amplification Attacks Based on HTTP Range Requests

Threat I: Range-based Amplification Attack

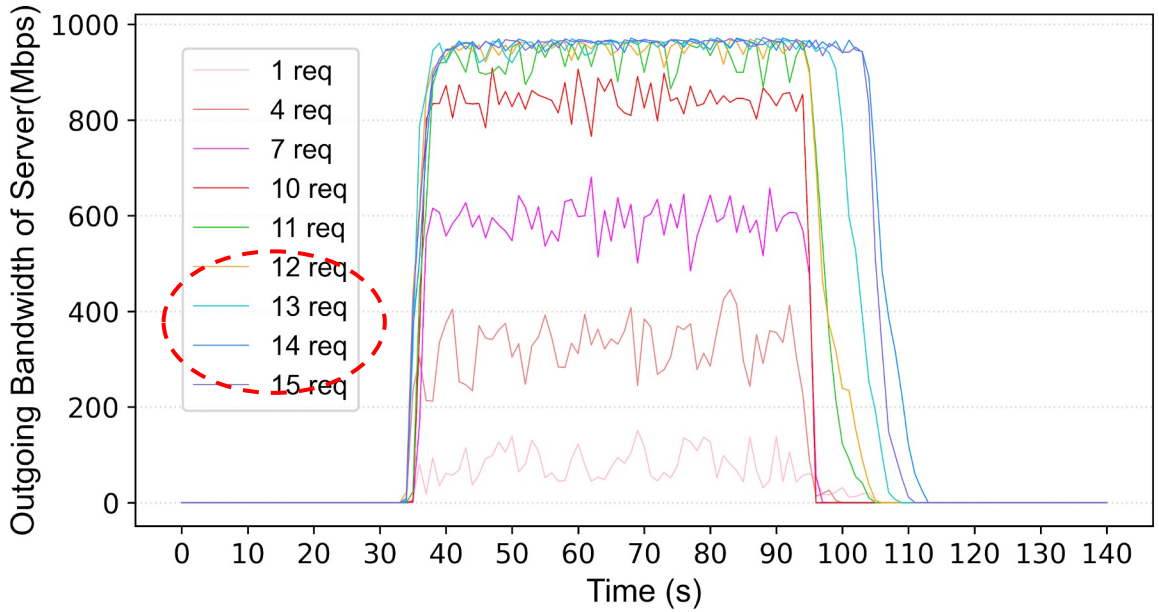
- 13 popular CDN vendors are vulnerable.

CLOUDFLARE Tencent Cloud HUAWEI Alibaba Cloud fastly

- Amplification factor can be extremely high, making the origin's outgoing bandwidth exhausted.



Amplification Factors vs. Target Resource Sizes

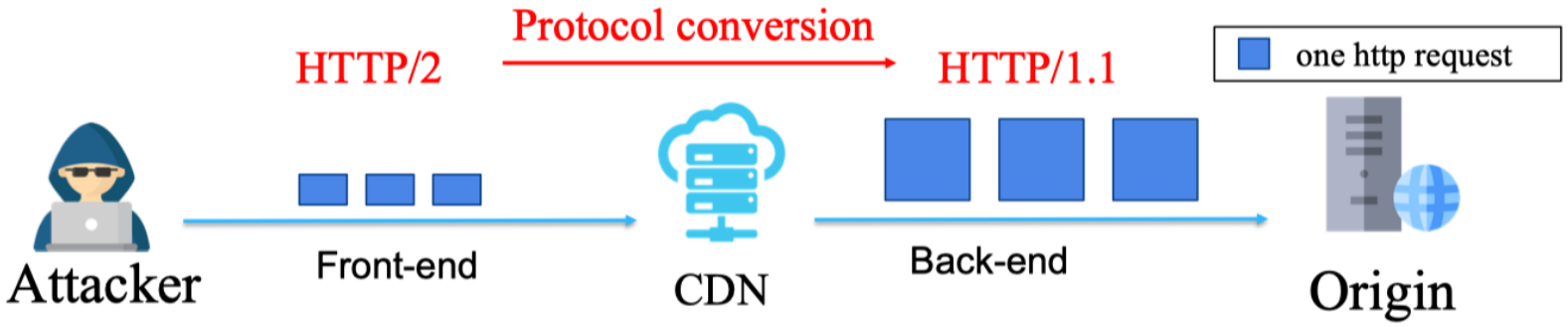


Origin's Outgoing Bandwidth Consumption

[DSN 2020, Best Paper Award] CDN Backfired: Amplification Attacks Based on HTTP Range Requests

Threat II: HTTP/2 Amplification Attack

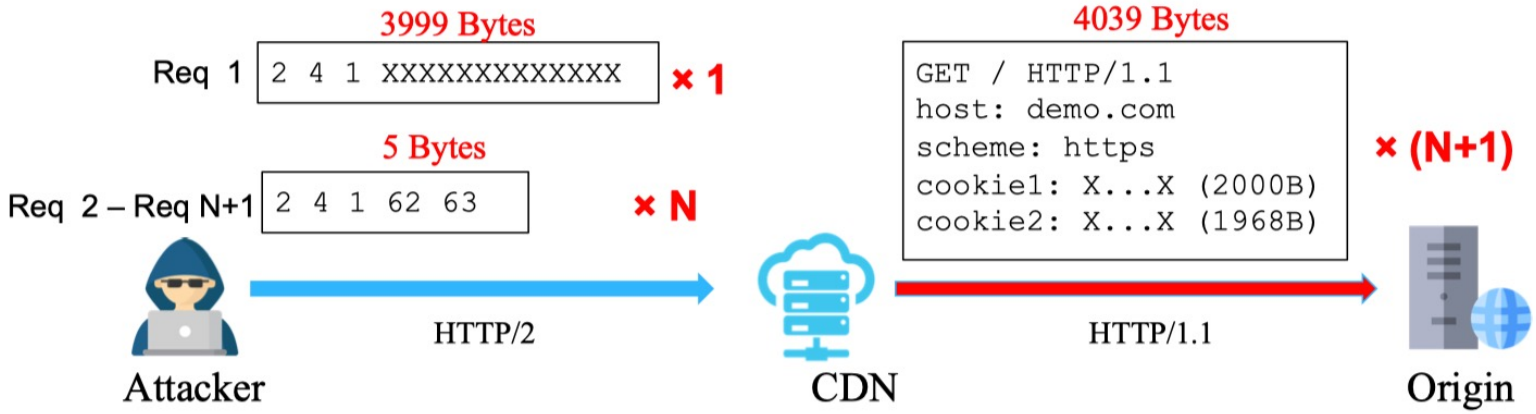
- HTTP/2 features
  - Compression: reduce header redundancy
  - Connection reuse: reduce TCP connections
- However, HTTP/2-HTTP/1.1 conversion of CDN will cause amplification attack.



[NDSS 2020] CDN Judo : Breaking the CDN DoS Protection with Itself

Threat II: HTTP/2 Amplification Attack

- HTTP/2 features
  - Compression: reduce header redundancy
  - Connection reuse: reduce TCP connections
- However, HTTP/2-HTTP/1.1 conversion of CDN will cause amplification attack.
- For example:



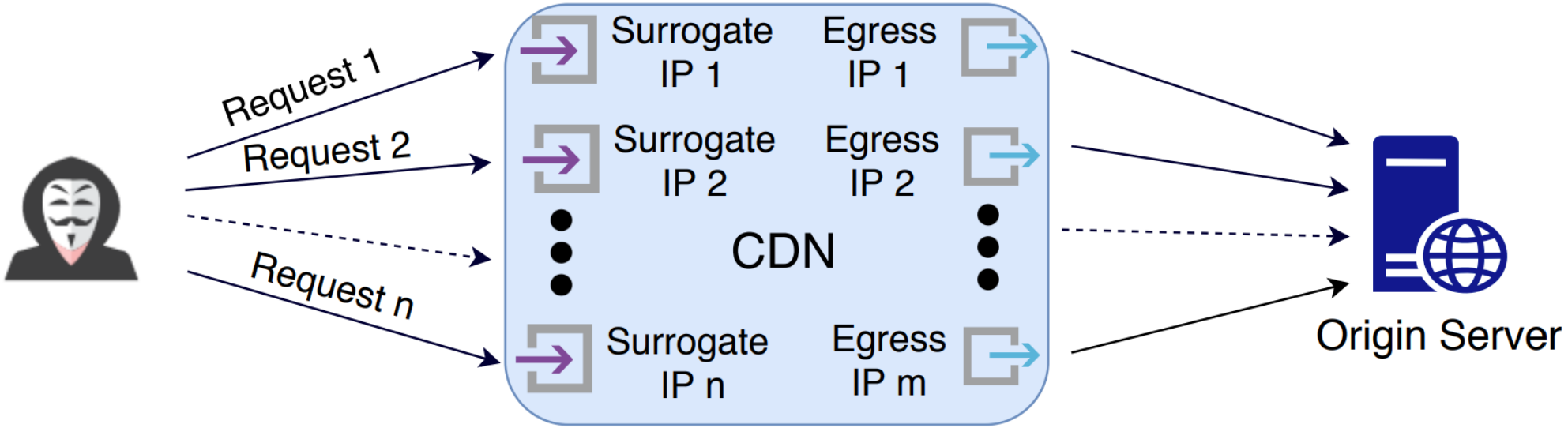
Bandwidth amplification factor: $4039B \times (N+1) \; / \; 3999B + 5B \times N = \frac{4039 + 4039N}{3999 + 5N}$

For example, when N is 100, the factor is 88.70.

[NDSS 2020] CDN Judo : Breaking the CDN DoS Protection with Itself

Threat II: HTTP/2 Amplification Attack

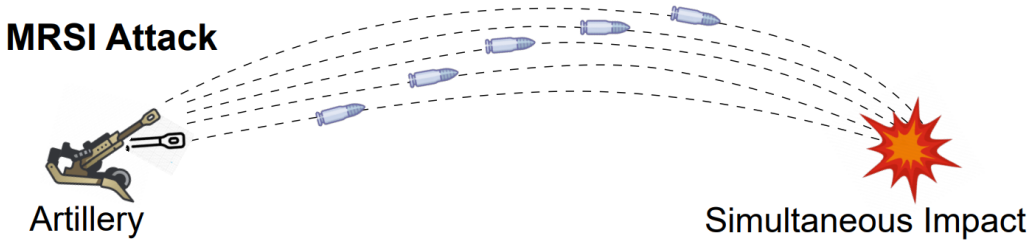
- Through sending requests to ingress IPs directly to simulate global access, a CDN is abused to proxy a DoS attack into a DDoS attack.



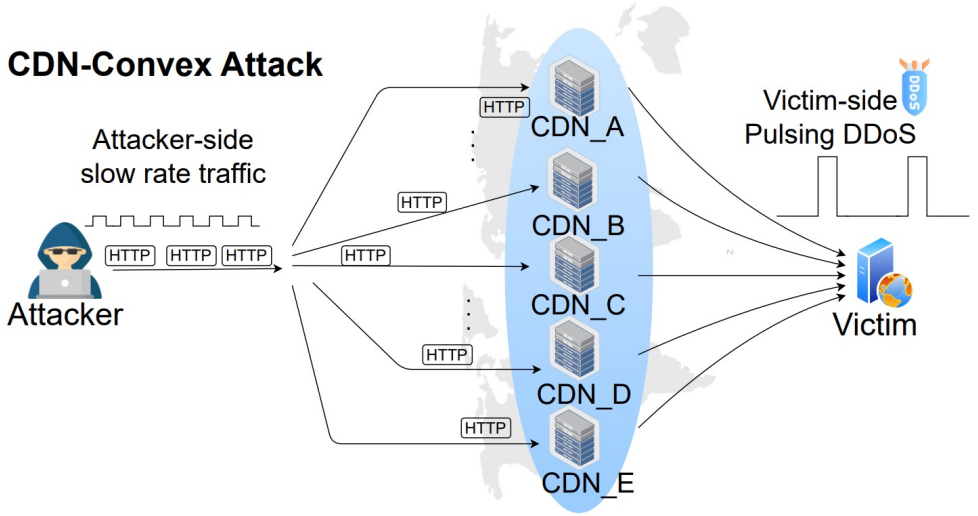
[NDSS 2020] CDN Judo : Breaking the CDN DoS Protection with Itself

Threat III: CDN-Convex Lens Attack

- Analogous to the military tactic "Multiple Round Simultaneous Impact (MRSI)"
- Leverage distributed edge servers of CDN to perform DDoS attack



MRSI Attack



CDN-Convex Lens Attack Model

[Usenix Security 2023] Temporal CDN-Convex Lens A CDN Assisted Practical Pulsing DDoS Attack

Threat IV: Subdomain Takeover Attack

- Adversaries could exploit the domain names outside of their authority for malicious activities
  - Botnet, phishing, malware distribution, etc.

Cited from bleepingcomputer.com

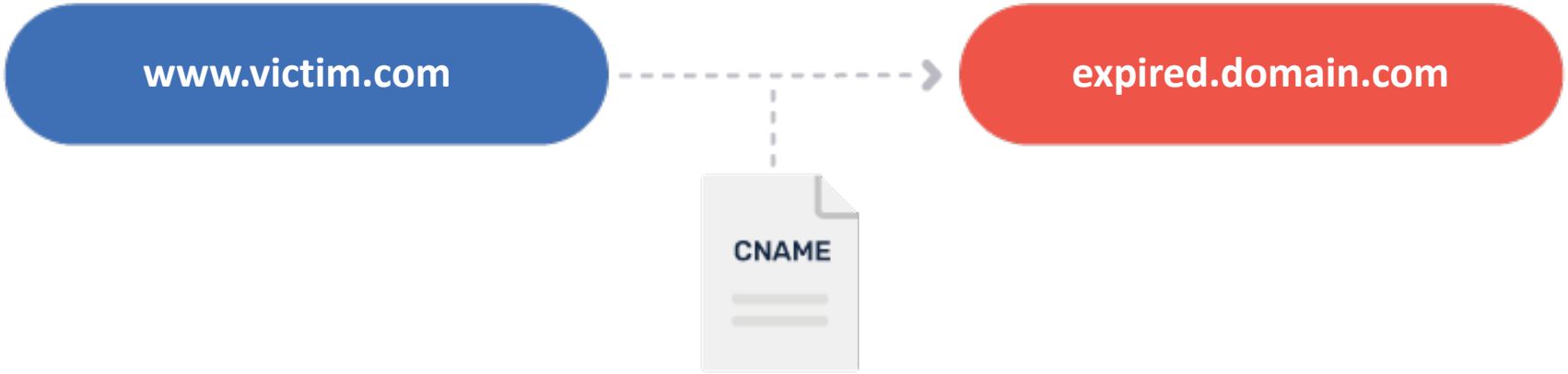
Cited from scmp.com

Cited from norton.com

[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat IV: Subdomain Takeover Attack

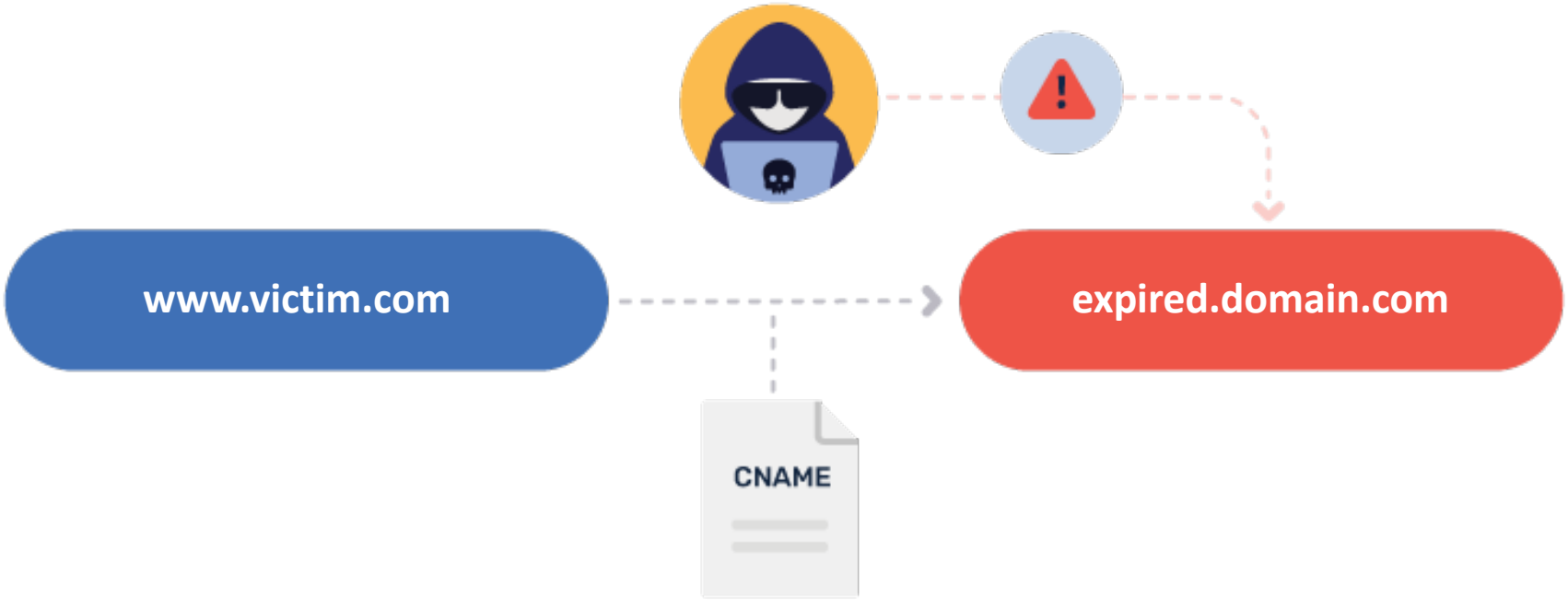
- Subdomain takeover threats are constantly emerging!
- Subdomain takeover may occur when a domain is pointed to a released or expired resource.



[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat IV: Subdomain Takeover Attack

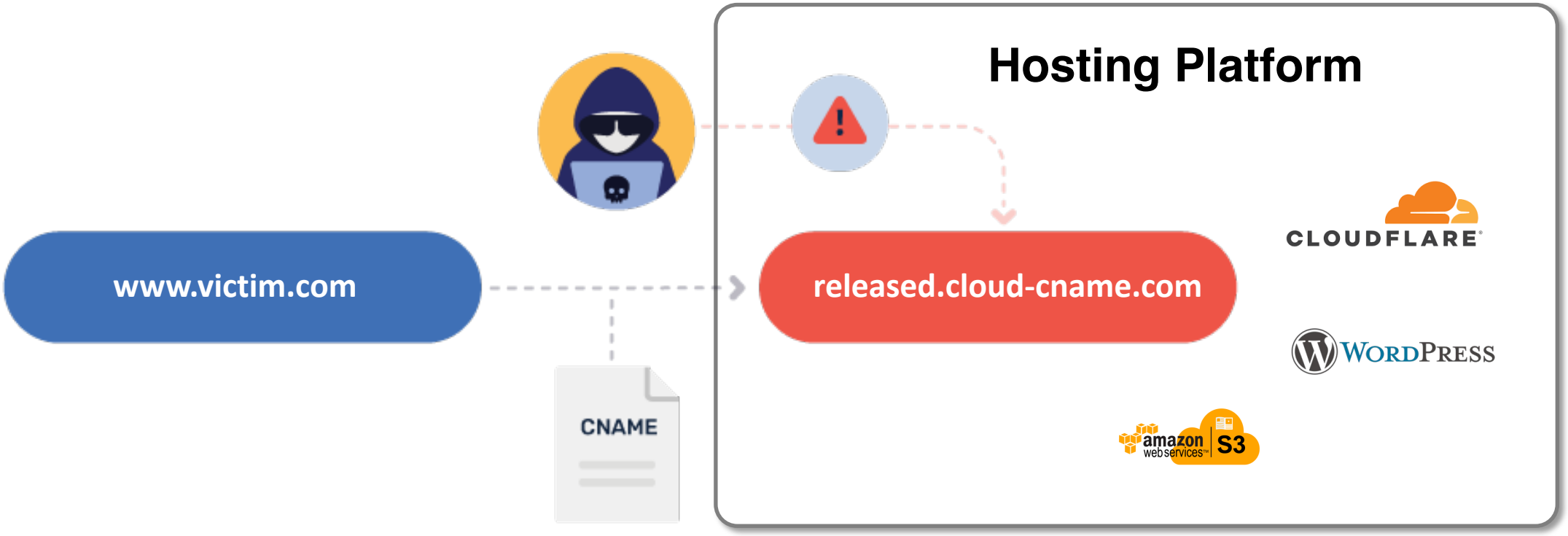
- What if the released resources can be reused by the attackers?



[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat IV: Subdomain Takeover Attack

- The released resources can be discontinued services of public hosting platforms or deprovisioned Cloud IPs.

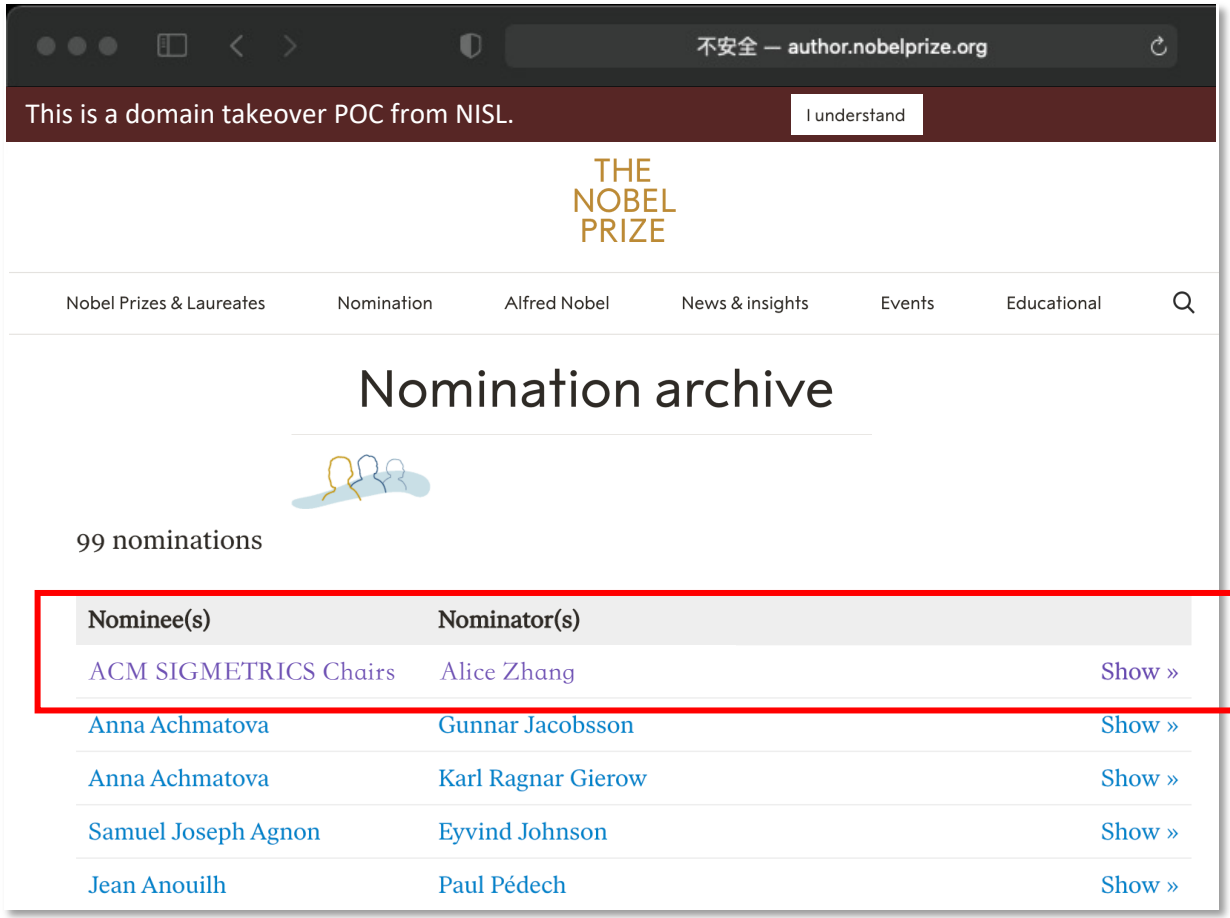


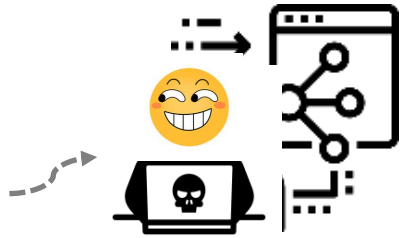
[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat IV: Subdomain Takeover Attack

- Seeing is not believing...

author.nobelprize.org





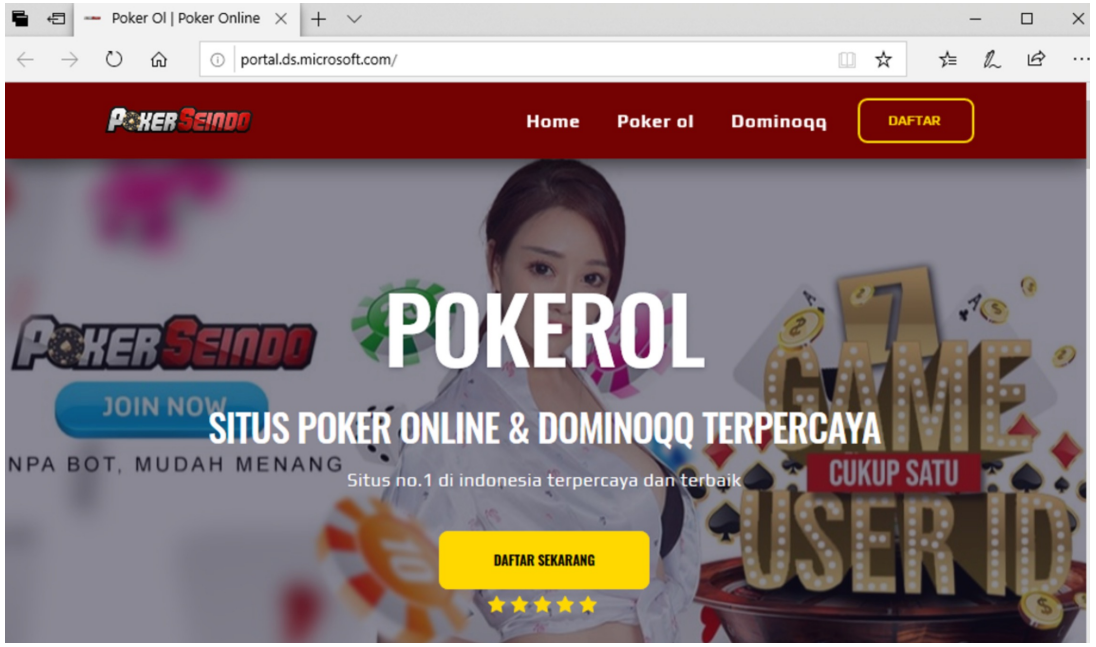
Attacker

[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat IV: Subdomain Takeover Attack

- Subdomain takeover threats are constantly emerging!

Hundreds of Microsoft domains are vulnerable.



A real-world example of taking over Microsoft's domain.

[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat IV: Subdomain Takeover Attack

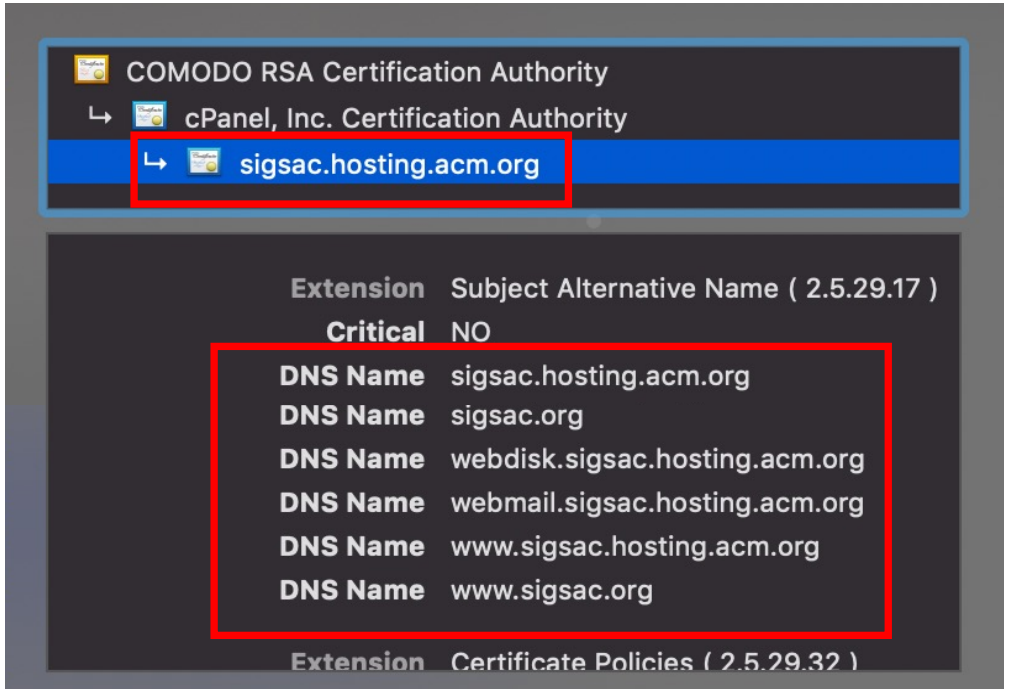
- Over 65 hosting services are vulnerable to domain takeover, including
  - Cloud Storage, CDN, Website Builder, DNS Hosting...
- Top 20 hosting vendors with 70% market share are vulnerable.

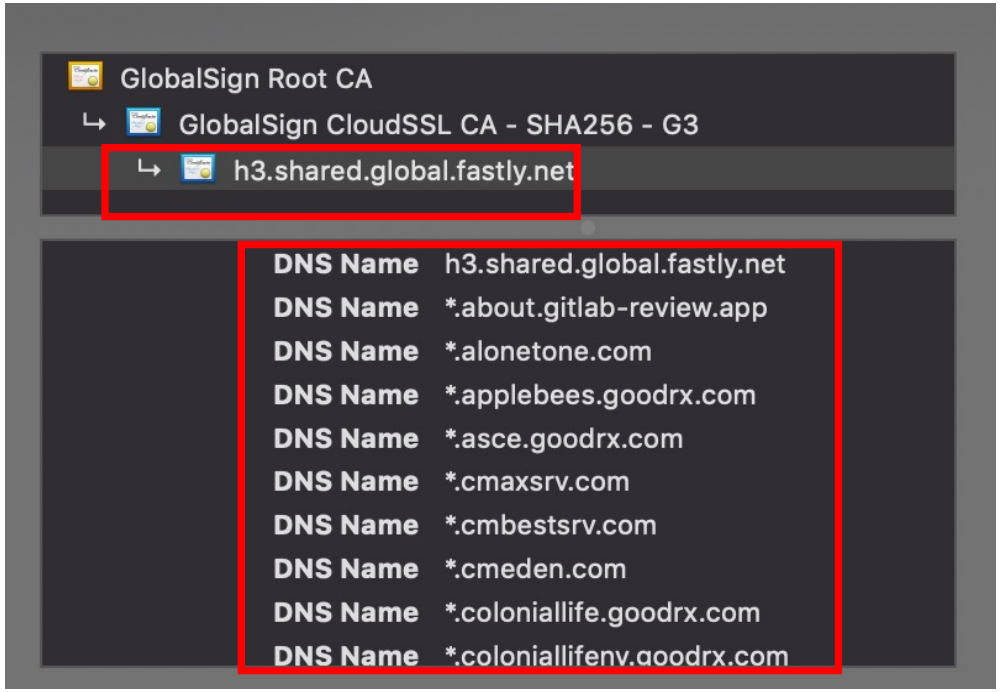
- Over 10,351 FQDNs are vulnerable to hijacking attacks, affecting
  - Famous universities (e.g., Stanford, Rice), corporations (e.g., Marriott, The Walt Disney Company, Mckesson), organizations (e.g., Nobel Prize)

[SIGMETRICS 2023] Detecting and Measuring Security Risks of Hosting-Based Dangling Domains

Threat V: TLS Certificate Sharing

- Public hosting vendors tend to share TLS certificates for multiple customers
  - One certificate for multiple domains: Multi-domain and Wildcard certificates
  - Multiple servers with one certificate: Sharing the same certificate is common (e.g., CDN nodes, virtual hosts, associated services, commercial cooperation parties)

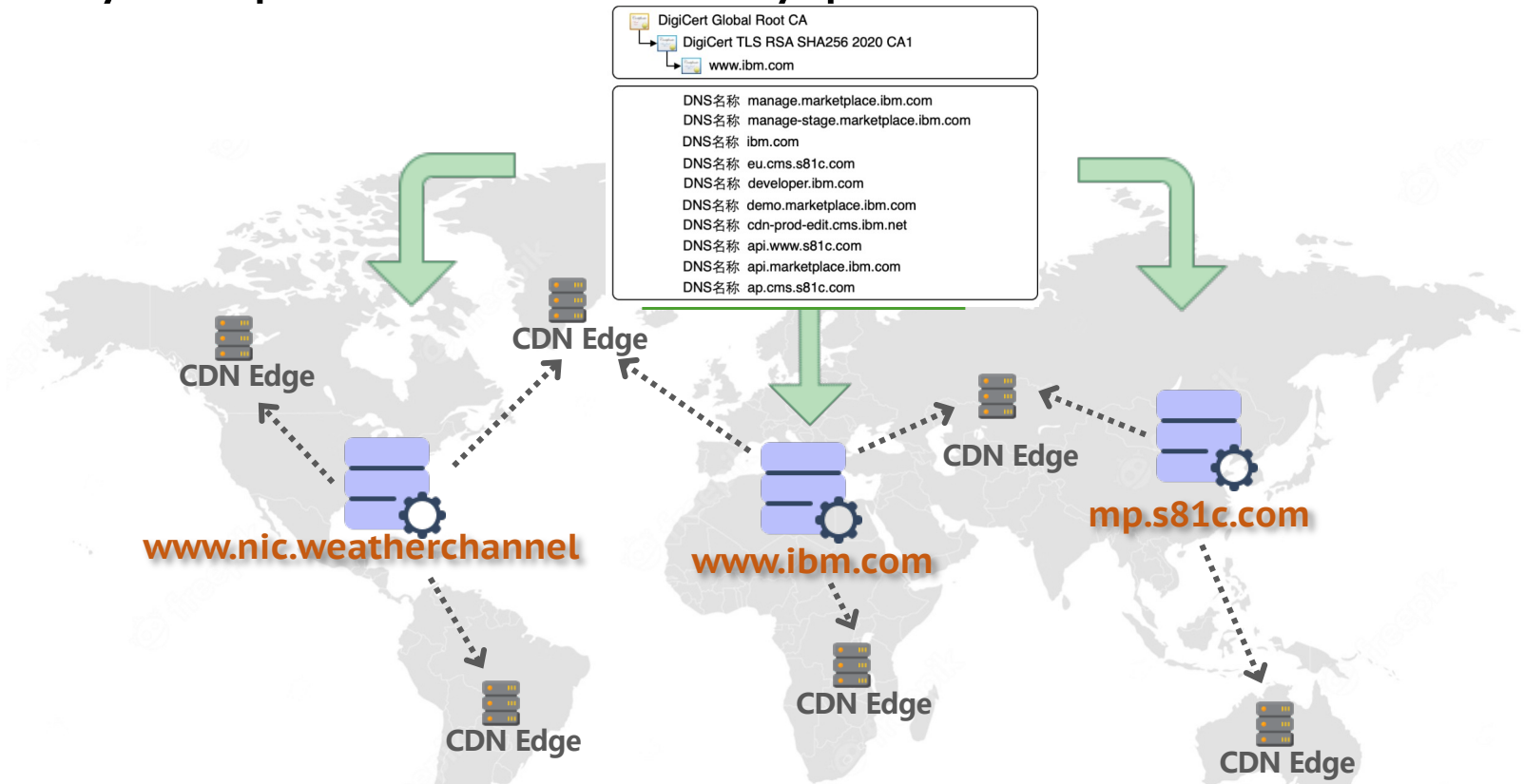




[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

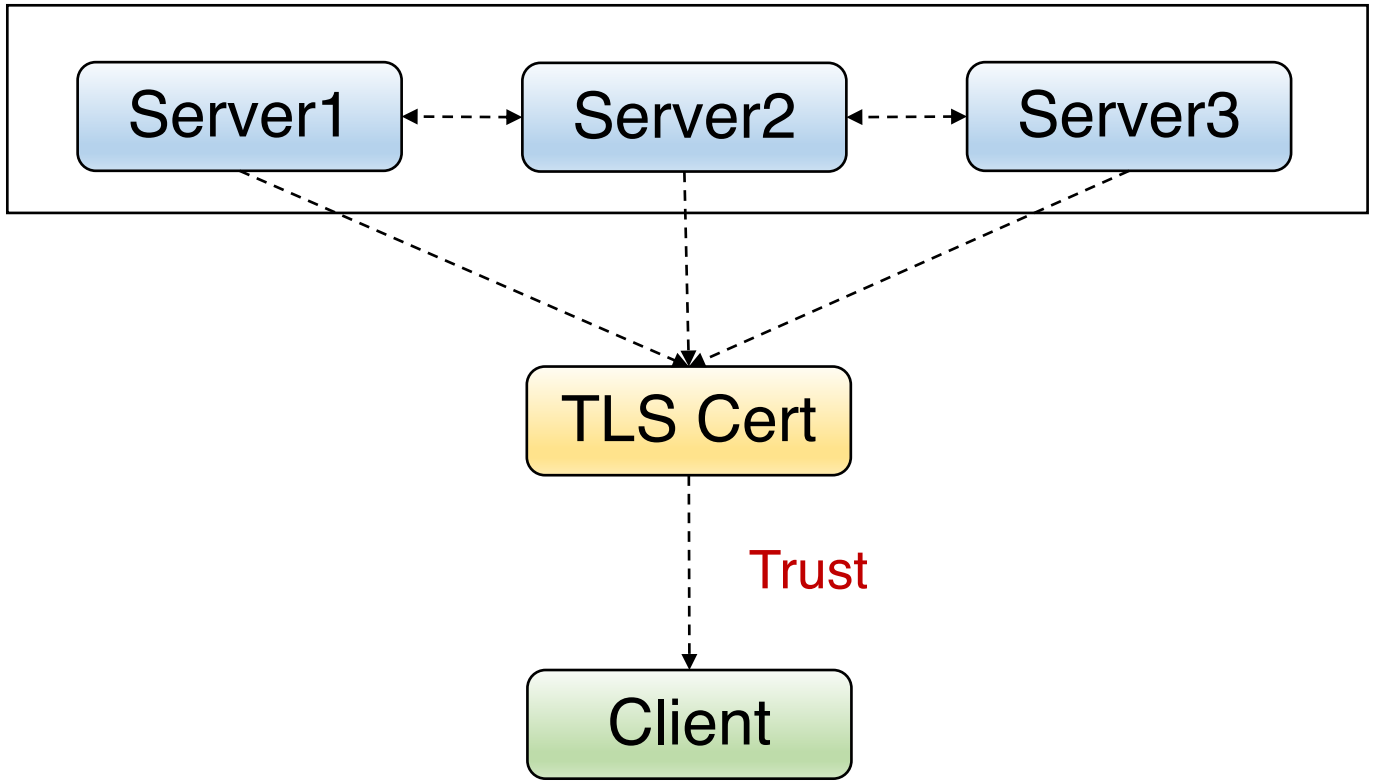
- The websites sharing one certificate may controlled by different parties.
- They may adopt different security practices.



[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

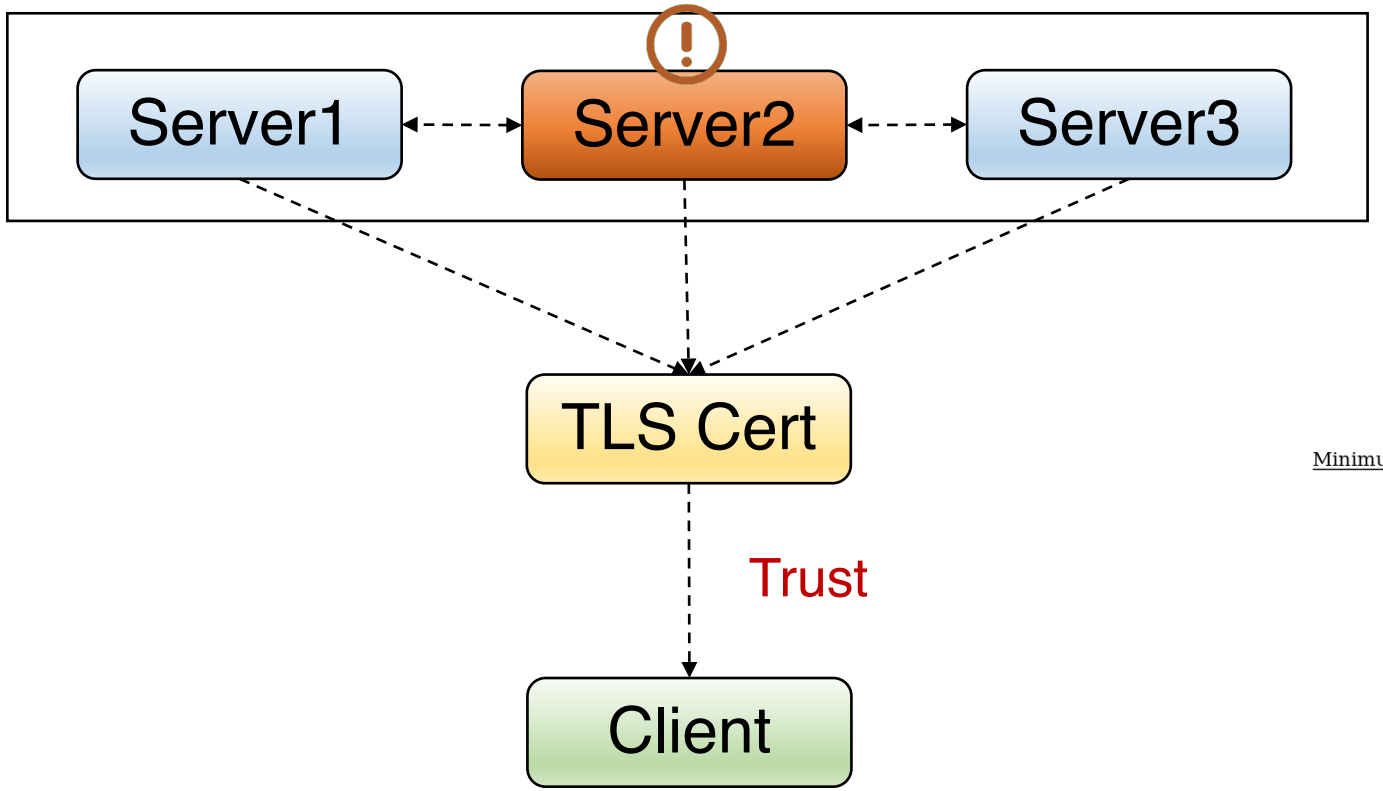
- However, the shared TLS certificates introduce security dependencies to different servers/parties.

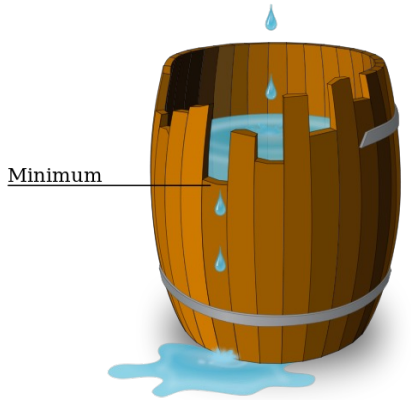


[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- However, the shared TLS certificates introduce security dependencies to different servers/parties.

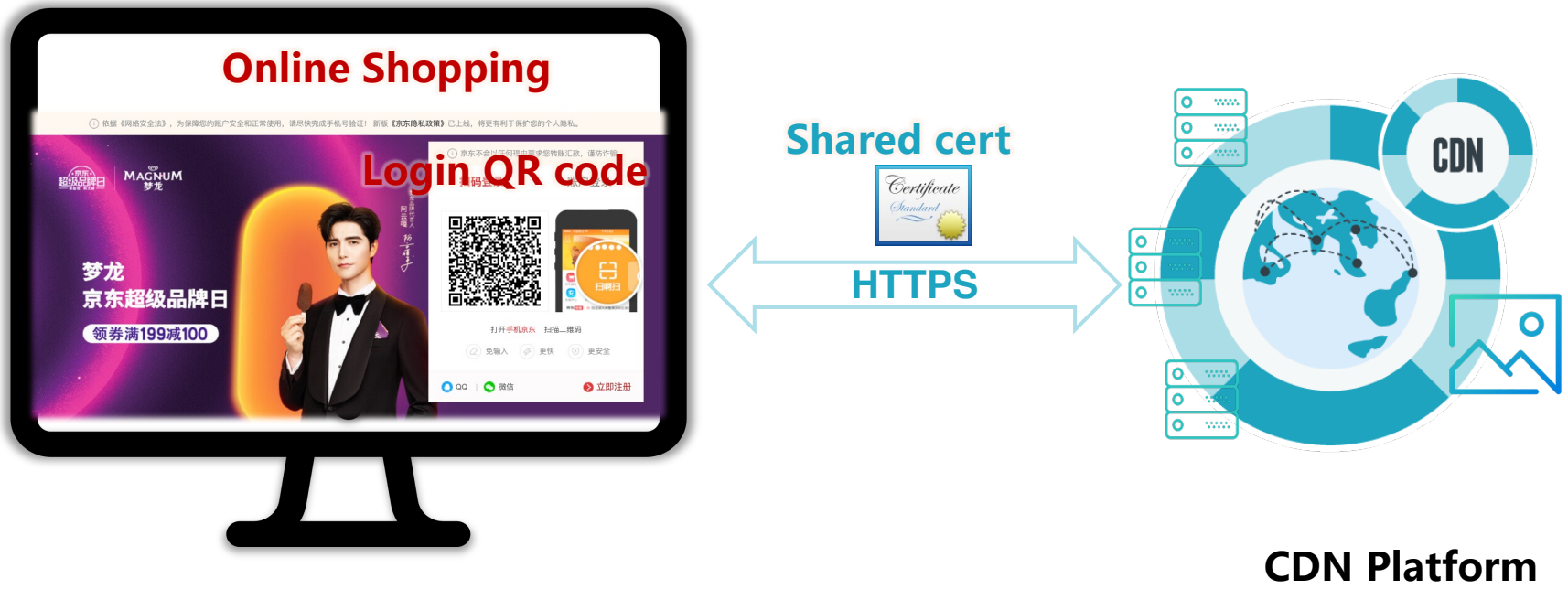




[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- Attackers can leverage flawed servers to downgrade HTTPS to HTTP and replace the transferred resources (e.g., images, executables, scripts)



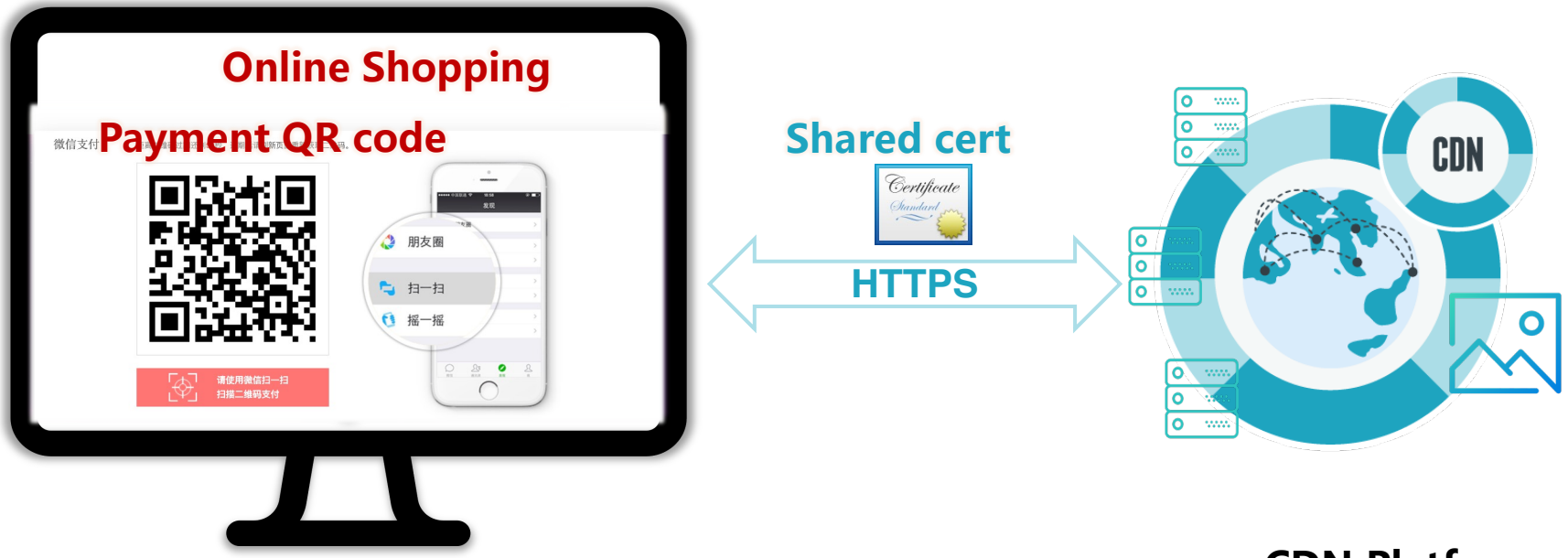
Client loads and renders passive contents (e.g., QR code)

CDN Platform

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- Attackers can leverage flawed servers to downgrade HTTPS to HTTP and replace the transferred resources (e.g., images, executables, scripts)



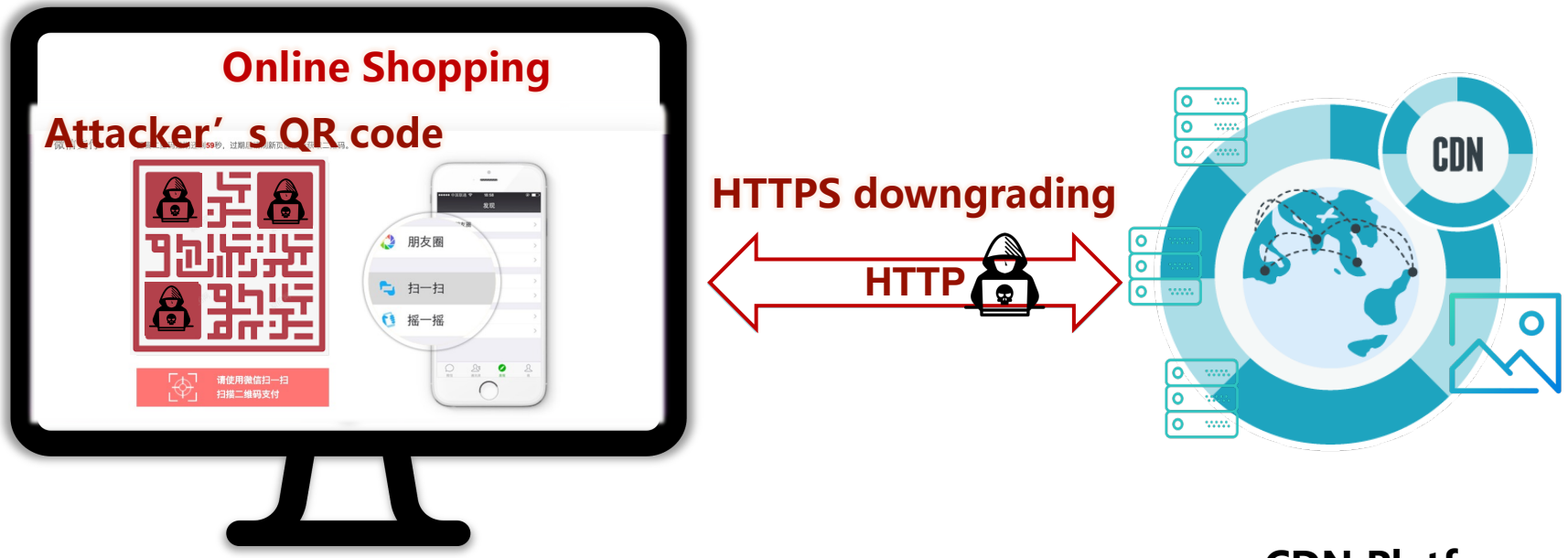
Client loads and renders passive contents (e.g., QR code)

CDN Platform

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- Attackers can leverage flawed servers to downgrade HTTPS to HTTP and replace the transferred resources (e.g., images, executables, scripts)



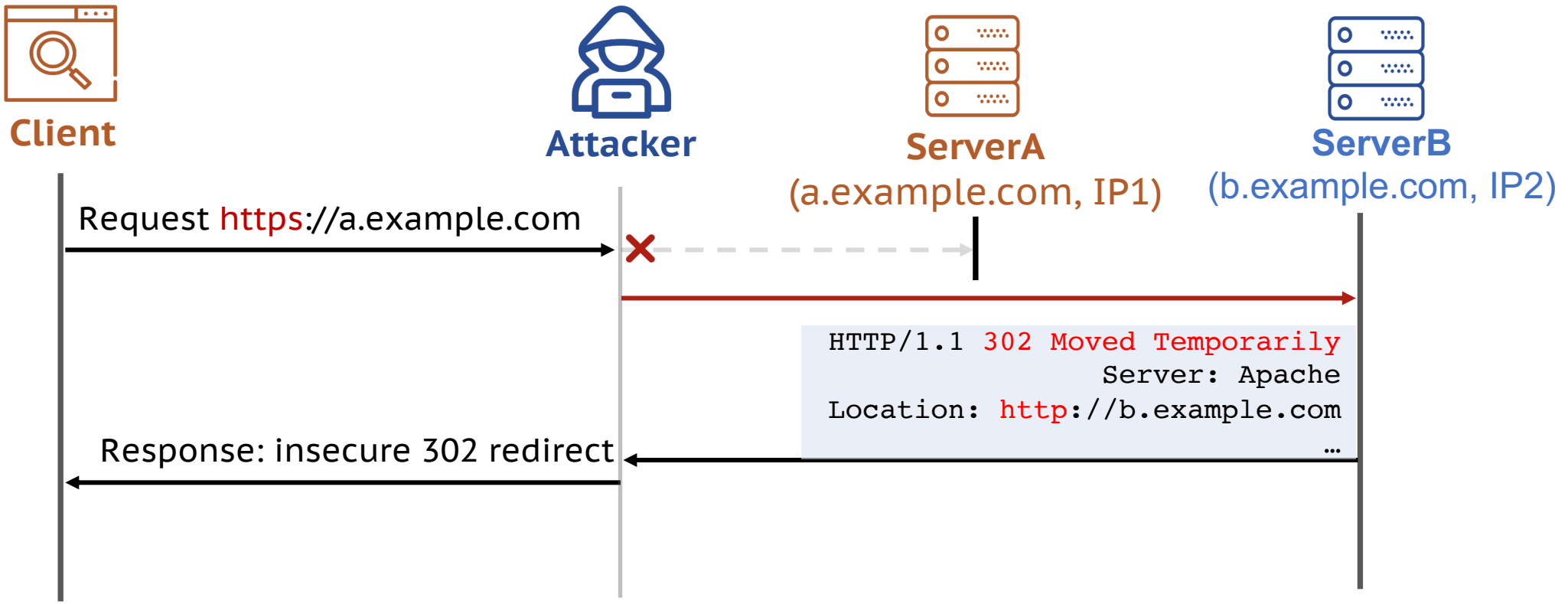
Client loads and renders passive contents (e.g., QR code)

CDN Platform

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

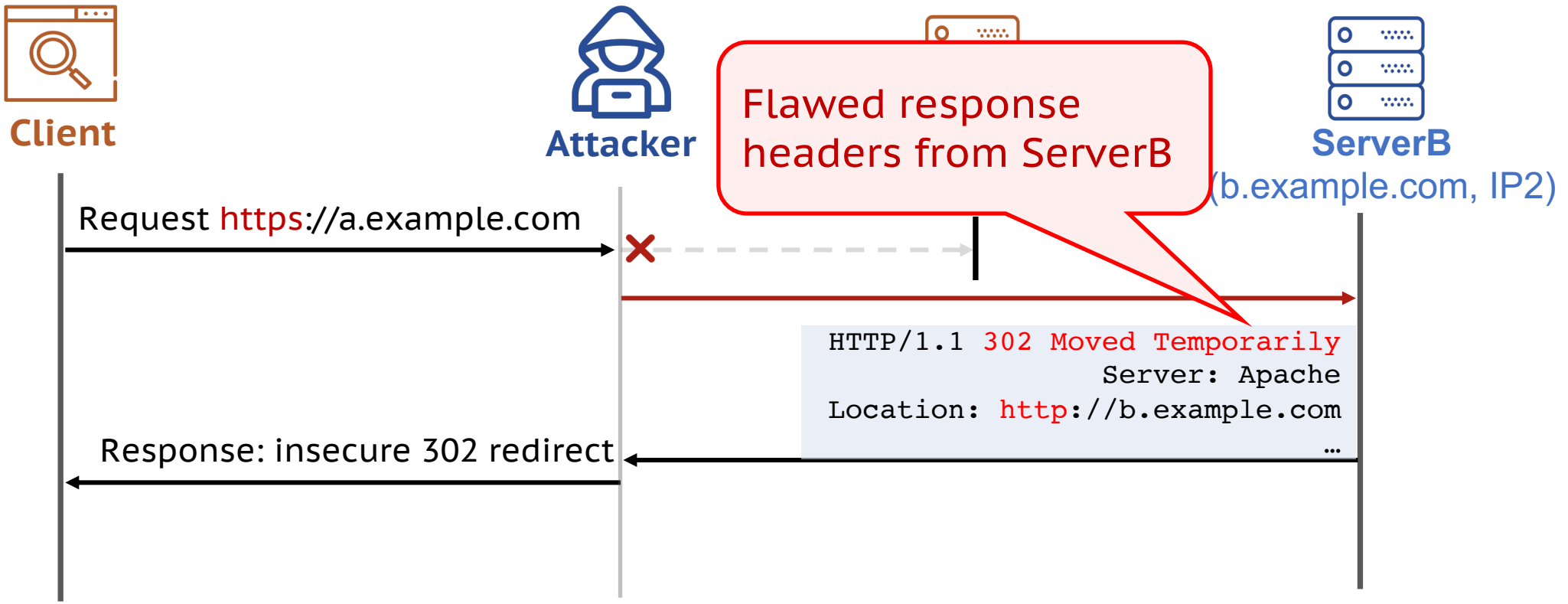
- Bypass HTTPS security policies to perform HTTPS downgrading attacks.



[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

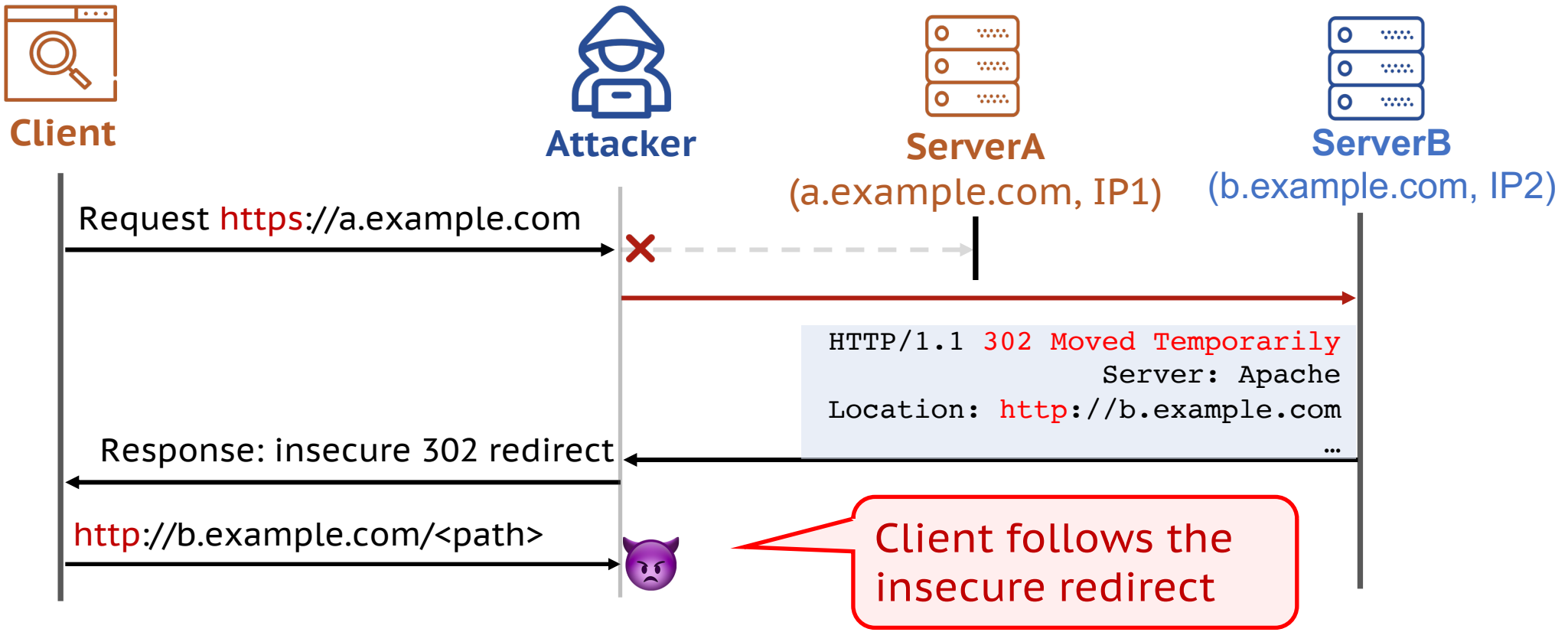
- Bypass HTTPS security policies to perform HTTPS downgrading attacks.



[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

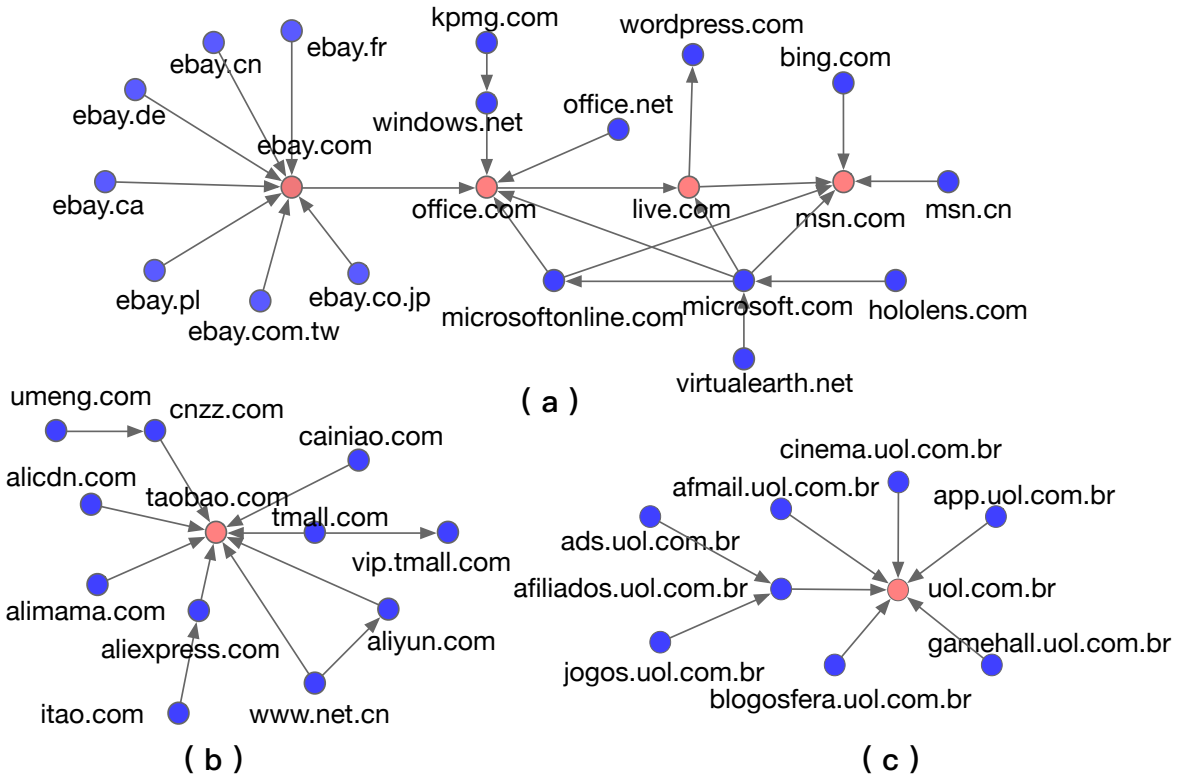
- Bypass HTTPS security policies to perform HTTPS downgrading attacks.



[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- Shared certificates introduce wide security dependencies among websites.



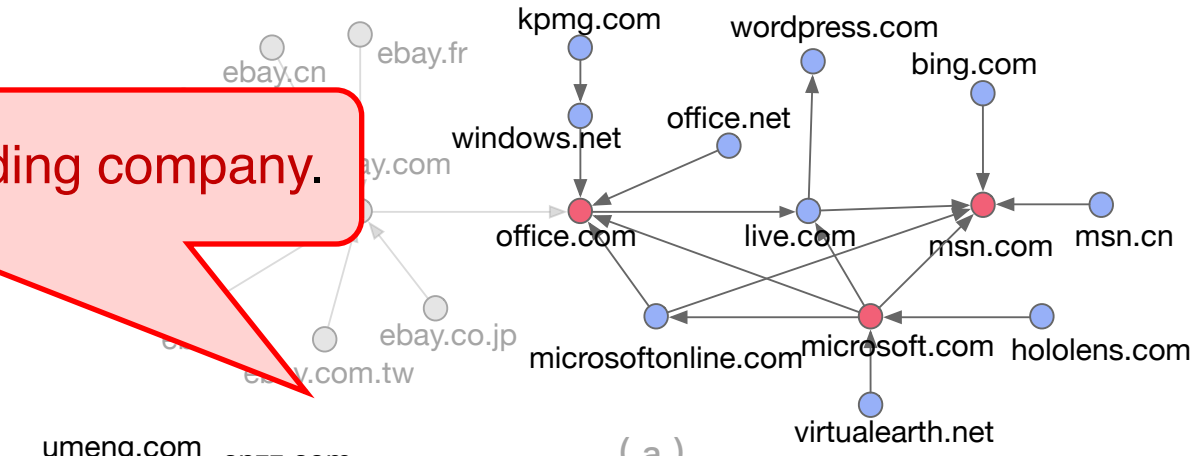
If the domains at the convergent nodes are vulnerable, there will be potential security threats for those around them.

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

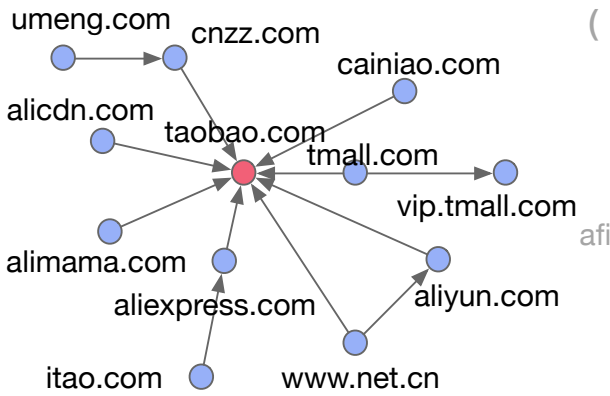
Threat V: TLS Certificate Sharing

- The shared certificates introduce wide-spread security dependencies among websites.

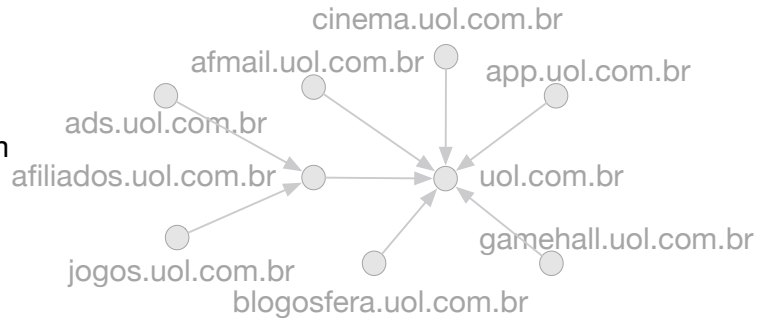
The subsidiary and the holding company.



(a)



(b)

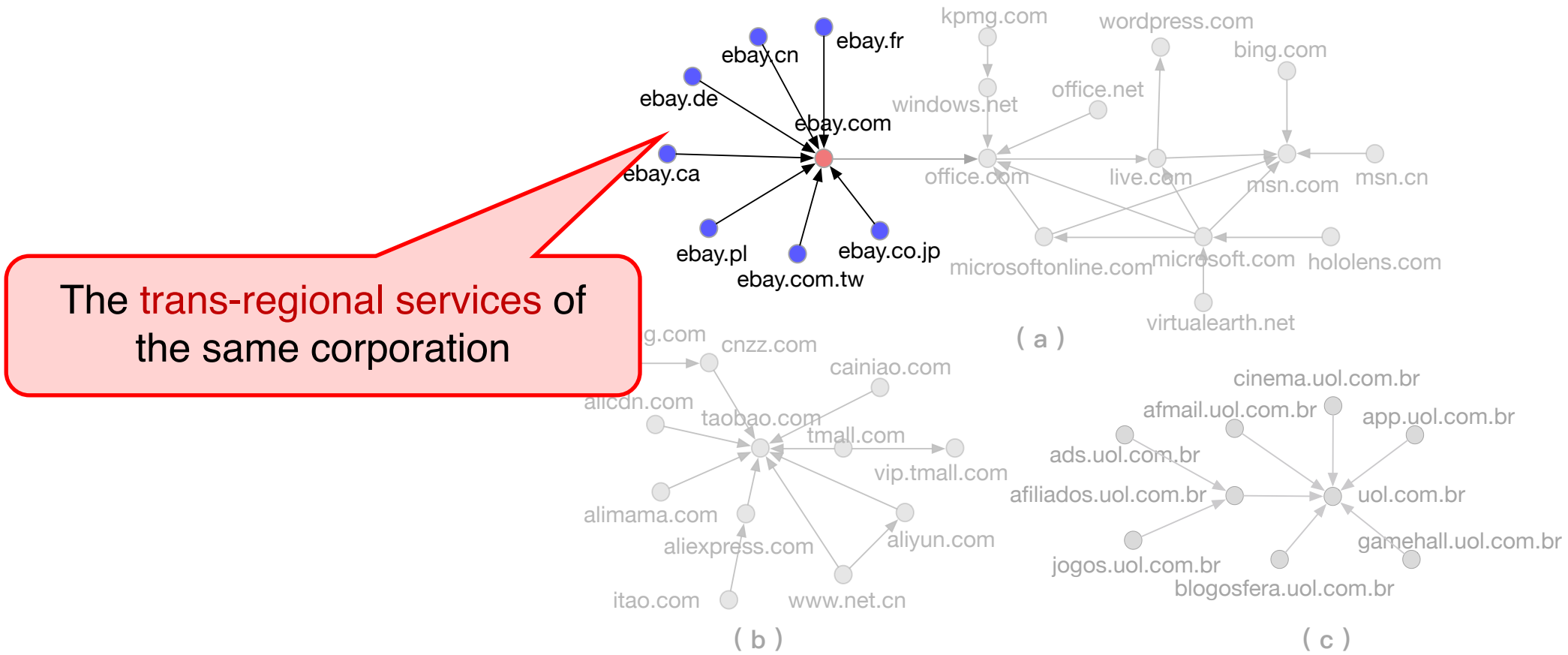


(c)

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- The shared certificates introduce wide-spread security dependencies among websites.



The trans-regional services of the same corporation

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Threat V: TLS Certificate Sharing

- ~3K FQDNs under Alexa Top 500 apex domains are vulnerable
- A number of popular applications could be affected.

Case Study:

- Online Payment Hijacking
- Download Hijacking
- Website Phishing

[CCS 2020] Talking with Familiar Strangers: An Empirical Study on HTTPS Context Confusion Attacks

Practice Suggestions

- Implement the best security practices
  - Deploy HTTP Strict-Transport-Security (HSTS) policy for essential websites
  - Configure CDN security features
  - Do not share certificates with untrusted websites
- Monitor traffic and logs
  - Monitor traffic patterns for anomalies that could indicate a security breach.
  - Check CDN and website logs for suspicious activities.
  - Access control and rate limit.
- Strengthen management, regularly update and patch
  - Remember to update DNS settings without leaving stale DNS records in the zones.
  - Release the unused cloud services endpoints.

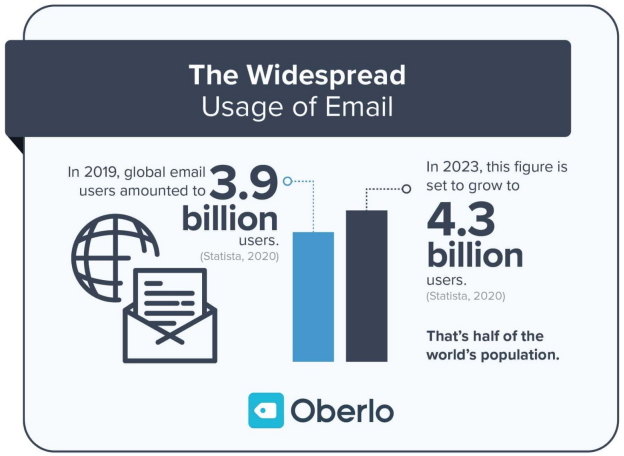
Part II.3: Email services & security

- Email Service
- Email Spoofing Attack
- Secure Practice Suggestions

Email Service

- ❑ One of the popular services on the Internet
  - ✓ **4.26** billion users, **3.13** million emails per second[1]

- ❑ One of the oldest applications on the Internet
  - ✓ First email (**1971**) , SMTP (**1982**)
- ❑ Plays a crucial role in modern communication
  - ✓ Academic communication or business communication



- ❑ A special Internet ID card
  - ✓ Registration validation, Password recovery

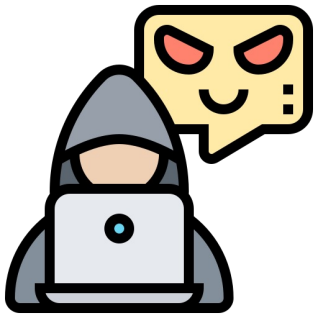
[1] How Many Email Users Are There in 2023 | 99firms

Email Security is Important

- Email service has also become an important target for attackers.

Phishing

Ransomware

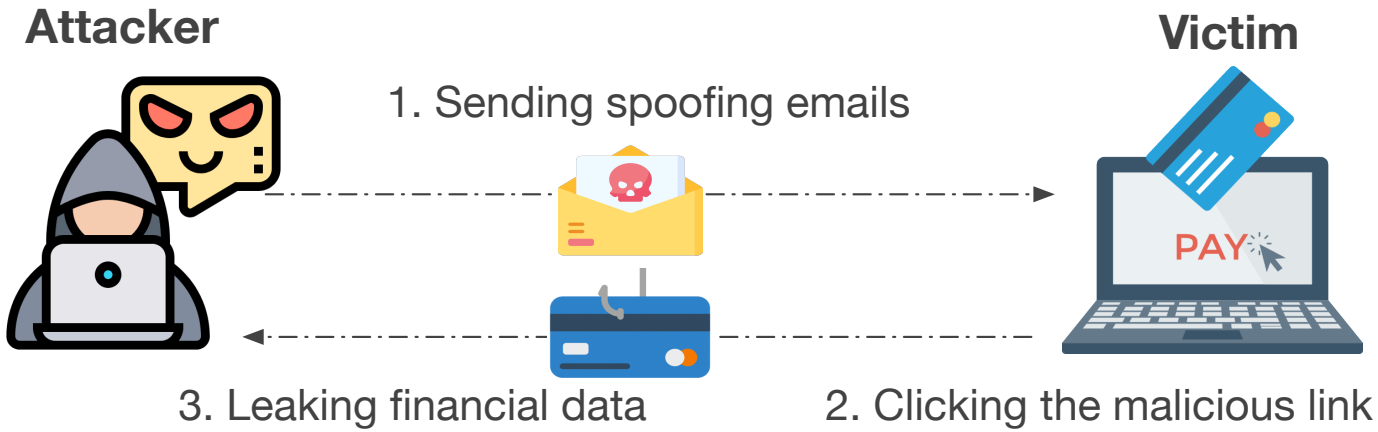


Email Spoofing

Data Stealing

Email Spoofing Attack

❑ How email spoofing attacks happen?



❑ Impact of email spoofing attacks today.

600%

Increase over 600% due to coronavirus pandemic (**COVID-19**).

"The most devastating attacks by the most sophisticated attackers, almost always begin with the simple act of spearphishing." Jeh Johnson Former Secretary, Department of Homeland Security

$5.3B → $12.5B

FBI reports business have lost over $12.5B. More than **double** in just over two years.

Email Spoofing Attack

❑ An example of email spoofing attack.

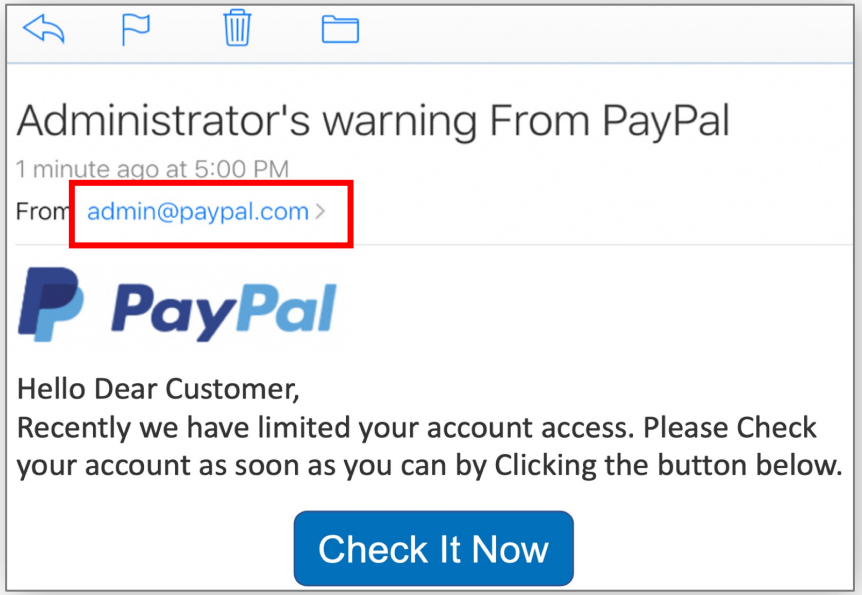
SMTP DATA

HELO sender.com
MAIL FROM: <attack@sender.com>
RCPT TO : <victim@receiver.com>

From: <admin@xn--aypal-uye.com>
To: <victim@receiver.com>
Subject: Adminstrator's warning From Paypal.

Hello Dear Customer,
.....
Check It Now

Displayed Email



IDN homograph attack (A12): from paypal.com to iCloud

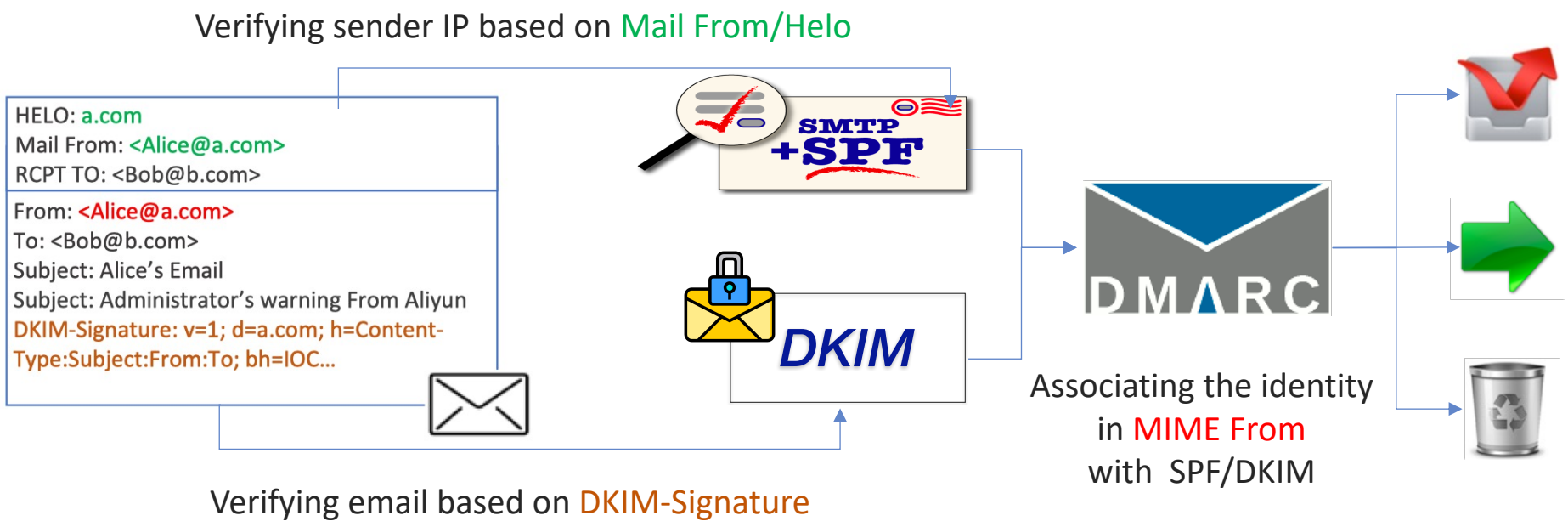
It's so hard to spot spoofing email !

Email Spoofing Protections

- **Email Spoofing Extension Protocols**
  - Sender Policy Framework (SPF, RFC 7208)
    - Verifying sender IP based on Mail From/Helo
  - DomainKeys Identified Mail (DKIM, RFC 6376)
    - Verifying email based on DKIM-Signature
  - Domain-based Message Authentication, Reporting and Conformance (DMARC, RFC 7489)
    - Offering a policy suggesting solution to handle unverified emails
    - Associating the identity in MIME From with SPF/DKIM

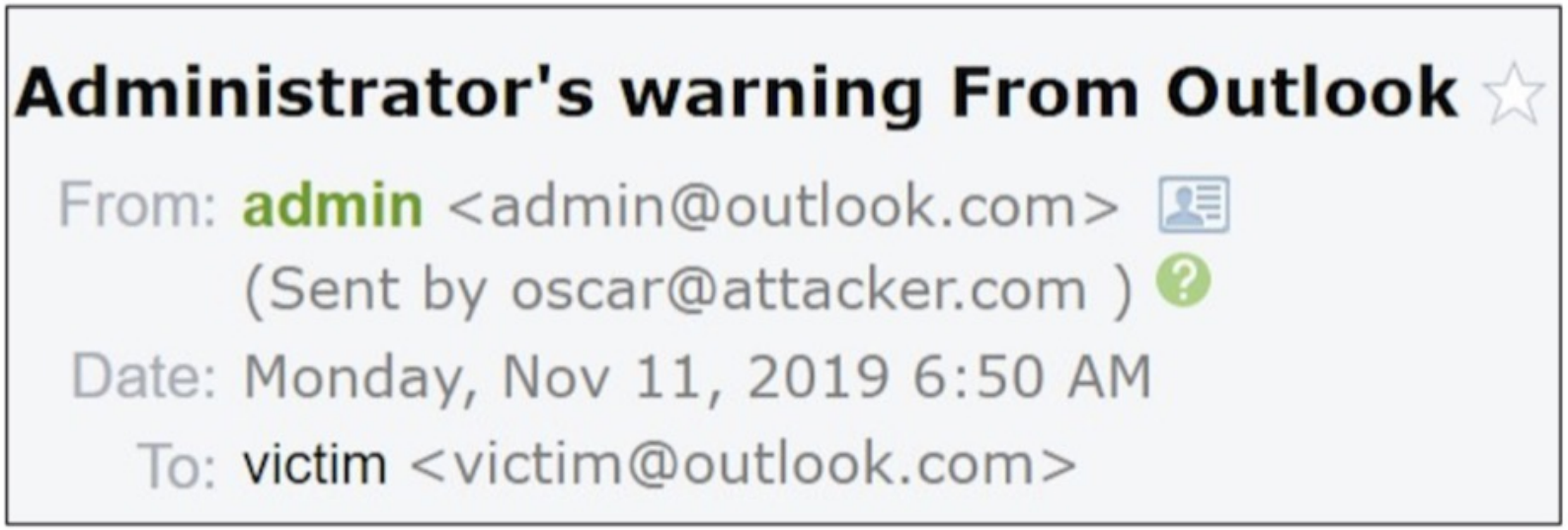
Email Spoofing Protections

❑ How do the three email security protocols work?



Email Spoofing Protections

- UI-level spoofing protection
  - Sender Inconsistency Checks (SIC)



A spoofing email that fails the Sender Inconsistency Checks.

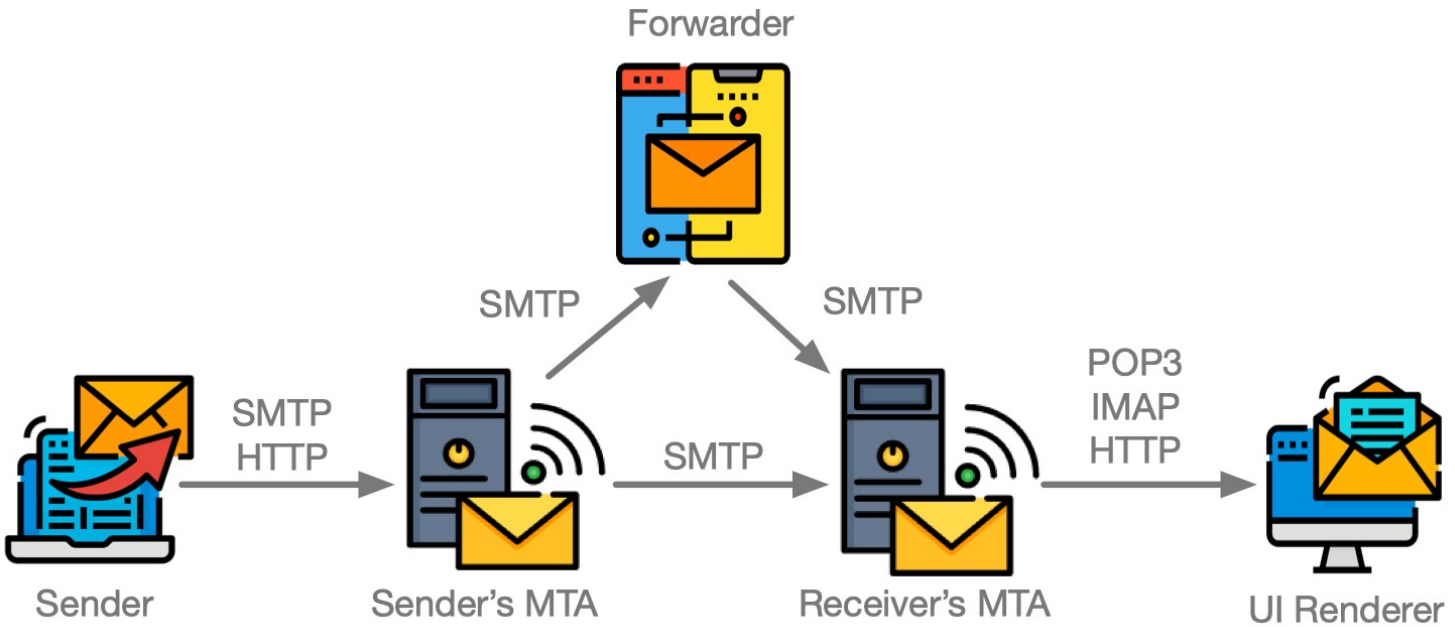
However...

With these anti-spoofing protections,

email spoofing attack is still possible.

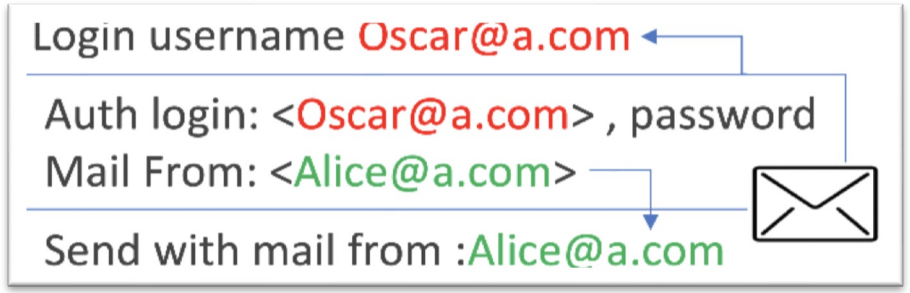
Attacks in Email Sending Authentication

- **Successful Attack:** modifying Auth Username, Mail From, From arbitrarily.
- **Benefit:** abusing IP reputation of well-known email services.



Attacks in Email Sending Authentication

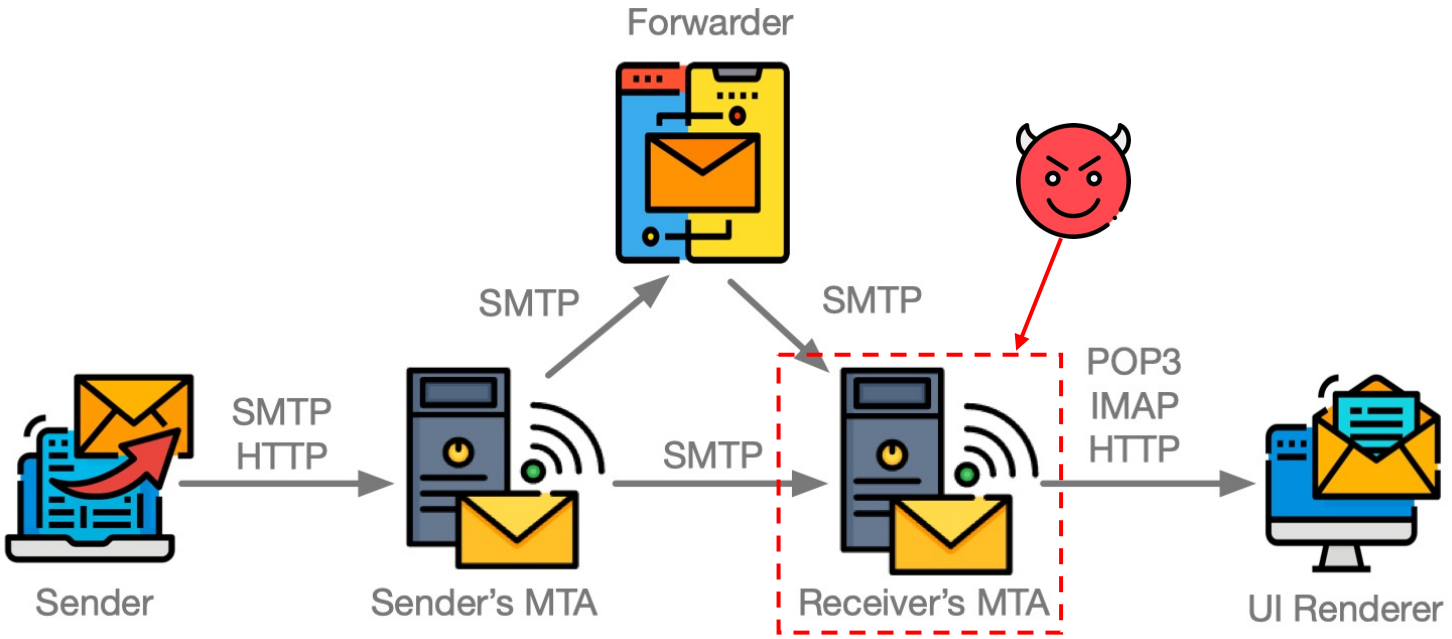
- Auth Username ≠ Mail From (A1)



- Mail From ≠ From (A2)

Attacks in Email Receiving Verification

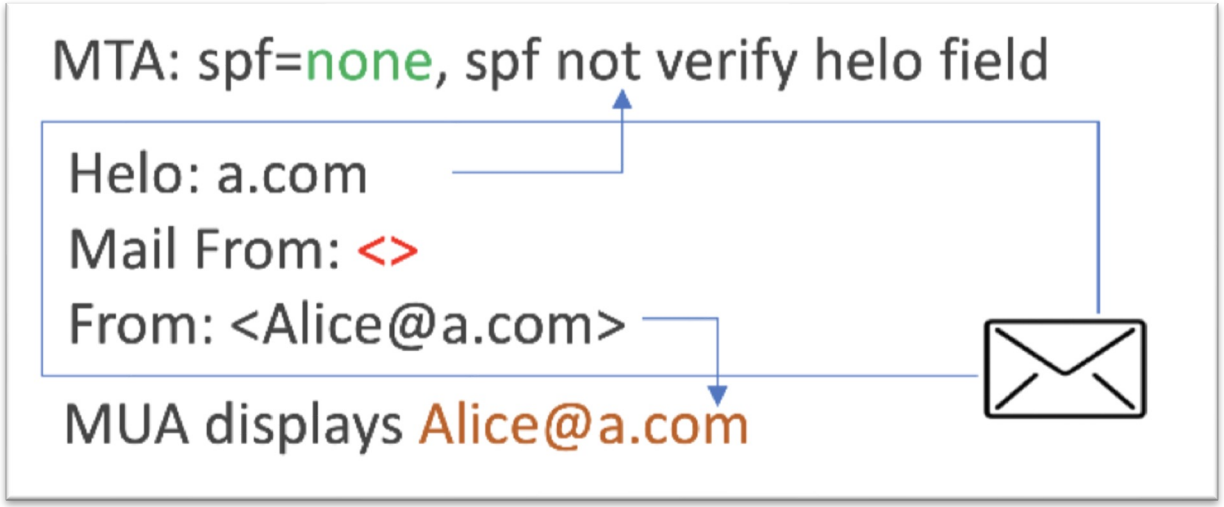
- **Successful Attack:** bypassing SPF, DKIM and DMARC.
- **Benefit:** hard to spot spoofing email passing three security protocols.



Attacks in Email Receiving Verification

❑Empty Mail From (A3)

- **RFC 5321**: Empty mail from is allowed to prevent bounce loop-back
- **RFC 7208**: Use helo field as an alternative, if mail from is empty

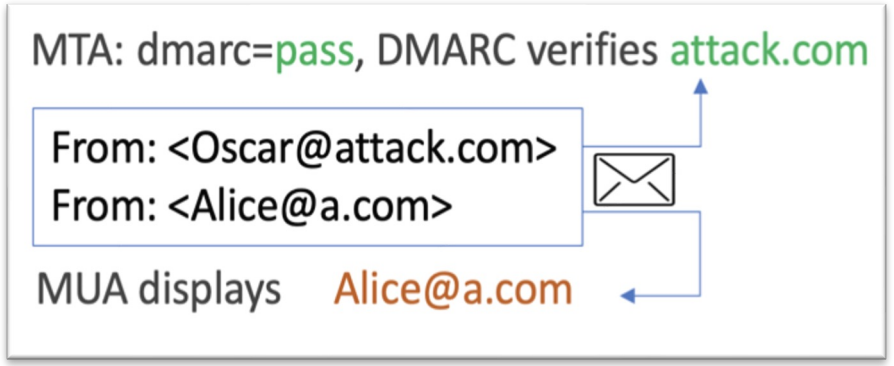


Empty Mail From attack bypassing the SPF verification

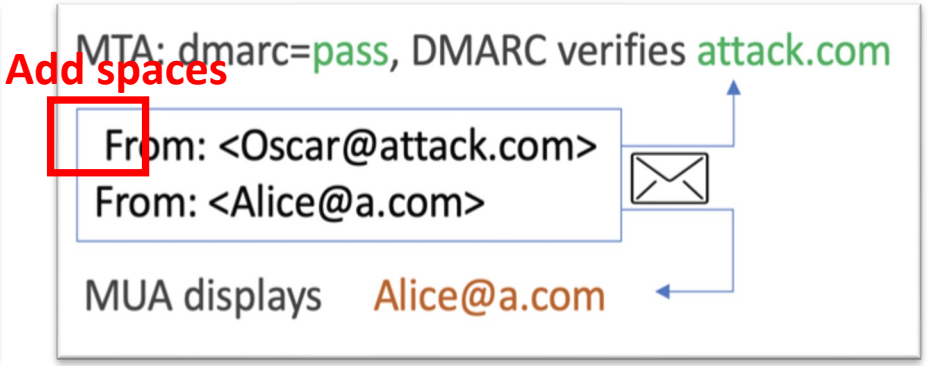
Attacks in Email Receiving Verification

❑ Inconsistent Parsing of Ambiguous Emails

❖ Multiple From headers (A4)



Ordinary multiple From attack

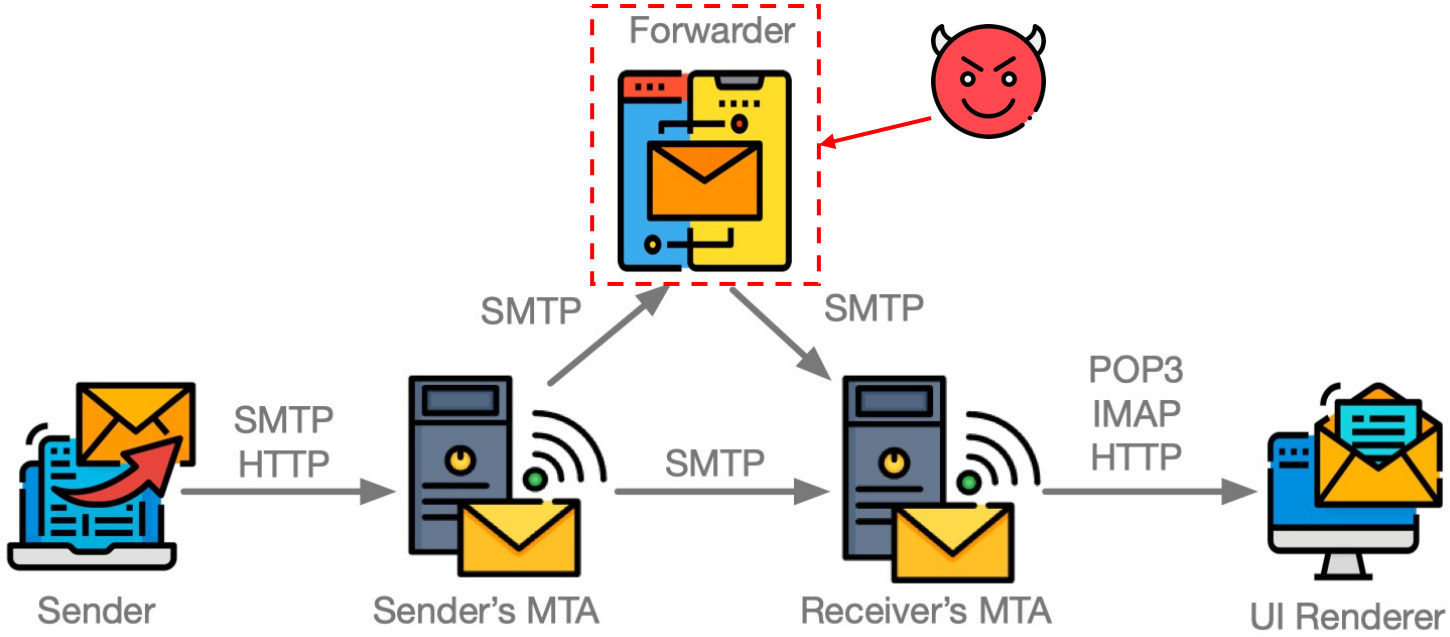


Multiple From attack with spaces

Attacks in Email Forwarding Verification

❑ Successful Attack:

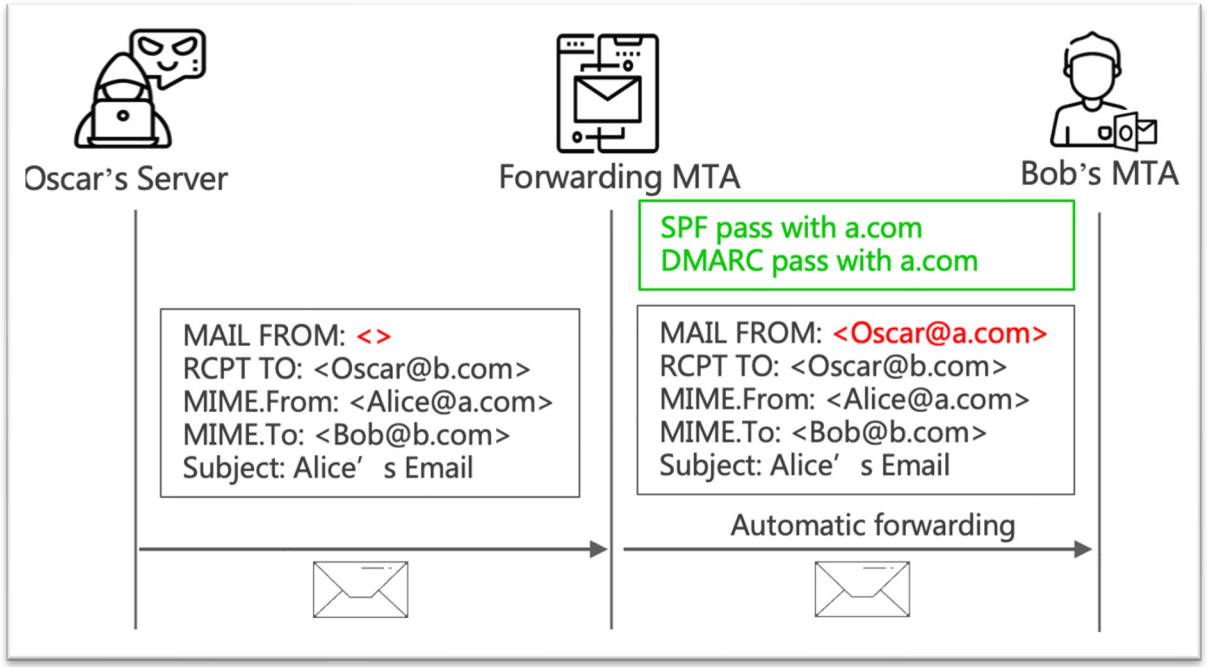
- ❖ Freely configure without authentication verification
- ❖ A higher security endorsement



Attacks in Email Forwarding Verification

❑Unauthorized Forwarding Attack (A5)

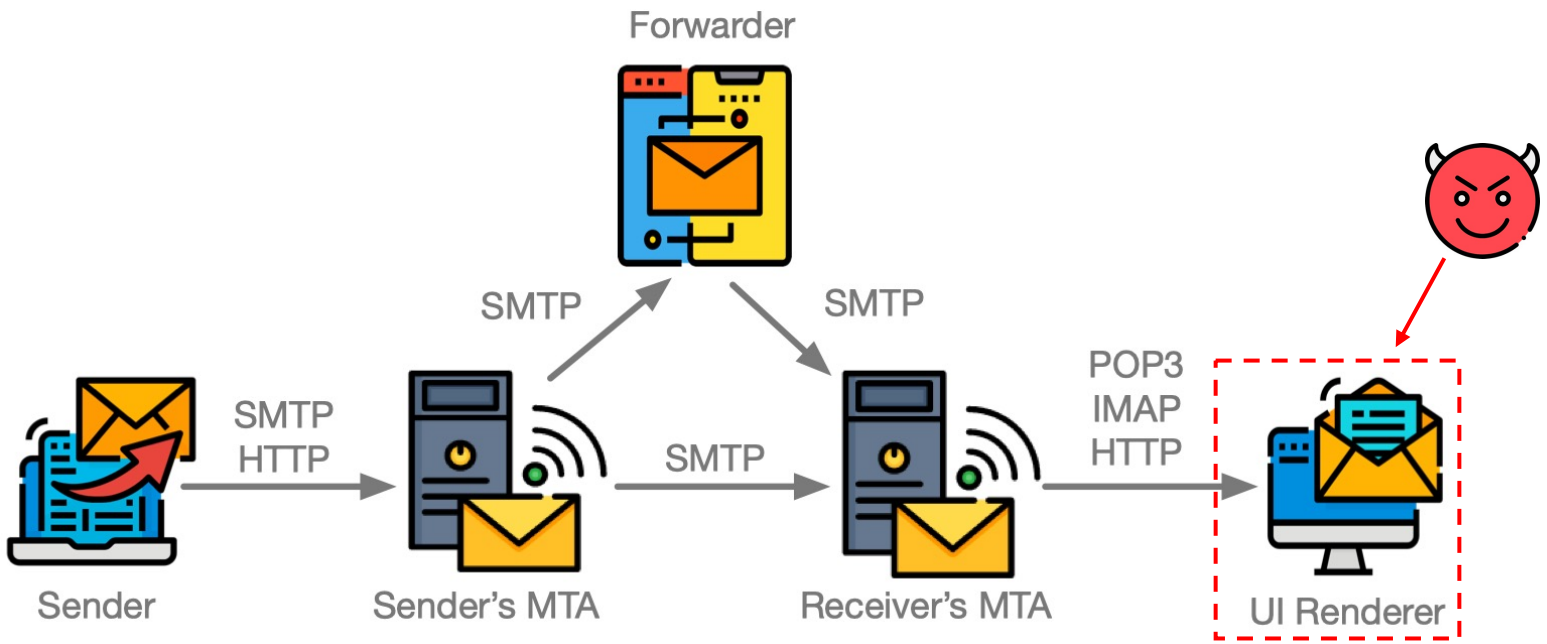
- Abusing trusted IP: Exploiting forwarding service to bypass SPF and DMARC



Attacks in Email UI Rendering

❑Successful Attack

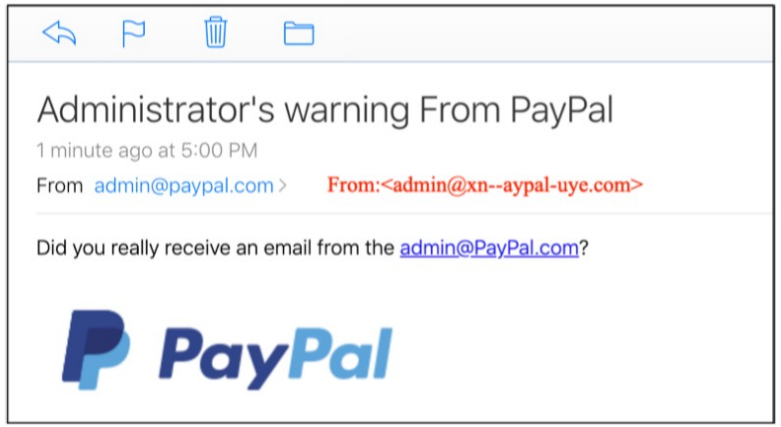
- The displayed address is inconsistent with the real one.
- No any security alerts on the MUA.



Attacks in Email UI Rendering

❑New Challenge: International Email

- Internationalized domain names (IDN) + email address internationalization (EAI)
- Allow Unicode characters in email address



IDN homograph attack (A12)

admin@gm@ail.com ==> admin@gmail.com

Missing UI Rendering Attack (A13)

\u202emoc.a@\u202dalice ==> alice@a.com

Right-to-left Override Attack (A14)

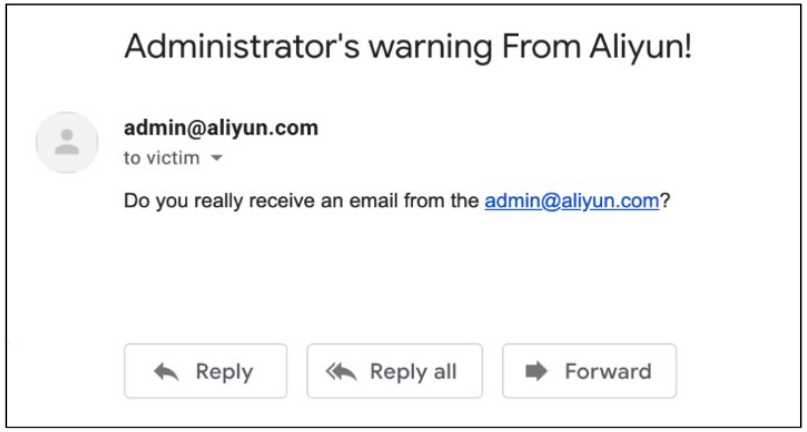
Combined Attack

❑ Limitations of a single attack

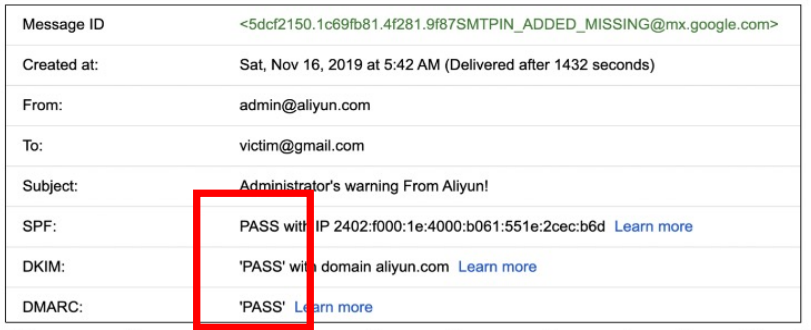
- ❖ Some attacks do not bypass all protections.
- ❖ Most vendors have fixed the attacks (bypassing all SPF,DKIM,DMARC and SIC).

❑ Combined Attack:

- ❖ More realistic emails (bypassing all prevalent email security protocols).



(a) Gmail's Web UI does not display any spoofing alerts

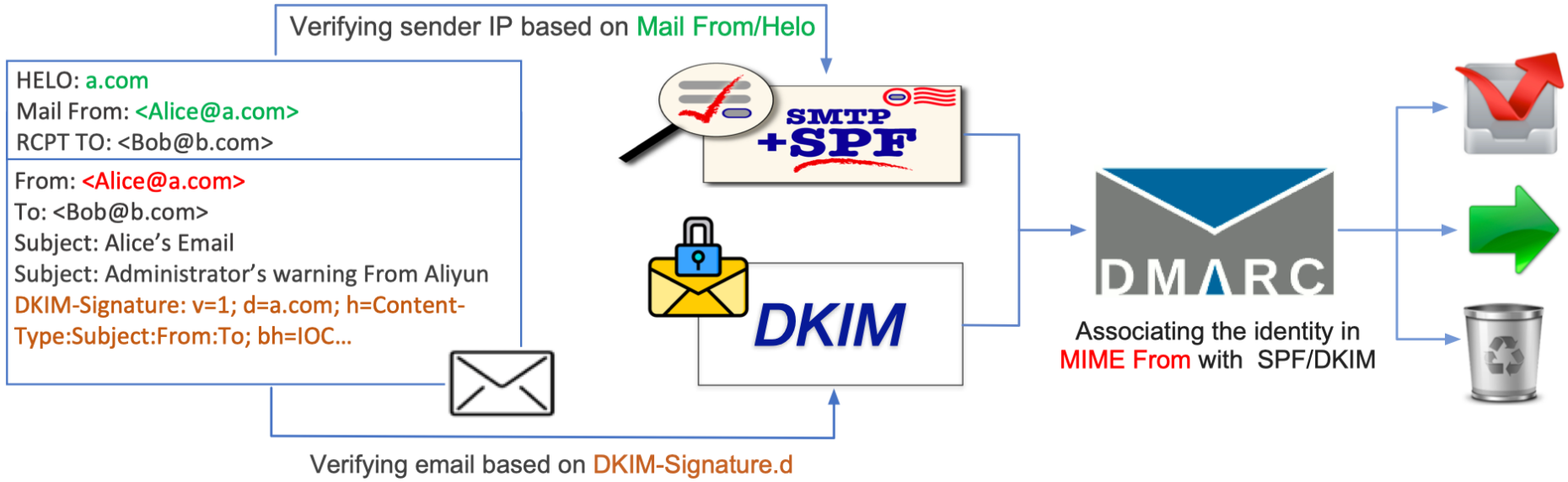


(b) The spoofing email passes all email security protocol verification

A example to impersonate admin@aliyun.com on Gmail.

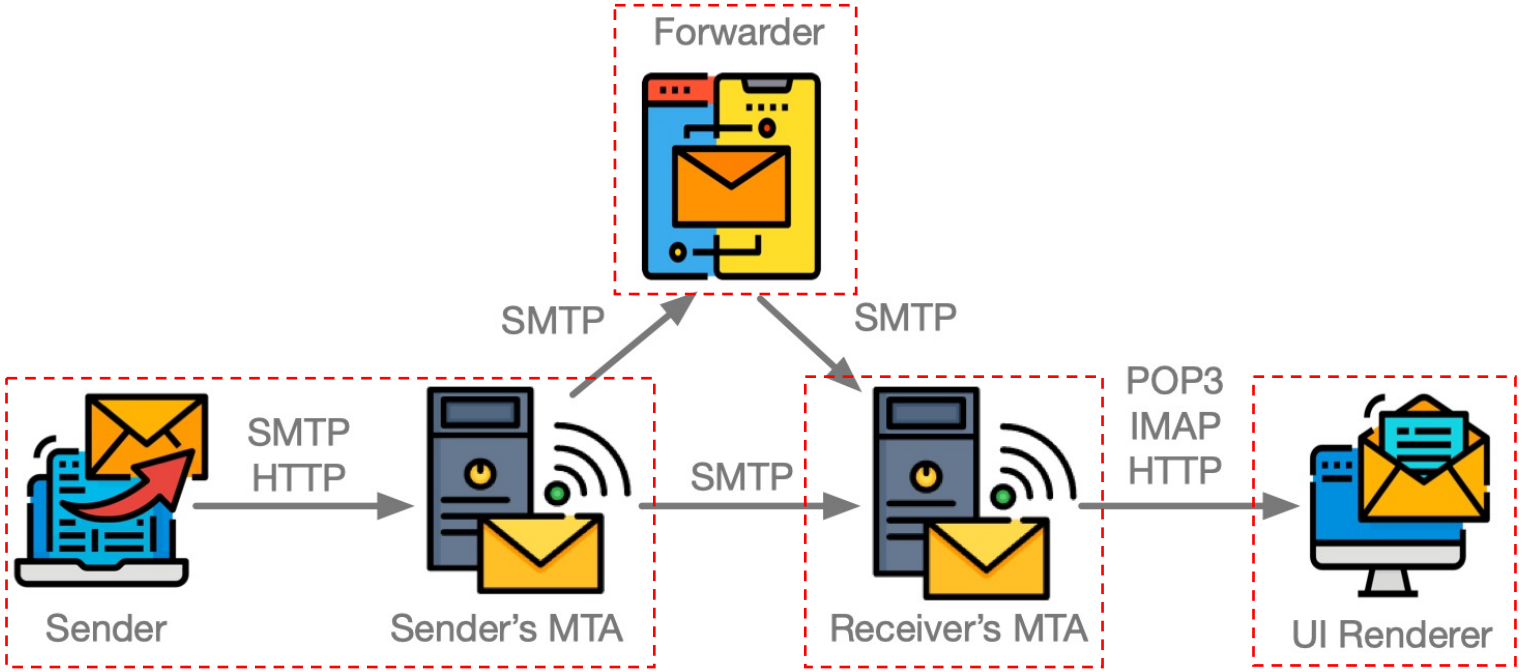
Weak Links among Multi-protocols

- Spoofing attacks still succeed due to the inconsistency of entities protected by different protocols.



Weak Links among Multi-roles

- Four different roles: senders, receivers, forwarders and UI renderers.
- The specifications do not state clear responsibilities of four roles.
- Any failed part can break the whole chain-based defense.



Weak Links among Multi-services

- Different email services have different configurations and implementation procedures.
- Numerous email components deviate from RFC specifications while dealing with ambiguous header.

The inconsistency among different services creates security threats.

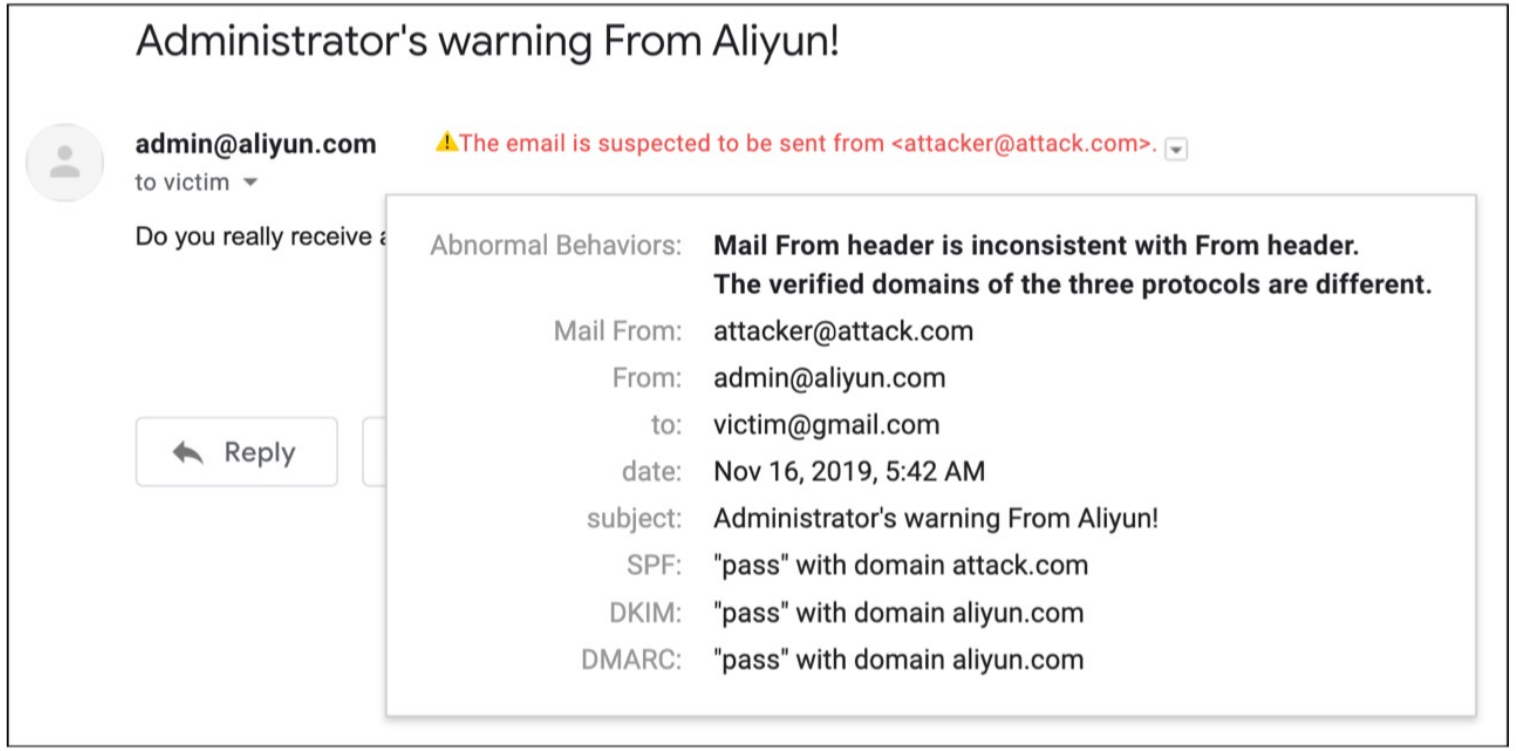
QQ邮箱 mail.qq.com
新浪邮箱
163 网易免费邮 mail.163.com
Coremail 邮件系统专家 沟通创造价值
阿里邮箱
搜狐闪电邮箱 mail.sohu.com
中国电信 CHINA TELECOM | 189邮箱
中国移动通信 CHINA MOBILE | 139邮箱

Gmail
Outlook
YAHOO! MAIL
Yandex Mail
Thunderbird
FOXMAIL
iCloud
eM Client

Mitigation and Solutions

❑UI Notification

NoSpoofing: a chrome extension for Gmail.



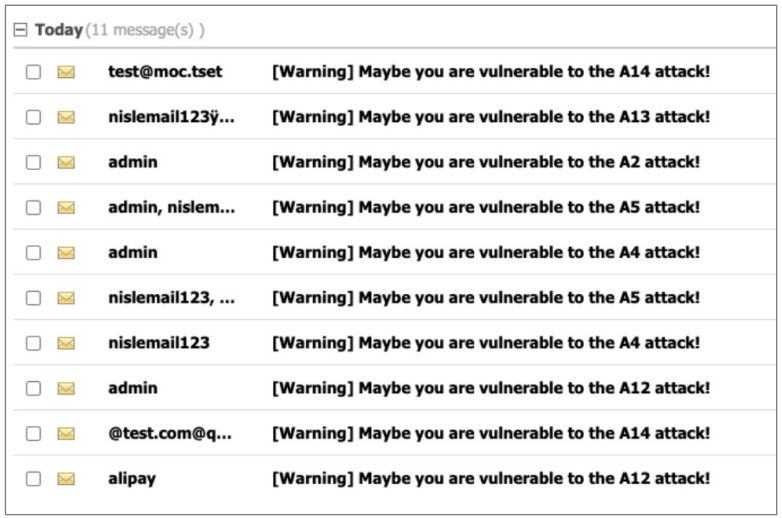
NoSpoofing
提供方：wchhlbt
★★★★★ 1 | 社交与通讯

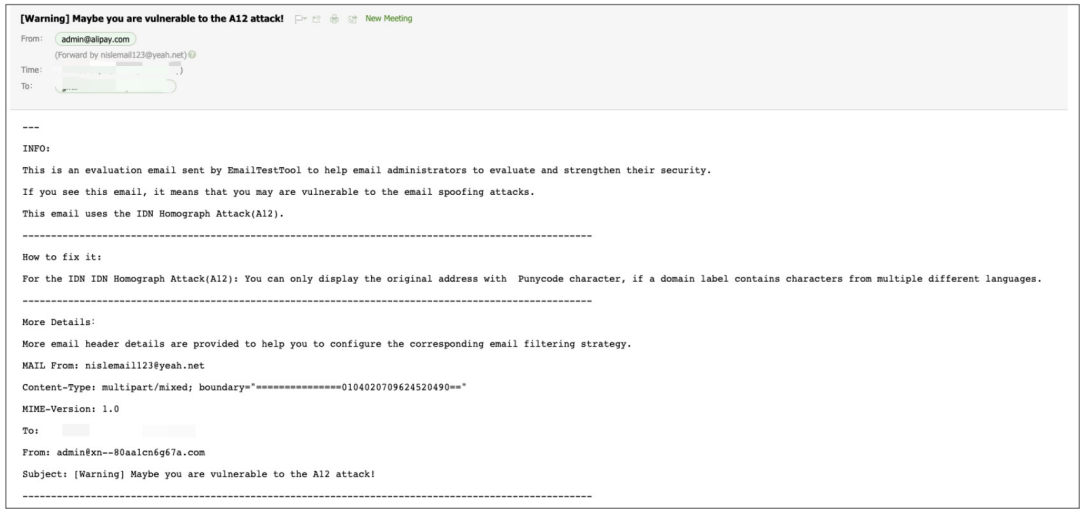
An example of UI notification against the combined attack
https://chrome.google.com/webstore/detail/nospoofing/ehidaopjcnapdglbbbjgeoagpophfjnp

Mitigation and Solutions

❑A Evaluation Tool

Espoofing: helping email administrators to evaluate and strengthen their security.





An example of using this tool to evaluate the security of target email system.

https://github.com/mo-xiaoxi/ESpoofing

Practice Suggestions for Deployment

❑Follow the best security practices

DKIM Key Expiration Date

Adding an expired date for DKIM keys can help:

- alleviate the problem of the unclear transition period
- promote regular key replacement.

```
v=DKIM1; k=rsa; h=sha256;
p=MIGfMA0GCSqGSIb3DQCyOmR3diPVt1...
```

add a field of DKIM key expired time

```
v=DKIM1; k=rsa; h=sha256;
expired-date: Sun, 24 Jul 2022 10:28:34 GMT;
p=MIGfMA0GCSqGSIb3DQCyOmR3diPVt1...
```

Default Oversigning Mechanism

Setting oversigning as the default mechanism can help:

- improve the protective effect of DKIM signatures
- prevent DKIM signatures from being used for replay attacks.

```
DKIM-Signature: v=1; d=example.com; s=selector;
h=From:To:Subject:Content-Type:Reply-To:Date:Cc;
bh=IOC…
```

use default oversigning mechanism

```
DKIM-Signature: v=1; d=example.com; s=selector;
h=From:From:To:To:Subject:Subject:Content-
Type:Content-Type:Reply-To:Reply-To:Date:Date:Cc:Cc;
bh=IOC…
```

Summary

- **Importance of Infrastructure:** The security and resilience of network infrastructure are vital to the success of business.
- **Increased Attention:** Businesses must prioritize and invest in the security of these infrastructures.
- **Proper Deployment of Security Strategies:** Implement comprehensive and correctly configured security measures for DNS, cloud, and email services.
- **Employee Training:** Educate staff about security best practices and potential threats.
- **Use of Advanced Tools:** Employ advanced security tools and services for enhanced protection.
- **Incident Response Planning:** Have a robust plan to quickly respond to and mitigate security breaches.

CYBER 100

27TH DECEMBER 2023

Cyber Security & Infrastructure: Concepts, Threats and Best Practices

Speakers:

Chaoyi Lu *(Tsinghua University)*

Mingming Zhang *(Zhongguancun Laboratory)*

December 27, 2023