# Security 101

Hsu-Chun Hsiao

hchsiao@csie.ntu.edu.tw

NSLAB

National Taiwan University

# Agenda

What is (cyber)security?

Introduction to network & systems security

- … via very short examples

Appendix: Security principles

# What is Security?

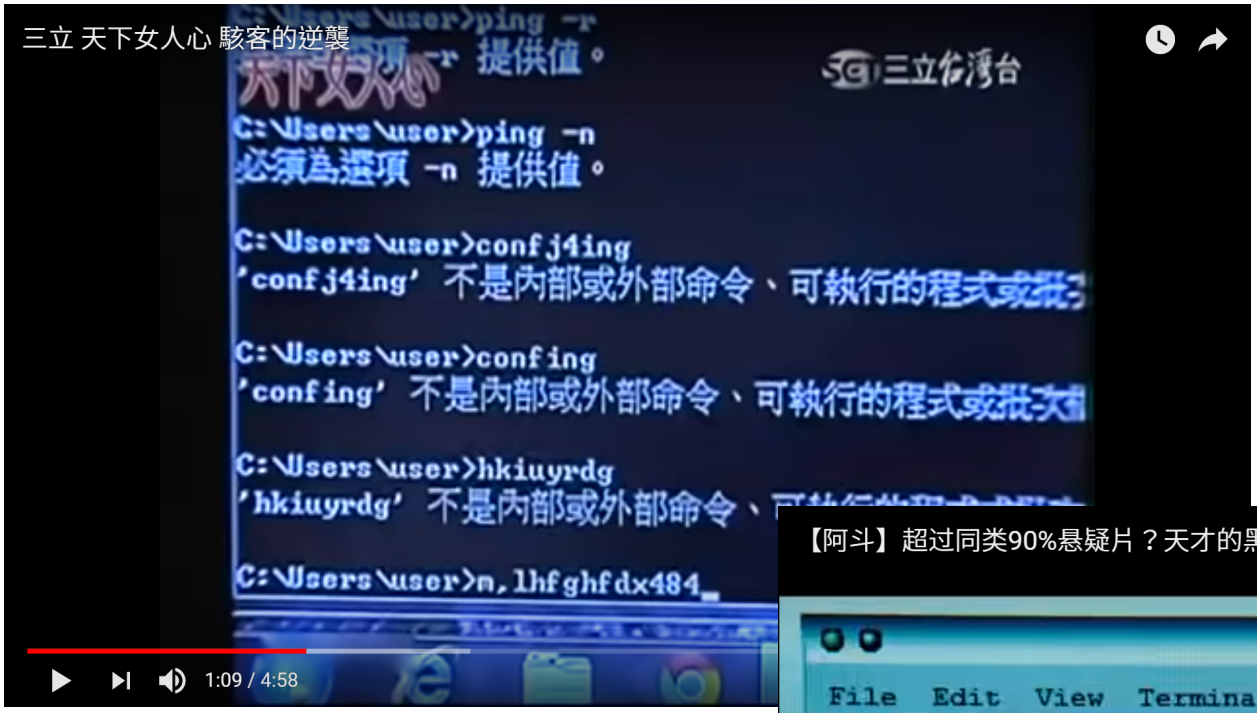
Security requirements

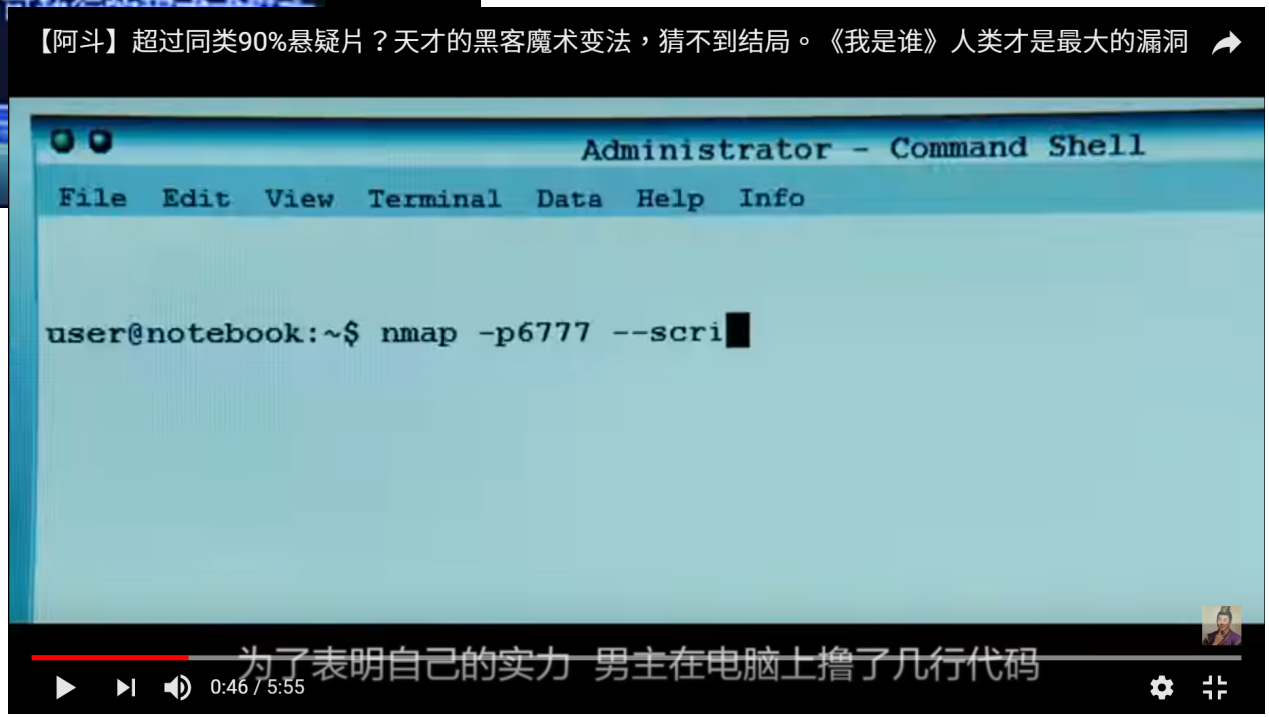
Threat model

Cost of security

# 從電影認識資安…？

# 從電影認識資安...？


三立 天下女人心 駭客的逆襲
三立台灣台
C:\Users\user>ping -n
必須為選項 -n 提供值。
C:\Users\user>confj4ing
'confj4ing' 不是內部或外部命令、可執行的程式或批
C:\Users\user>confing
'confing' 不是內部或外部命令、可執行的程式或批
C:\Users\user>hkiuyrdg
'hkiuyrdg' 不是內部或外部命令、
C:\Users\user>n,lhfghfdx484
1:09 / 4:58


【阿斗】超过同类90%悬疑片？天才的黑客魔术变法，猜不到结局。《我是谁》人类才是最大的漏洞
Administrator - Command Shell
File Edit View Terminal Data Help Info
user@notebook:~$ nmap -p6777 --scri
为了表明自己的实力 男主在电脑上撸了几行代码
0:46 / 5:55

# What’s NOT security

Security != cryptography

- Cryptography != encryption
- Cryptography != bitcoin

Security != CTF

# What is security?

Protect assets (e.g., data and communication) from unauthorized actions

# What is security?

Protect assets (e.g., data and communication) from unauthorized actions

Attackers = entities attempt to do unauthorized actions

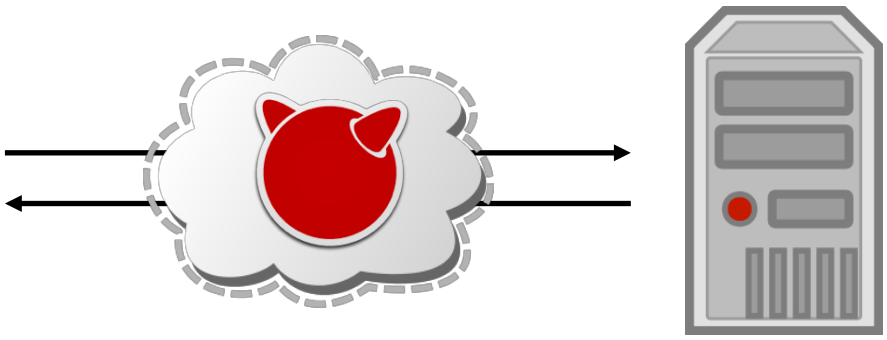
Attacker may

- Eavesdrop
- Manipulate
- Denial of service
- …

# Example

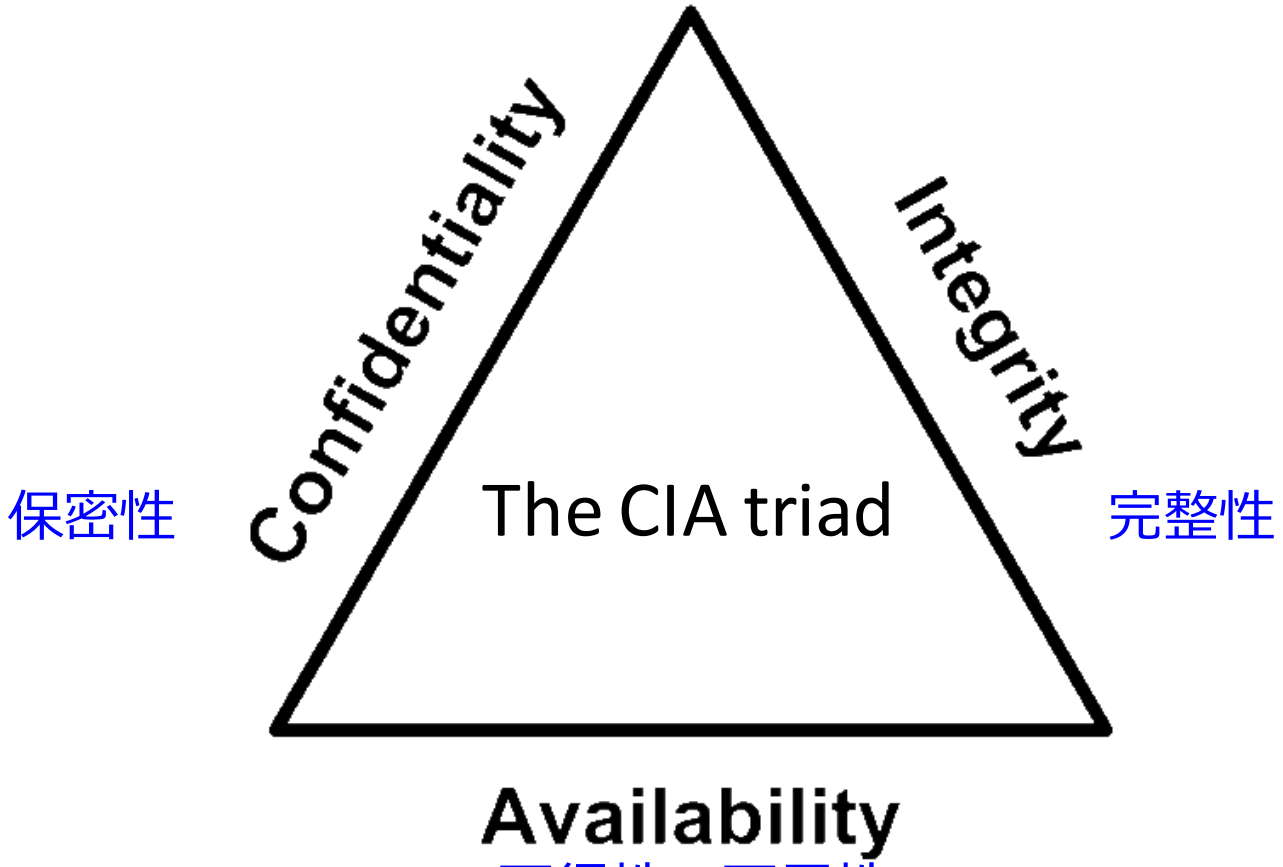
Ensure program or system works correctly even in the face of attack

- Is it the right website? Is it really the owner of the account?
- Is the transaction content correct?
- Can anyone see my account information?
- Is the service available?

# Security requirements

Properties that the protection should achieve




保密性

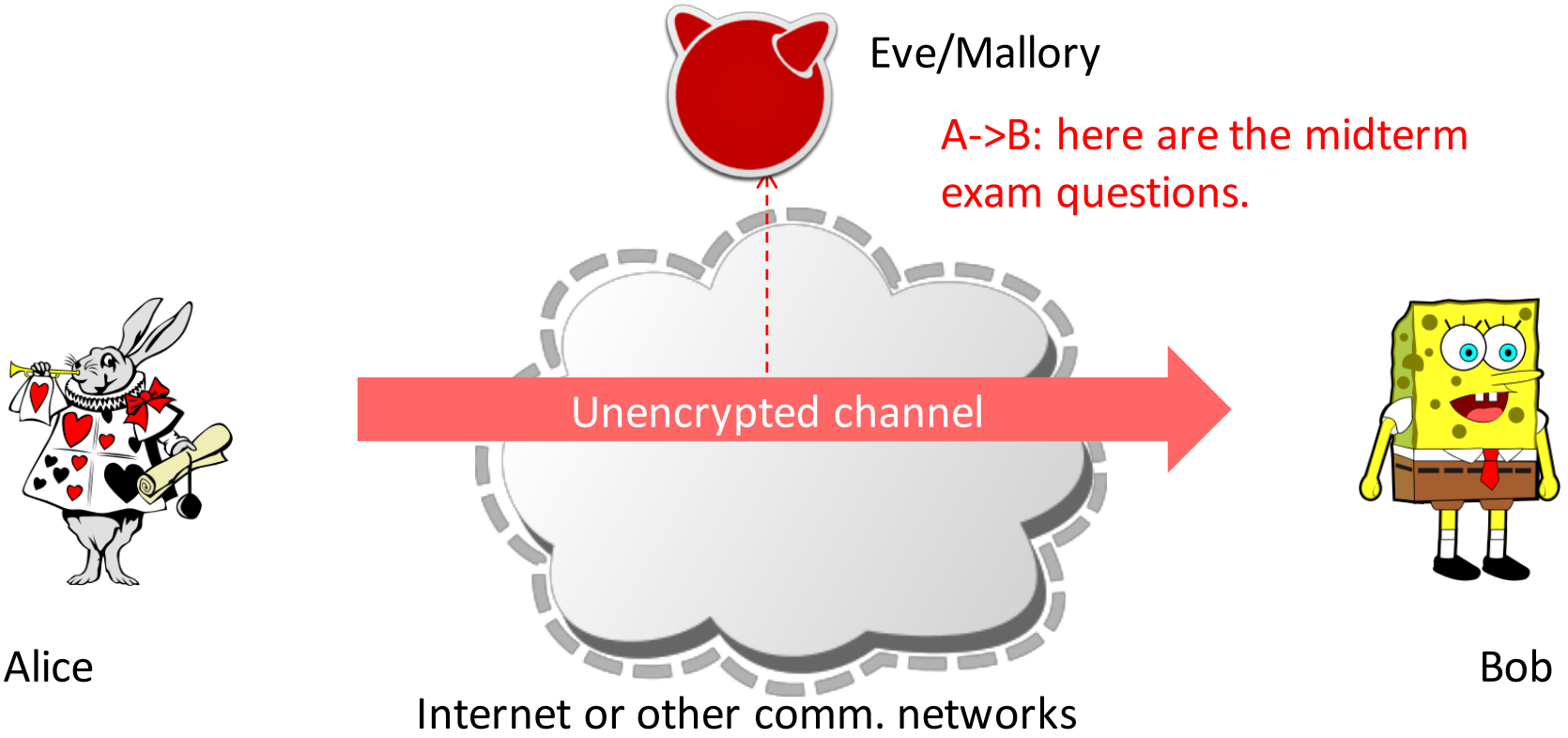
完整性

可得性、可用性

# Confidentiality (保密性)

Confidentiality is protection from unauthorized disclosure

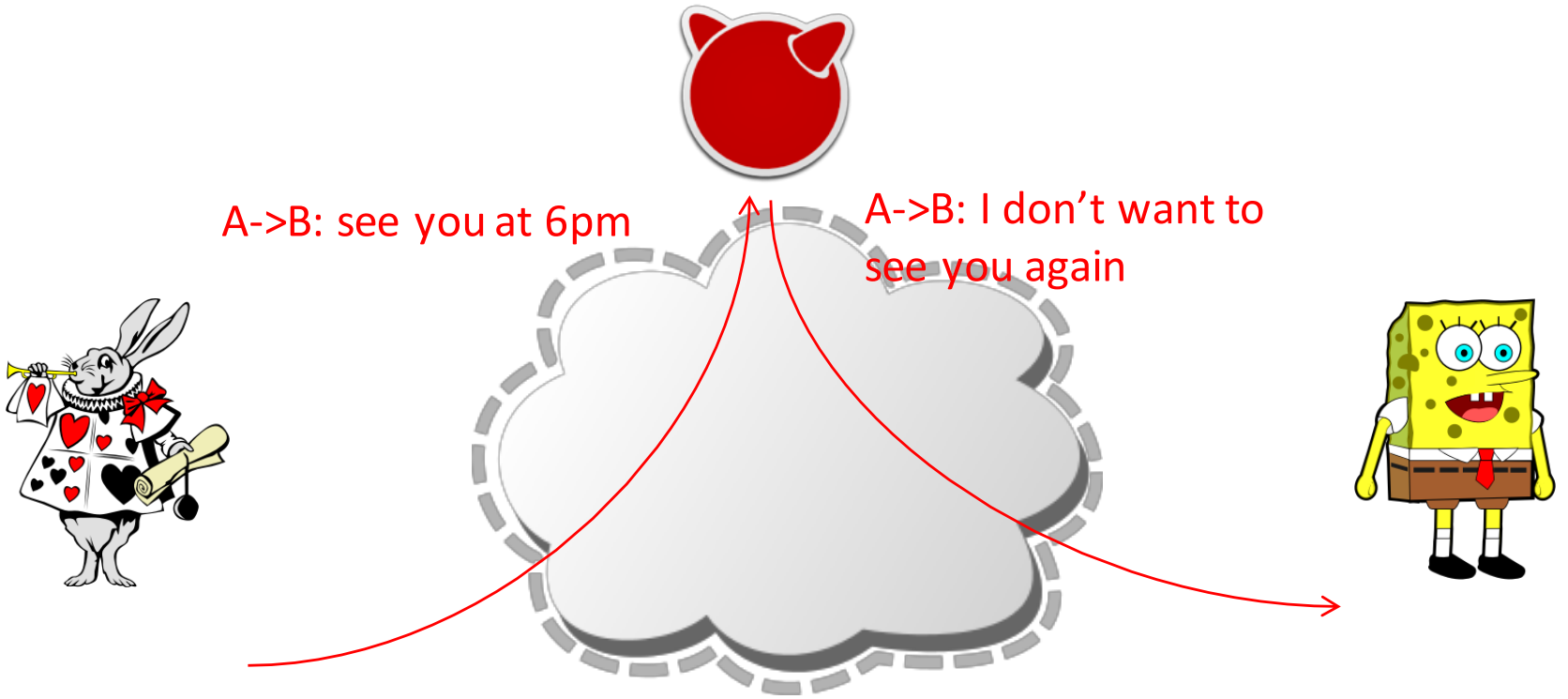
Eavesdropping on messages violates confidentiality



# Integrity (完整性)

Integrity is protection from unauthorized changes

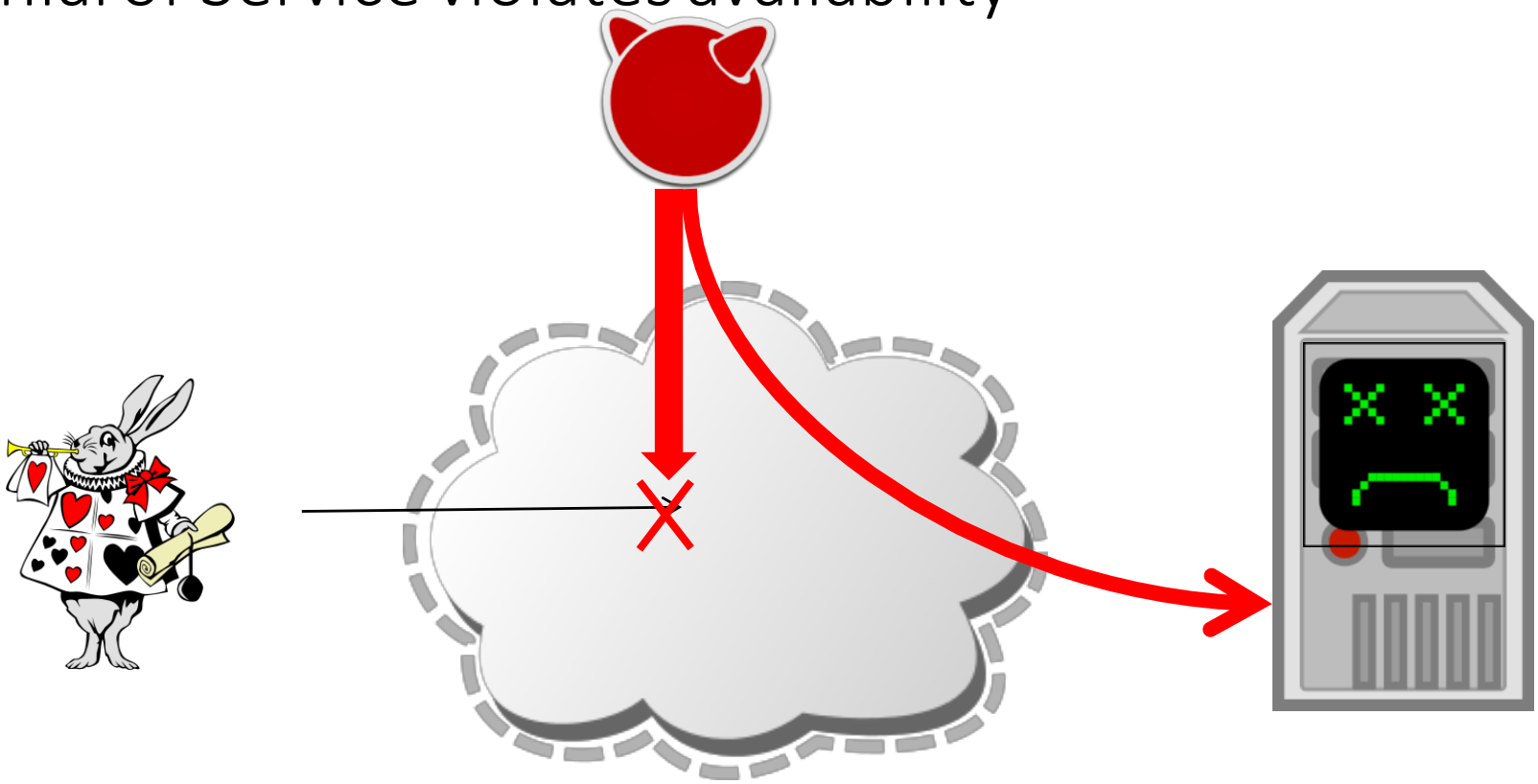
Modification of messages violates integrity



# Availability (可用性)

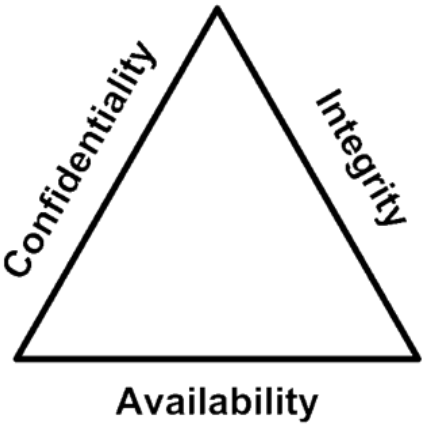
Availability ensures intended users can access service

Denial of Service violates availability



zuvio

# Exercise: which security requirement is violated?




## 聯邦網站成為DNS挾持目標，美國國土安全部發出緊急指令

數個美國聯邦網站的網域名稱系統（DNS）遭挾持，駭客將使用者流量變更至駭客所控制的架構，再轉回合法服務，所造成的風險高過於短期重新定向使用者流量的作法

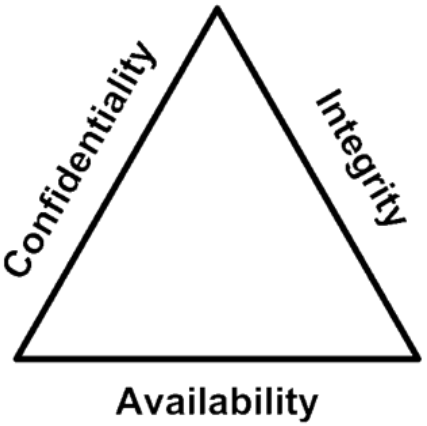
文/ 陳曉莉 | 2019-01-24 發表

讚 5.2 萬 按讚加入iThome粉絲團 讚 264 分享

https://cyber.dhs.gov/ed/19-01/
https://www.ithome.com.tw/news/128433

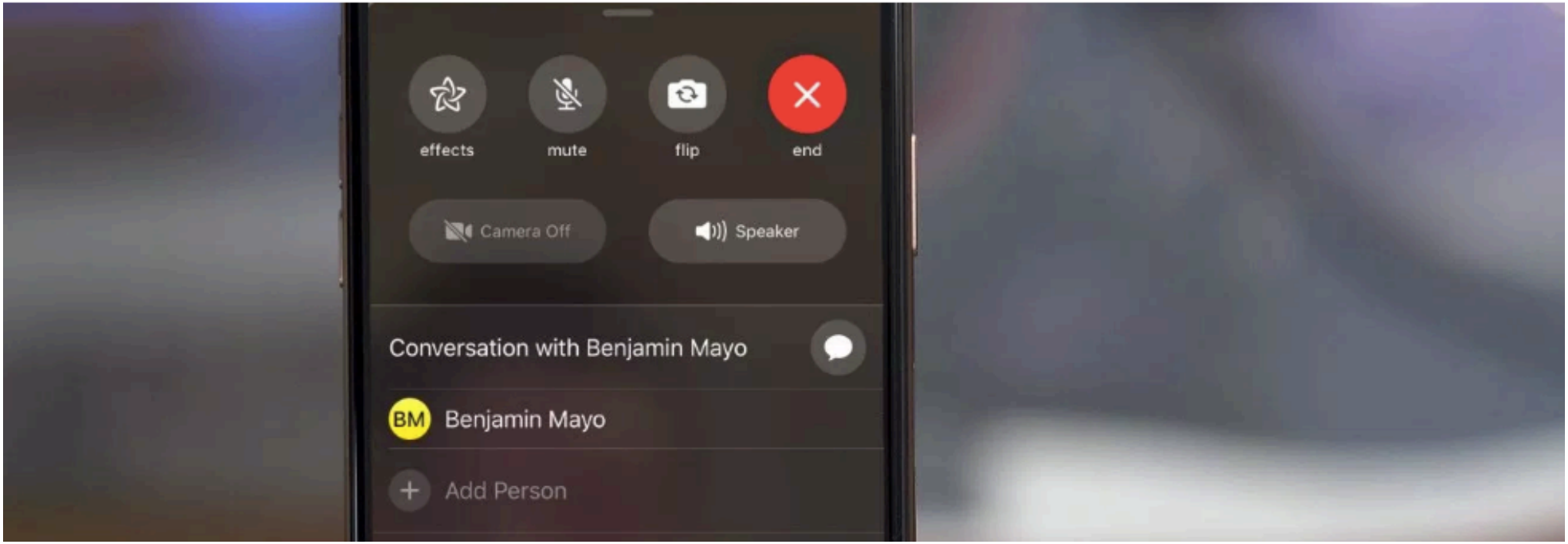
zuvio

# Exercise: which security requirement is violated?



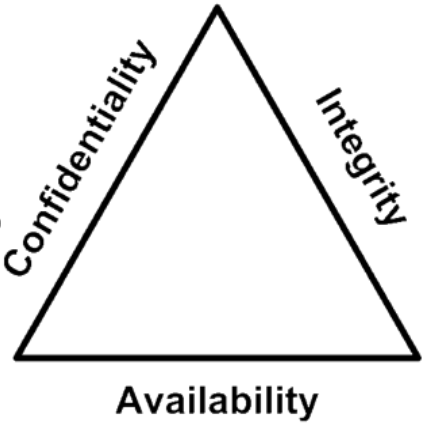

## Major iPhone FaceTime bug lets you hear the audio of the person you are calling ... before they pick up

Benjamin Mayo - Jan. 28th 2019 3:41 pm PT @bzamayo



zuvio

# Exercise: which security requirement is violated?

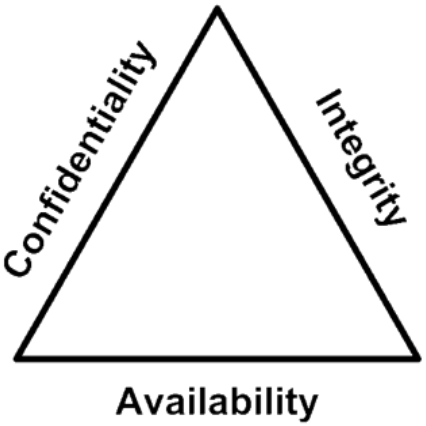



## 健保當機2.5小時 全台看診大亂

11504　出版時間：2019/02/19

zuvio

# Exercise: which security requirement is violated?




**Workstation Team** <217ta@csie.ntu.edu.tw> Fri, Nov 2, 2018, 3:42 PM

to faculty, Workstation

Chinese (Traditional) > English Translate message Turn off for: Chinese (Traditional)

教授、同仁們，您們好：

因系上IMAP遭受惡意D-DOS攻擊，目前IP已被計中防火牆隔離，故將導致教授群組受到影響（因目前只有教授群組未完全設定信件轉寄，只能透過IMAP管理信件）；
現已將影響程度降到最低，但特定使用族群仍會有信件伺服器無法連線的情況產生（如下表）：

| CSIE WEBMAIL | NTU MAIL | GMAIL | 手機APP或Outlook等 |
|---|---|---|---|
| 信件收發不受影響 | 信件收發不受影響 | 信件收發不受影響 | 限制必須於CSIE網域進行連線 |

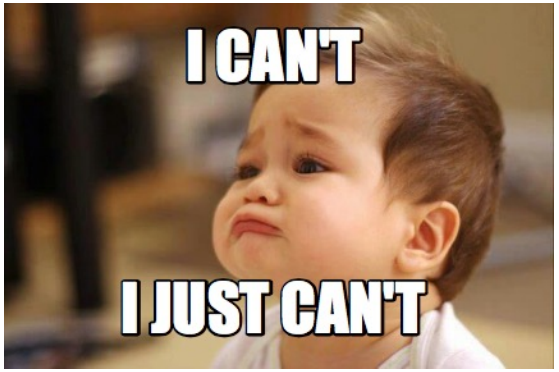
如透過CSIE WEBMAIL（https://webmail.csie.ntu.edu.tw）收發CSIE Domain的信件皆能正常使用，
藉由CSIE Mail Server轉信至NTU Mail或Gmail之信件亦不受影響。

# Other security requirements

Authorization (授權)
Access control (存取控制)
Accountability (可歸責性)
Auditability (可稽核性)
Authenticity (鑑別性)
Non-repudiation (不可否認性)
Anonymity (匿名)
Privacy (隱私)
…

# 那要怎麼做到滴水不漏？

Wrong question!




100%安全、防禦所有攻擊，實務上是做不到的，為什麼？

- 預算有限
- 效能需求
- 未知的攻擊 (zero-day attacks)
- 難以掌控的因素 (如使用者的使用方式)

~~The system is 100% secure~~

The system provides [Security Requirement] against [Threat Model] under [Assumption]

針對攻擊者的假設：攻擊者的能力、知識、資源等

其他的假設：E.g., 假定所有的客戶都不將新發的提款卡照片po上網或是把密碼告訴別人

# 例子

The [system] provides [security requirement] against [Threat Model] under [Assumption]

System = ATM提款系統

Security requirement= 身份認證

Threat model = 撿到提款卡並亂試pin碼

Assumption = 使用者沒把pin碼寫在卡片套上或是用生日當pin碼

# 合理的threat model很重要

# Threat model

Assumptions about the adversary

- Remember, we can't fight against every possible attack.

Several well-known models exist

- Chosen-plaintext attack (CPA), chosen-ciphertext attack (CCA)
- Honest-but-curious
- Adversary in the Dolev-Yao model
- …

# Threat model

Define by attacker's **capability**, **knowledge**, and **resource**

Capability – what can the attacker do?

- E.g., passive vs. active

Knowledge – what does the attacker know?

- E.g., insider vs. outsider

Resource – how much resource does the attacker have?

- E.g., script kiddies vs. government-funded groups

What's a reasonable threat model? It depends.

- Risk = impact of the attack × likelihood of the attack

# 沒有白吃的午餐 – Cost of Security

Security comes with a price

- 開發和維護的成本
- 系統效能降低
- 使用者抱怨

Technical challenge: making security mechanisms cheaper, faster, and more usable

Non-technical challenge: justify such cost to your boss/customer!

# 沒有白吃的午餐 – Cost of Security

可能的攻擊這麼多怎麼辦？

沒辦法全防，但可以盡量提升攻擊成功的難度

定義一個合理的threat model

- 如根據risk排序
- Risk = impact of the attack × likelihood of the attack

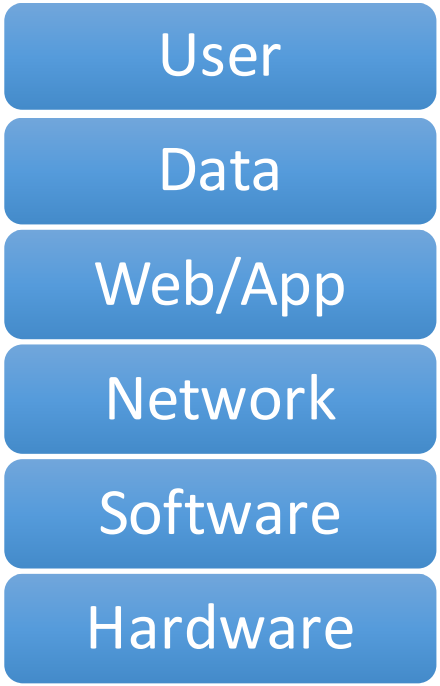
善用共享資源及時修補已知、一般性的漏洞

- Sharing intel to help timely fixes
- Many exploit kits for known attacks; even script kiddies can cause great damage.

把精力放在未知的、針對性的攻擊

# 安全性取決於最弱的環節

**Security is only as strong as the weakest link**




Attack: Find one place to penetrate

Defense: Need to secure every place

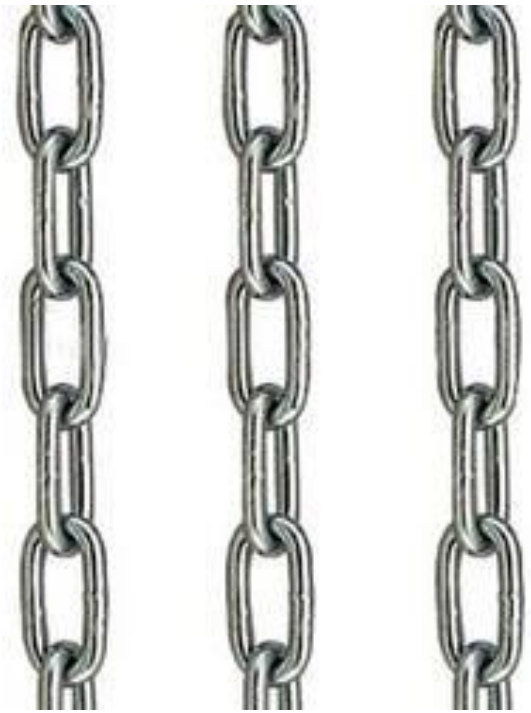
# Defense in depth


Examples

- Two-factor authentication
- Anti-virus + firewall + IDS

We can combine multiple strategies

- Prevention
- Detection & Recovery
- Resilience
- Deterrence



zuvio

# Exercise

**Security mindset:**
Think about how to make it fail instead of how to make it work!

What would be a reasonable threat model?

What might be the weakest link?

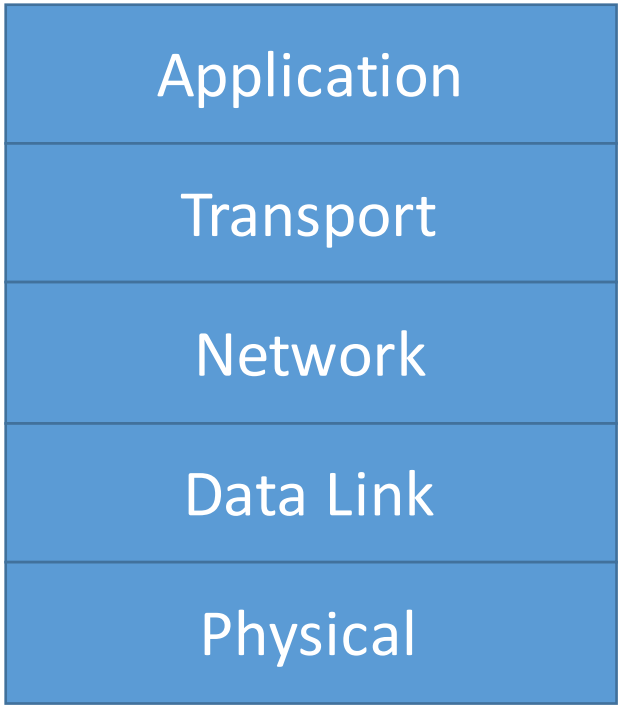
系館門禁系統

# TCP/IP (In)security

IP spoofing

TCP SYN flood

# Securing Network Protocols




HTTP, Telnet, SMTP, DNS, BGP DNSSEC, SBGP

SSL/TLS, SSH

TCP, UDP

IP IPSec

Wi-Fi WEP, WPA

We may also need: Entity authentication, anonymous communication, DDoS defense

# IP Spoofing

Forging the source IP address of an IP packet

Why IP spoofing?

- Concealing the sender's identity
- Impersonating another entity

Exploited by many DDoS attacks

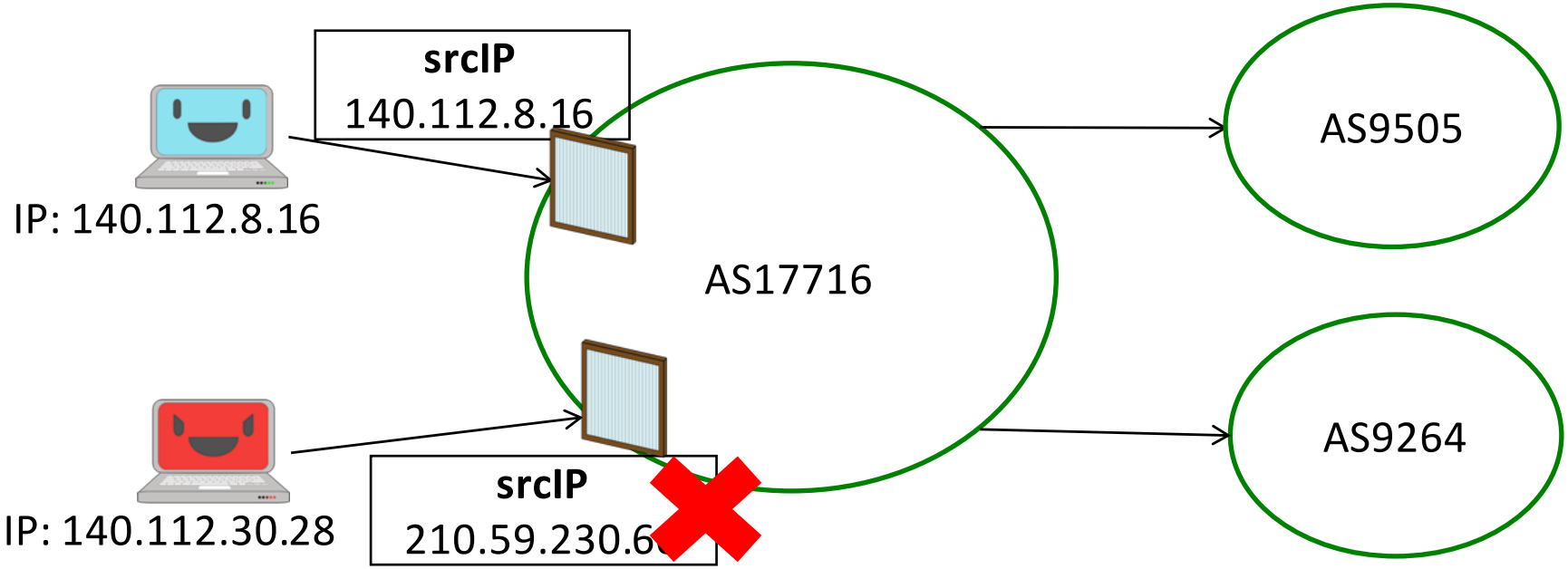
A fundamental problem in the current Internet architecture

- Packets are routed based on destination IP addresses
- No explicit authentication of source IP addresses

# Ingress Filtering

Aims to mitigate IP spoofing

RCF 2827 / BCP 38 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing



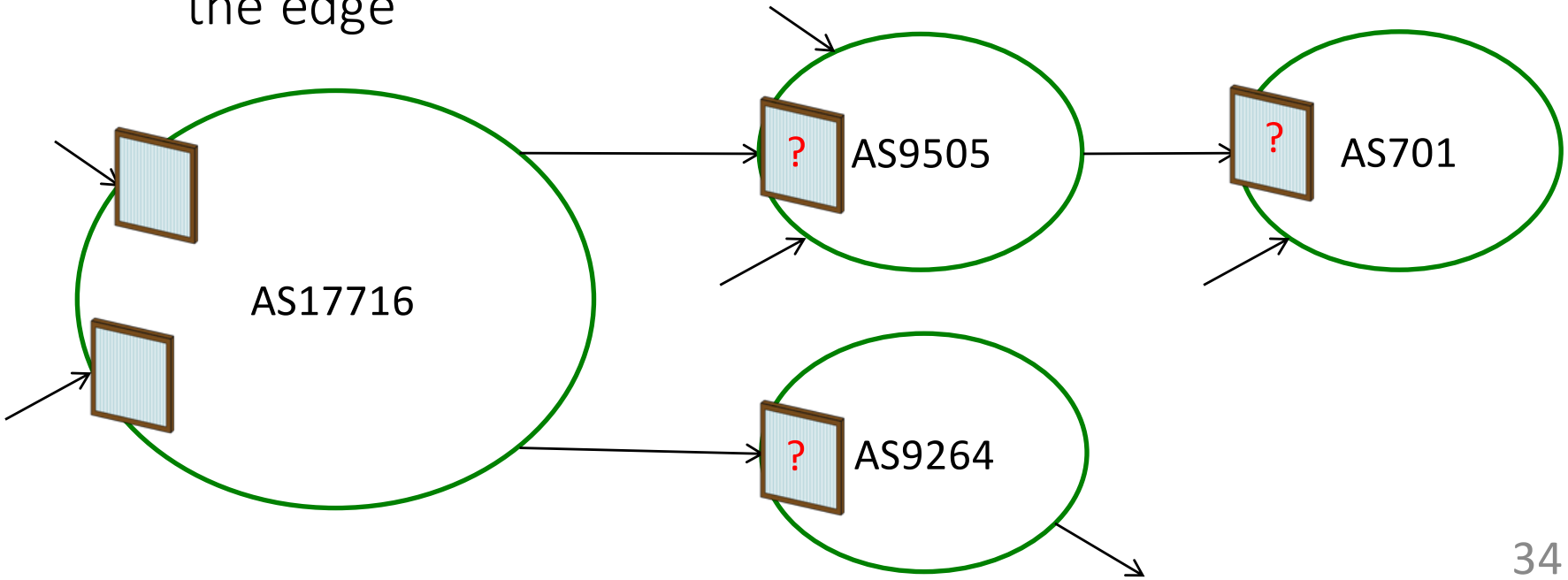
# Ingress Filtering

Only forwards packets with **legitimate** source IPs

- "Legitimate" is defined as "expected at the ingress point"

Challenge: How can an Autonomous System (AS) know which IPs are legitimate?

- Hard to determine unambiguously as it moves away from the edge



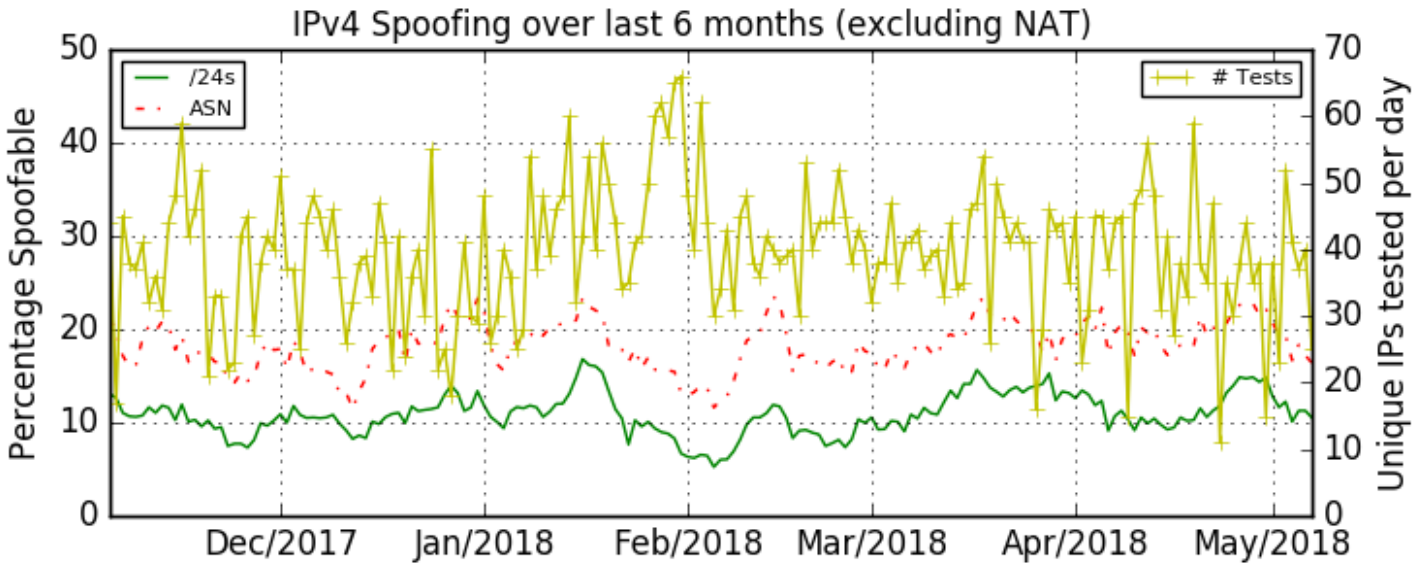
# Deployment Issues of Ingress Filtering

Require 100% deployment to be effective

- Less effective as moving away from the source

No incentive for ISPs to be an early adopter

- Preventing spoofing does not necessarily makes one's own network less vulnerable

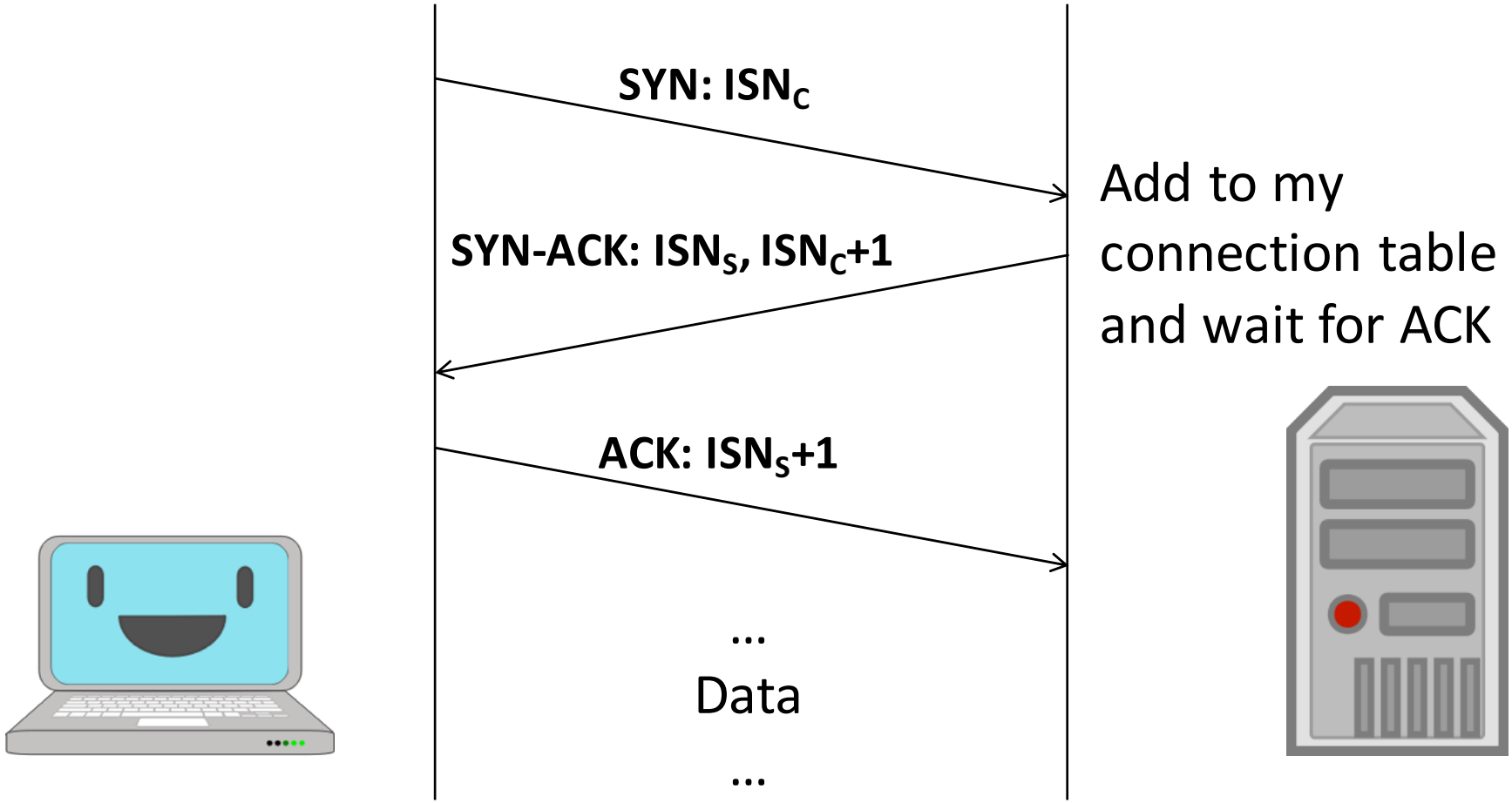



https://spoofer.caida.org/

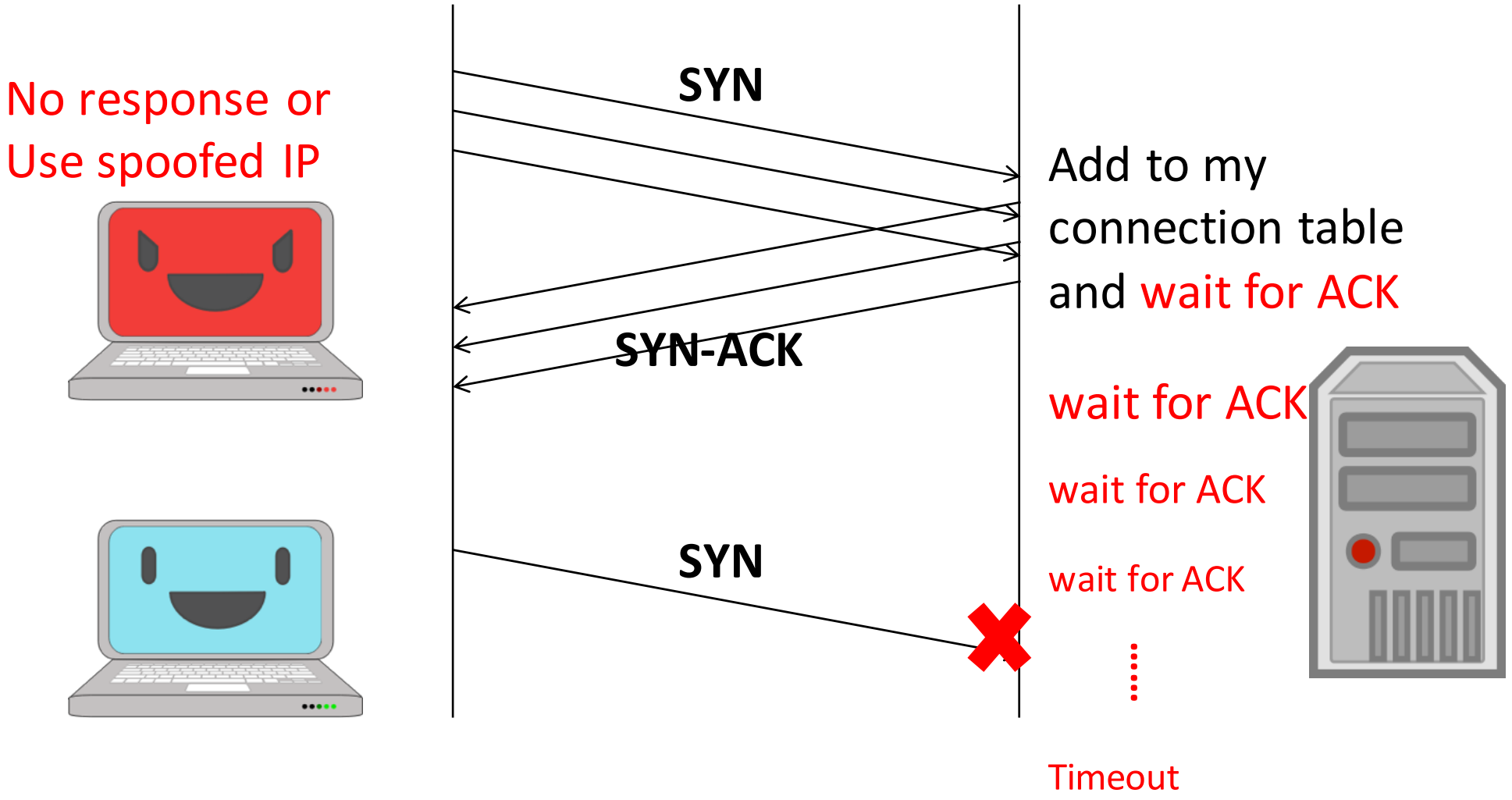
# TCP SYN Flood

# TCP Connection Establishment: Three-way Handshake

ISNs (initial sequence number) are picked at random



# TCP SYN Flood



# TCP SYN Flood

First serious DoS attack

Single attacker could tie up server resources to prevent other clients from connecting to server

Problem exploited by SYN Flooding?

- Server needs to keep state after receiving initial SYN
- Connection table has limited size
- Attacker floods server with SYN packets, does not follow up with ACK packet to complete TCP handshake
- Server keeps state, waits for ACK, exhausts resources

# Countermeasures

Buy more memory?

Shorter timeout?

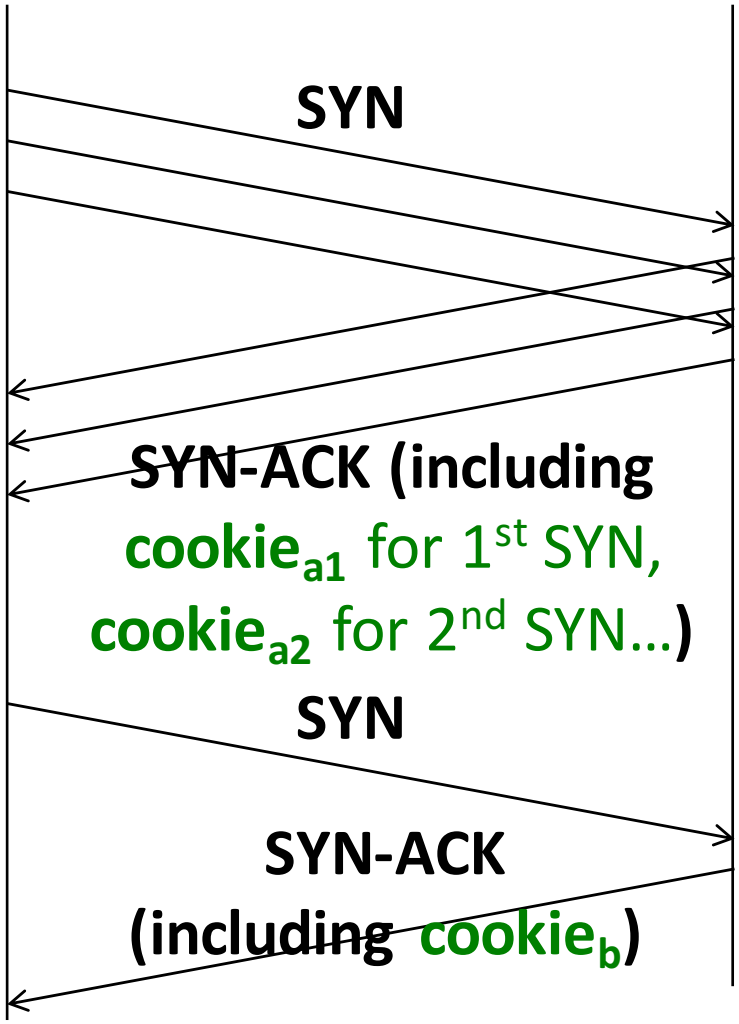
IP-based filtering?

Better solution: TCP SYN Cookie

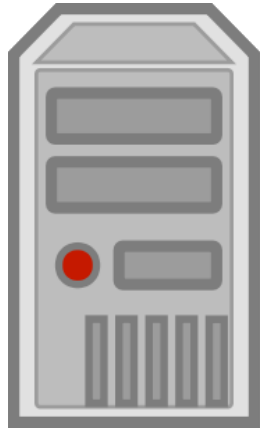
- By D. J. Bernstein, http://cr.yp.to/syncookies.html
- Server keeps no state before handshake completion
- Disadvantages: computational overhead, TCP options lost

# TCP SYN Cookies

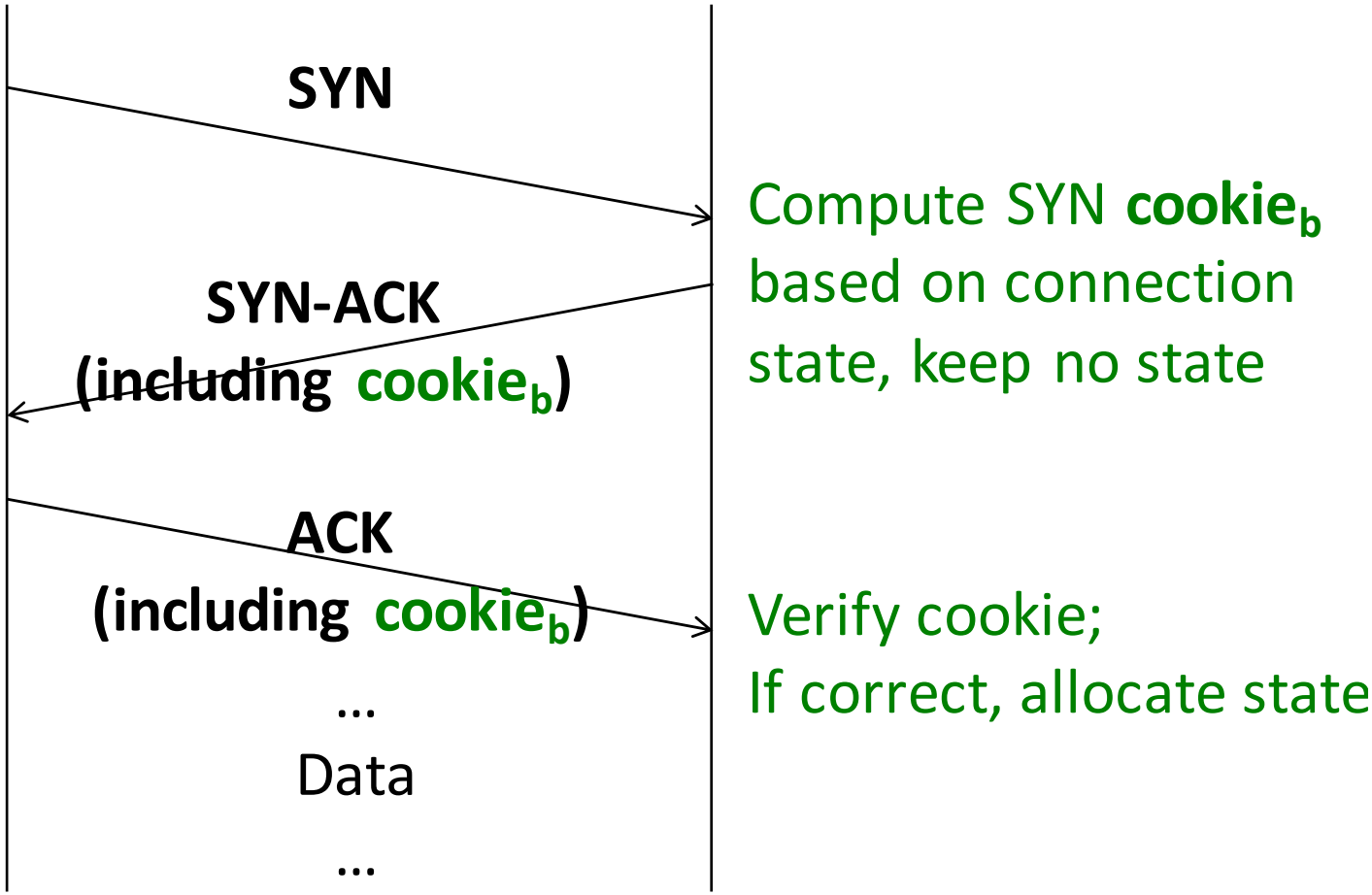
No response or
Use spoofed IP




Compute SYN cookie per SYN request based on connection state, no state kept



# TCP SYN Cookies



# TCP SYN Cookies

TCP SYN Cookie is encoded as a particular chosen server ISN (initial sequence number)

- ISN was picked randomly before

How to generate TCP SYN Cookie?

What about?

```
Cookie = H(Server_IP, Client_IP, Server_port,
Client_port, Client_state, time)
```

Better:

```
Cookie = MAC_key(Server_IP, Client_IP, Server_port,
Client_port, Client_state, time)
```

**Key** is kept to server only

# Why not attack by establishing thousands of connections?

Works too, but less efficient and easier to detect

- Less efficient: attacker needs to keep state too
- Easier to detect: Server can easily identify the attacker, since it uses its real IP with thousands of open connections

Work better for application-layer DDoS

- Some applications reserve very small state and can be easily saturated

# Denial of Service (阻斷服務攻擊)

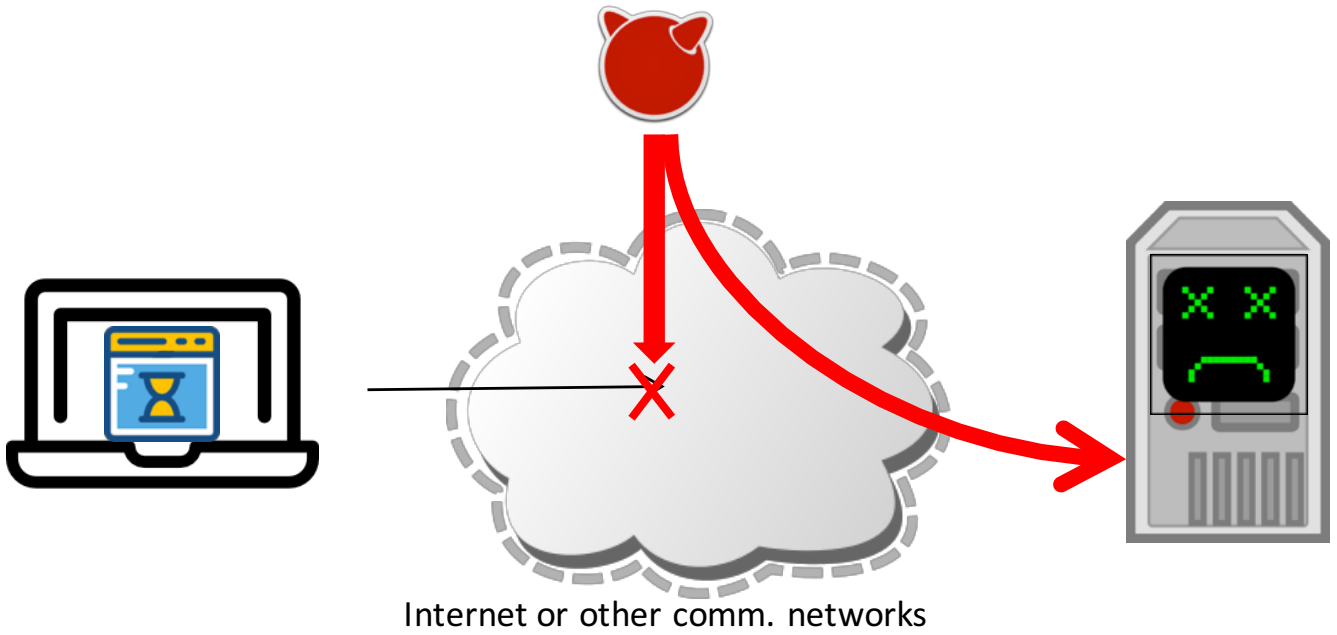
讓使用者無法使用想要的服務

針對可用性(availability)的攻擊

SYN flood是一種Denial of Service

# 阻斷服務攻擊常見手法

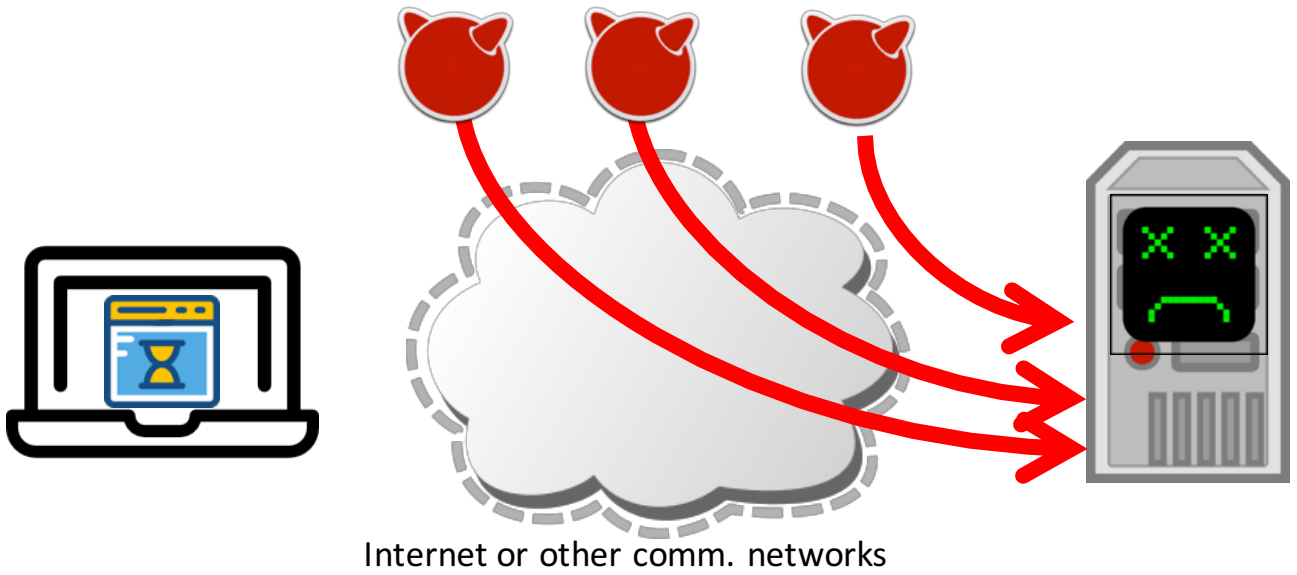
大量消耗共用的資源（e.g. bandwidth, CPU, memory）



# 分散式阻斷服務攻擊 (Distributed Denial of Service)

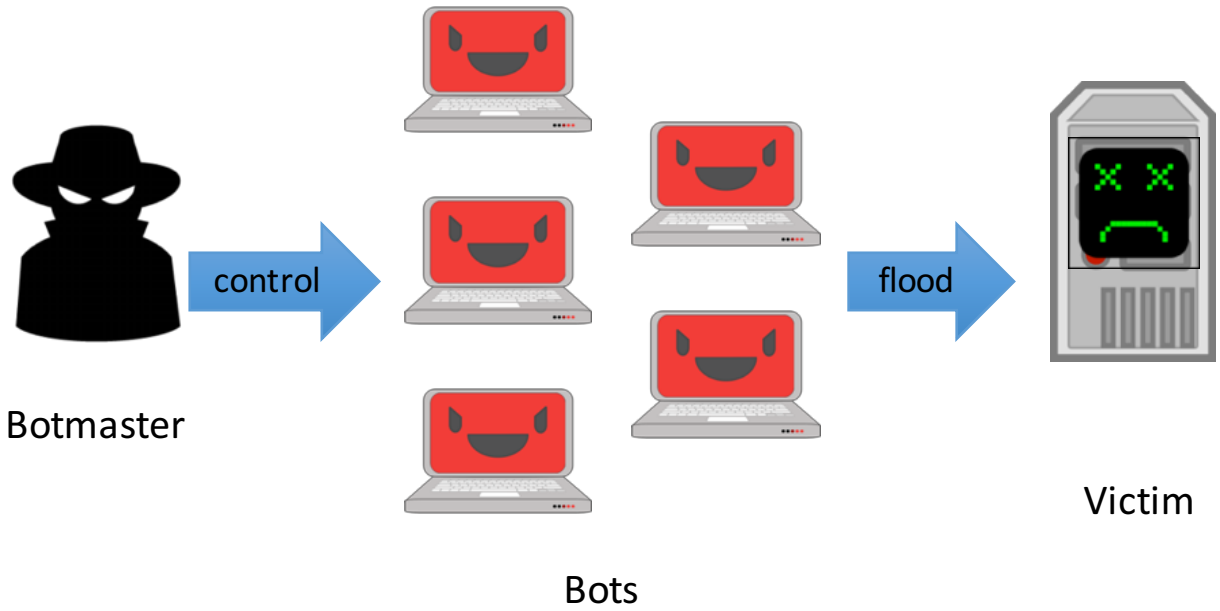
多於一個攻擊來源

提高攻擊強度、降低單一來源被偵測的風險



# Botnet-driven DDoS

Botnet = 殭屍網路



zuvio

# Exercise

選擇一個NASA服務，討論其效能（如運算、儲存、頻寬）瓶頸

請估計此服務被癱瘓的的難易度（e.g.,需要同時多少人上線）

# DNS (In)security

zuvio

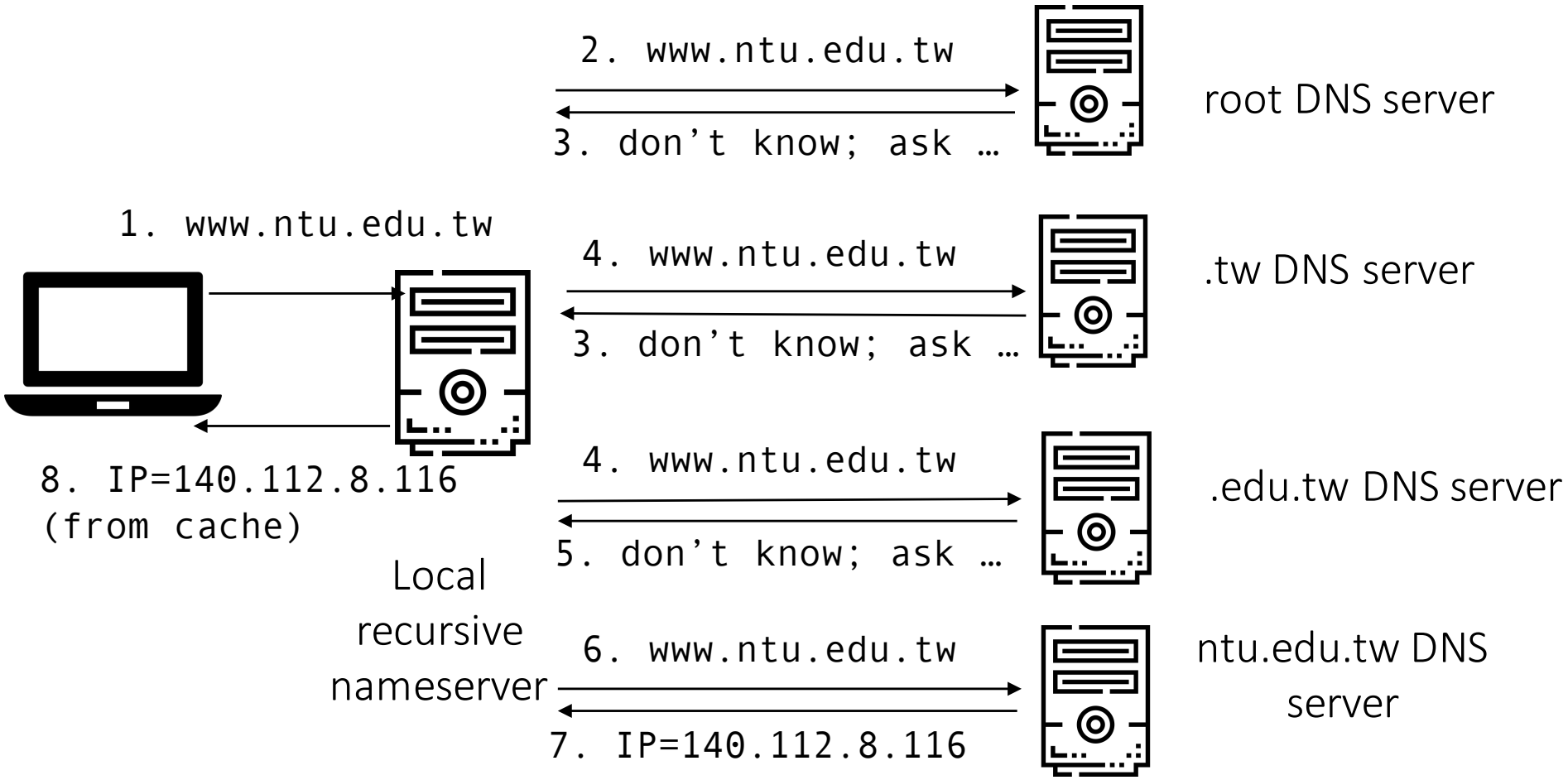
# Domain Name System (DNS)

DNS maps domain names to IP addresses

- `csie.ntu.edu.tw -> 140.112.30.28`
- `www.ntu.edu.tw ->` ?
- Can also map to other types of *resources* (e.g., nameserver, mail exchanger, …)

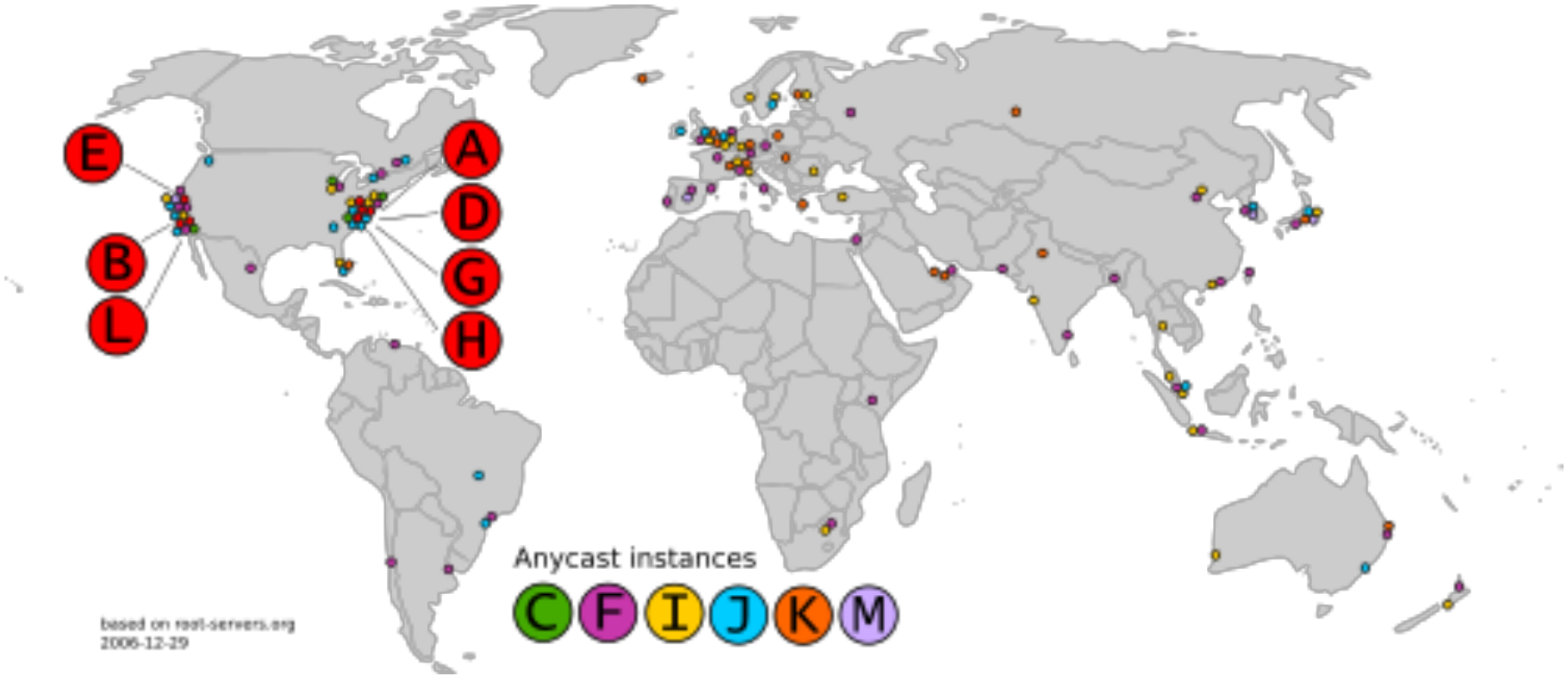
```
> dig csie.ntu.edu.tw

;; QUESTION SECTION:
;csie.ntu.edu.tw.               IN      A

;; ANSWER SECTION:
csie.ntu.edu.tw.        600     IN      A       140.112.30.28
```

# Domain Name System (DNS)




http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

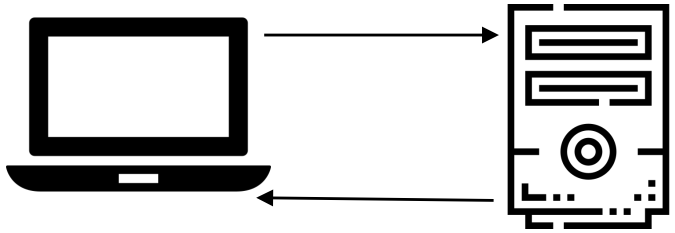
# Root Name Servers




https://en.wikipedia.org/wiki/Root_name_server

# DNS Cache

1. Ask again www.ntu.edu.tw



2. IP=140.112.8.116 (from cache)

```
;; ANSWER SECTION:          TTL
www.ntu.edu.tw.         86400   IN      A       140.112.8.116

;; AUTHORITY SECTION:
ntu.edu.tw.             86400   IN      NS      ntu3.ntu.edu.tw.
ntu.edu.tw.             86400   IN      NS      dns.tp1rc.edu.tw.
ntu.edu.tw.             86400   IN      NS      dns.ntu.edu.tw.

;; ADDITIONAL SECTION:
dns.ntu.edu.tw.         86400   IN      A       140.112.254.4
dns.tp1rc.edu.tw.       259200  IN      A       163.28.16.10
ntu3.ntu.edu.tw.        604800  IN      A       140.112.2.2
dns.ntu.edu.tw.         86400   IN      AAAA    2001:288:1001:254::4
```

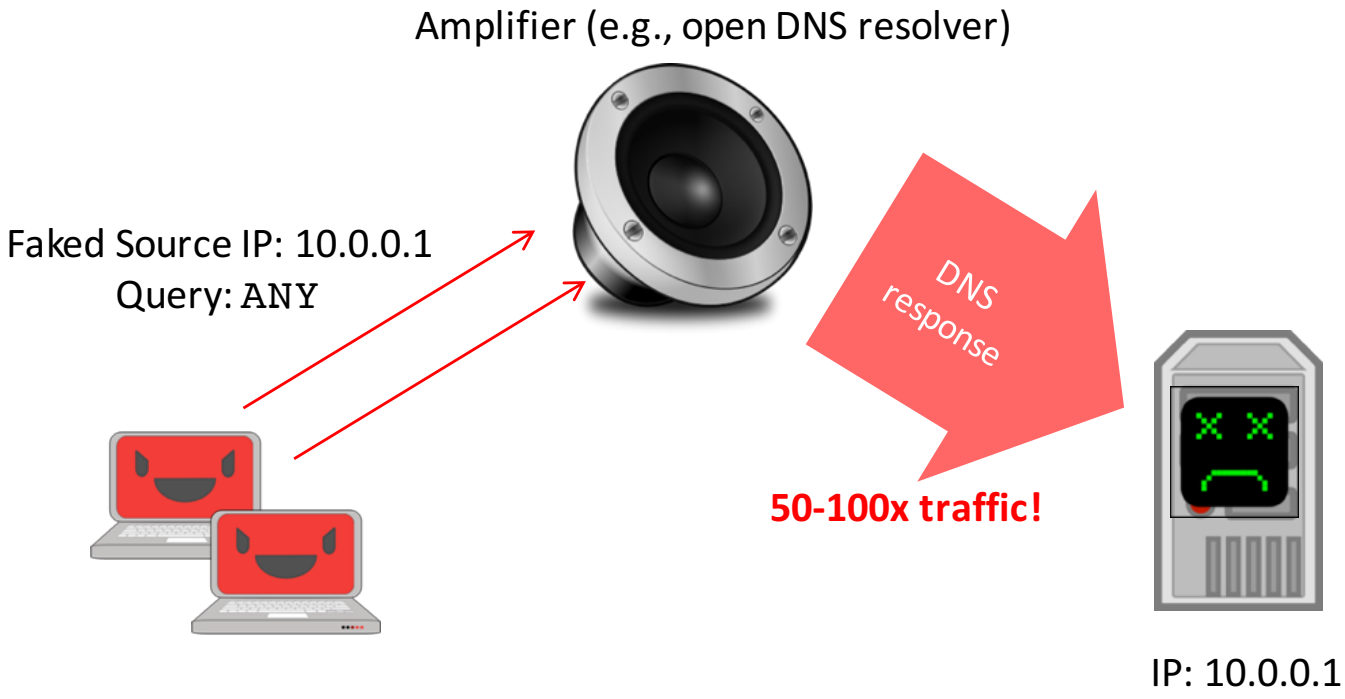
# Attacking DNS

DNS amplification attack

DNS hijacking

- DNS cache poisoning

# DDoS Amplification



# Amplification Factor

## Memcached: 51,200x

| Protocol | BAF *all* | BAF 50% | BAF 10% | PAF *all* | Scenario |
|---|---|---|---|---|---|
| SNMP v2 | 6.3 | 8.6 | 11.3 | 1.00 | *GetBulk* request |
| NTP | 556.9 | 1083.2 | 4670.0 | 3.84 | Request client statistics |
| $DNS_{NS}$ | 54.6 | 76.7 | 98.3 | 2.08 | ANY lookup at author. NS |
| $DNS_{OR}$ | 28.7 | 41.2 | 64.1 | 1.32 | ANY lookup at open resolv. |
| NetBios | 3.8 | 4.5 | 4.9 | 1.00 | Name resolution |
| SSDP | 30.8 | 40.4 | 75.9 | 9.92 | *SEARCH* request |
| CharGen | 358.8 | n/a | n/a | 1.00 | Character generation request |
| QOTD | 140.3 | n/a | n/a | 1.00 | Quote request |
| BitTorrent | 3.8 | 5.3 | 10.3 | 1.58 | File search |
| Kad | 16.3 | 21.5 | 22.7 | 1.00 | Peer list exchange |
| Quake 3 | 63.9 | 74.9 | 82.8 | 1.01 | Server info exchange |
| Steam | 5.5 | 6.9 | 14.7 | 1.12 | Server info exchange |
| ZAv2 | 36.0 | 36.6 | 41.1 | 1.02 | Peer list and cmd exchange |
| Sality | 37.3 | 37.9 | 38.4 | 1.00 | URL list exchange |
| Gameover | 45.4 | 45.9 | 46.2 | 5.39 | Peer and proxy exchange |

Rossow, Christian. "Amplification hell: Revisiting network protocols for DDoS abuse." Symposium on Network and Distributed System Security (NDSS). 2014.

How can we mitigate amplification attacks?

# DNS Hijacking

What if the attacker can somehow manipulate the mapping?

- `csie.ntu.edu.tw -> 1.2.3.4`

聯邦網站成為DNS挾持目標，美國國土安全部發出緊急指令

數個美國聯邦網站的網域名稱系統（DNS）遭挾持，駭客將使用者流量變更至駭客所控制的架構，再轉回合法服務，所造成的風險高過於短期重新定向使用者流量的作法

文/ 陳曉莉 | 2019-01-24 發表

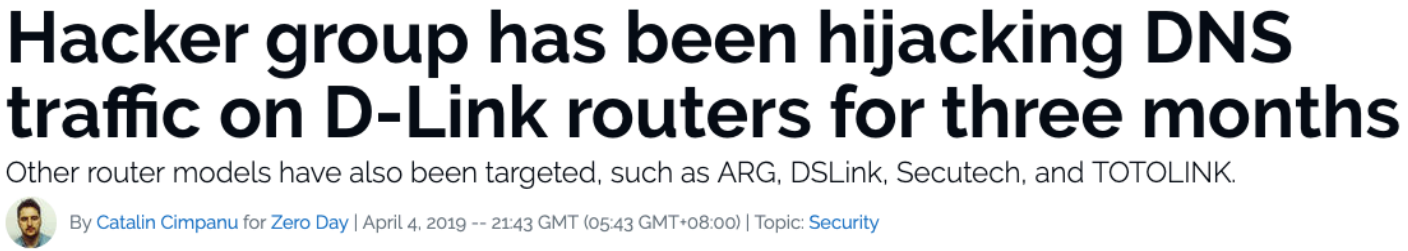
讚 5.3 萬 按讚加入iThome粉絲團 讚 266 分享

思科：國家級駭客持續攻擊中東及北非國家的DNS系統

一起名為「海龜」的國家級攻擊行動，從2017年開始鎖定中東及北非地區超過40個政府及能源組織，發動DNS攻擊，以竊取目標系統或網路的存取憑證

文/ 陳曉莉 | 2019-04-19 發表

讚 5.3 萬 按讚加入iThome粉絲團 讚 251 分享

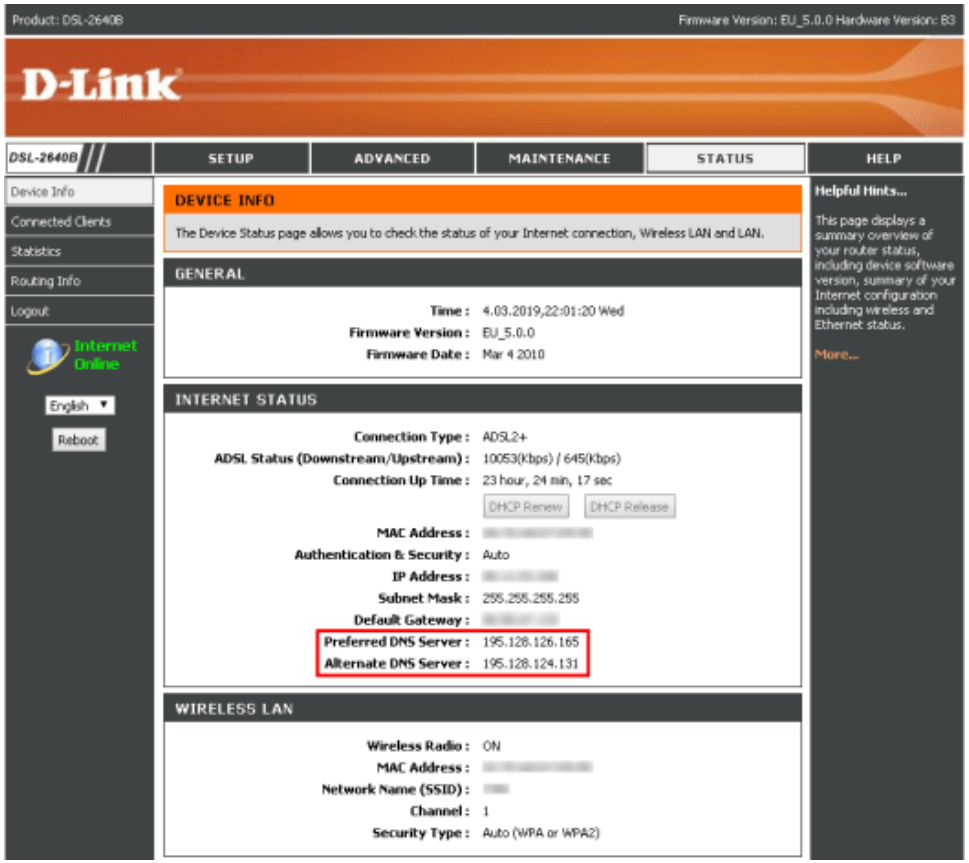


Hacker group has been hijacking DNS traffic on D-Link routers for three months

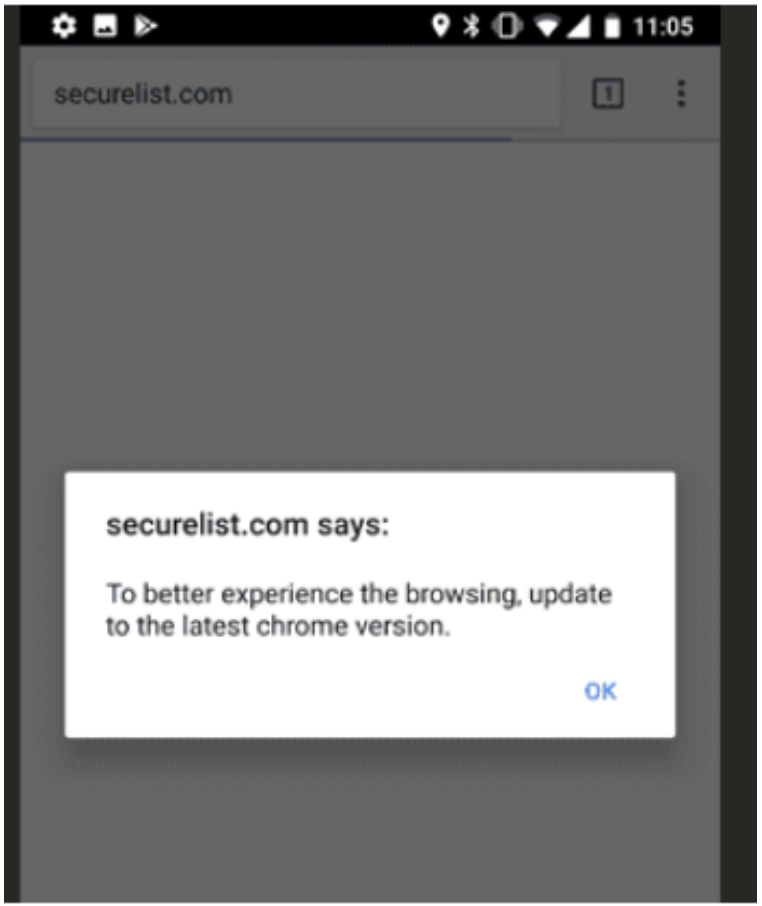
Other router models have also been targeted, such as ARG, DSLink, Secutech, and TOTOLINK.

By Catalin Cimpanu for Zero Day | April 4, 2019 -- 21:43 GMT (05:43 GMT+08:00) | Topic: Security

# DNS hijacking via malware

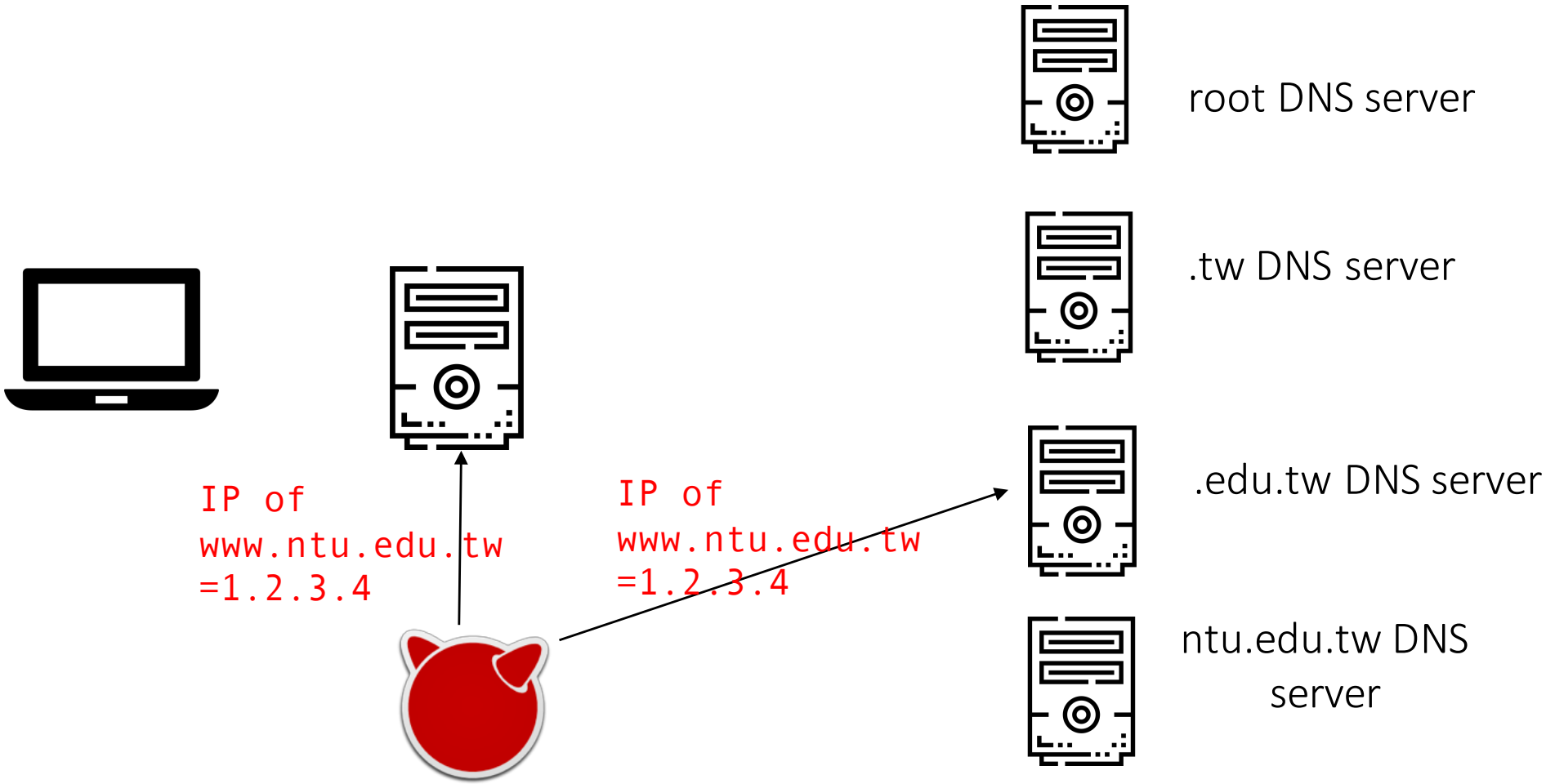



*Example compromised D-Link DSL-2640B router with DNS servers set to rouge DNS servers used in this campaign.*
https://badpackets.net/ongoing-dns-hijacking-campaign-targeting-consumer-routers/




https://thehackernews.com/2018/04/android-dns-hijack-malware.html

# DNS Cache Poisoning

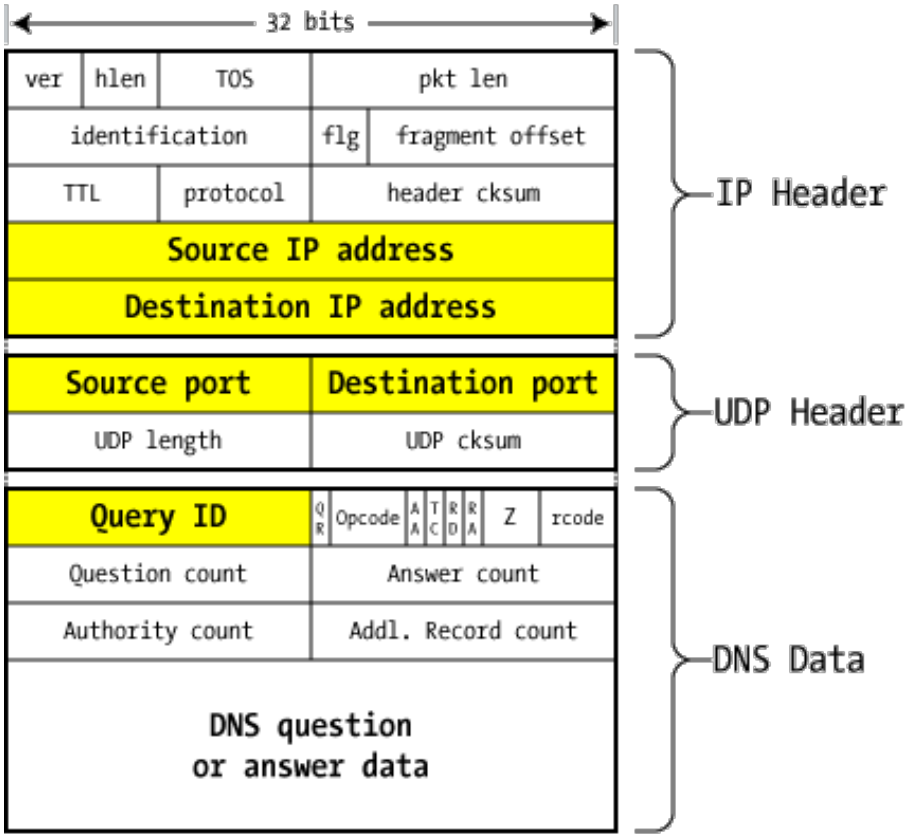



Can an attacker forge the response and poison the cache?

# DNS Cache Poisoning

A response will be accepted if:

1. UDP port matches
2. **Question** section (which is duplicated in the reply) matches
3. **Query ID** matches
4. The Authority and Additional sections represent names that are within the same domain as the question



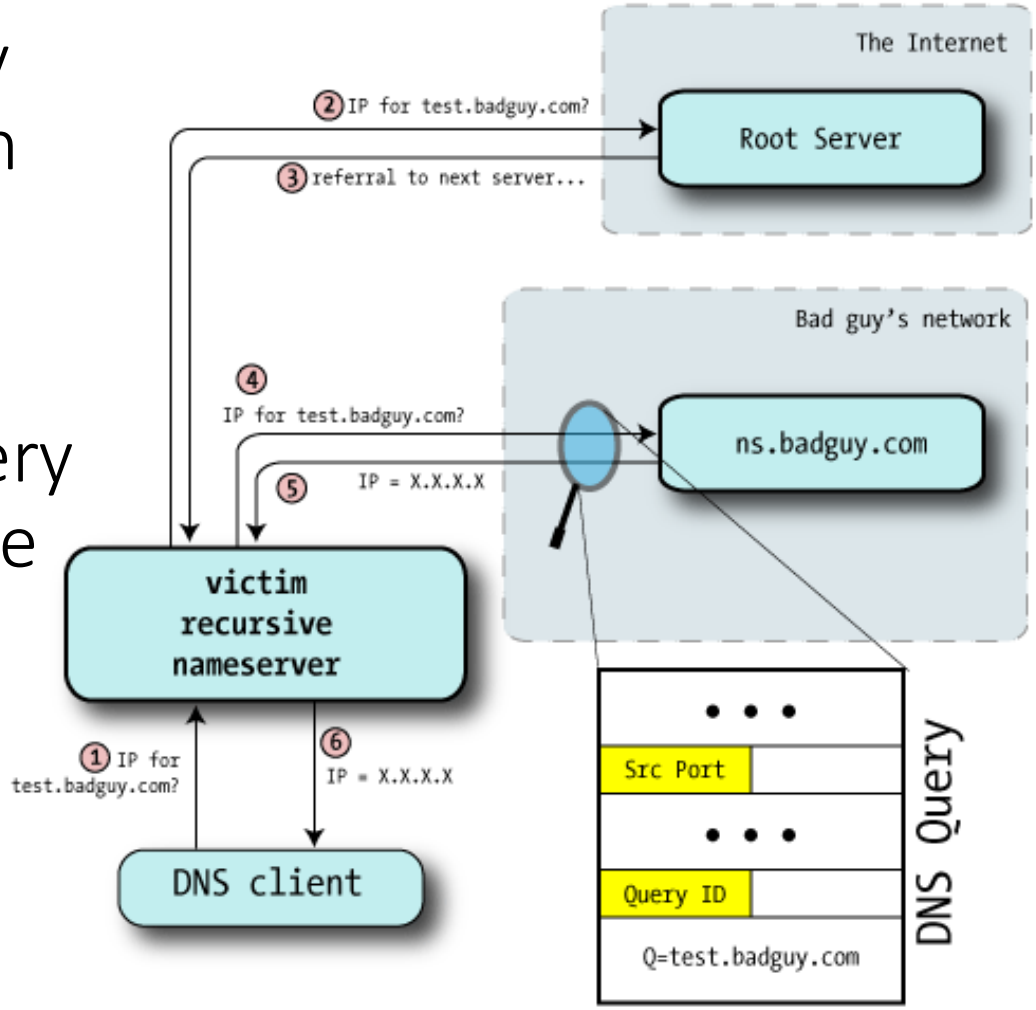

***DNS packet on the wire***

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

# Guess the Query ID

Old implantation: Query ID increments by one on each outgoing request

To learn the current query ID, the attacker tricks the victim nameserver to query the attacker's domain

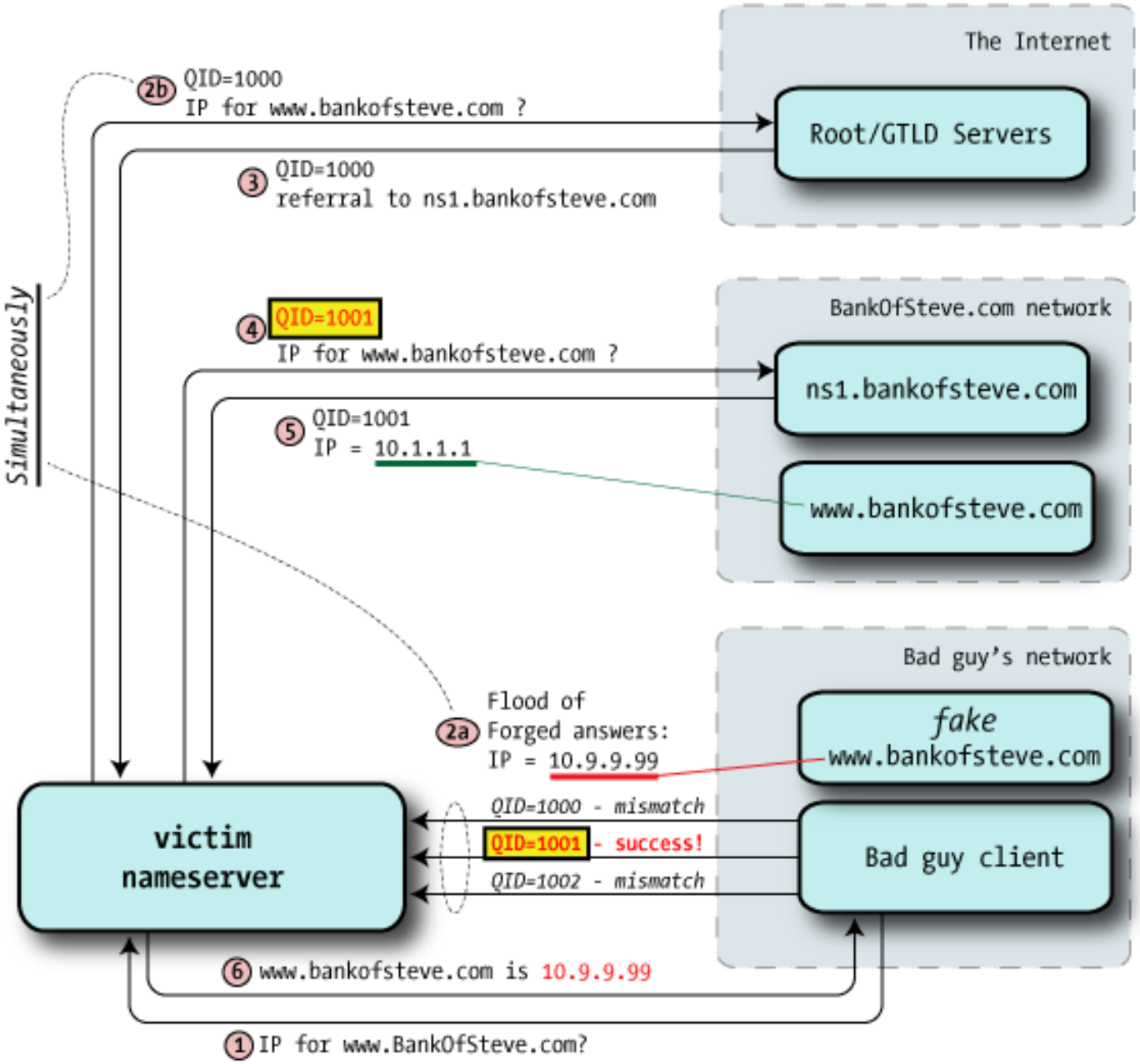



http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

# Guess the Query ID

Flood the victim nameserver with forged answers; first good answer wins.

Set a very high TTL in the poisoning responses to keep the bogus data in cache.




http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

zuvio

# DNS Cache Poisoning

Success Conditions

- The name cannot already be in the cache
- The attacker has to guess the 16-bit query ID
- The attacker has to be faster than the real nameserver

Exercise: Possible mitigation?

- ?

What else can the attacker do to handle randomized query ID?
The attack only poisoned one domain; Can it be more powerful?

# The Kaminsky attack

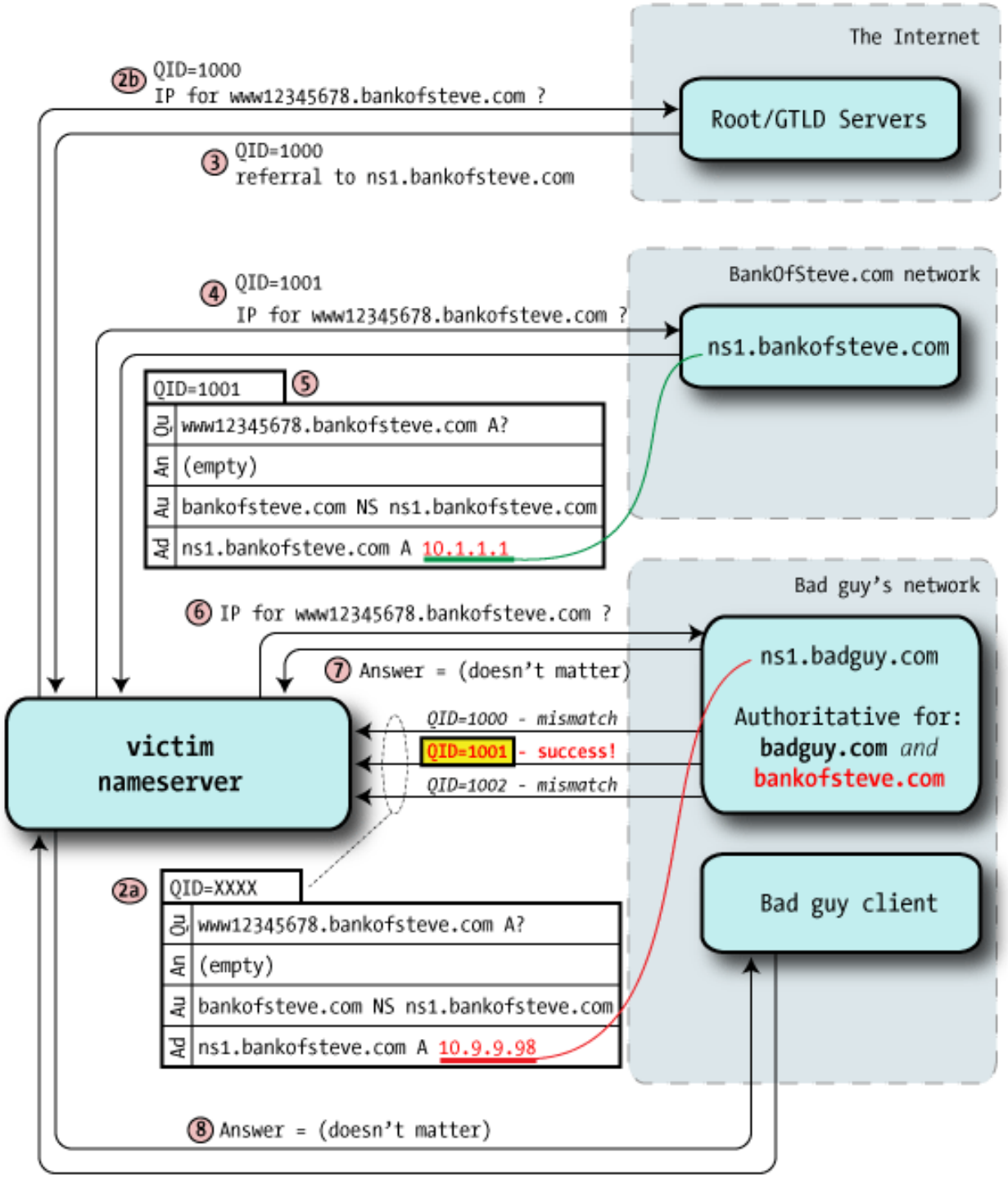
More powerful: **hijack the authority records** instead

Beat random query ID: query many different (non-existing) subdomains

```
;; ANSWER SECTION:
www.ntu.edu.tw.         86400   IN      A       140.112.8.116

;; AUTHORITY SECTION:
ntu.edu.tw.             86400   IN      NS      ntu3.ntu.edu.tw.
ntu.edu.tw.             86400   IN      NS      dns.tp1rc.edu.tw.
ntu.edu.tw.             86400   IN      NS      dns.ntu.edu.tw.

;; ADDITIONAL SECTION:
dns.ntu.edu.tw.         86400   IN      A       140.112.254.4
dns.tp1rc.edu.tw.       259200  IN      A       163.28.16.10
ntu3.ntu.edu.tw.        604800  IN      A       140.112.2.2
dns.ntu.edu.tw.         86400   IN      AAAA    2001:288:1001:254::4
```

Put attacker controlled nameservers

# The Kaminsky attack




http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

# Mitigation to the Kaminsky attack

Increase query ID length: need to change the spec; cannot be done quickly

Increase TTL: ?

Randomize the source port

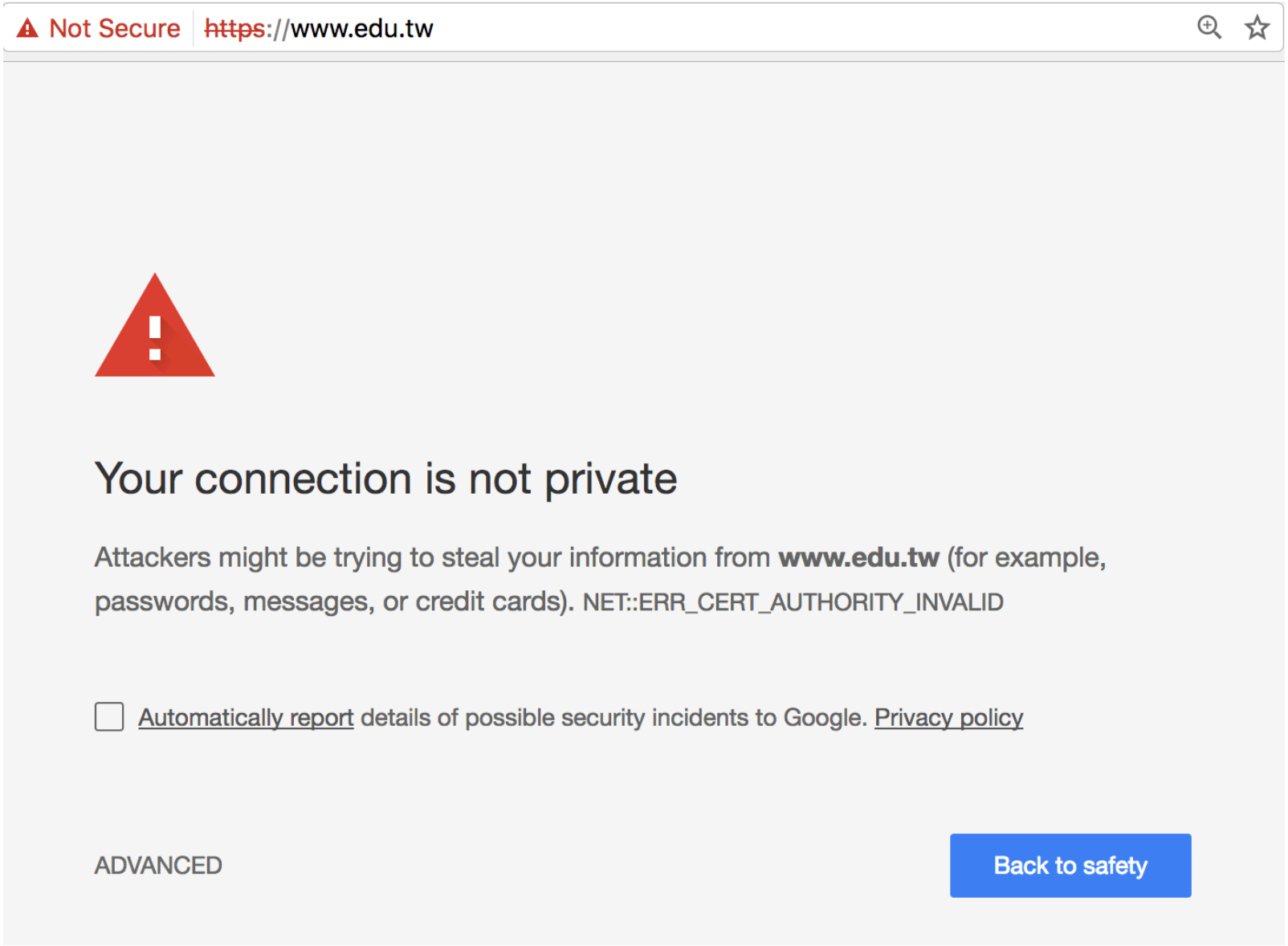
- Microsoft's updated DNS server is said to preallocate 2,500 UDP ports to use for these random queries
- Increase the space from $2^{16}$ to $2^{27}$

Domain Name System Security Extensions (DNSSEC)

- DNS queries are digitally signed to prevent forgery and manipulation

# HTTPS

# 這個網站安全嗎？


Not Secure
https://www.edu.tw
Your connection is not private
Attackers might be trying to steal your information from www.edu.tw (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID
Automatically report details of possible security incidents to Google. Privacy policy
ADVANCED
Back to safety

# 這個網站安全嗎？


https://my.ntu.edu.tw
請使用計中帳號登入！
SSO1.3
登入
※ 預防帳號遭盜用，請定期修改密碼！
National Taiwan University
myNTU
搜尋
學生專區
個人資訊 >
課務資訊 >
生活資訊 >
助學資訊 >
社團活動資訊 >
畢業生資訊 >
課程學習
選課專區
停修課程網路申請系統
臺大實習計畫
more ...
教職申辦
自然人憑證簽到退
薪資入帳變更申請
新進人員健檢系統
more ...
十大熱門服務 >
成績查詢
到勤差假申請/簽核
活動報名
學生請假
滿意度問卷調查
學士班修課檢視表
April

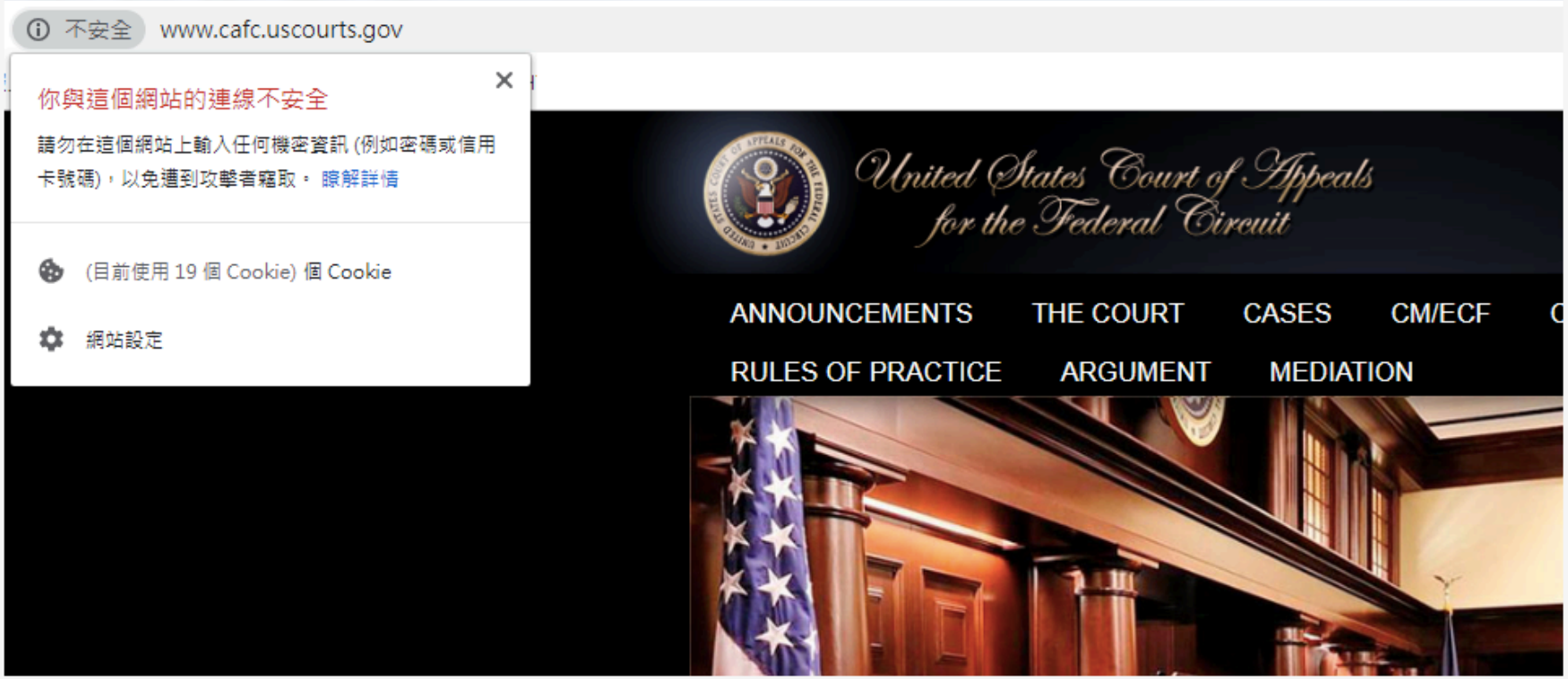
# 這個網站安全嗎？

## 美國政府停擺，聯邦網站所使用的逾80個TLS憑證失效

由於美國參議院與川普之間的歧義造成政府機構的預算不足，已持續停擺超過24天，連美國政府旗下聯邦網站到期的TLS憑證都無法續約

文/ 陳曉莉 | 2019-01-14 發表

讚 5.2 萬 按讚加入iThome粉絲團 讚 428 分享



# SSL/TLS overview


Goal: building a secure end-to-end channel

- SSL = Secure Sockets Layer (predecessor)
- TLS = Transport Layer Security (standard)
- HTTPS = HTTP over SSL/TLS

HTTPS is a dominant protocol for securing HTTP communication

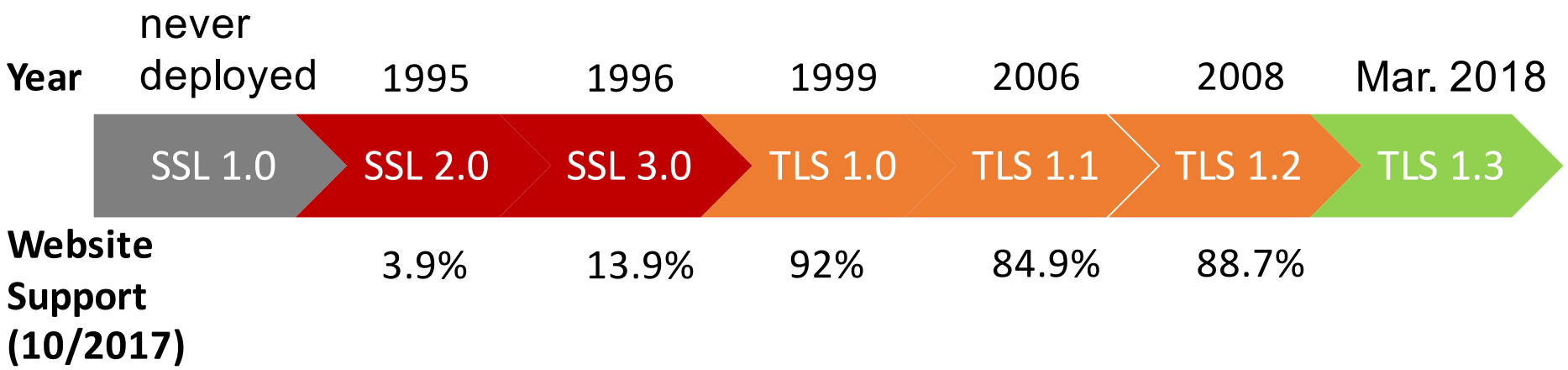
# SSL/TLS overview


Security requirements

- Confidentiality
- Integrity
- Authentication (mostly server authentication, client authentication in TLS is rare)

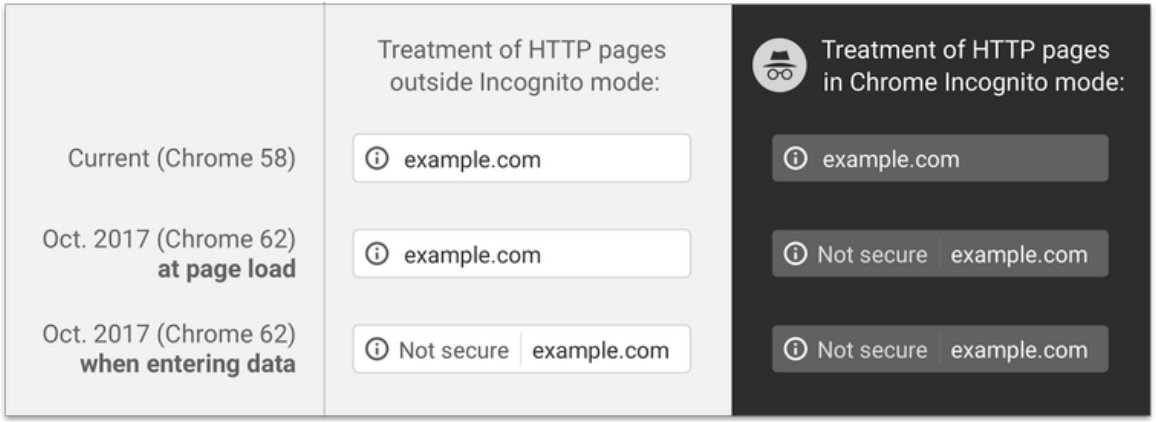
=> prevents a man-in-the-middle attacker from eavesdropping, manipulation, or impersonation

# SSL/TLS history

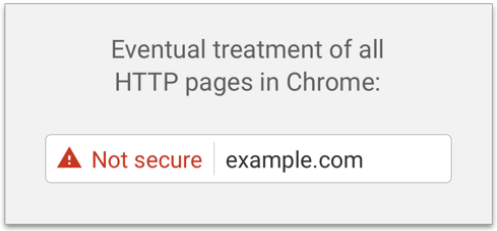



* SSL 2.0 and 3.0 are disabled by default or not supported anymore for Chrome after v40, Firefox after v34, IE 11, Android 5.1, OSX 10.11.
* IE6 only supports SSL 2.0 and 3.0.

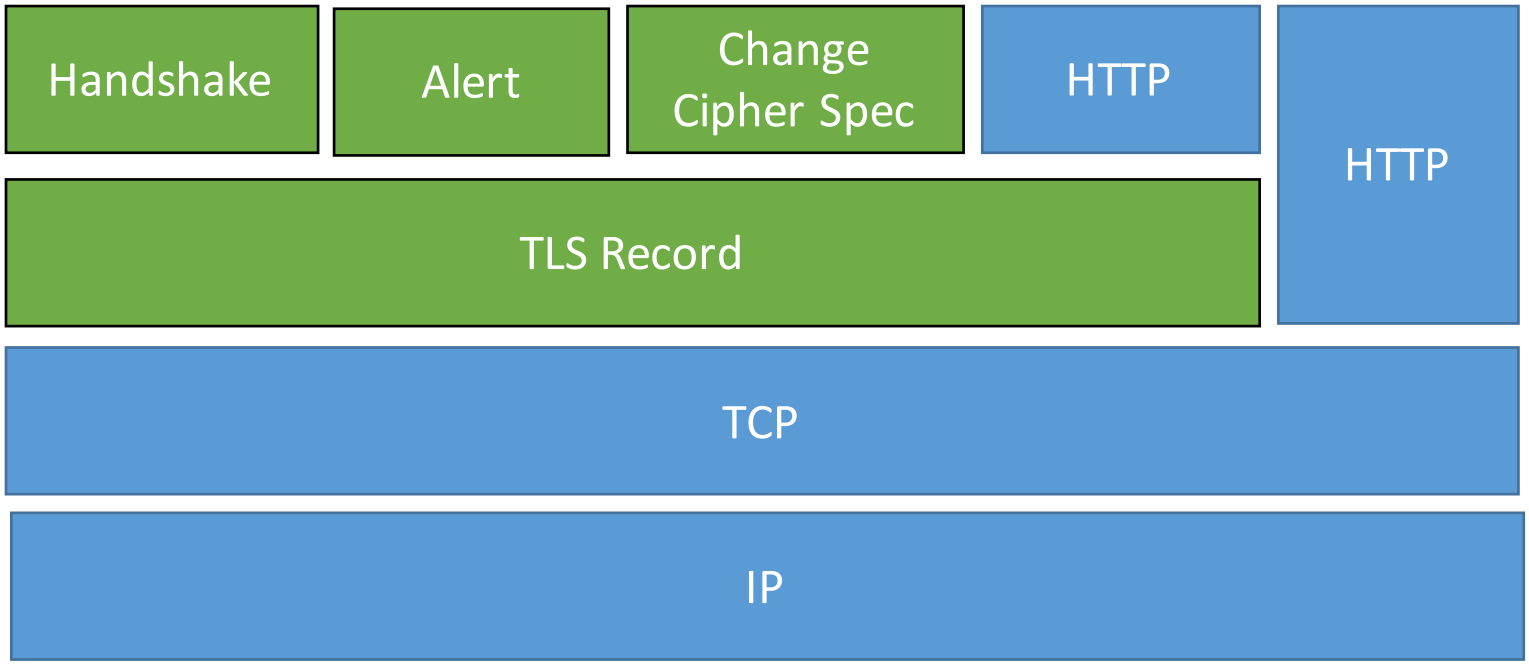
# Google Chrome and Firefox marked HTTP as a non-secure protocol




"Eventually, we plan to label all HTTP pages as non-secure, and change the HTTP security indicator to the red triangle that we use for broken HTTPS."

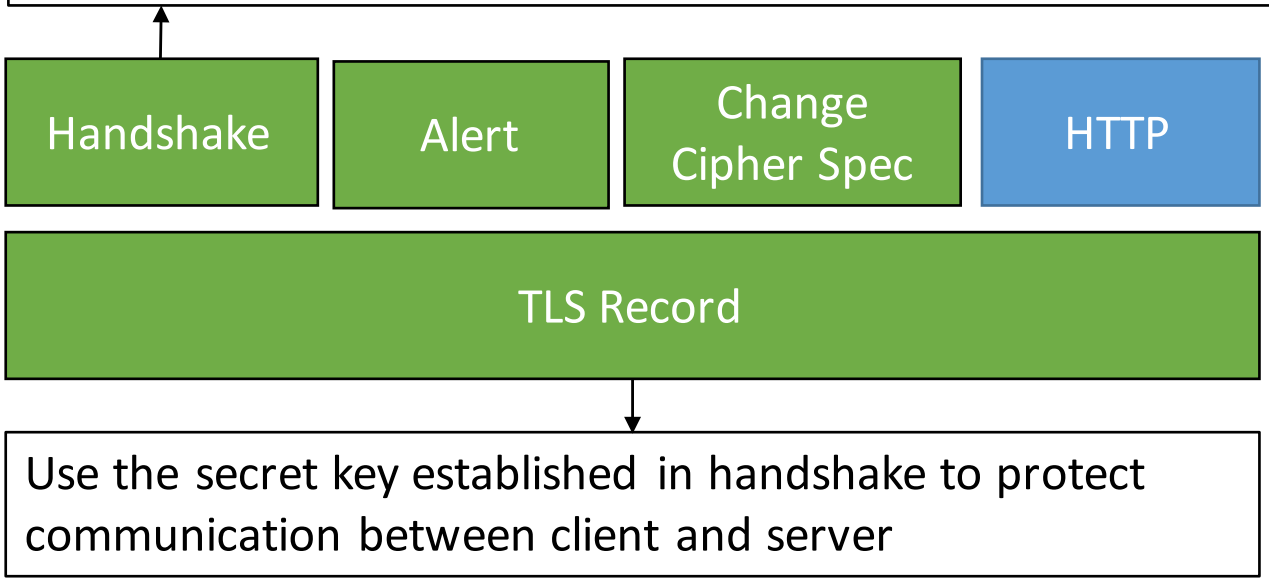


# TLS overview



# TLS overview

- **Negotiate** protocol version and cryptographic parameters
- Use **digital certificates to authenticate** server and client
- Use public-key cryptography to **establish a shared secret key** (a session key) between client and server



# Public Key Infrastructures (PKI)

A PKI = a secure system to manage **digital certificates**

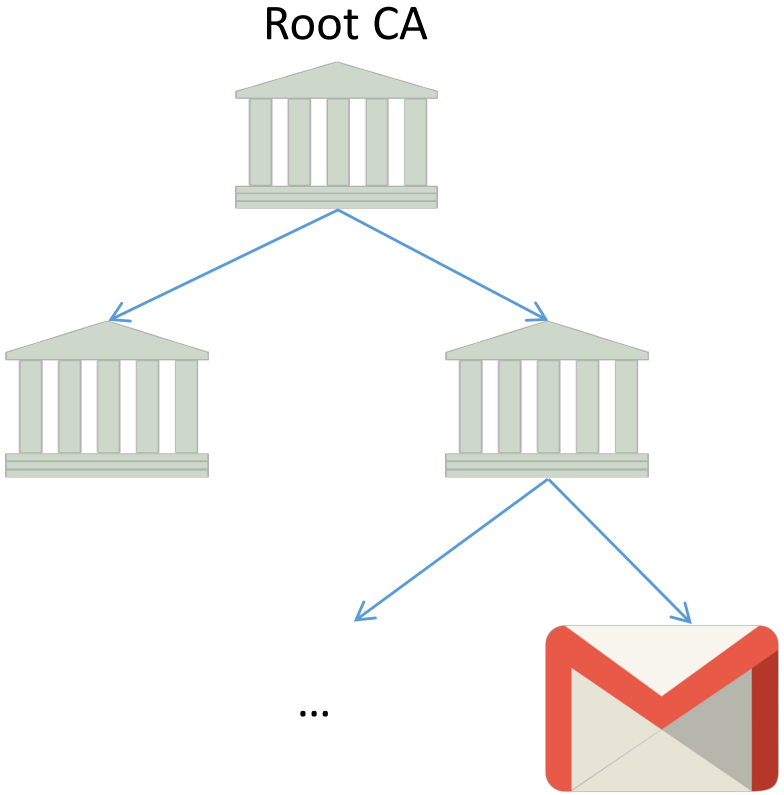
- Certificate issuance
- Certificate revocation

Many security protocols and applications rely on PKI: TLS, IPSec, S/MIME, DNSSEC, code signing…

X.509 is an ITU-T standard for a public key infrastructure (PKI)

# How it is done today: X.509 Public Key Infrastructure (PKI)

## A hierarchy of Certification Authorities




**GeoTrust Global CA**

Root certificate authority

Expires: Saturday, May 21, 2022 at 12:00:00 PM Taipei Standard Time

This certificate is valid

**Google Internet Authority G2**

Intermediate certificate authority

Expires: Sunday, January 1, 2017 at 7:59:59 AM Taipei Standard Time

This certificate is valid

**mail.google.com**

Issued by: Google Internet Authority G2

Expires: Tuesday, May 31, 2016 at 8:00:00 AM Taipei Standard Time

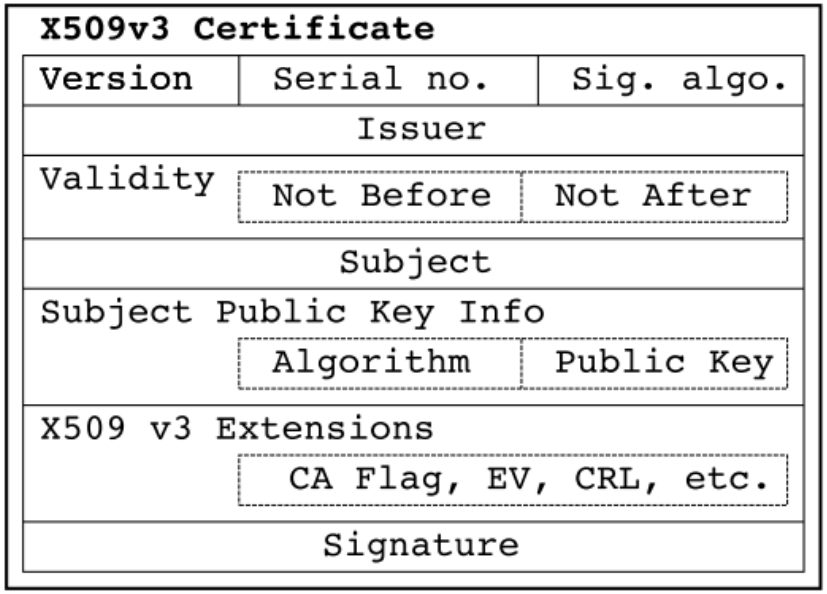
This certificate is valid

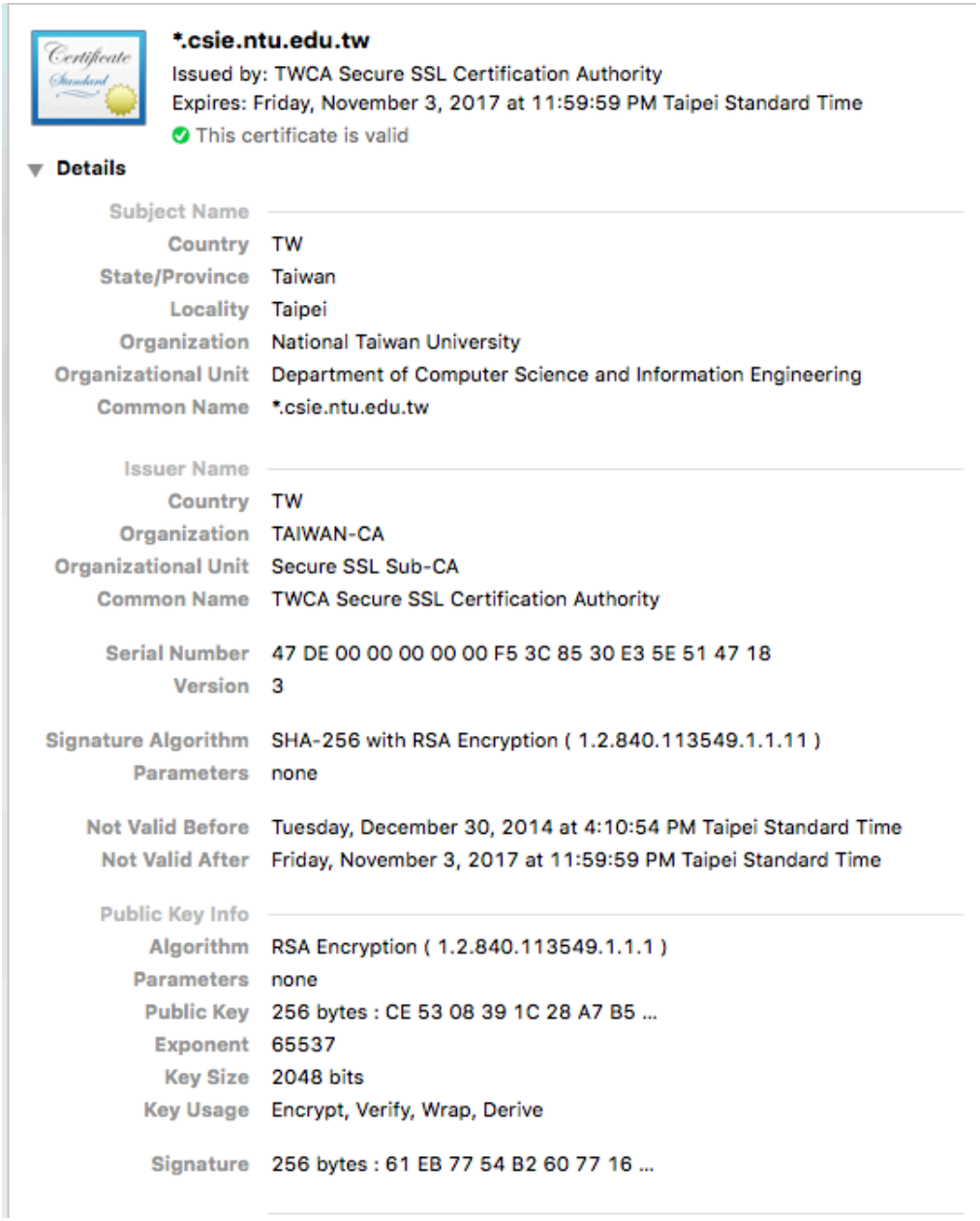
# How it is done today: X.509 Public Key Infrastructure (PKI)

**Root certificates**: All your trust relationships online are reduced to trusting this list of root certificates

| | |
|---|---|
| ePKI Root Certification Authority | certificate |
| Equifax Secure Certificate Authority | certificate |
| Equifax Secure eBusiness CA-1 | certificate |
| Equifax Secure eBusiness CA-2 | certificate |
| Equifax Secure Global eBusiness CA-1 | certificate |
| Federal Common Policy CA | certificate |
| GeoTrust Global CA | certificate |
| GeoTrust Primary Certification Authority | certificate |
| GeoTrust Primary Certification Authority - G2 | certificate |
| GeoTrust Primary Certification Authority - G3 | certificate |
| Global Chambersign Root | certificate |
| Global Chambersign Root - 2008 | certificate |
| GlobalSign | certificate |
| GlobalSign | certificate |
| GlobalSign | certificate |
| GlobalSign | certificate |
| GlobalSign Root CA | certificate |
| Go Daddy Class 2 Certification Authority | certificate |
| Go Daddy Root Certificate Authority - G2 | certificate |
| Government Root Certification Authority | certificate |

OS X Keychain

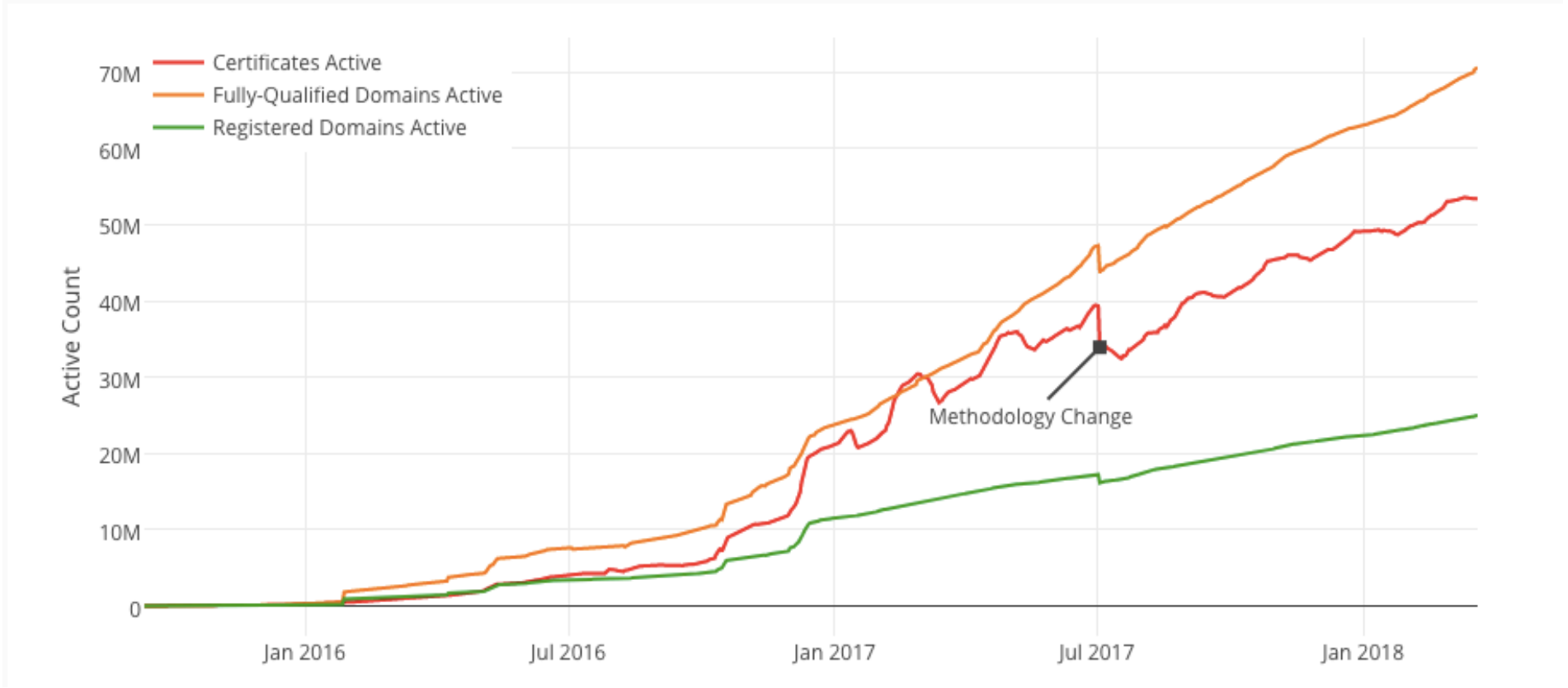



R. Holz, L. Braun, N. Kammenhuber, and G. Carle, "The SSL landscape: a thorough analysis of the x. 509 PKI using active and passive measurements," in *Proceedings of ACM IMC*, 2011.

# Let’s Encrypt

More than 50 Million Websites Install Free Certificate (and Counting...)



# TLS 1.3

Simplicity, ”fewer, better choices"

No weak crypto

- No RC4, MD5, 3DES

Fewer choices

- No AES-CBC
- No arbitrary DH groups, curves

1-RTT, 0-RTT

https://tools.ietf.org/html/draft-ietf-tls-tls13-28

# 分組討論時間

zuvio

# Exercise

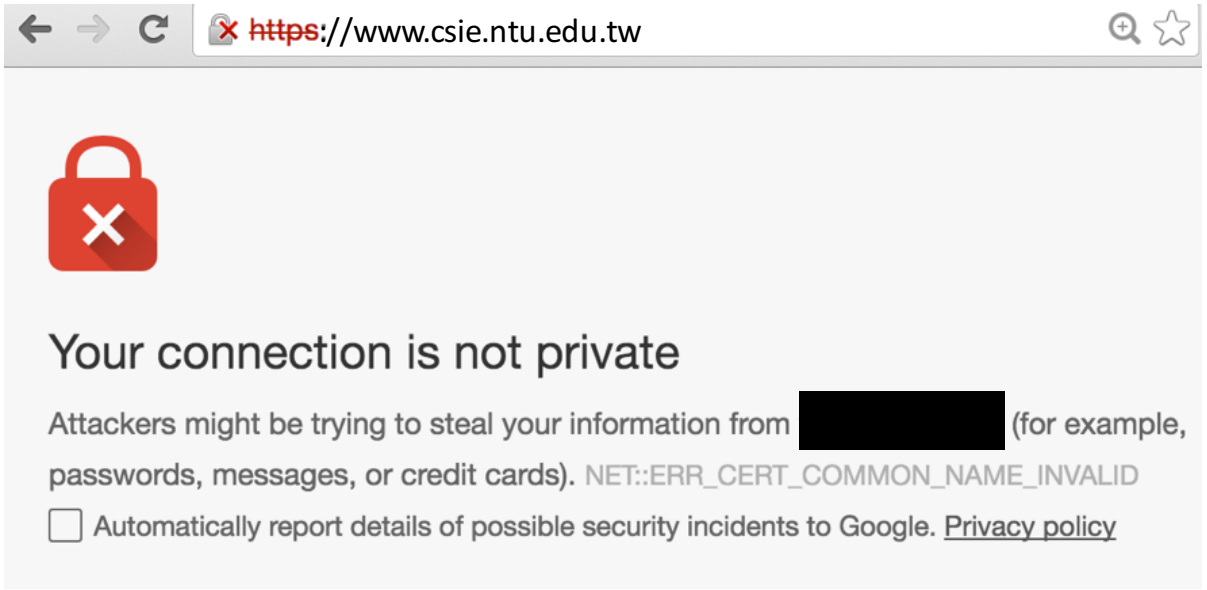
選擇一個NASA服務，討論其效能（如運算、儲存、頻寬）瓶頸

請估計此服務被癱瘓的的難易度（e.g.,需要同時多少人上線）

zuvio

# Exercise: 假設情境題

要如何協助遭遇以下錯誤訊息的系上同學？



zuvio

# Exercise: 假設情境題

計中發現NTU的帳號密碼似乎有部分外洩了！NASA團隊能提供什麼建議給系上同學，以提升csie account的安全性？

未來如何及早發現帳號外洩事件？

zuvio

# Exercise: 假設情境題

要如何偵測惡意/假冒的AP？