BGP and DNS Security

CSIE 7190 Cryptography and Network Security, Spring 2019

https://ceiba.ntu.edu.tw/1072csie_cns

cns@csie.ntu.edu.tw

Hsu-Chun Hsiao

Housekeeping

5/07: Project proposal due

4/30: Reading critique #8 due

HW2 will be released this week

Reading critique #8

Write a critique on one of the following:

- A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in NDSS, 1999.
- A. Yaar, A. Perrig, and D. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks," in IEEE S&P, 2004.

Text only, one page

Outline

Review of HW1 and midterm

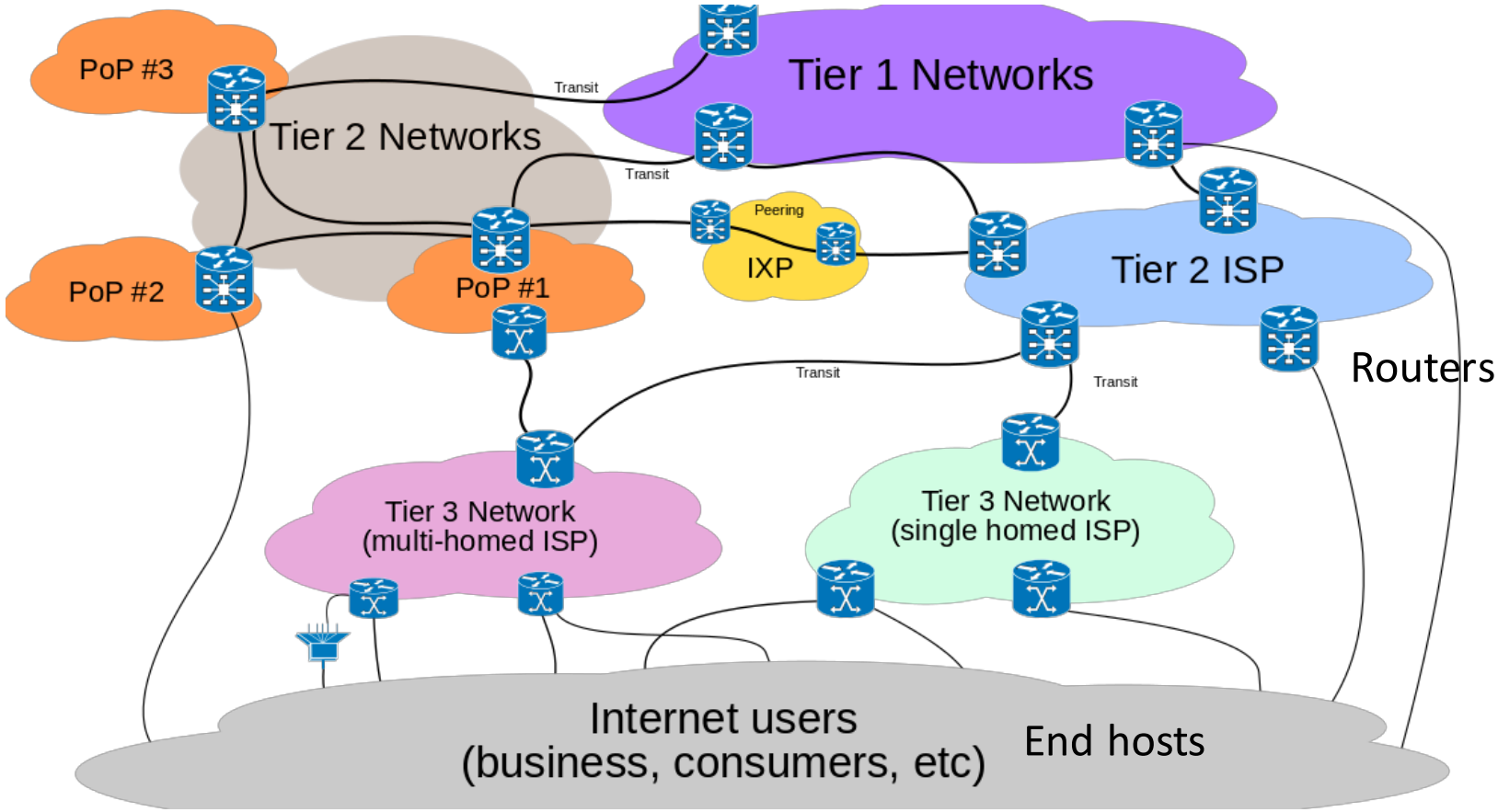
Project information

BGP security

DNS security

Border Gateway Protocol (BGP)

Internet = Interconnected Networks



例如：台大、中華電信
每個國家有自己的法律

http://en.wikipedia.org/wiki/Tier_1_network

Autonomous System

The Internet comprises of *Autonomous Systems (AS)*

AS = A network under the administrative control of a single organization, under the same intra-domain routing policy

- Campus networks
- Corporate networks
- Internet Service Provider (ISPs)

Autonomous System Numbers (ASN)

- AS17716 NTU-TW National Taiwan University, TW
- AS36039 GOOGLE - Google Inc., US
- AS17714 CHTI-DC Chunghwa Telecom Co. , Ltd., TW

http://www.cidr-report.org/as2.0/autnums.html

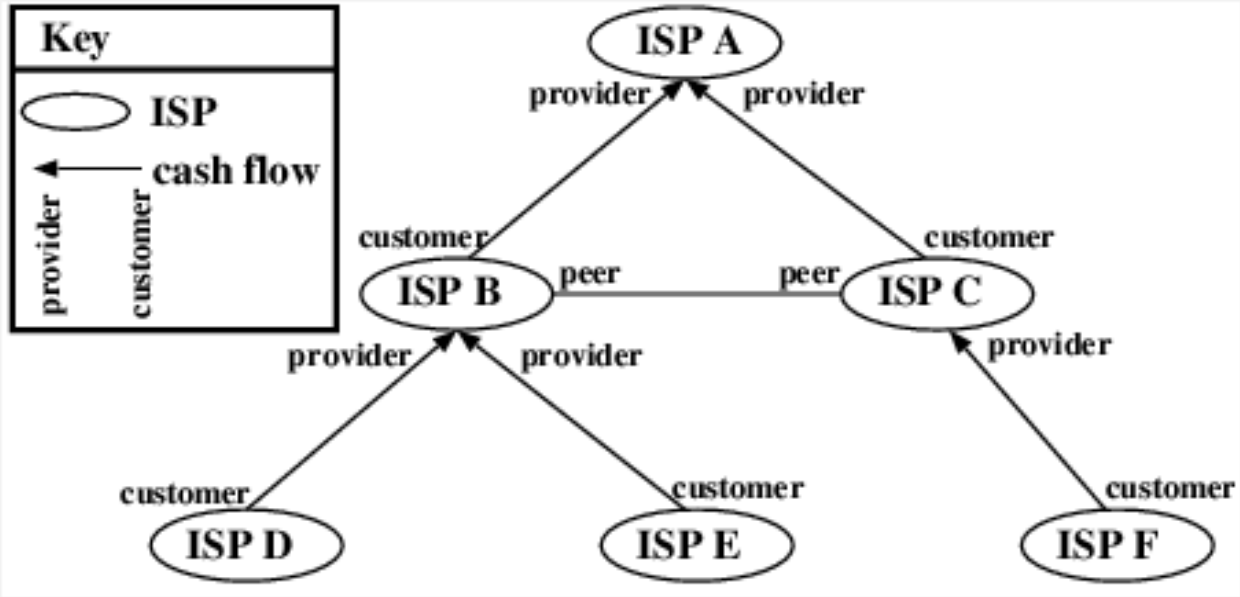
Business relationships，e.g. 中華電信可能要付錢給 AT&T

AS Relationships

A *provider* AS sells transit to a *customer* AS

A *customer* AS pays a *provider* AS to access the rest of the Internet

Peering ASes exchange each other's traffic for free



http://www.caida.org/data/as-relationships/

臺灣學術網路(TANet)與ISP互連現況

國內連線頻寬資料

互連單位 英文簡名	互連單位 中文簡名	AS NUMBER	頻寬種類	數量(條)	總頻寬 (MBPS)
ASNeT	中研院	9264	10G	3	30000
ASNeT	中央研究院	9264	1G	2	2000
CNS-KBT	中嘉和網	9416	Other	1	11000
EBIX	亞太交換中心	17709	Other	1	3500
GSN	政府網際服務網	4782	FasteThernet	3	300
HINeT	中華電信	3462	1G	34	34000
NCIC	速博	9919	1G	13	13000
NCIC	速博	9919	FasteThernet	4	400
NCIC	速博	9919	T3	1	44.736
NCREE	國家地震中心	18183	GigaEthernet	1	1000
NHRINeT	國家衛生研究院	18181	1G	1	1000
SO-net	台灣碩網	18182	Other	1	7000
TFN	台灣固網	9924	Other	1	5710
TWAREN	國家高速電腦中心	7539	10G	4	40000
TWGate	中華電信(轉國際)	9505	10G	1	5000

摘要：臺灣學術網路(TANet)與ISP互連現況

上版日期：101-10-07

https://depart.moe.edu.tw/ed2700/News_Content.aspx?n=697CD84F427DE922&sms=954B3E2521E9F948&s=26999226FE73A691

Internet Address Space Ownership

還是會有一個 centralize 的 organization

Internet Assigned Number Authority (IANA) allocates IP addresses and AS numbers to ASes

Addresses are assigned hierarchically

- IANA -> RIR -> … -> end host

highest in the hierarchy

Addresses are assigned in blocks of contiguous addresses (IP prefixes)

- e.g., NTU has 140.112.0.0/16

學校 IP 的第一組數字以 140 開頭為主，原因是 140.92、140.109 至 140.138 為臺灣學術網路 TANet 的網段。而 IP 的第二組數字開始，各學校的代碼如下：

https://www.iana.org/numbers

Internet Address Space Ownership

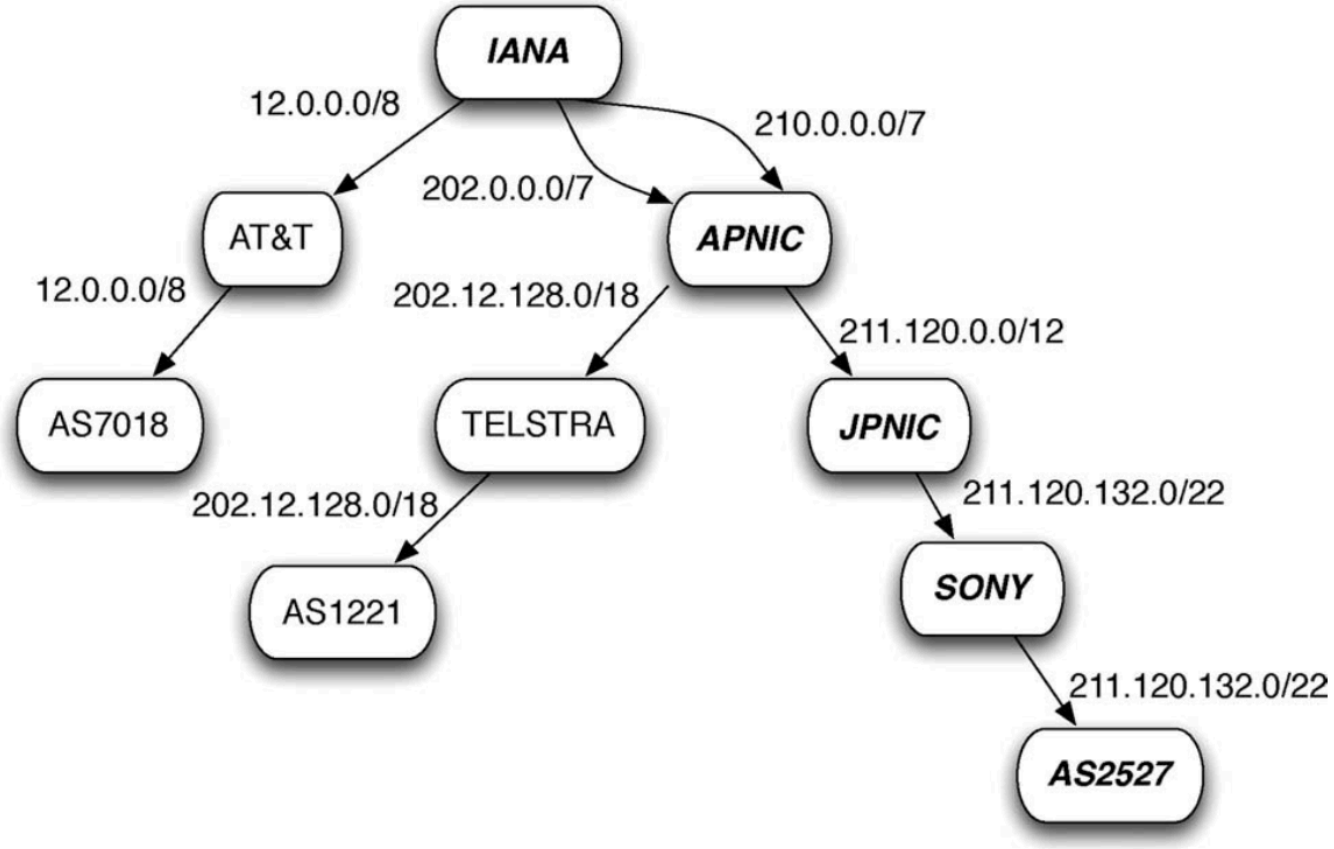
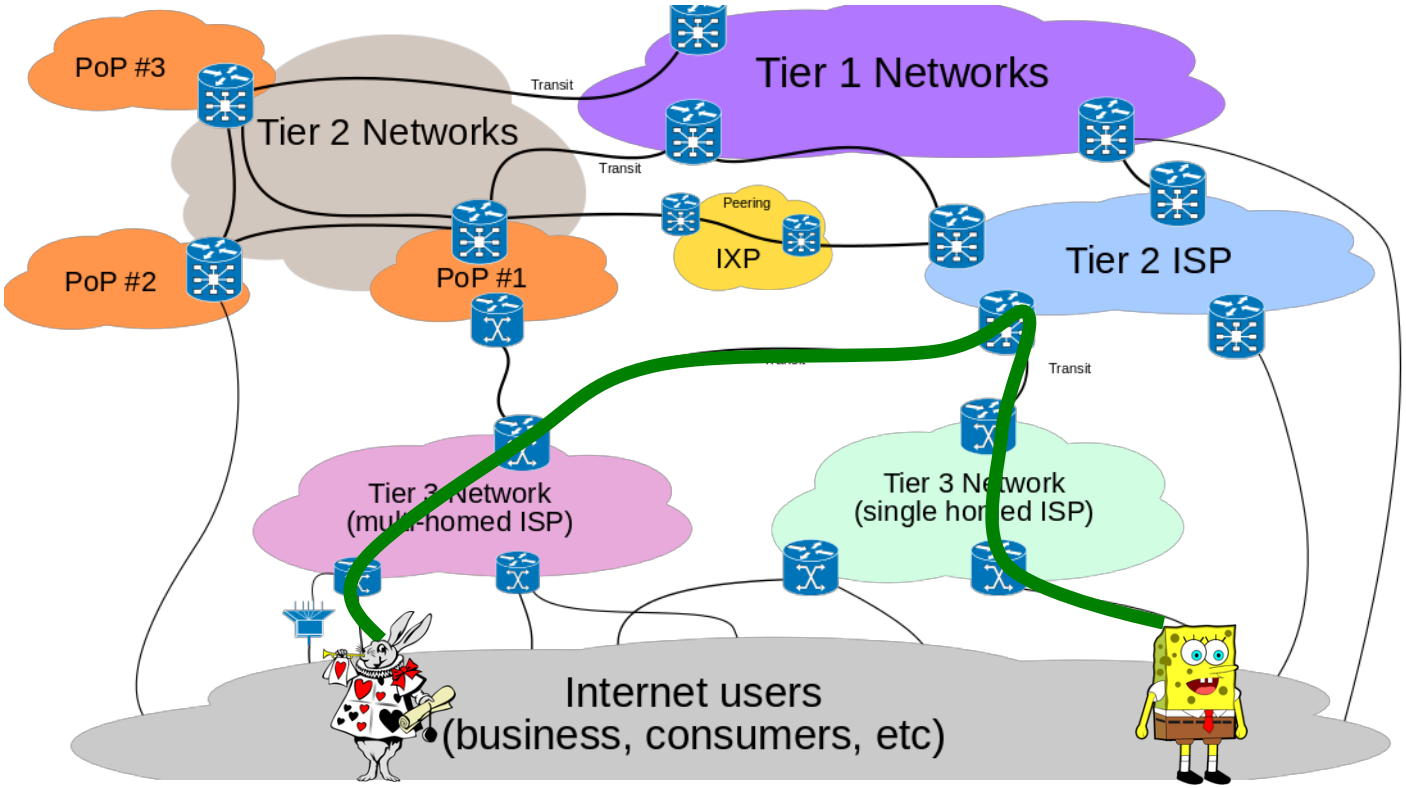


Fig. 1. ***An example of address delegation from the root (IANA) to regional and national registries.***

Routing

Routing = the process of exchanging reachability information and performing path selection



140.112.8.116

216.58.200.238

Intra-/Inter-domain Routing

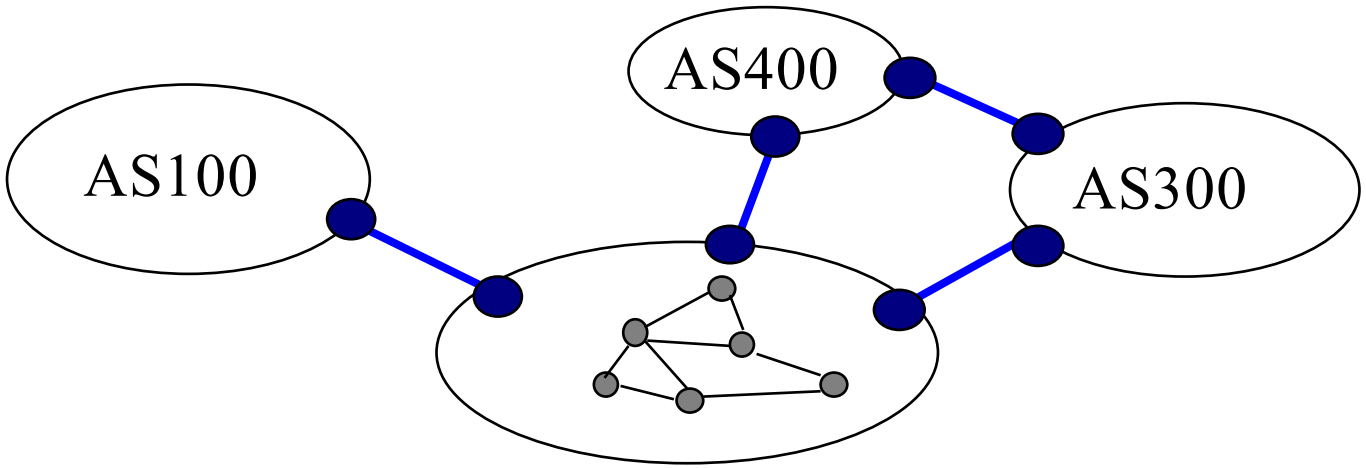
Routing hierarchy

- Intra-domain routing: routing within an AS e.g. 國家內部的郵件系統
- Inter-domain routing: routing between ASes

Analogy of mail delivery hierarchy: intra-country, inter-country e.g. 從美國寄信到台灣，我只要 TAIWAN 寫英文就好

ASes can run *different* intra-domain routing protocols

But all ASes need to use the *same* inter-domain routing protocol to interconnect!



Border Gateway Protocol (BGP)

BGP is ***the*** inter-domain routing

BGP is a path-vector routing protocol

跟路徑有關的資訊

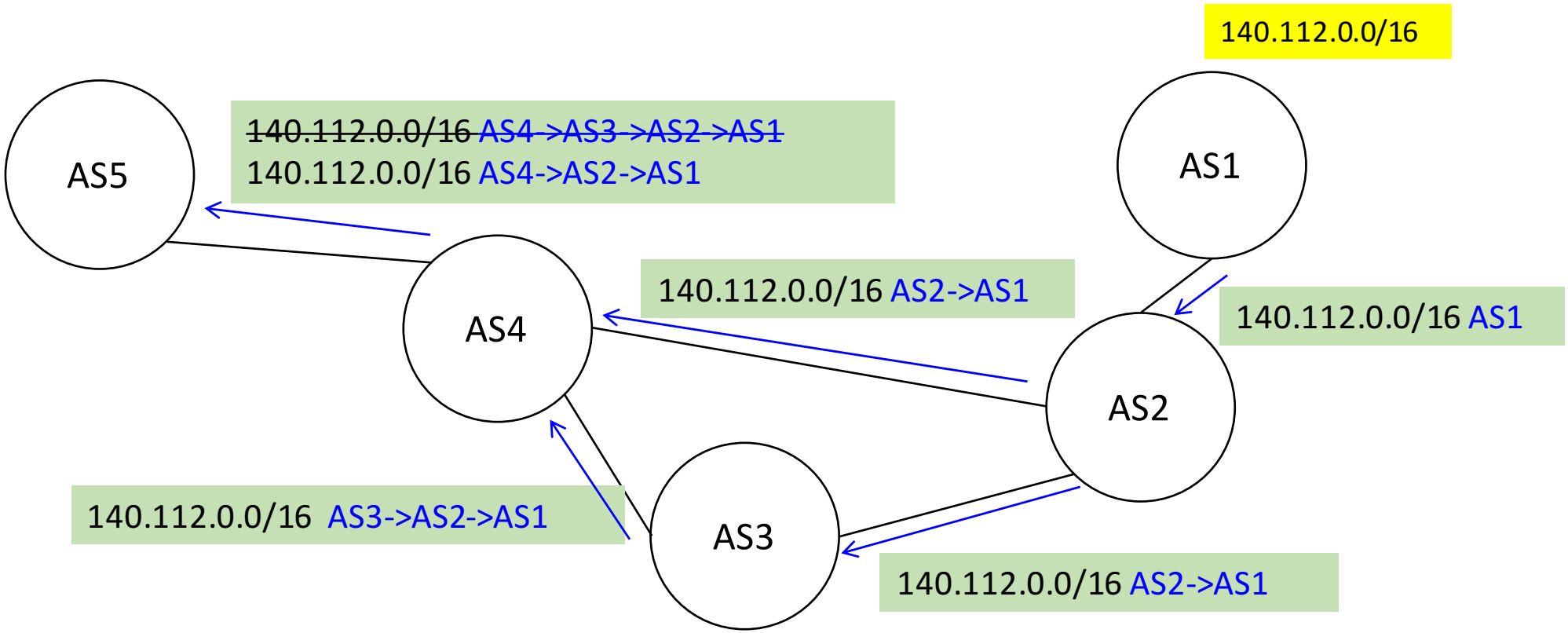
e.g. 可能有某一條路徑較便宜，而不是無腦的看長度

- Path-vector routing keeps path info and update it dynamically and thus can support diverse routing policies.
  - Can avoid certain unwanted ASes on the route
  - Can flexibly prioritize routes (instead of using a universal criterion like path length)
- Why path-vector routing?
  - Recall that ASes may be administrated by different organizations, and ASes connect to each other based on *contractual* relationships

A BGP route is identified by an *AS Path*

- AS Path is a set of ASNs: 9, 5050, 11537, 2153

BGP Advertisement



BGP Advertisement

p.15 頁的 AS1

A **destination AS** advertises its prefix blocks to neighbors

An **intermediate AS** can decide whether and where to propagate the advertisement by checking AS_PATH

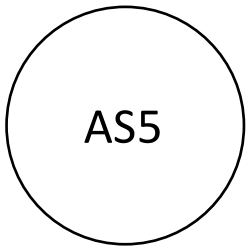
- The intermediate AS adds its ASN to AS_PATH in the propagated advertisement.
- Loops can be detected easily.
- By propagating the advertisement from AS X to AS Y, the intermediate AS implicitly agrees to forward traffic from AS Y to AS X.

Routing Policies

A BGP router selects a preferred route for **each destination prefix** based on route attributes

Route attributes (from the highest priority to lowest)

- Local preference
  - E.g., assign high value to paying customers
- AS path length
  - Can use *AS prepending* to make a route less attractive
- Origin type
- Multi-Exit Discriminator (MED)

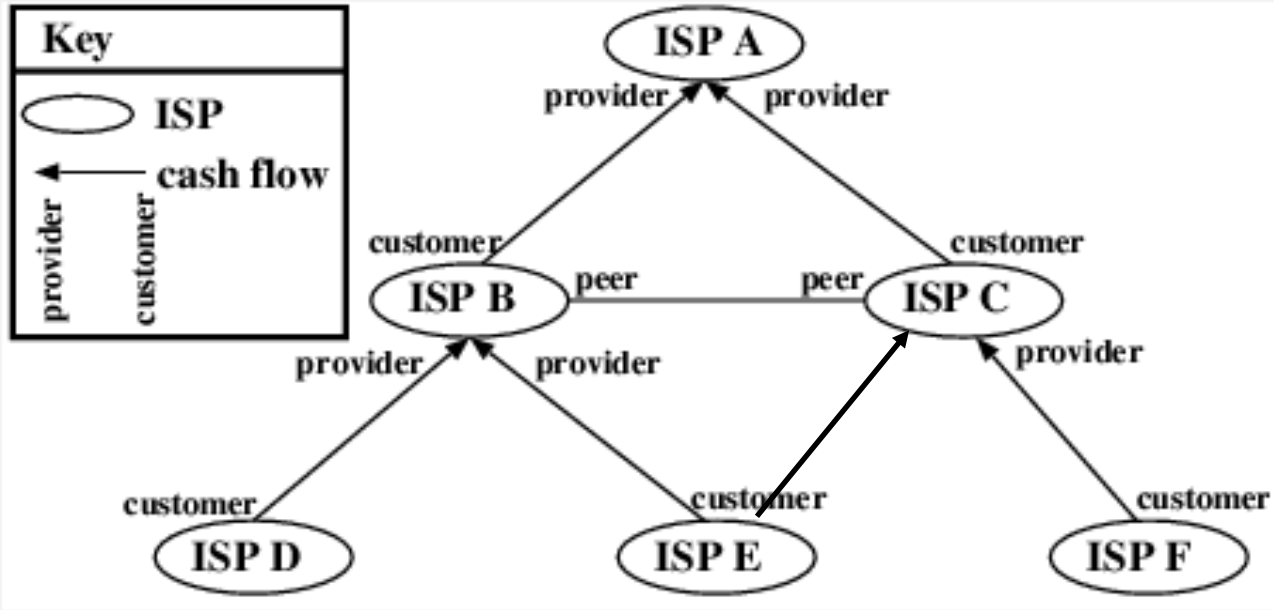


~~140.112.0.0/16 AS4 ->AS3 ->AS2 ->AS1~~
140.112.0.0/16 AS4->AS2->AS1

Routing Policies

Rule of thumb B 和 C 要傳訊息，E 沒理由還幫 B 送訊息

- Valley-free (e.g., E will not forward traffic between B and C)
- Prefer customer, then prefer peer

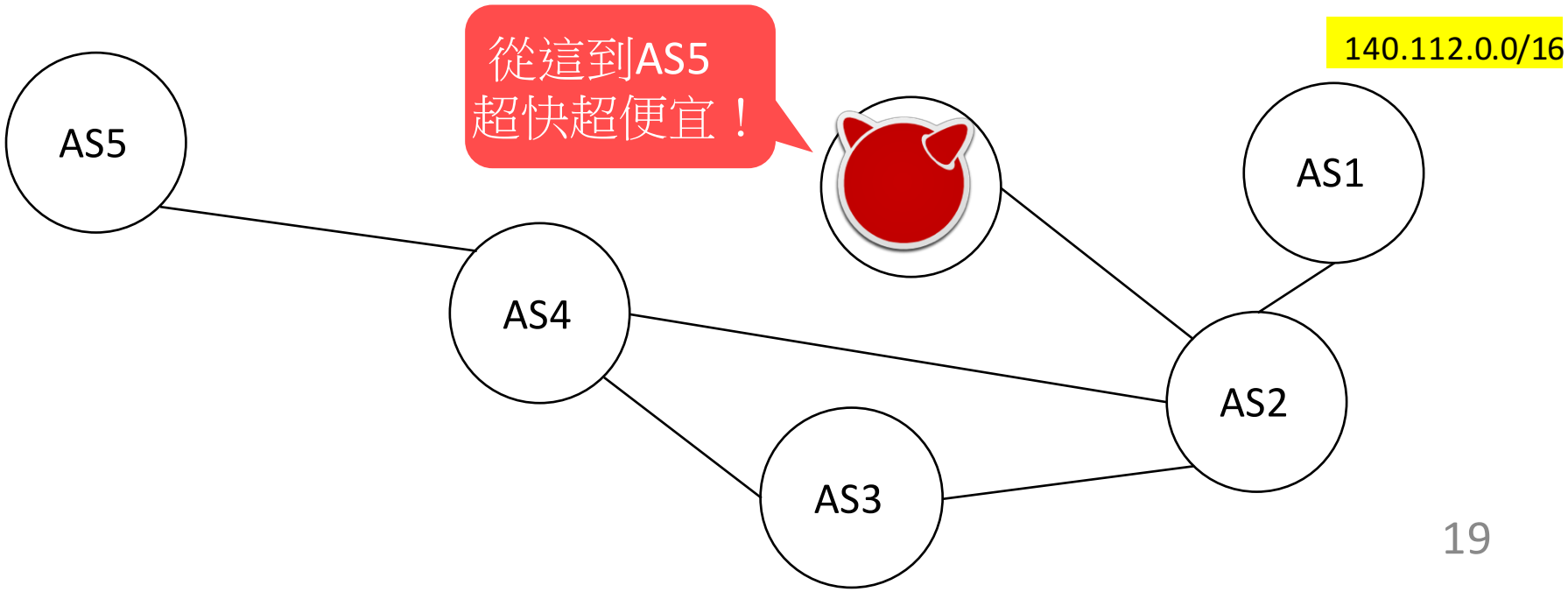


BGP Security Issues

BGP was designed for a trusted environment

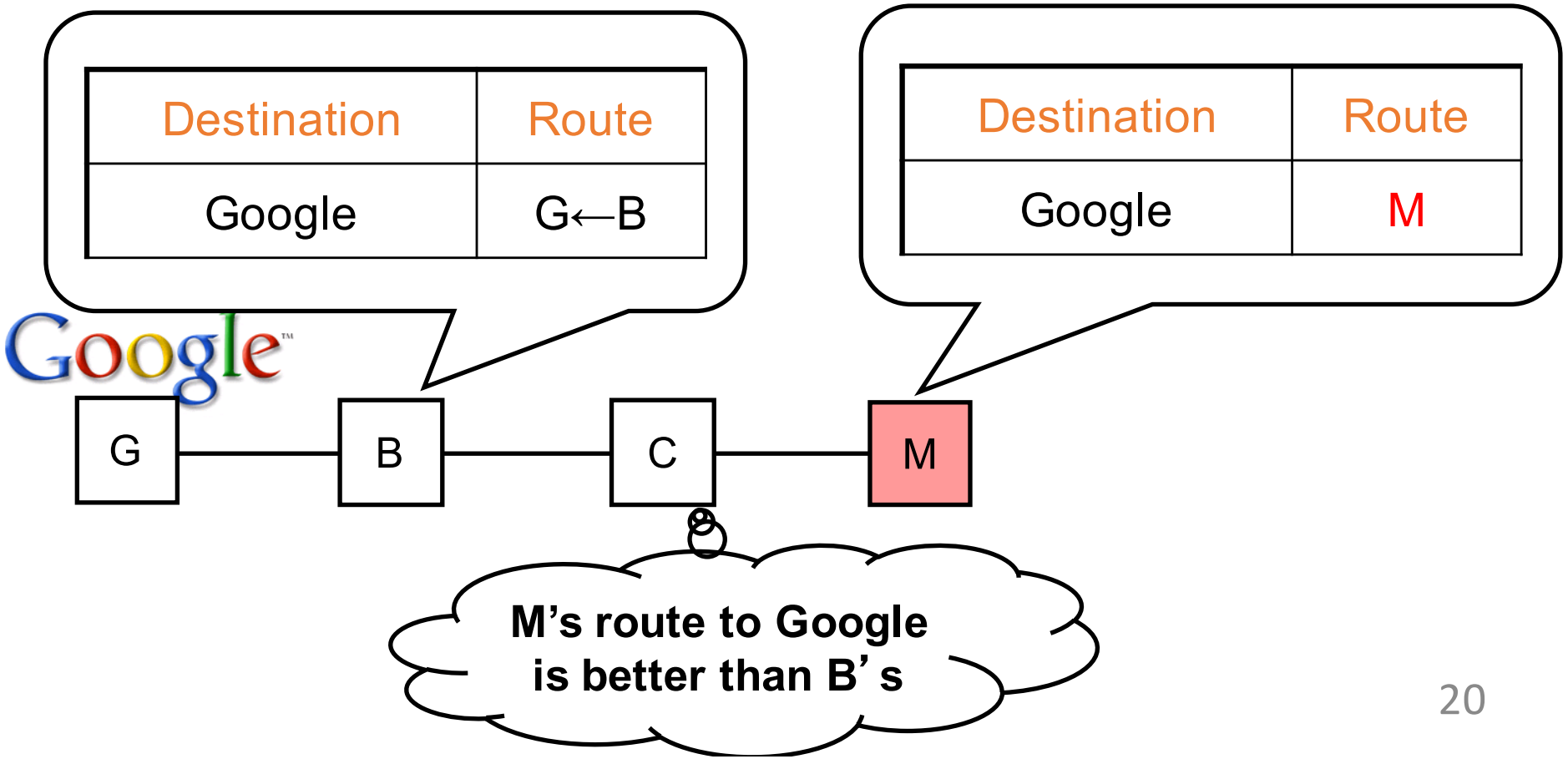
BGP advertisements are not authenticated!

- The attacker can announce arbitrary prefixes
- The attacker can manipulate others' BGP advertisements



Possible Attacks: Prefix Hijacking

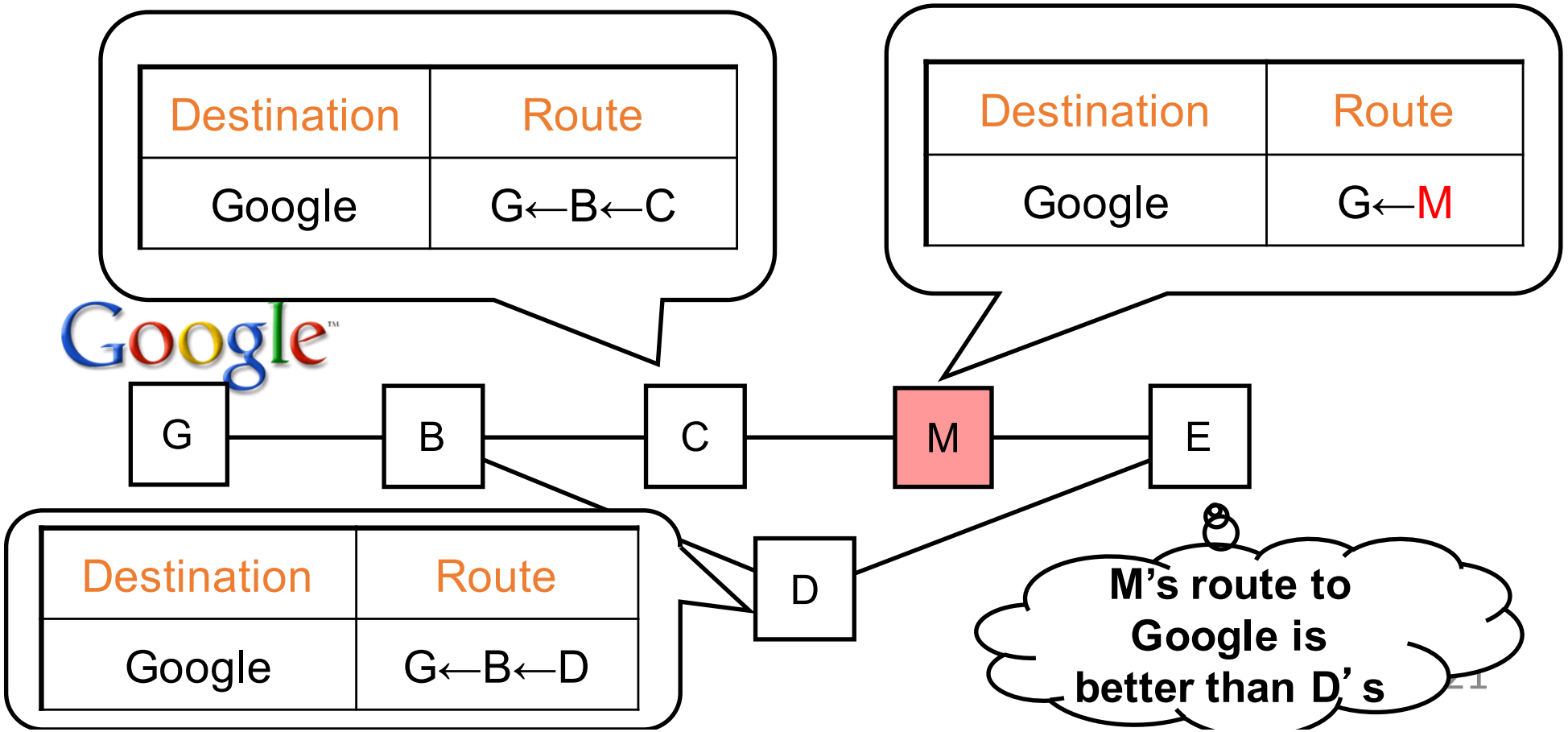
Unauthorized origin ISP (prefix hijacking)



Possible Attacks: Path Truncation

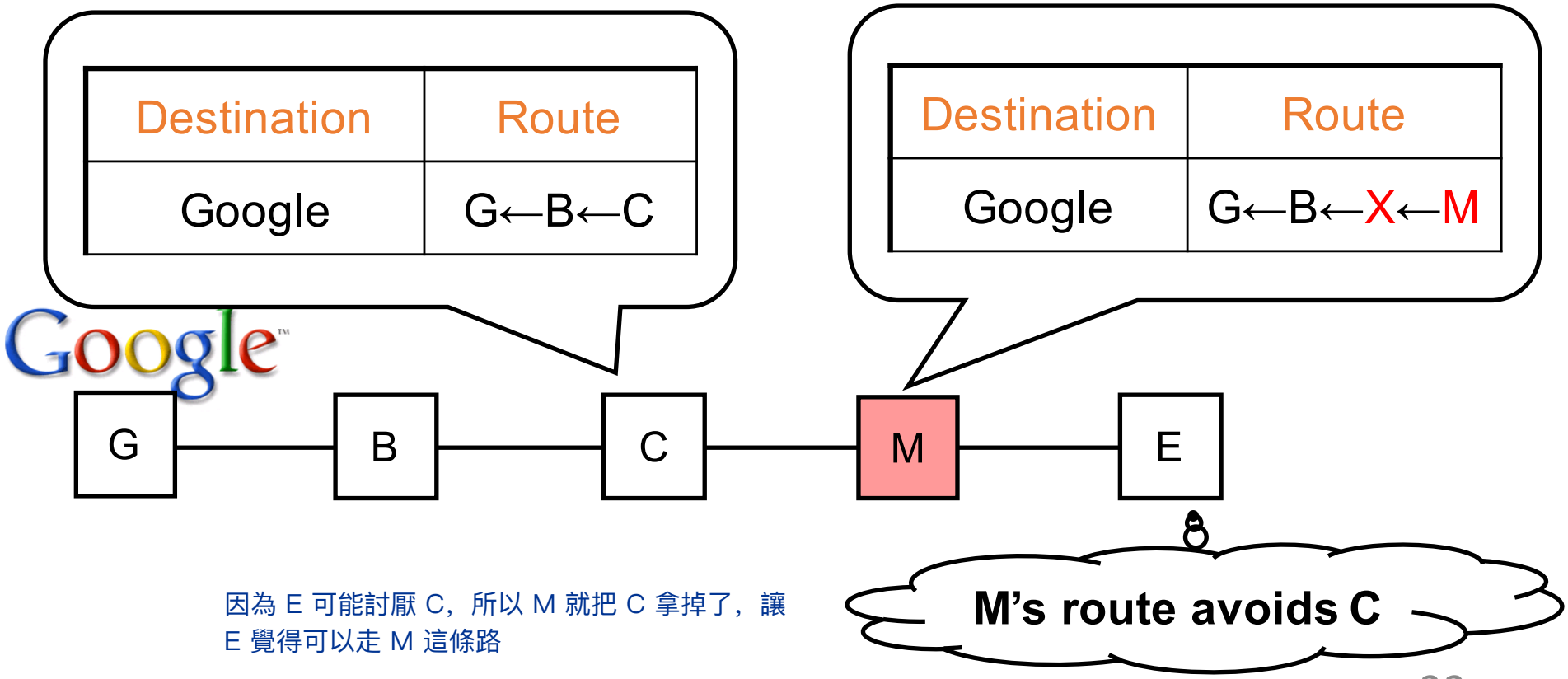
AS path truncation

M 收到 C 的 G<-B<-C 後，本應該傳 G<-B<-C<-M 給大家，但卻把 B、C routes 丟掉，改成 G<-M，導致 E 看到時，誤以為從 M 會比從 D（G<-B<-D）還要快到 G



Possible Attacks: Path Alteration

AS path alteration



因為 E 可能討厭 C，所以 M 就把 C 拿掉了，讓 E 覺得可以走 M 這條路

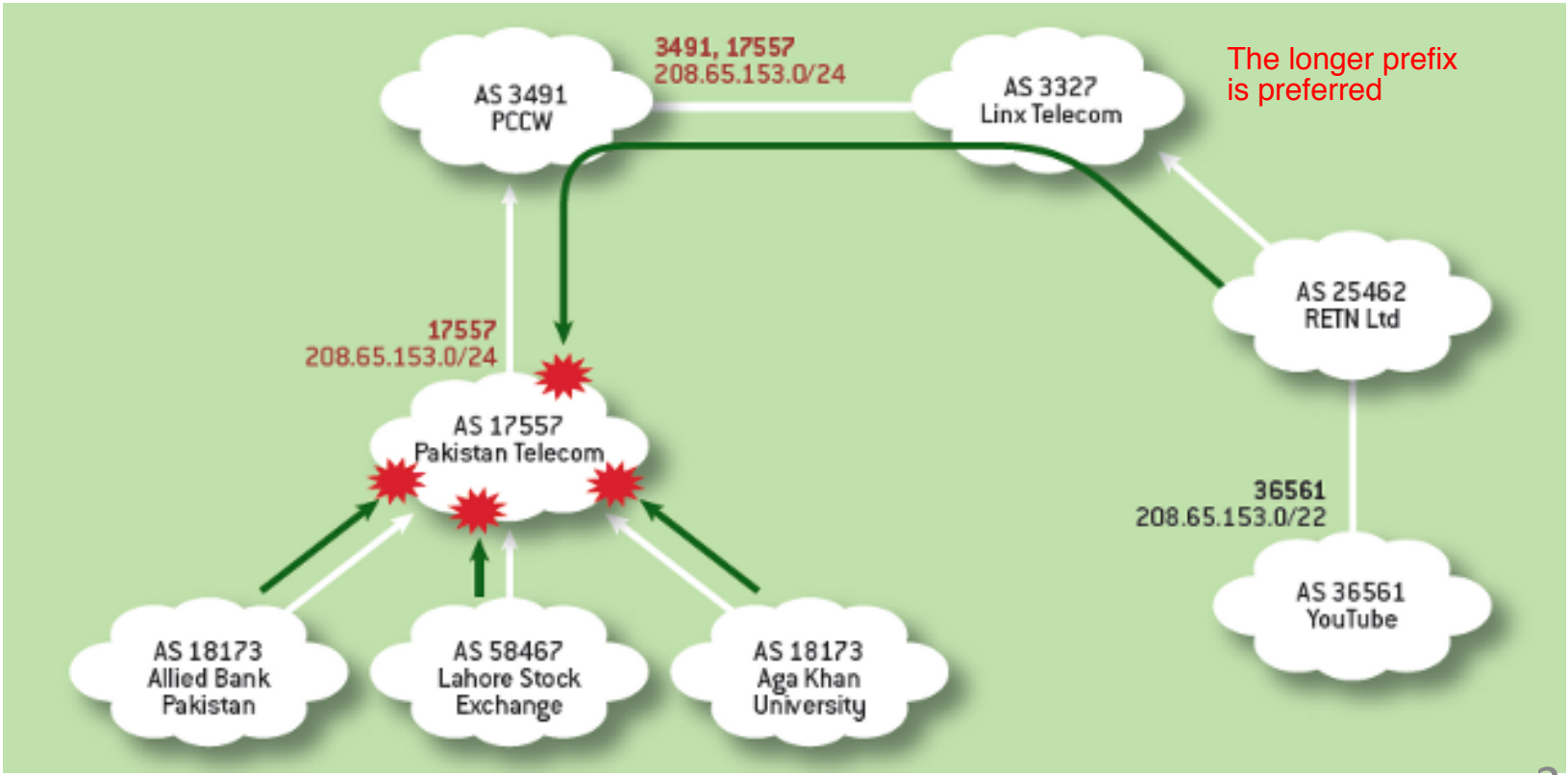
Pakistan Telecom Hijacked YouTube

SHARON GOLDBERG, BOSTON UNIVERSITY. Routing security incidents can still slip past deployed security defenses. http://queue.acm.org/detail.cfm?id=2668966

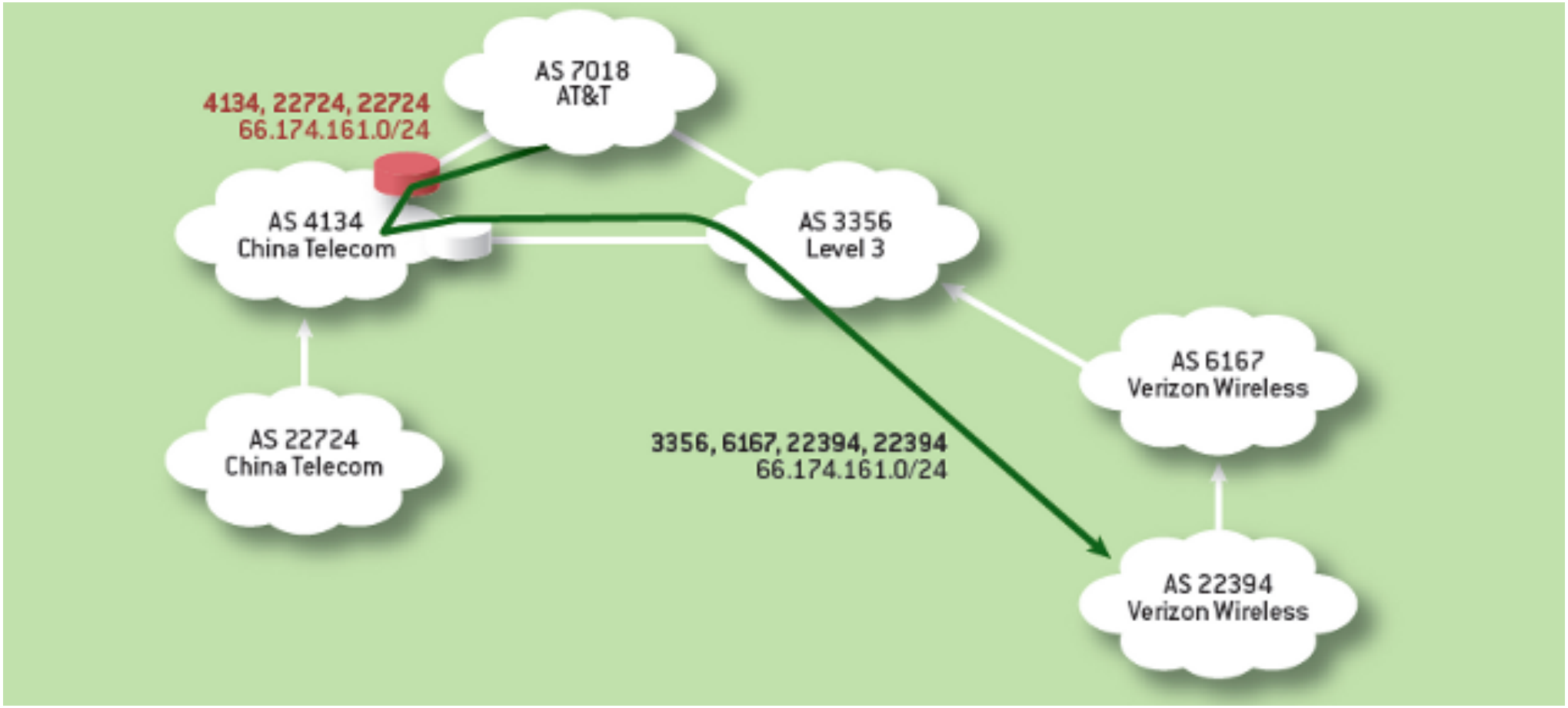
Pakistan Telecom Hijacked YouTube

Route selection always matches the longest prefix.

The attacker announced a longer prefix to make the route more attractive.



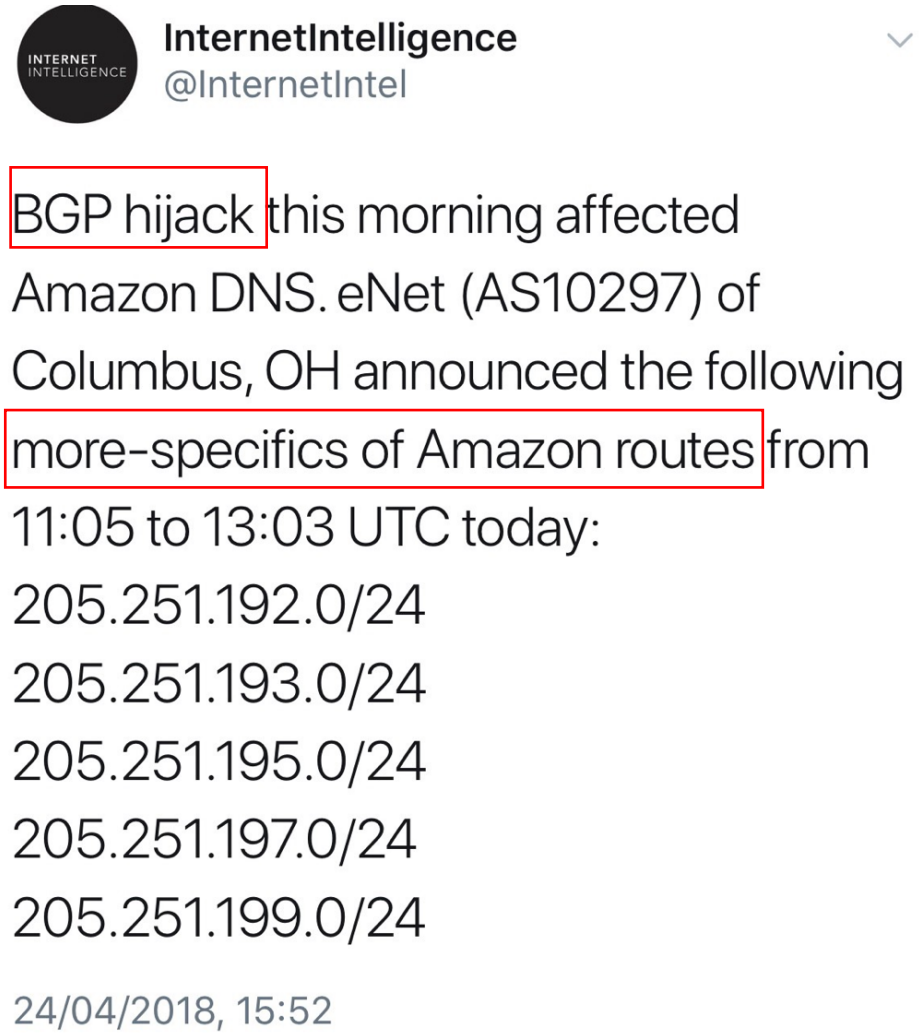
China Telecom Intercepted Verizon Wireless



SHARON GOLDBERG, BOSTON UNIVERSITY. Routing security incidents can still slip past deployed security defenses. http://queue.acm.org/detail.cfm?id=2668966

Hijack of Amazon's internet domain service used to reroute web traffic for two hours unnoticed

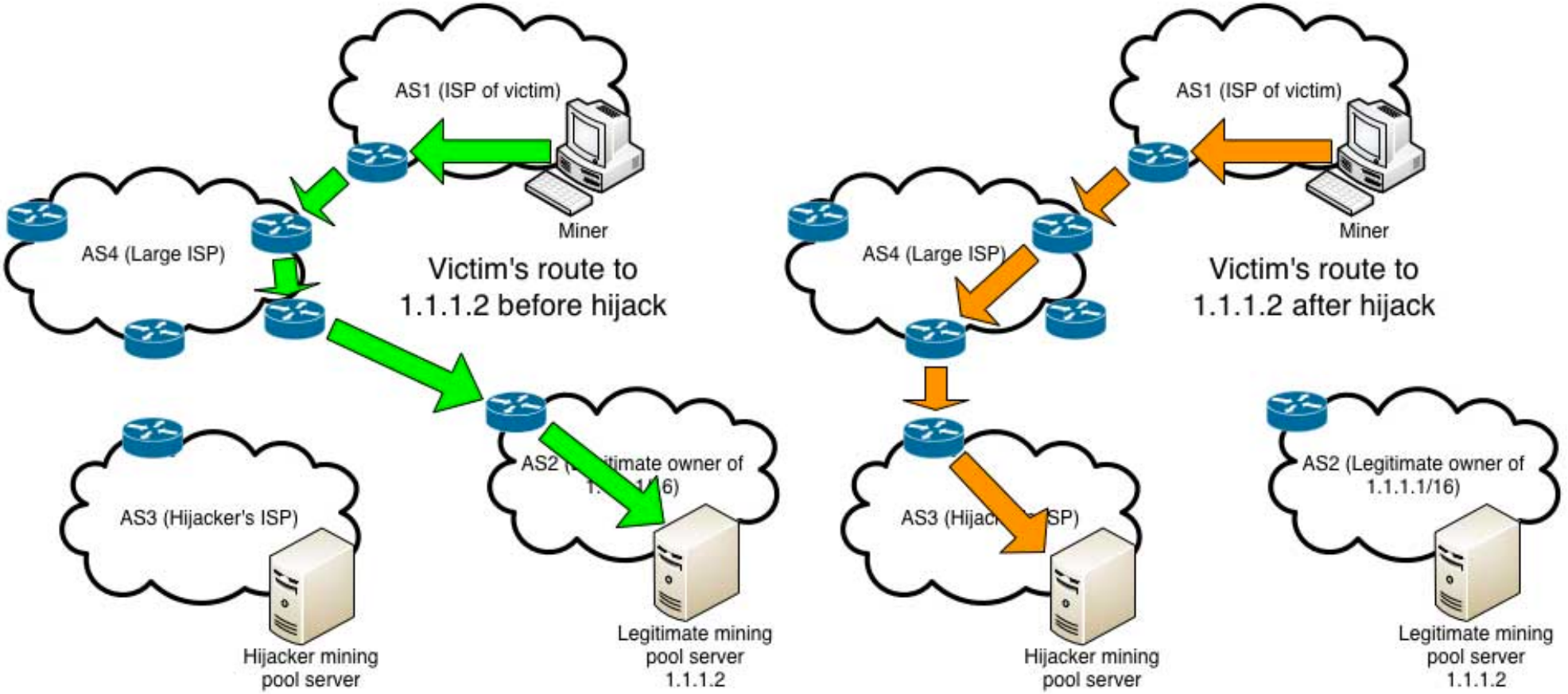
Traffic to MyEtherWallet.com was redirected to a server hosted in Russia



https://doublepulsar.com/hijack-of-amazons-internet-domain-service-used-to-reroute-web-traffic-for-two-hours-unnoticed-3a6f0dda6a6f

BGP Hijacks on Cryptocurrencies

between February and May 2014



https://www.secureworks.com/research/bgp-hijacking-for-cryptocurrency-profit

BGP Hijacks on Cryptocurrencies

Isolation

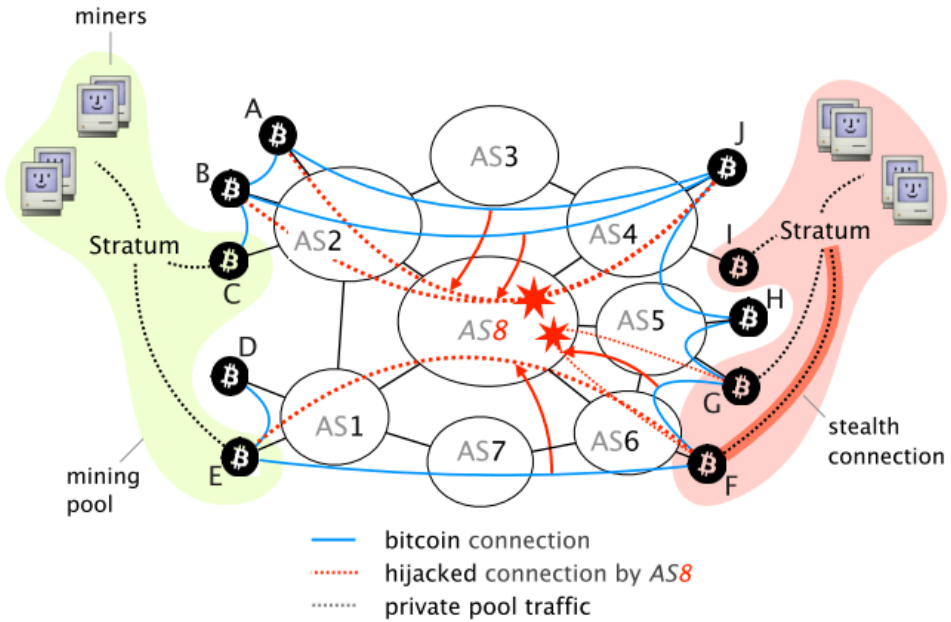


Fig. 1: Illustration of how an AS-level adversary (AS8) can intercept Bitcoin traffic by hijacking prefixes to isolate the set of nodes $P = (A, B, C, D, E, F)$.

Delay block propagation

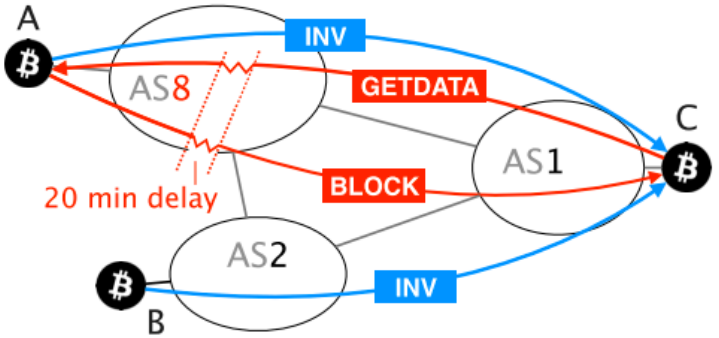


Fig. 2: Illustration of how an AS-level adversary (AS8) which naturally intercepts a part of the traffic can delay the delivery of a block for 20 minutes to a victim node (C).

M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," in *IEEE Symposium on Security and Privacy*, 2017.

Securing BGP

S-BGP: consisting of three security mechanisms

- Public Key Infrastructure (PKI)
- Attestations
  - Address attestation
  - Route attestation
- IPsec IP Security

Resource Public Key Infrastructure (RPKI) S-BGP 的其中一部分

- Only the PKI part of S-BGP
- Route Origination Authorizations
- 只保護origin，沒有保護路徑

做比較少，但比較容易 deploy

http://www.ir.bbn.com/sbgp/
https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure

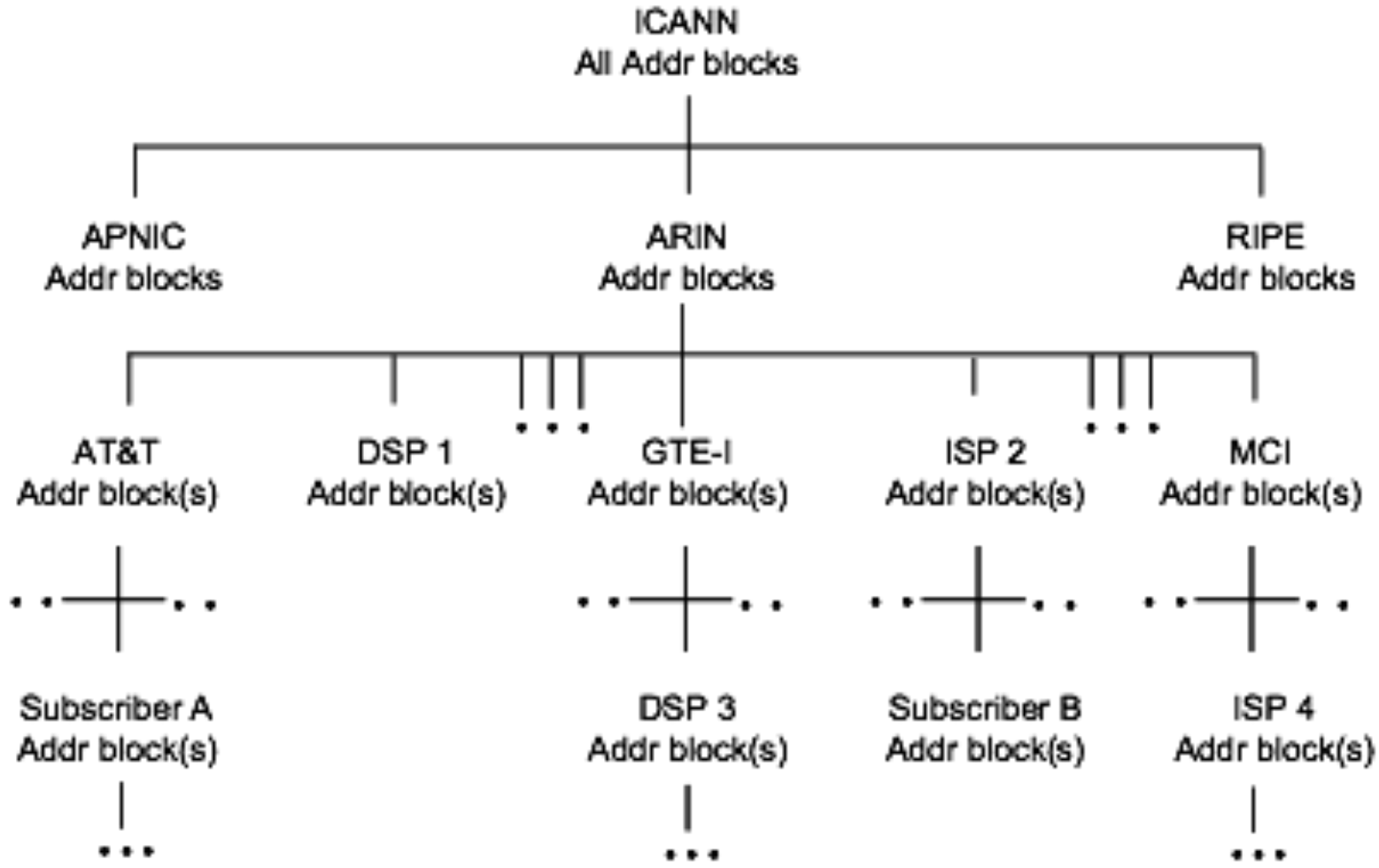
Certificates and Address Attestations

Public Key Infrastructure (PKI)

- “Support the authentication of ownership of IP address blocks, ownership of Autonomous System (AS) numbers, an AS's identity, and a BGP router's identity and its authorization to represent an AS”

ICANN issues certificates for address space ownership to regional authorities and to entities that have direct address allocations (from IANA).

Simplified PKI for Address Blocks



Certificates and Route Attestations

ICANN issues certificates for AS ownership to ISPs and organizations that run BGP

AS operators issue certificates to routers, as AS representatives

Holders of AS (or router) certificates generate route attestations, authorizing advertisement of a route by a specified next hop AS

Route attestations are used to express a secure route as a sequence of AS hops

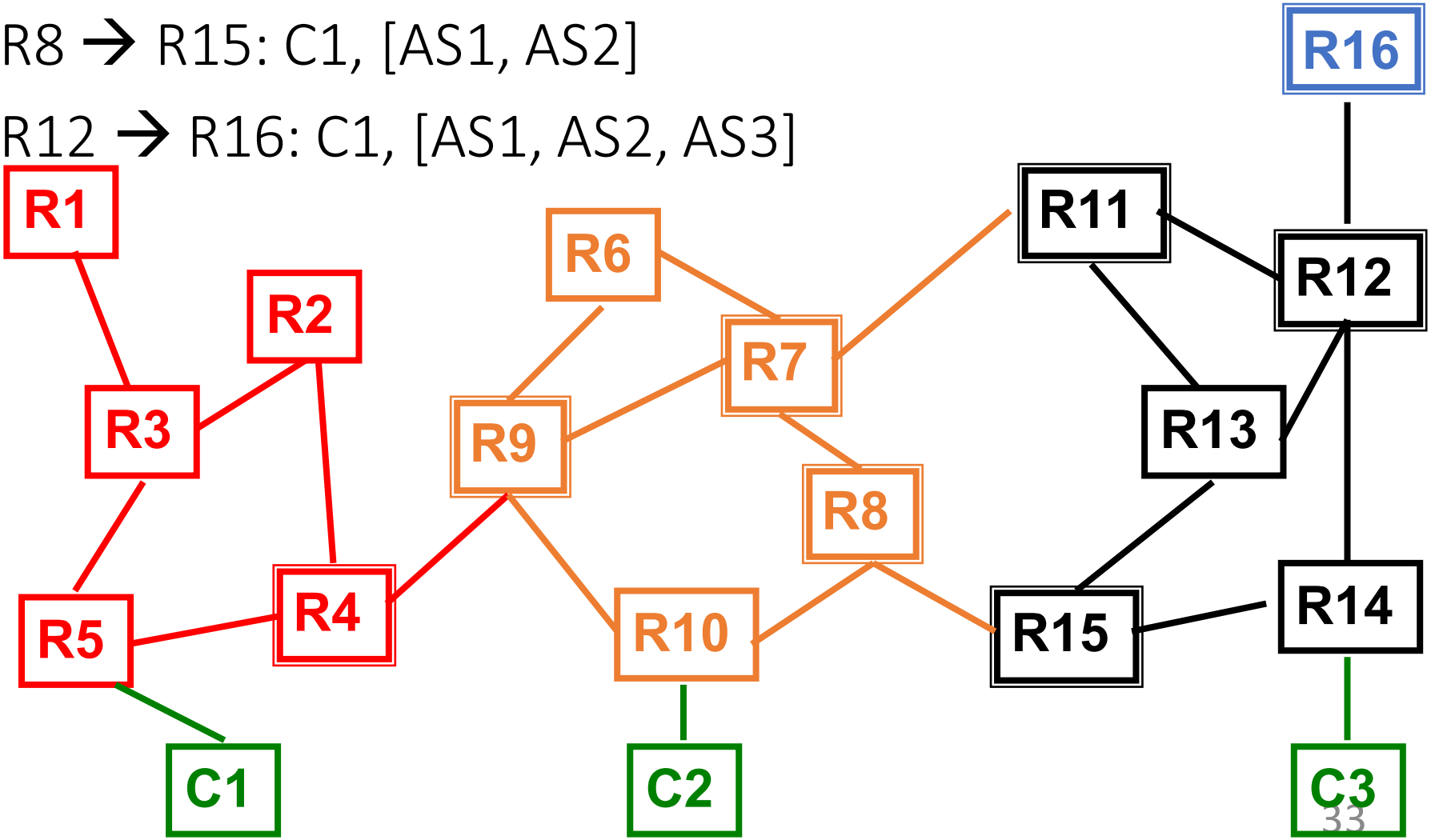
Sample BGP Update Messages

R4 → R9: C1, [AS1]

R7 → R11: C1, [AS1, AS2]

R8 → R15: C1, [AS1, AS2]

R12 → R16: C1, [AS1, AS2, AS3]



Secure BGP Update Message

address attestation

AS1: $Sign(sk_{c1}, \{C1, AS1\})$

AS1 之間的所有 router，intra

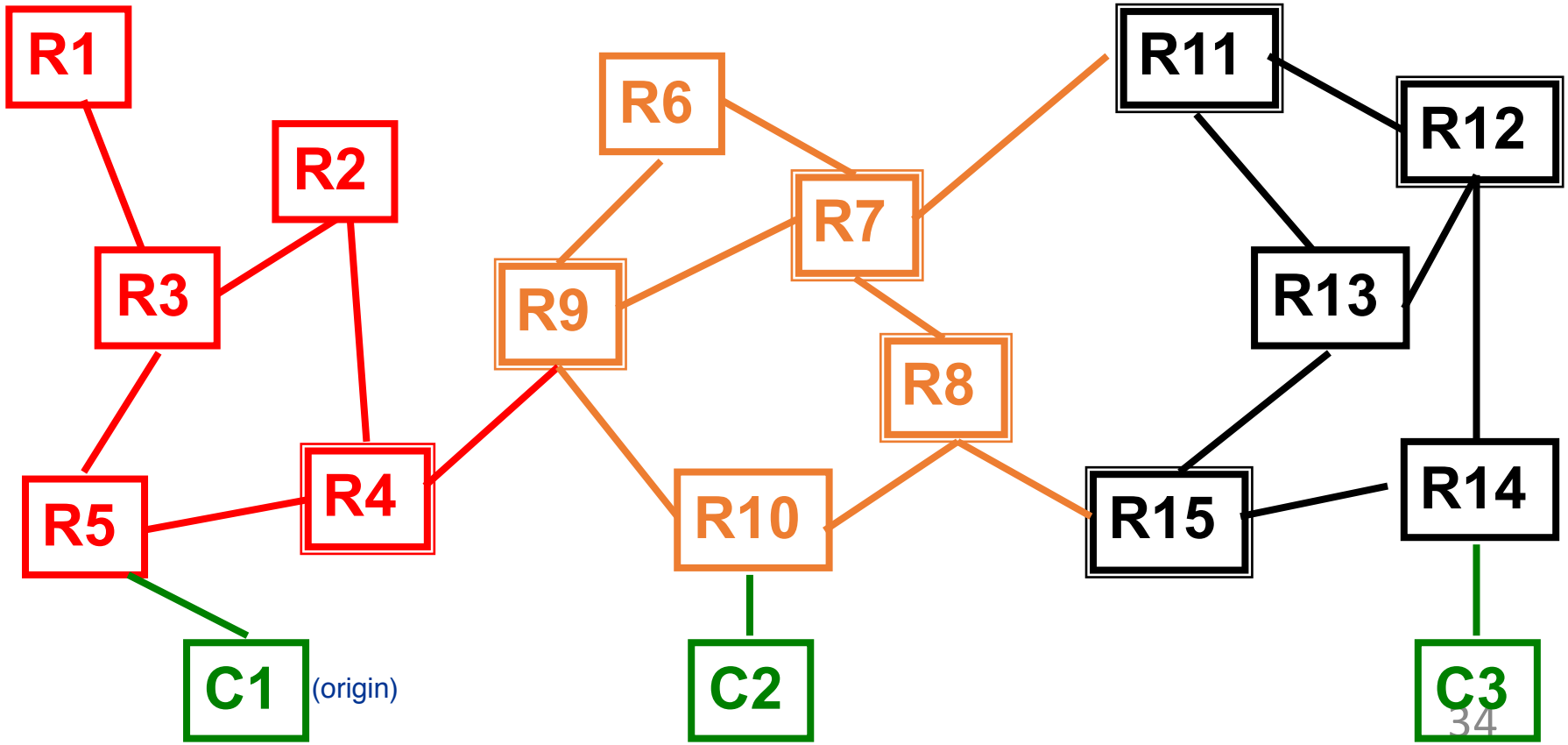
route attestation

R4 → R9: $Sign(sk_{c1}, \{C1, AS1\})$, [AS1], $Sign\ (sk_{AS1}, \{AS1, AS2\})$

R7 → R11: $Sign(sk_{c1}, \{C1, AS1\})$, [AS1, AS2], $Sign\ (sk_{AS1}, \{AS1, AS2\})$

, $Sign\ (sk_{AS2}, \{AS2, AS3\})$

RPKI 不加綠色部分，雖可防黑洞，大家還是一定會走到 C1，但 attacker 還是可以「幫」繞路



Discussion of S-BGP Security

RPKI ok How is prefix hijacking attack prevented?

因為我們沒有別人 domain 的 key
在 p34 中的 C1

RPKI gg How is ASpath truncation prevented?

RPKI gg How is ASpath alteration prevented?

What about partial deployments (where only a subset of ISPs deploy S-BGP)?

- What happens at boundary of S-BGP/legacy ISP?
- Are prefix hijacking, ASpath truncation attacks still possible?

問助教

Unfortunately, S-BGP is not widely deployed.

Fundamental BGP Limitations

Destination or ISP have no control over inbound paths

Lack of routing isolation

假設任一路由器掛了，其它以這為 relay 的 path 都會受到影響，造成 global effects，且沒辦法彌補（not scalable）

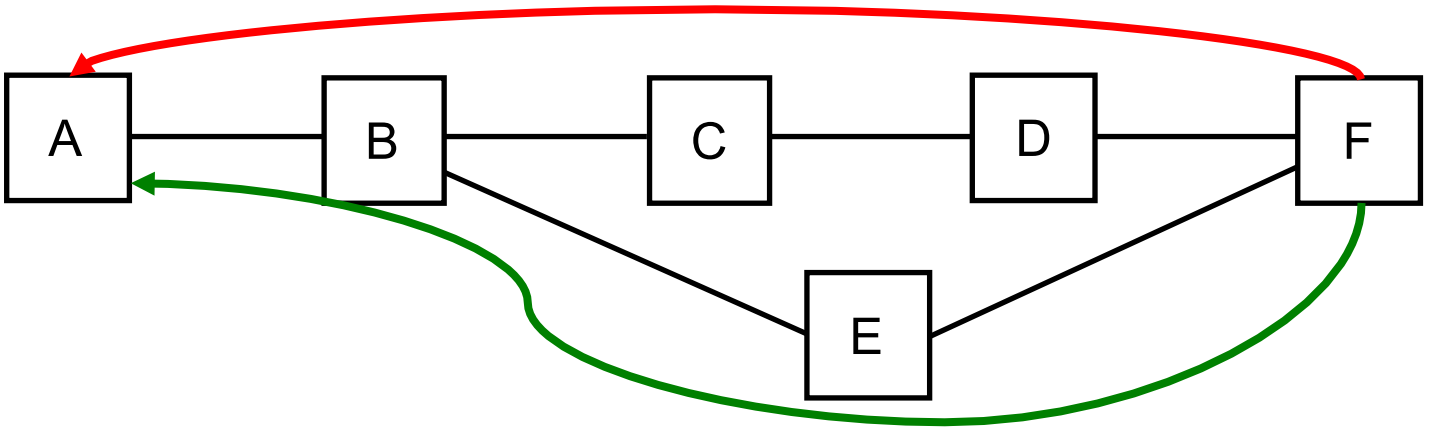
- A failure/attack can have global effects
- Global visibility of paths is not scalable

Slow convergence / route oscillation

每個路由器動態地計算我走哪條路較好，因為還有加密相關的計算負荷，以至於難以收斂，容易被 DDoS

Large routing tables

- Multi-homing / flat namespaces prevent aggregation



Fundamental BGP Limitations

Destination or ISP have no control over inbound paths

Lack of routing isolation

- A failure/attack can have global effects
- Global visibility of paths is not scalable

Slow convergence / route oscillation

Large routing tables

- Multi-homing / flat namespaces prevent aggregation

總而言之，這些問題都牽涉到網際網路的骨幹，局部性的修補效果不彰。

The Internet was not designed with security in mind

Assumption that there is no malicious entity is no longer valid!

Issues with prior approaches that patch the Internet for better availability:

- Mostly focus on reliability, not security aspects
- Inefficient or ineffective against strong attacks
- Constrained by the underlying Internet architecture

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF FUTURE INTERNET ARCHITECTURE PROJECT

MEETINGS

FIA project overviews
November 16-17, 2010
Meeting description

Security
May 25-26, 2011
Meeting description
Meeting report

Economics and Industry viability
April 19-20, 2012
Meeting agenda
Meeting report

INTRODUCTION

The Internet has created unprecedented opportunities for advancing knowledge across the spectrum of human endeavors. It has evolved from a small scale network of networks to become integral to our lives and vital to the operation of all critical sectors of our society. The continued success of the Internet, however, is increasingly threatened by the ever-mounting sophistication of security attacks and by the lack of performance reliability of Internet services. As our reliance on a secure and highly dependable information technology infrastructure continues to increase, it is no longer clear that emerging and future needs of our society can be met by the current trajectory of incremental changes to the current Internet.

Recognizing the need for a secure and highly dependable information technology infrastructure and building on NSF's on-going investments in network science and engineering, the Directorate for Computer and Information Science and Engineering (CISE) has formulated this program to stimulate innovative and creative research to explore, design, and evaluate trustworthy future Internet architectures. The objective is to engage the research community in collaborative, long-range, transformative thinking - unfettered by the constraints of today's

Domain Name System (DNS)

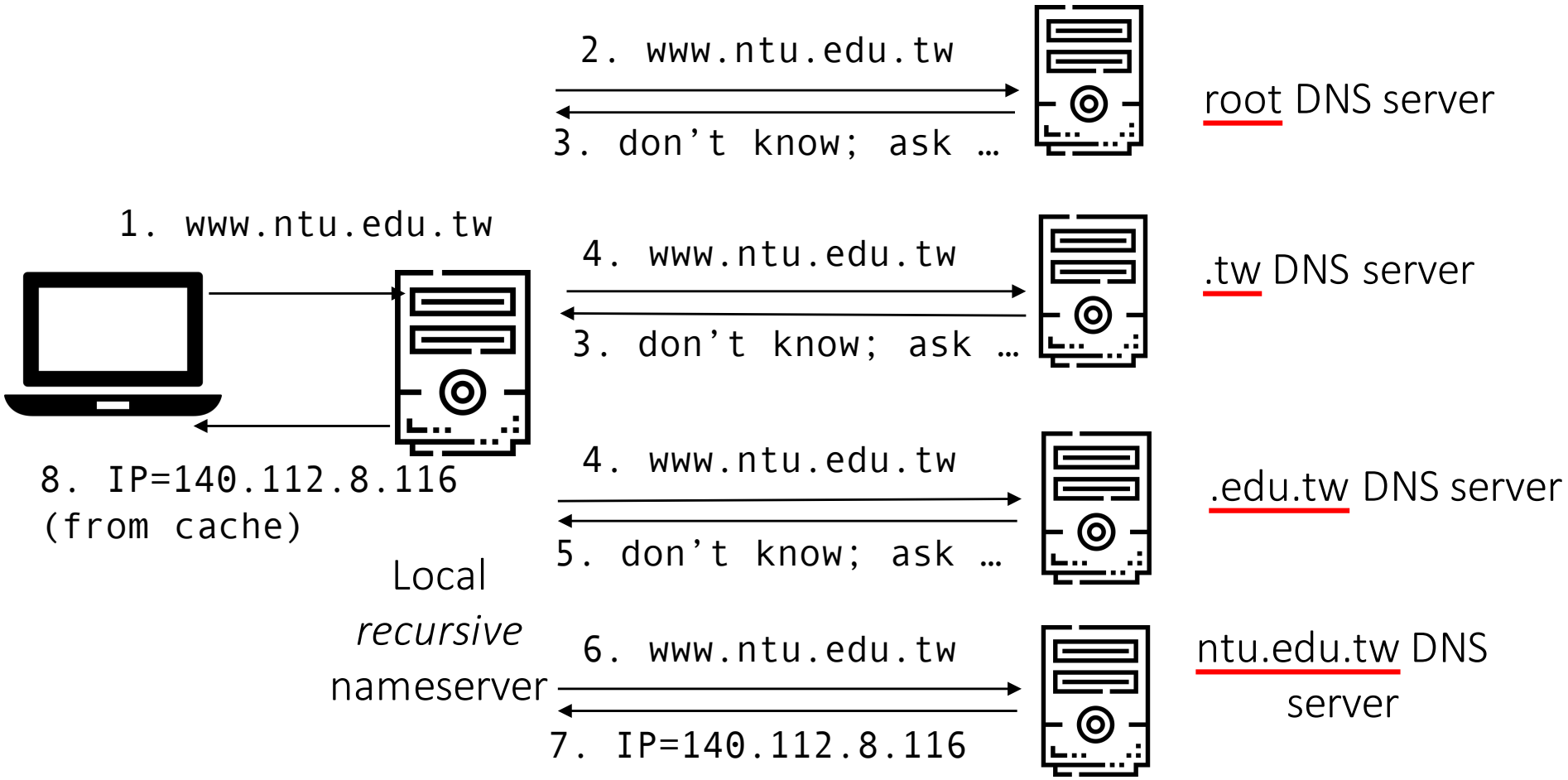
Domain Name System (DNS)

DNS maps domain names to IP addresses

- `csie.ntu.edu.tw -> 140.112.30.28`
- `www.ntu.edu.tw -> 140.112.8.116`
- Can also map to other types of *resources* (e.g., nameserver, mail exchanger, …)

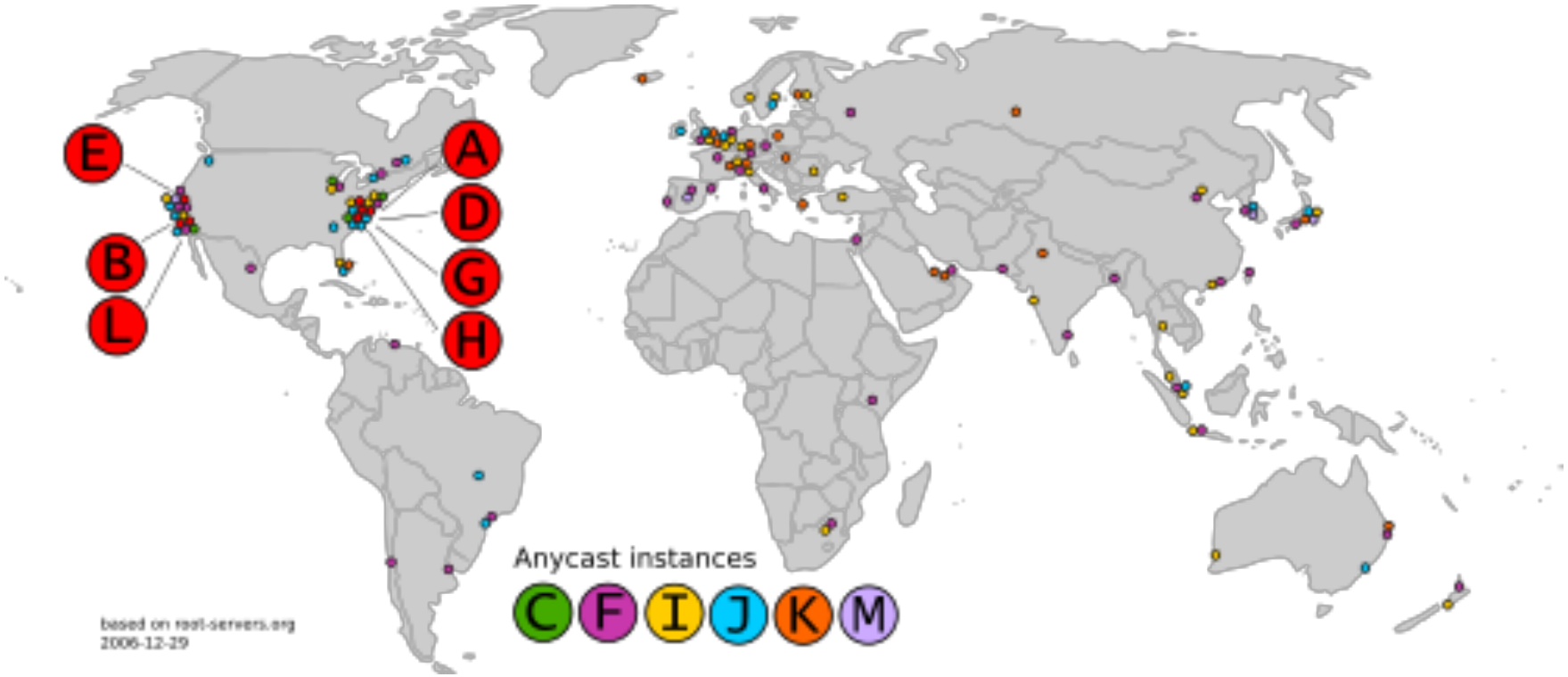
```
> dig csie.ntu.edu.tw

;; 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

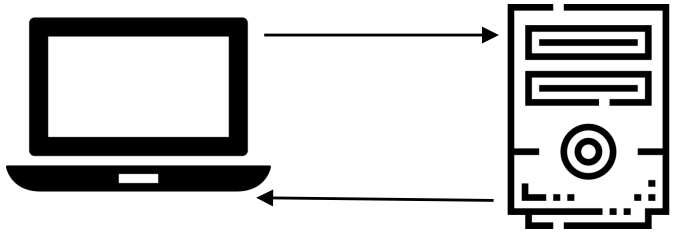
Root Name Servers



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

DNS Cache

1. Ask again www.ntu.edu.tw



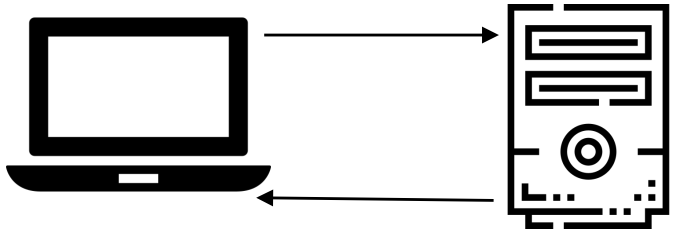
2. IP=140.112.8.116 (from cache)

Cache allows reuse of previous results

- Faster response to identical queries
- Nameservers and negative queries are also cached

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

Filtering and Censorship

DNS amplification attack (Next topic)

DNS hijacking

- DNS cache poisoning

Filtering and Censorship

DNS is a convenient place for filtering or censoring Internet access

- CleanBrowsing: adult-filter-dns.cleanbrowsing.org
- COMODO Dome Shield

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

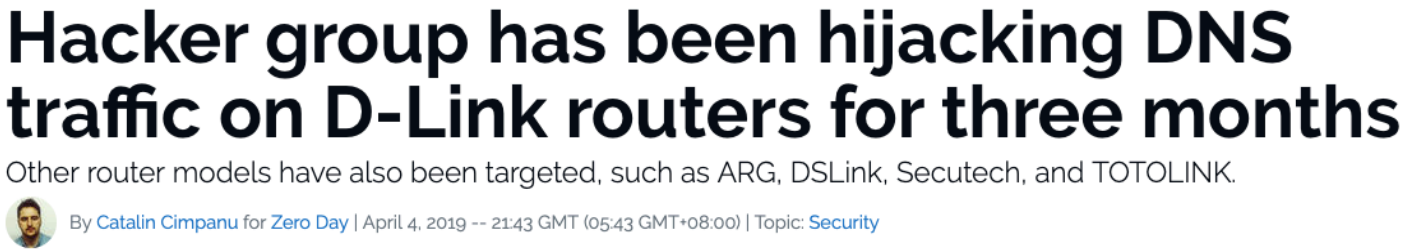
讚 5.3 萬 按讚加入iThome粉絲團 讚 266 分享

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

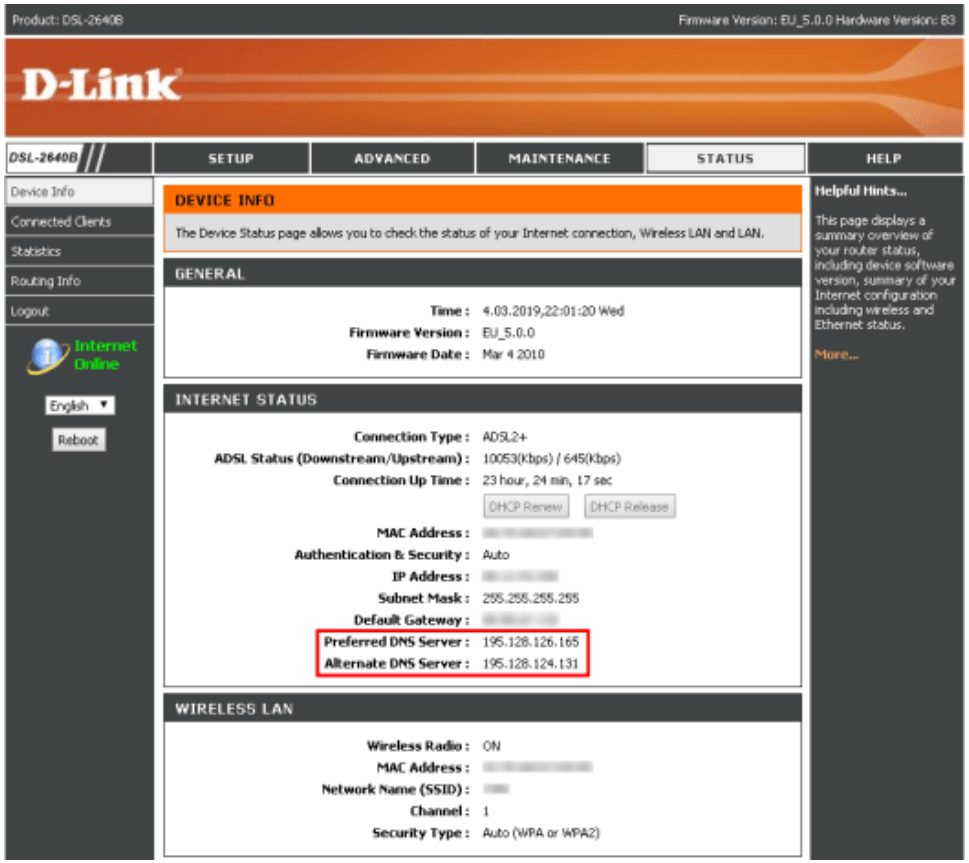


Hacker group has been hijacking DNS traffic on D-Link routers for three months

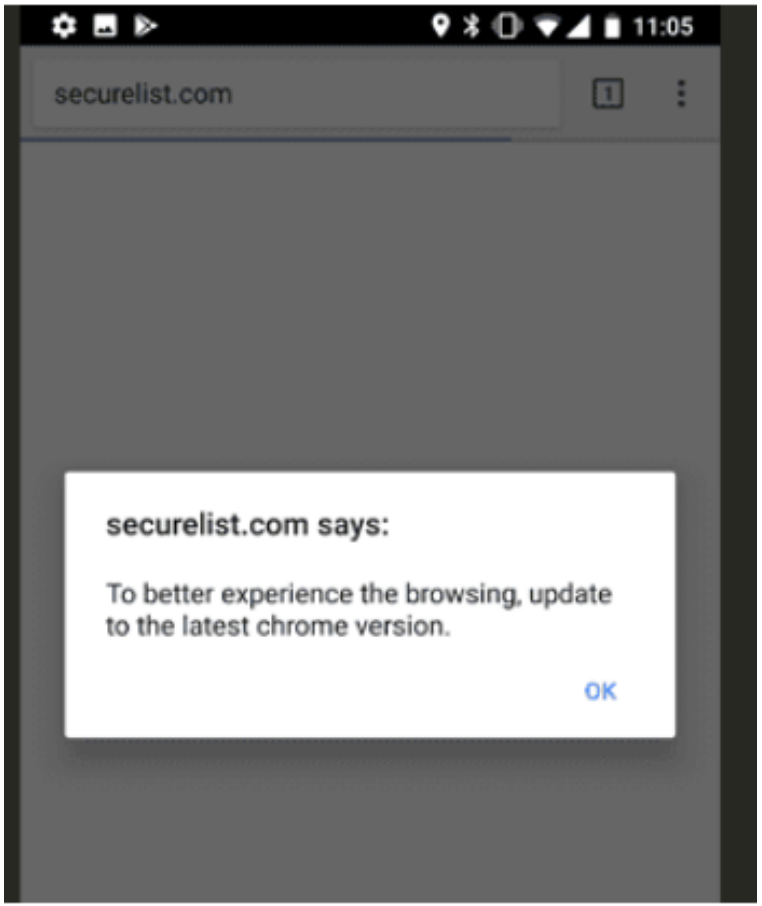
Other router models have also been targeted, such as ARG, DSLink, Secutech, and TOTOLINK.

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

DNS hijacking via malware

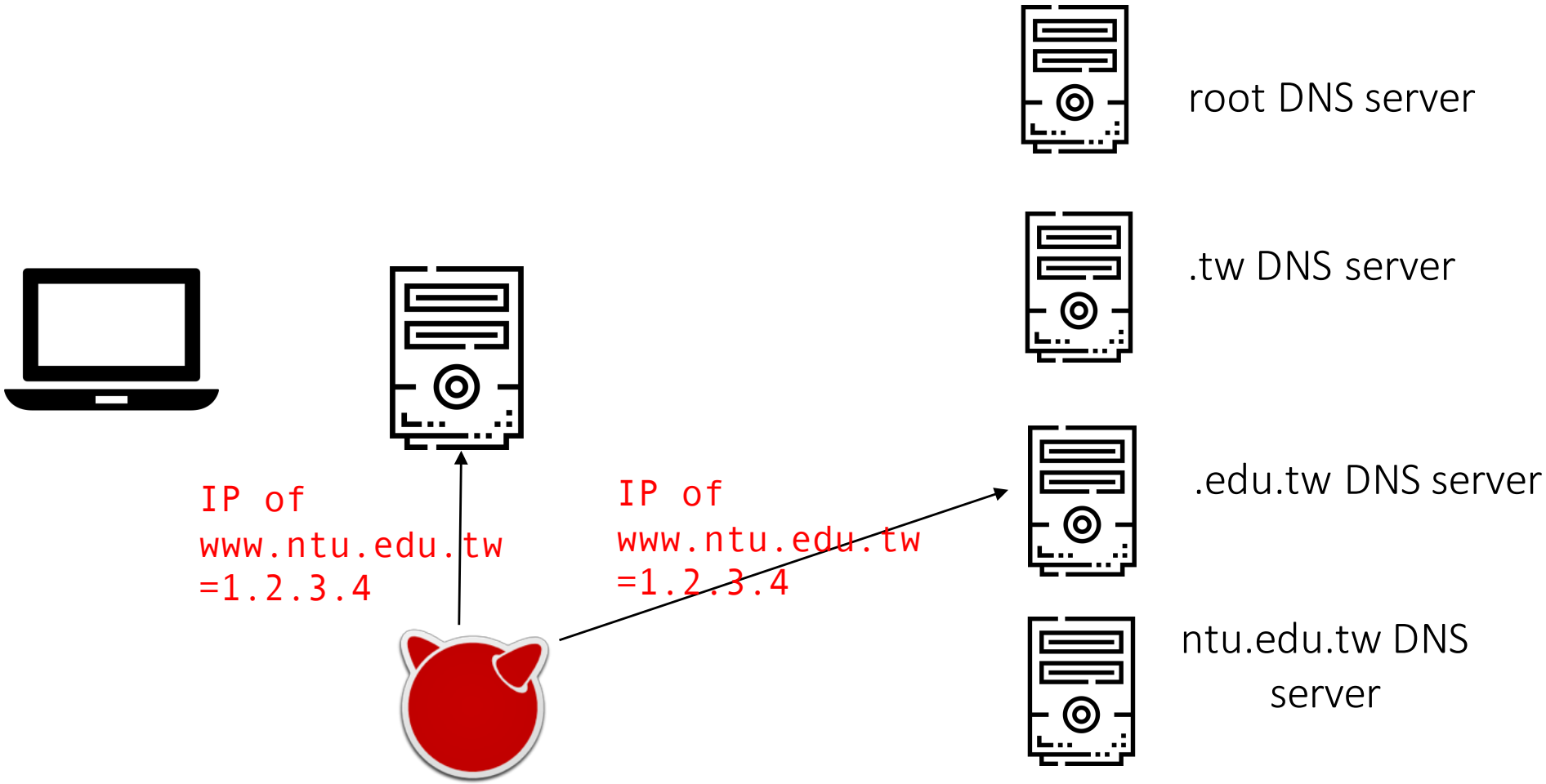


Example compromised D-Link DSL-2640B router with DNS servers set to rouge DNS servers used in this campaign.
https://badpackets.net/ongoing-dns-hijacking-campaign-targeting-consumer-routers/



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

DNS Cache Poisoning

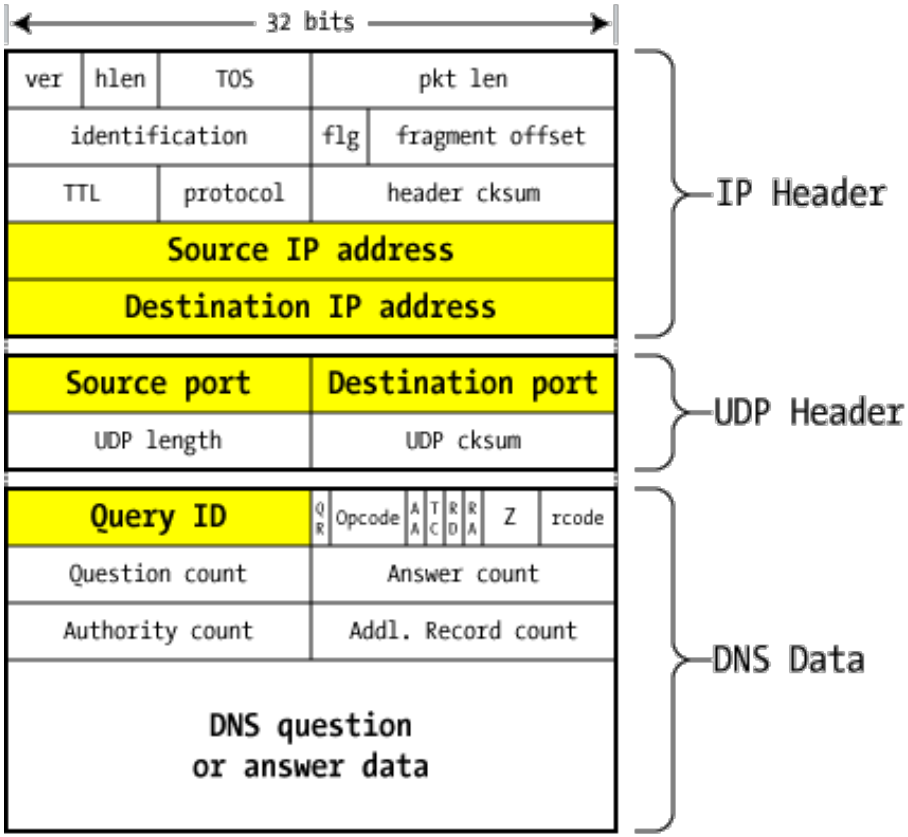


Can an attacker forge the response and poison the cache?

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



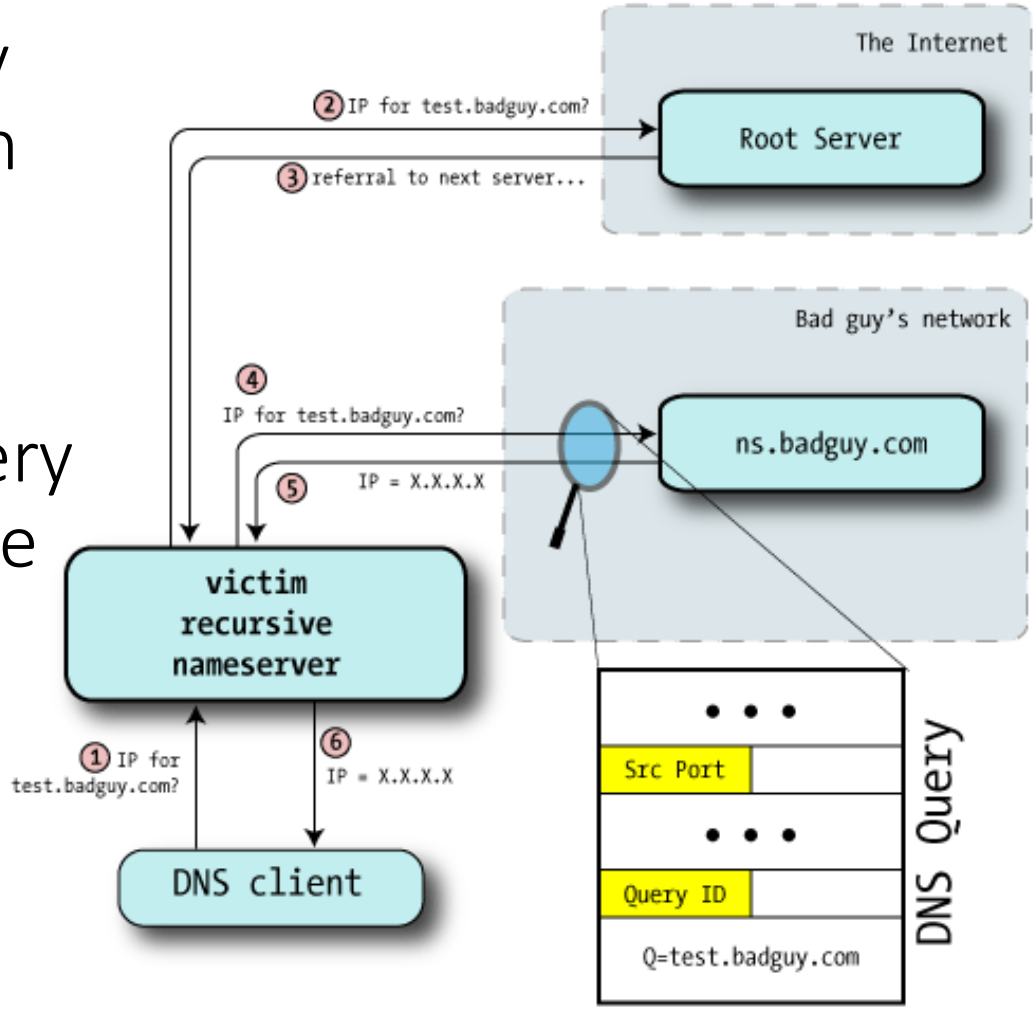
DNS packet on the wire

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

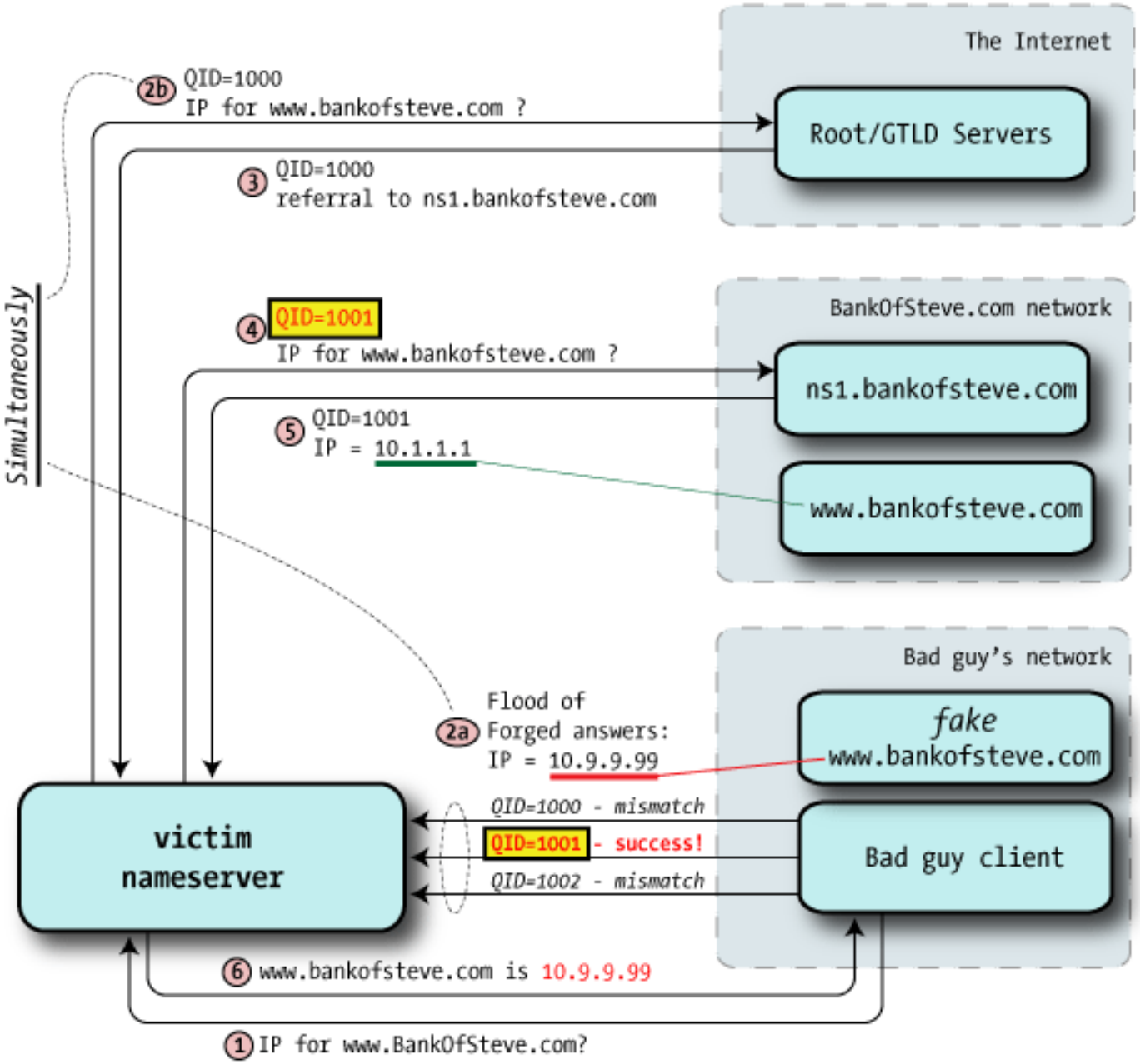


http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

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

DNS Cache Poisoning

Success Conditions

因為 www.BandOfSteve.com 還沒有在 cache 中，所以 attacker 才有機可乘

- 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?

- Use an unpredictable query ID

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

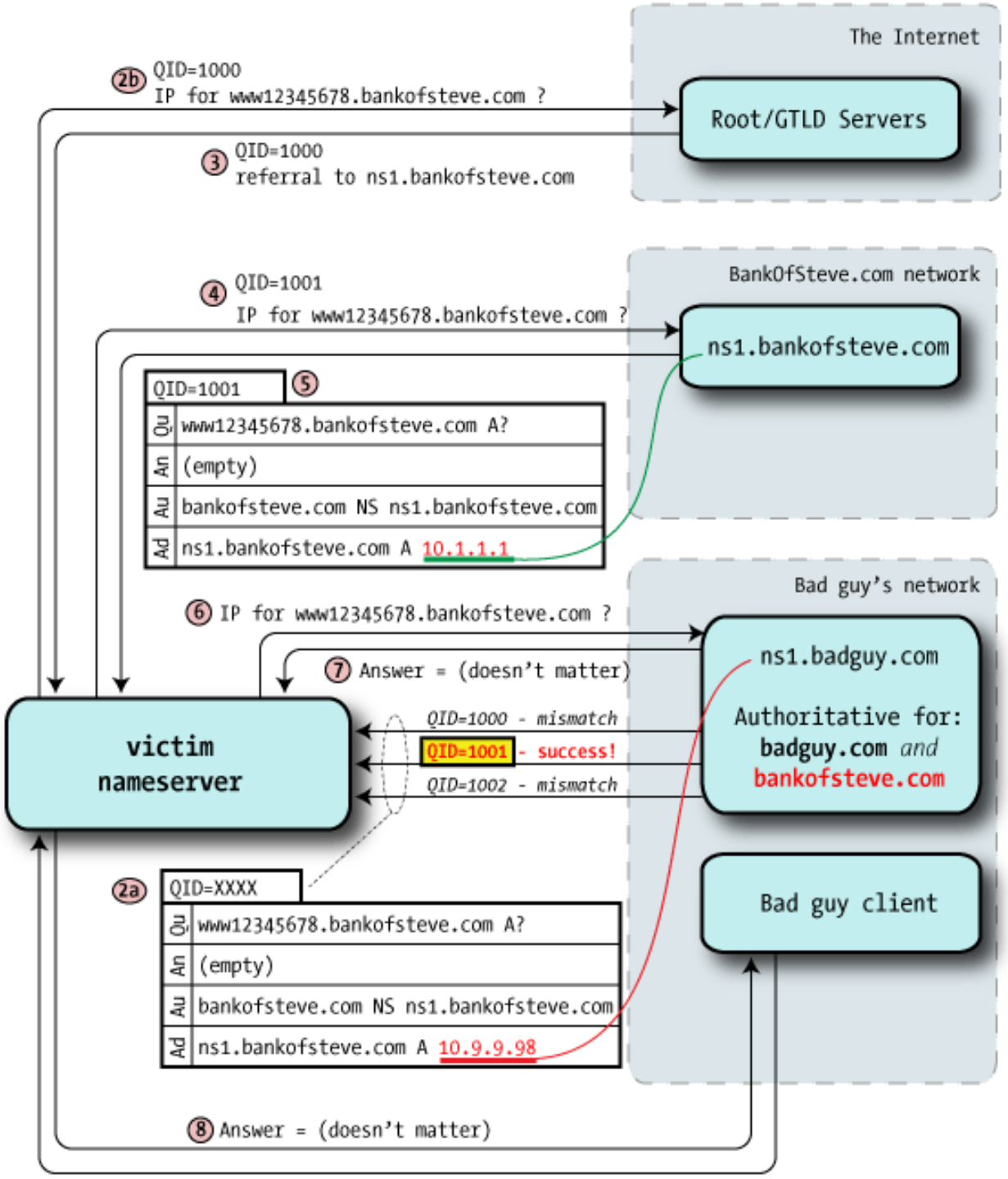
More powerful: **hijack the authority records** instead

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

DNS-over-TLS

- Similar to HTTP over TLS (known as HTTPS)

Extension mechanisms for DNS (EDNS)

EDNS is a spec for increasing DNS parameter size

- Needed to support DNS-over-TLS, DNSSEC

Supported starting from February 1st, 2019

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
```

https://dnsflagday.net/

Conclusion

The Internet was not designed for security

Need additional mechanisms to ensure the authenticity of BGP and DNS

Ad hoc fixes vs. new internets?