The Internet is for Everyone. Become an ISOC Member.

Cyber Security Symposium 2011

Where is Hong Kong in the secure Internet infrastructure development

Warren Kwok, CISSP
Internet Society Hong Kong
12 August 2011

Outline

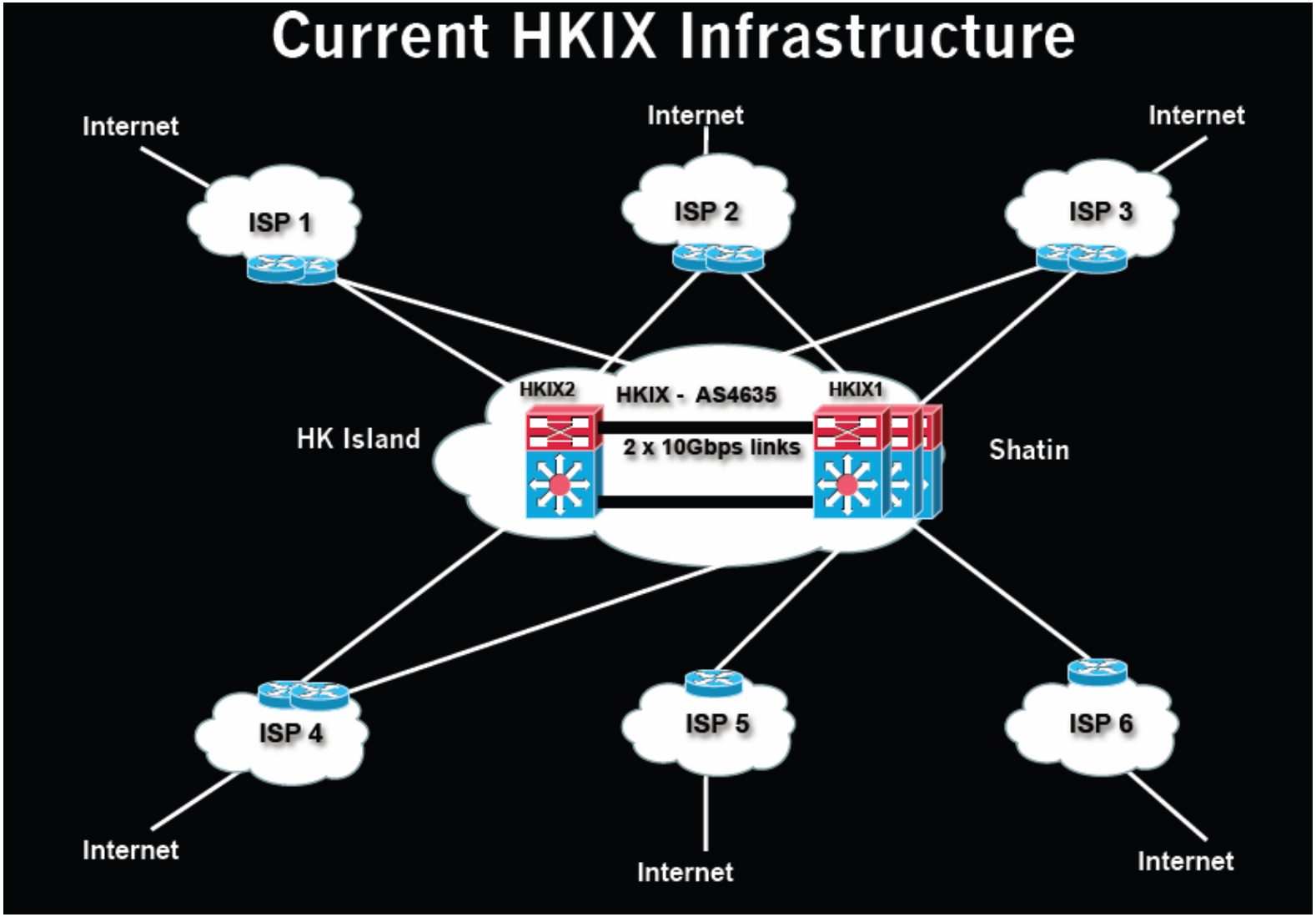
1. Security of common critical Internet infrastructure
   - Internet Exchange (HKIX)
   - Domain name infrastructure (root, .hk, .com, .asia)
   - Public Key Infrastructure
   - Standard Time Server
2. Security of Internet facilities of ISPs
   - Spam control measures
   - Authoritative Name Servers & Resolvers
   - DDoS prevention and source address filter
3. DNSSEC overview

A look at common critical Internet facilities

Introduction to HKIX

- Most critical Internet infrastructure in HK since 1995
- Layer-2 Internet Exchange Point
- Supports IPv4 and IPv6
- Security measures of HKIX
  - Backup by HKIX2
  - Port security control

Network Diagram of HKIX



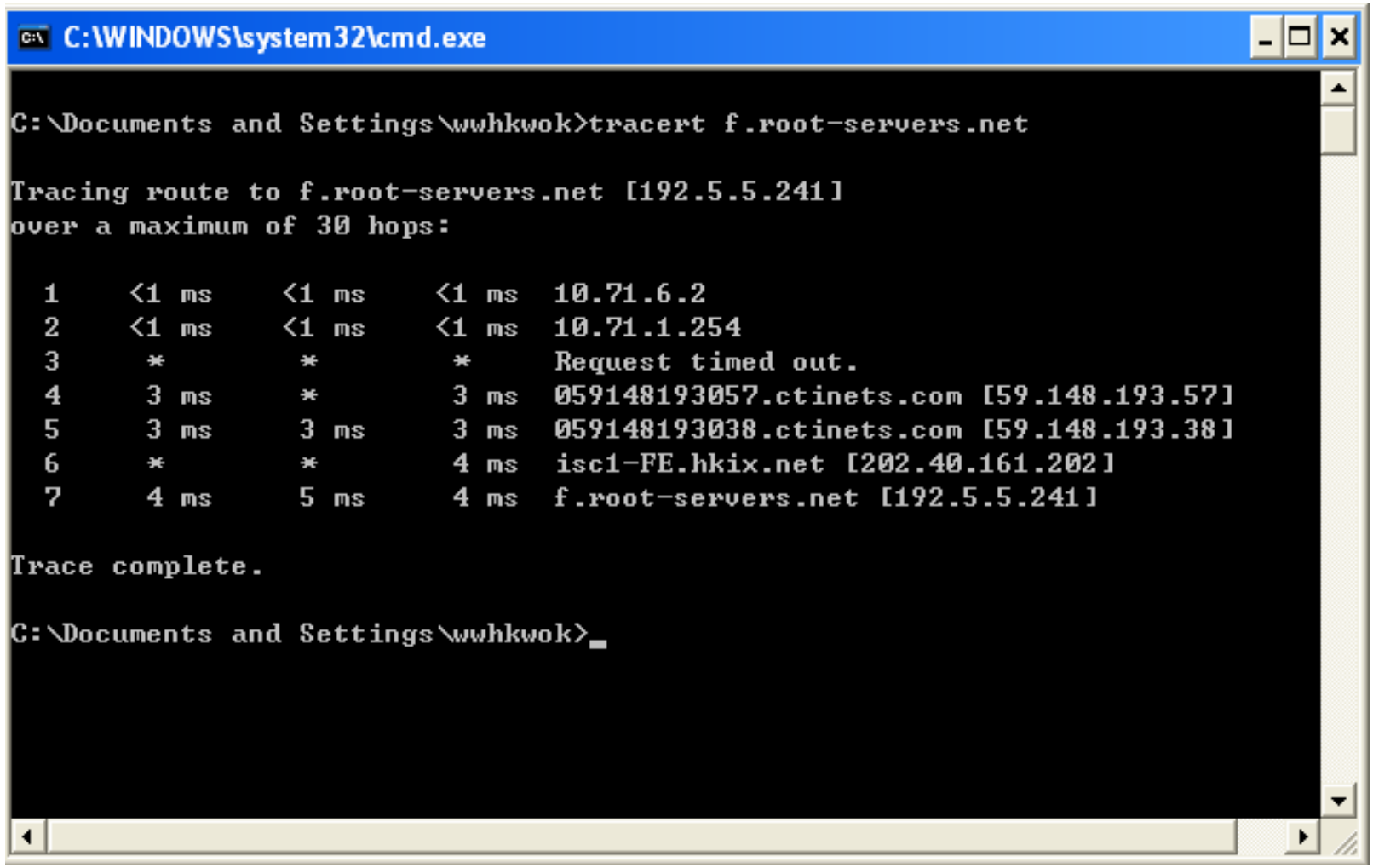
Intra-Asia Traffic

Security in Root domain

- DDoS attacks on 13 root name servers on 21 Oct 2002 resulted in 9 root name servers unserviceable for 1 hour
- Remedy : Add anycast instances in other countries
- An anycast instance has the same content and same IP address of the original name server
- Root domain system becomes 13 installations DNS
- Resolvers contact root instances by the shortest path (Anycast routing)
- “F”, “I” and “J” root name servers are established in HK at HKIX

Root Servers – 242 instances

Traceroute F root server



Submarine cable incidents in Dec 06 – Jan 07

- International backbone damaged but local Internet backbone still serving
- Local people accessed to .hk websites ok
- Accessed to local .com, .net and .org websites failed
- Since then, efforts been made to persuade TLD operators to place server instances at HKIX
- The following TLDs are now at HKIX:
  .com, .net, .org, .asia, .info, .hk, .mo, .tw, .sg, .my, .cn, and many more
- Most TLD instances support IPv6
- HK now has a highly resilient domain name infrastructure supporting IPv4 and IPv6 transport

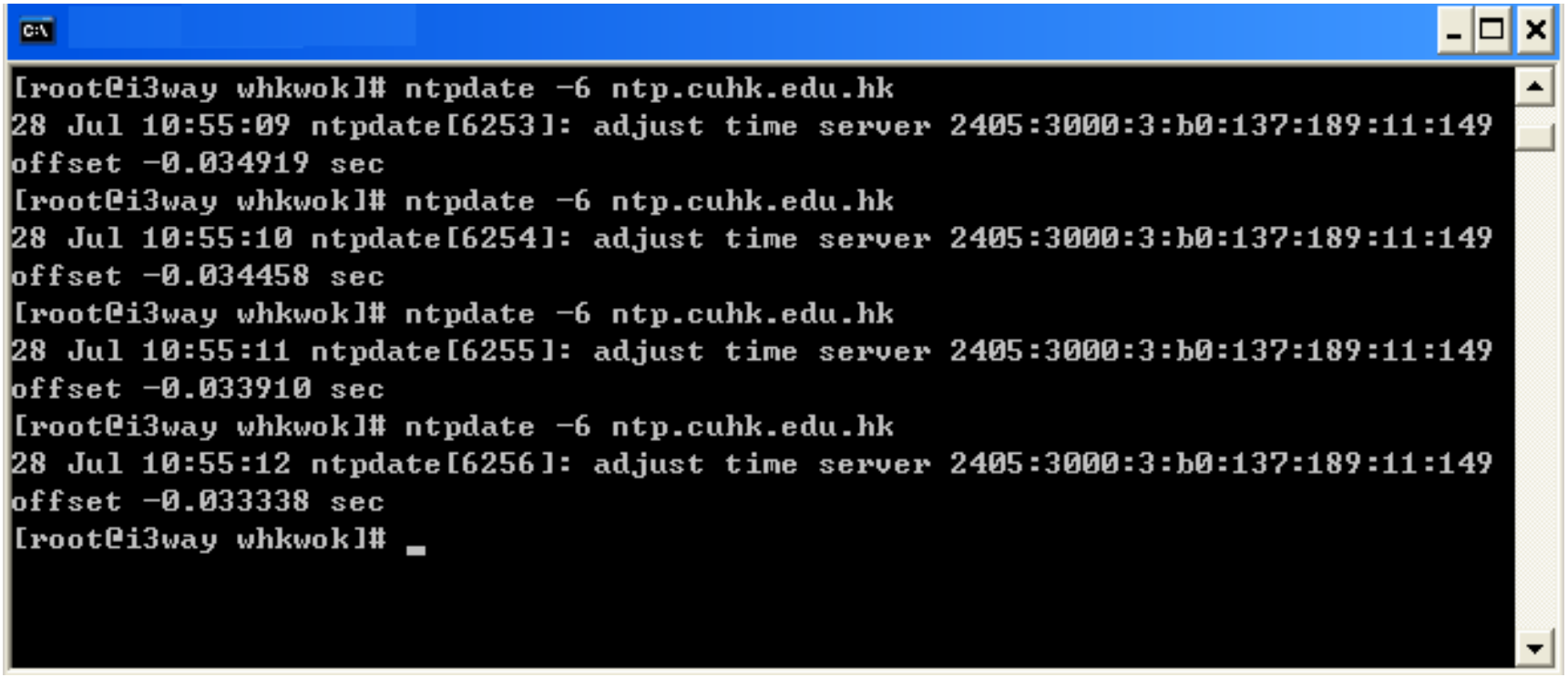
Standard Time Service

- In terms of security, all event logs and access logs must have accurate clock
- Hong Kong Observatory providing Stratum 1 NTP Server at “stdtime.gov.hk”
- Based on Caesium atomic clock
- Accuracy in fractions of 1 micro-seconds
- 2.7 million sync per day or 1 billion per year
- A GPS clock for backing up

Lack of local v6 NTP Server

- Lack of authoritative v6 NTP Server (Stratum 1) in HK
- Overseas v6 NTP Servers can not be used due to latency issue
- IPv6 networks affected
- Not all routers and firewalls are dual-stack
- HKO will provide one set of v6 NTP by Dec 2011
- Interim - CUHK provides interim Stratum 2 NTP at ntp.cuhk.edu.hk

v6 NTP Sync


[root@i3way whkwok]# ntpdate -6 ntp.cuhk.edu.hk
28 Jul 10:55:09 ntpdate[6253]: adjust time server 2405:3000:3:b0:137:189:11:149
offset -0.034919 sec
[root@i3way whkwok]# ntpdate -6 ntp.cuhk.edu.hk
28 Jul 10:55:10 ntpdate[6254]: adjust time server 2405:3000:3:b0:137:189:11:149
offset -0.034458 sec
[root@i3way whkwok]# ntpdate -6 ntp.cuhk.edu.hk
28 Jul 10:55:11 ntpdate[6255]: adjust time server 2405:3000:3:b0:137:189:11:149
offset -0.033910 sec
[root@i3way whkwok]# ntpdate -6 ntp.cuhk.edu.hk
28 Jul 10:55:12 ntpdate[6256]: adjust time server 2405:3000:3:b0:137:189:11:149
offset -0.033338 sec
[root@i3way whkwok]#

Public Key Infrastructure in HK

- Hongkong Post is the designated Certificate Authority (CA) under the Electronic Transaction Ordinance (Cap. 553)
- Digi-Sign Certification Services Limited is another CA under the Voluntary Certification Authority Recognition Scheme under the ETO
- Both recognized CAs comply with the ETO and COP for Recognized CA
- They can issue digital certificates for personal and organizational use
- Common browsers and email clients must recognize the root certificate of CAs

Security Measures for PKI

- Employ stringent security procedures and control for:

  Key generations, management, database, LDAP, backup storage and other IT facilities
- Conduct compliance assessment every 12 months
- Backup by DR site
- Disaster recovery drills on incidents, key compromise and recovery

Security of Internet facilities of ISPs

Spam control by ISPs in Hong Kong

ISPs closely follow HKISPA Anti-spam Code of Practice :

- Block outgoing port 25 (SMTP) for dynamic IP addresses
- Disallow open relay
- Disable directory harvest attack on mail servers
- Restrict the amount of outgoing mail

Blocking Outbound Port 25

Hong Kong adopts an effective cybersecurity measure

- Spam is the catalyst of all cyber crimes
- Compromised hosts can not send spam email
- Reduce the spread of malware by spam
- Users use the legitimate SMTP servers of their ISPs for outgoing email

In Asia, Japan ISPs are doing the same with success in reducing the amount of spam.

Directory Harvest Attack

- SMTP servers accept all e-mail address at <RCPT TO> stage but reject invalid ones at DATA stage
- Directory harvest fails, no way to tell of e-mail address validity
- SMTP Servers cut connection after an allowable connection time.

Security in authoritative (hosting, SOA) name servers

Good Security Practice

- ISPs ban zone transfer (AXFR) from unauthorized hosts
- Zone transfer from primary to secondary servers by means of permitted hosts (access control list)

Probing further

- Can not prevent spoofed IP addresses as primary or secondary servers

Transaction Signature (TSIG)

- Improvement can be made by deploying DNS Transaction Signature (TSIG)
- A keyed-hash is applied (like a digital signature) so recipient can verify message
- Based on a shared secret - both sender and receiver are configured with it
- Not popular, only a few ISPs have implemented TSIG

TSIG Config Example

Primary server

10.33.40.46

```
key ns1-ns2.zone. {
        algorithm hmac-md5;
        secret "APlaceToBe";
};
server 10.33.40.35 {
        keys {ns1-ns2.zone.;};
};
zone "my.zone.test." {
        type master;
        file...;
        allow-transfer {
                key ns1-ns2.zone.;
                key ns1-
ns3.zone.;};
};
```

Secondary server

10.33.40.35

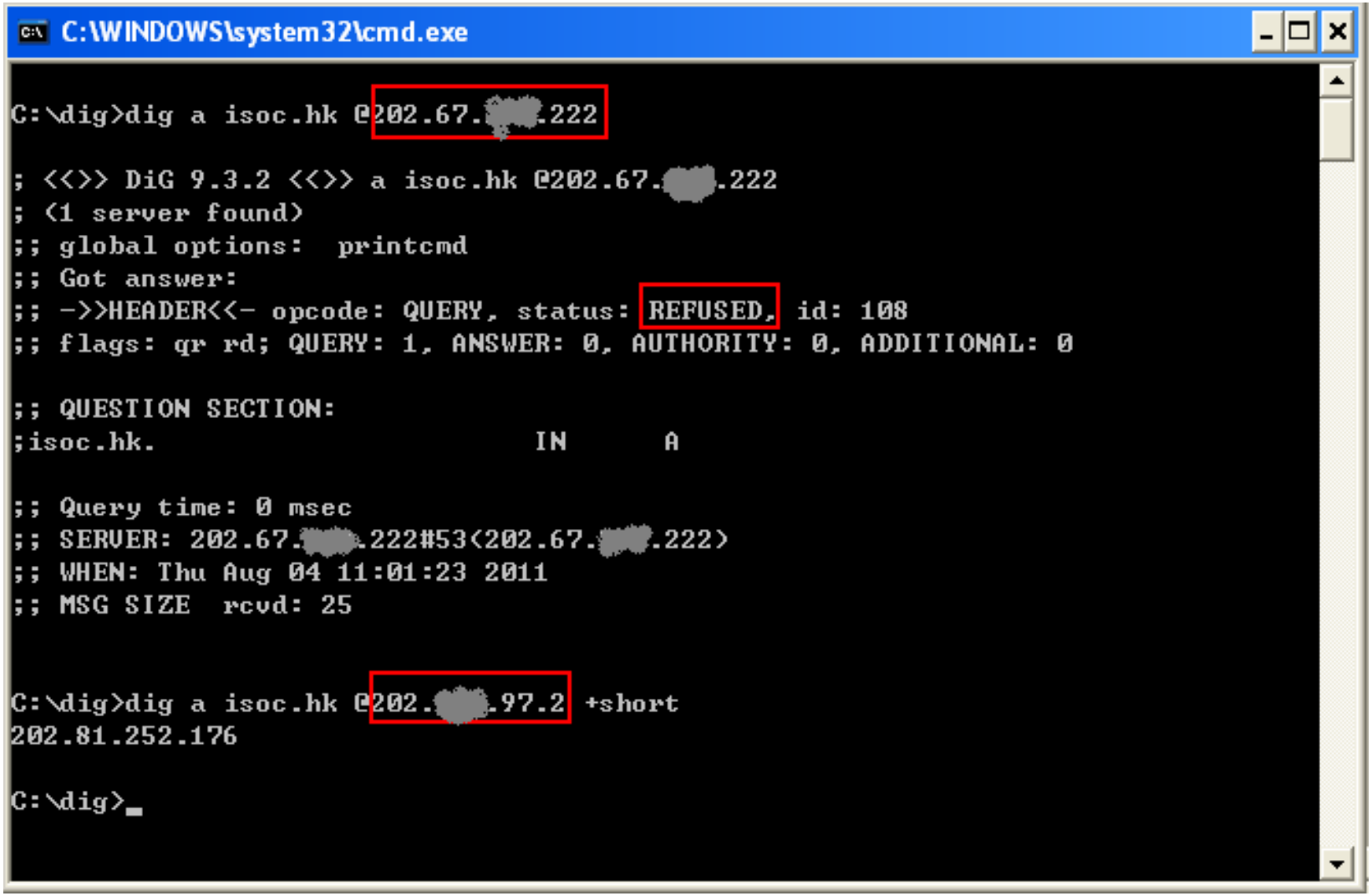
```
key ns1-ns2.zone. {
        algorithm hmac-md5;
        secret "APlaceToBe";
};
server 10.33.40.46 {
  keys {ns1-ns2.zone.;};
};
zone "my.zone.test." {
        type slave;
        file...;
        masters {10.33.40.46;};
        allow-transfer {
                key ns1-
ns2.zone.;};
};
```

Resolver Issues

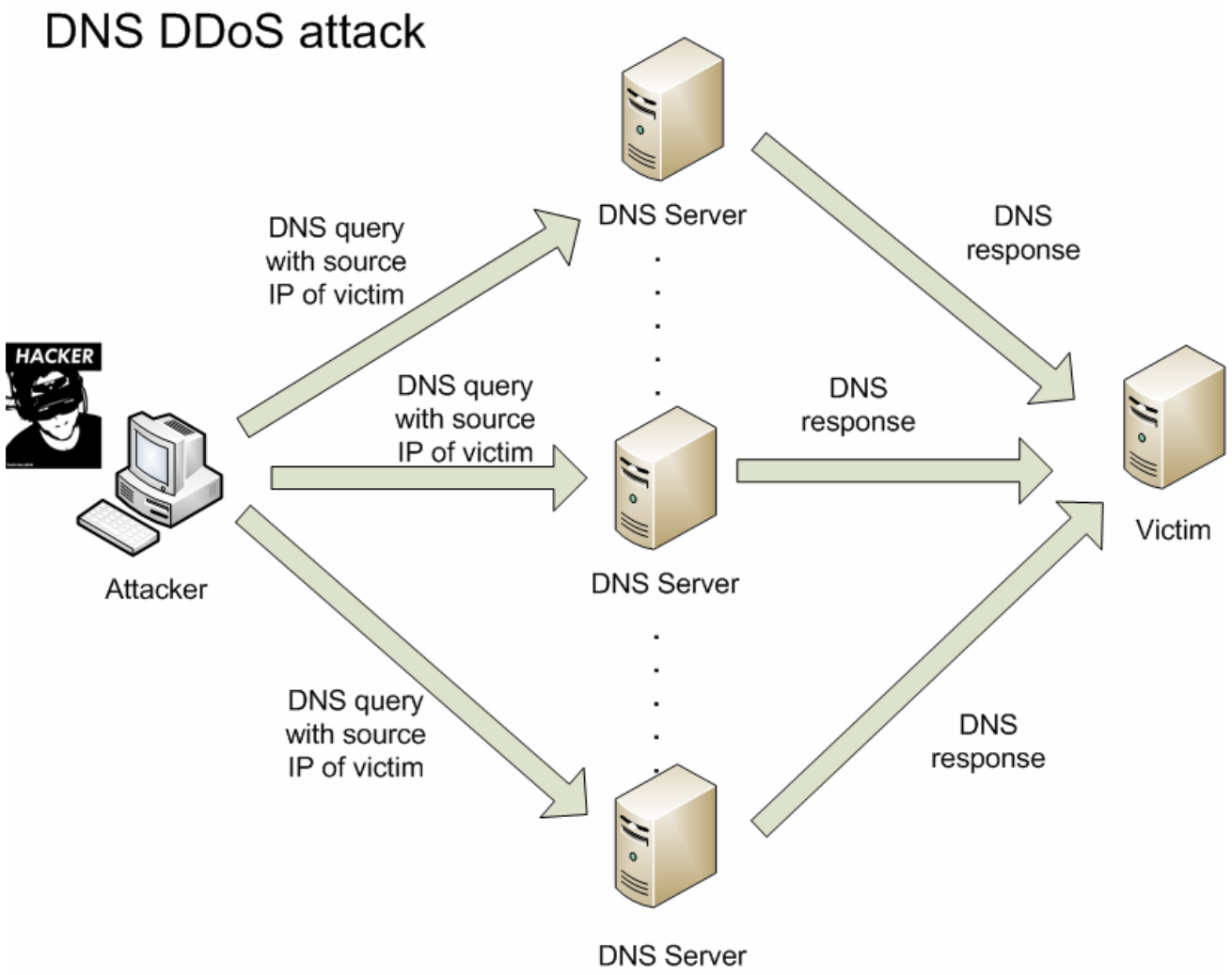
DNS Survey (October 2010) by Measurement Factory revealed 79 % resolvers are open resolvers (http://dns.measurement-factory.com/surveys/201010/dns_survey_2010.pdf)

- Estimated 11.9 million resolvers are vulnerable
- Answer recursive query from any IP addresses (Helping reflector attack and amplification attack)
- A recent sample survey of 50 resolvers in HK found 38 exhibited open recursion (i.e. 76 %)
- RFC5358 –Preventing Use of Recursive Name Servers in Reflector Attacks

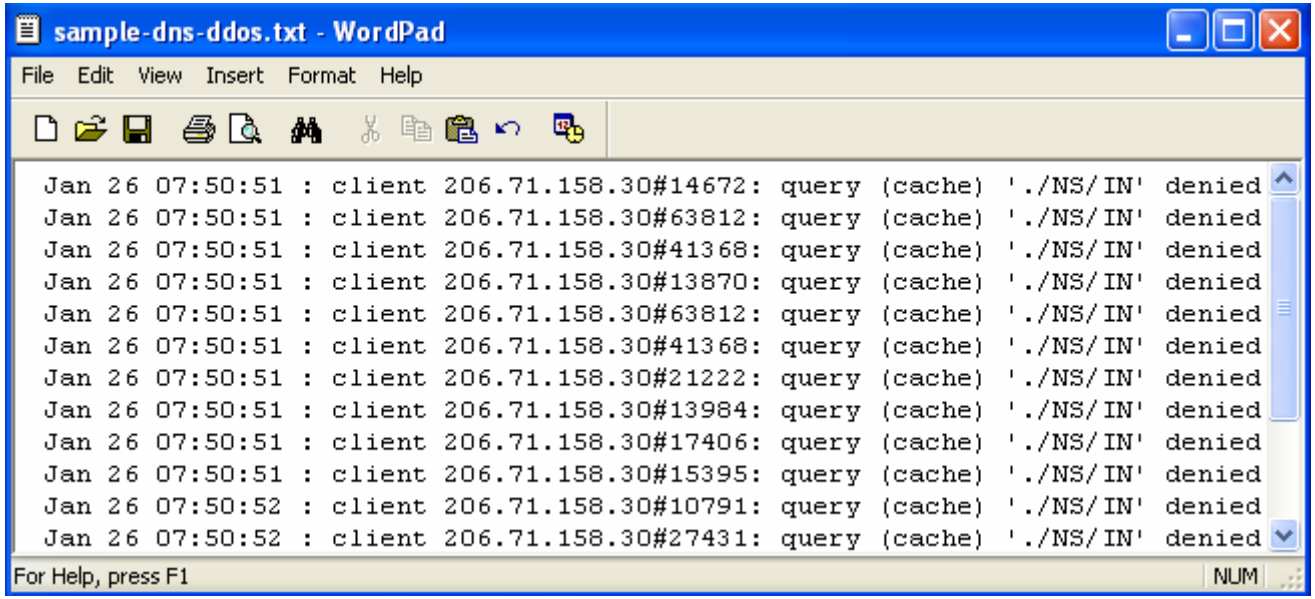
Test on open and closed resolvers



Reflector and Amplification Attack



Amplification Factor



Query (what are ns for root zone) – 45 bytes

Answers (large records) – 506 bytes

Amplification factor = 11.2

Akamai's State of the Internet – Q1 2011

- Hong Kong generated 3 % of attack traffic

	Country/Region	Q1 '11 % Traffic	Q4 '10 %
1	Myanmar	13%	N/A
2	United States	10%	7.3%
3	Taiwan	9.1%	7.6%
4	Russia	7.7%	10%
5	China	6.4%	7.4%
6	Brazil	5.5%	7.5%
7	India	3.8%	2.1%
8	Hong Kong	3.3%	0.3%
9	Romania	2.5%	2.6%
10	Italy	2.5%	3.6%
–	Other	36%	45%

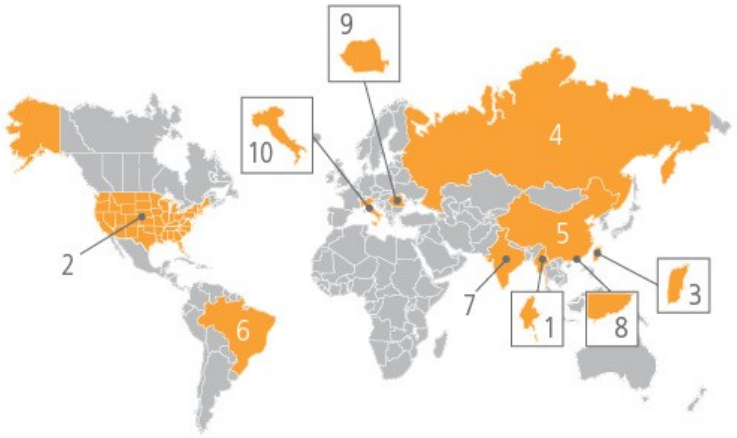


Figure 1: Attack Traffic, Top Originating Countries/Regions

- Attack sources use multiple fake source IP addresses to send attack traffic
- Victims can not specify any filtering rule

Source Address Filter

- Finnish Communications Regulatory Authority mandates operators to do source address filter (FICORA 13 A/2008 M)

- Section 6 - Regulation On Information Security and Functionality of Internet Access Services

  Address-based filtering in customer subscriptions

- A telecommunications operator ***must filter outgoing traffic*** from a customer subscription to a communications network in cases where the ***source address is not assigned to this particular customer*** subscription.

- Attack traffic of Finland is 0.1 % in Akamai's Q1 – 2011 Report

DDoS Attack Prevention

- A network should not send out packets with source address NOT belonging to the network
- Router deploys source address filtering
- Access Control List might be difficult :

  - due to fragmented prefixes

  - acquire different prefixes at different time
- unicast reverse packet forwarding (uRPF) - a standard feature in edge router
- uRPF adapts to changes in the routing tables
- Ideal implementation for IPv6 (a single /32 prefix in v6, but many fragmented prefixes in v4)

v4 and v6 source address filter

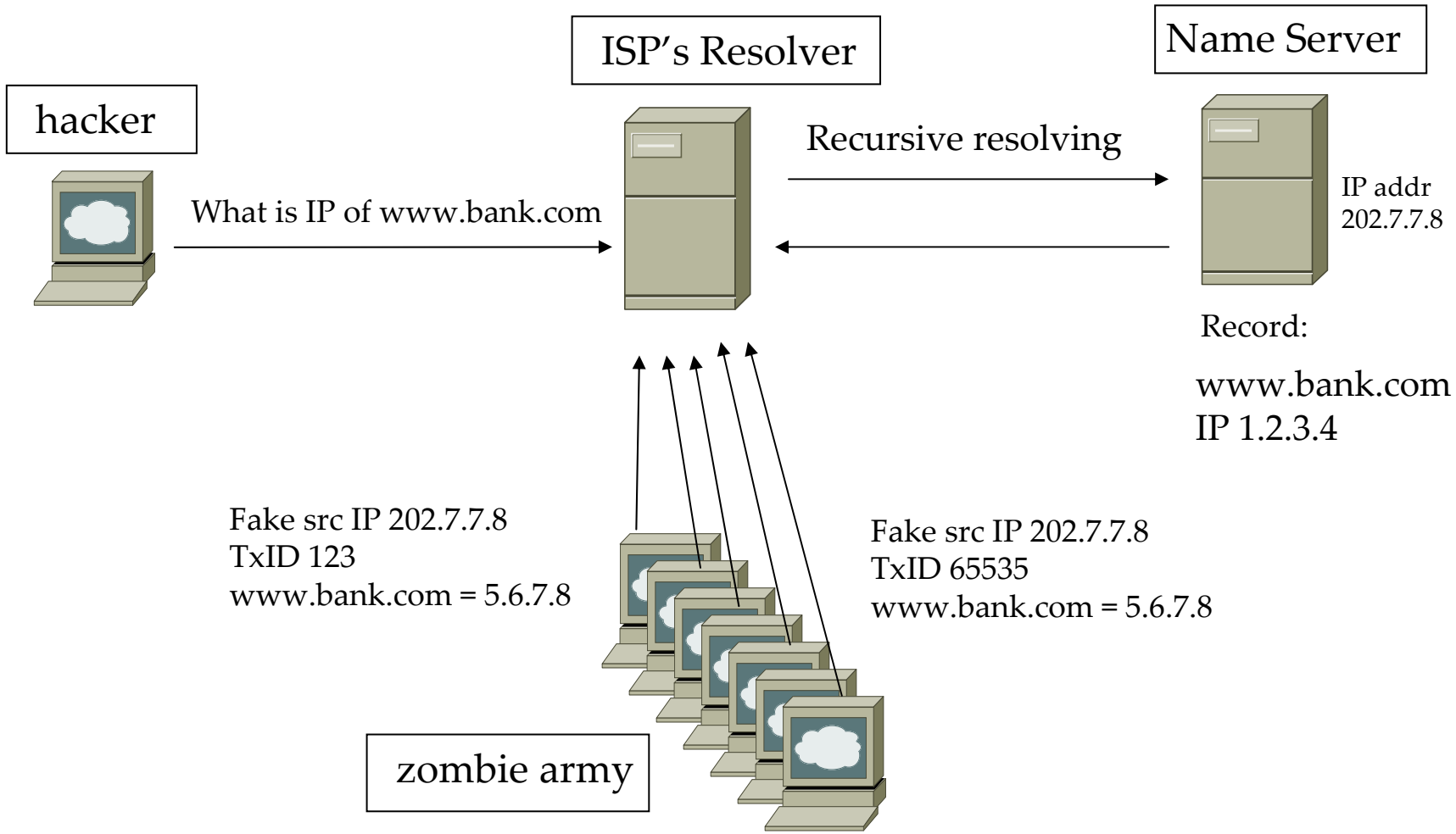
ASN9269

v4 - 1.4 million IPv4 addresses in 17 prefixes
v6 – 2^96 address in 1 prefix 2401:f400::/32

Match	Type	Size	Country	Start IP	End IP
1	/15	131,071	HK	58.176.0.0	58.177.255.255
2	/15	131,071	HK	59.148.0.0	59.149.255.255
3	/16	65,535	HK	61.92.0.0	61.92.255.255
4	/16	65,535	HK	61.93.0.0	61.93.255.255
5	/16	65,535	HK	61.238.0.0	61.238.255.255
6	/16	65,535	HK	61.239.0.0	61.239.255.255
7	/16	65,535	HK	61.244.0.0	61.244.255.255
8	/24	255	UK	91.207.192.0	91.207.192.255
9	/15	131,071	HK	119.246.0.0	119.247.255.255
10	/15	131,071	HK	123.202.0.0	123.203.255.255
11	/16	65,535	HK	124.244.0.0	124.244.255.255
12	/15	131,071	HK	183.178.0.0	183.179.255.255
13	/18	16,383	HK	203.80.64.0	203.80.127.255
14	/18	16,383	HK	203.80.192.0	203.80.255.255
15	/18	16,383	HK	203.185.0.0	203.185.63.255
16	/16	65,535	HK	203.186.0.0	203.186.255.255
17	/16	65,535	HK	210.6.0.0	210.6.255.255

Domain Name System Security Extension (DNSSEC)

Resolver Cache Poisoning



Impacts of Resolver Cache Poisoning

- Redirect to a fake bank website

  i.e. www.bank.com – 1.2.3.4 changed to 5.6.7.8
- Insert a fake host in the domain bank.com

  e.g. login1.bank.com – 5.6.7.9
- Denial of Service attack by answering no such domain records for www.bank.com

  (NXDOMAIN will also be cached in a resolver according to the “SOA Minimum”)

Why DNSSEC

- Stupid resolvers accept first response and cache the answer !
- Not really stupid, at least matching of return IP address, Transaction ID and random port number
- DNSSEC prevents cache poisoning
- In DNSSEC, resolvers verify the source of information by digital signatures from authoritative servers along the DNS tree (root -> TLD -> registrant's domain etc)
- With DNSSEC, ***resolvers*** become ***recursive validators*** or ***validating resolvers***

Operational Changes in DNSSEC

Authoritative Server – Internal

generate key pairs, sign zone with private keys, publish signed zone with public keys, change keys re-sign (or resign)

Authoritative Server – External

Pass the hash of the public key (Delegation Signer (DS) to parent zone through Registrar,

TLD Registries (.com, .org)

Sign the DS of child zones

Resolver (renamed to Recursive Validator

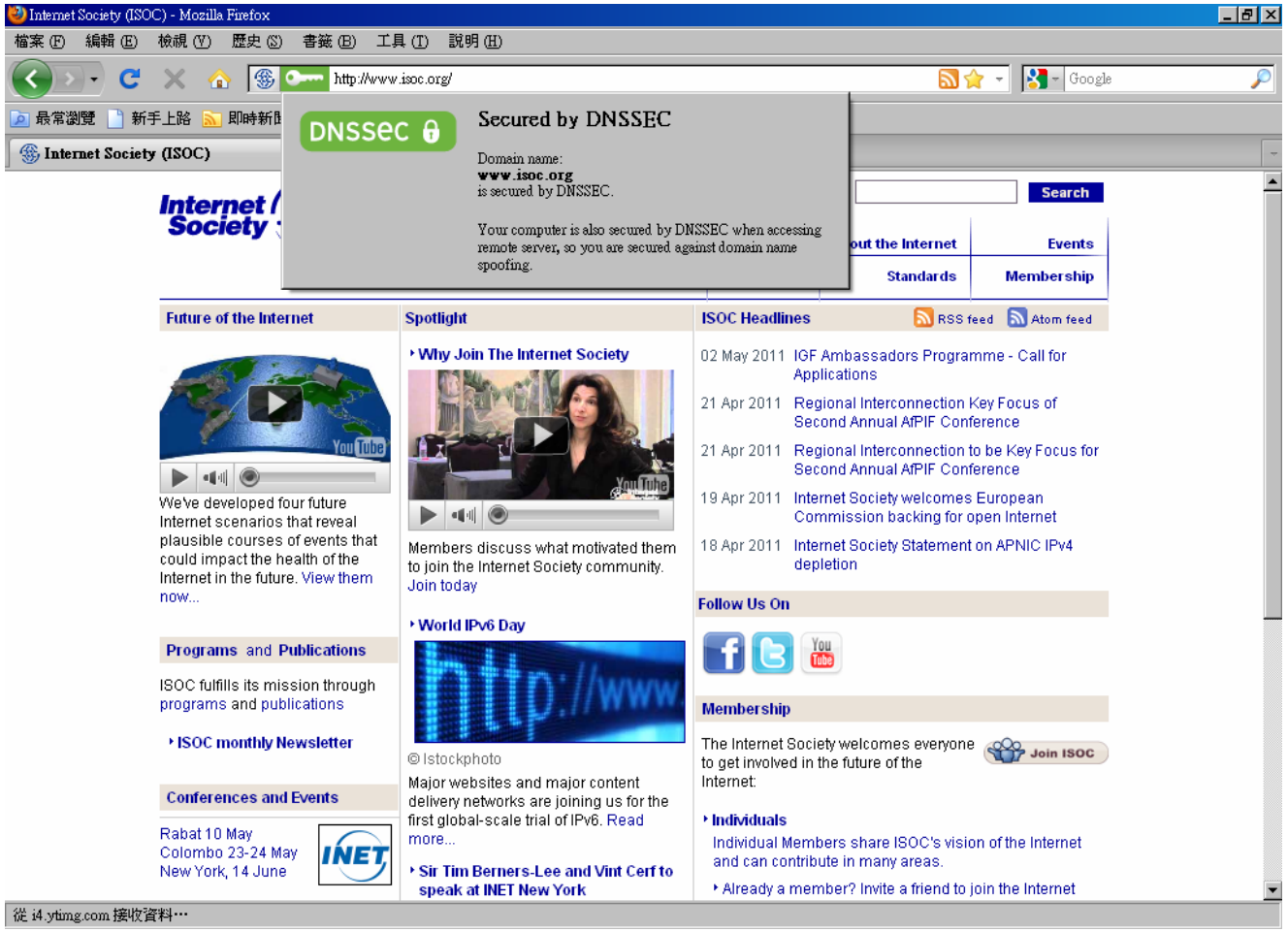
add root trust anchor(s), update trust anchor(s)

Add root trust anchor to Resolver (Bind 9.7)

/var/named/chroot/etc/named.conf

```
options {
   dnssec-validation yes;
   dnssec-enable yes;
};
trusted-keys {
"." 257 3 8
  "AwEAAagAIKlVZrpC6Ia7gEzahOR+9W29euxhJhVVLOyQbSEW0O8gcCjF
   FVQUTf6v58fLjwBd0YI0EzrAcQqBGCzh/RStIoO8g0NfnfL2MTJRkxoX
   bfDaUeVPQuYEhg37NZWAJQ9VnMVDxP/VHL496M/QZxkjf5/Efucp2gaD
   X6RS6CXpoY68LsvPVjR0ZSwzz1apAzvN9dlzEheX7ICJBBtuA6G3LQpz
   W5hOA2hzCTMjJPJ8LbqF6dsV6DoBQzgul0sGIcGOYl7OyQdXfZ57relS
   Qageu+ipAdTTJ25AsRTAoub8ONGcLmqrAmRLKBP1dfwhYB4N7knNnulq
   QxA+Uk1ihz0="; };
```

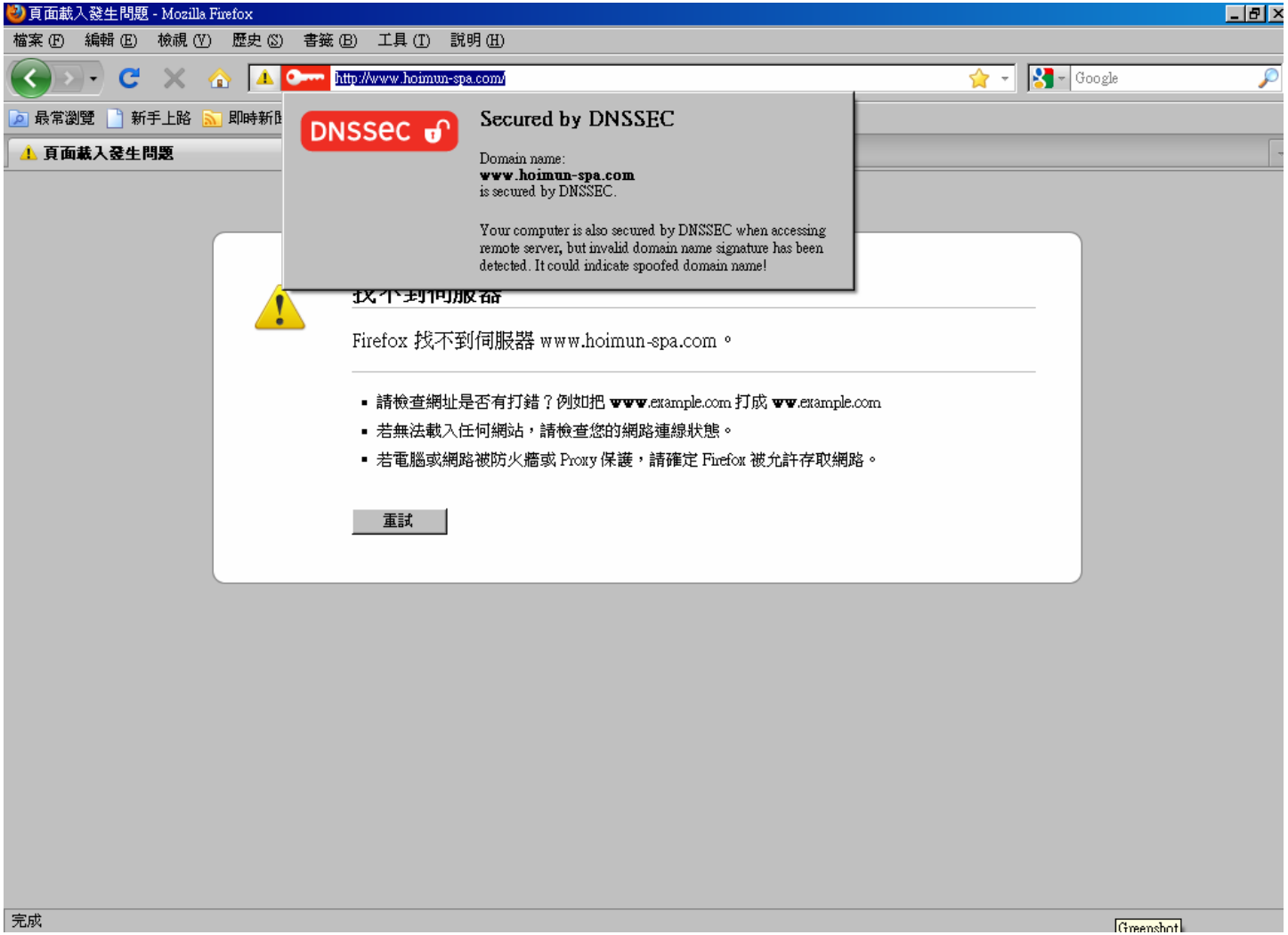
Successful access to a secure zone



Criteria:

- ✓Zone properly signed
- ✓Browser config with dnssec validator
- ✓Browser uses a DNSSEC-aware resolver with root trust anchor

Resolvers ban access to websites due to invalid signatures



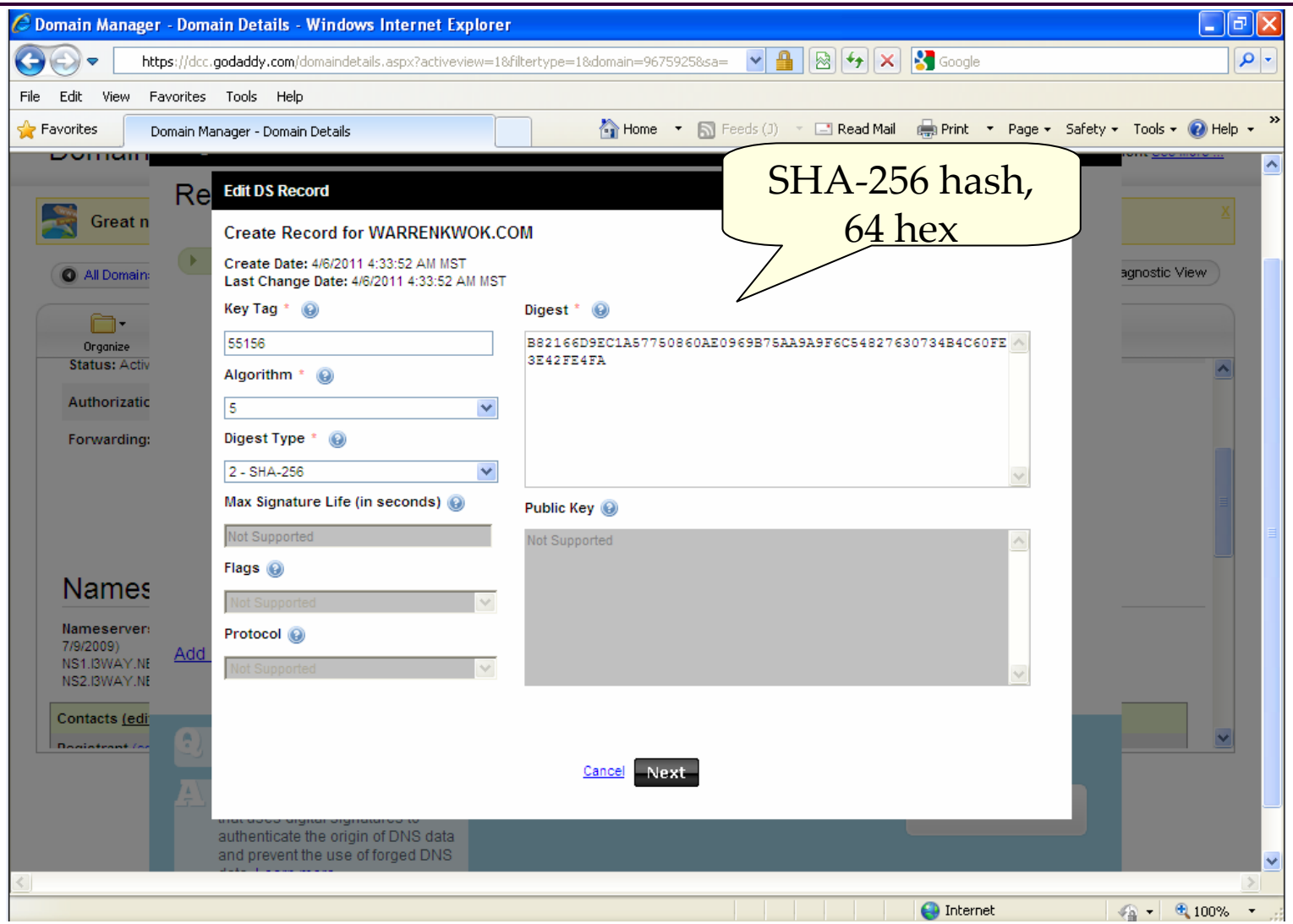
Readiness of DNSSEC

- Root zone activated on 15 July 2010
- 72 TLDs running DNSSEC
- For Hong Kong

  .asia activated in Nov 2010

  .hk will be ready by end of 2011
- Hong Kong ISPs or webhosting companies can now serve DNSSEC for companies with domain .com, .net, .asia, or .org
- Request is LOW, acceptance is LOW

Registrar Interface for DS Submission (.com)



Conclusions

- Hong Kong has maintained strong resilience in common critical facilities
- Source Address Filter can circumvent DDoS attacks based on spoofed source address
- Open resolvers is a risk to the Internet
- DNSSEC is the industry norm for securing the DNS architecture
- Acceptance of DNSSEC will grow in Hong Kong over time
- As Hong Kong enters IPv6 era, new threats and attacks targeted at IPv6 will emerge.

End

Thank You !