



Safe Browsing for Your
Customers - Enabling

DNSSEC & HTTPS

Ben Lee

Head of IT

HKIRC





About me



Ben Lee, Head of IT, HKIRC



also has the role of Information Security Officer



manages the technical and security of .hk and .香港 country code top level domain name (ccTLD)




has 17 years of experience in the domain name industry



actively participates in the Internet community of the region, e.g. CDNC and APTLD

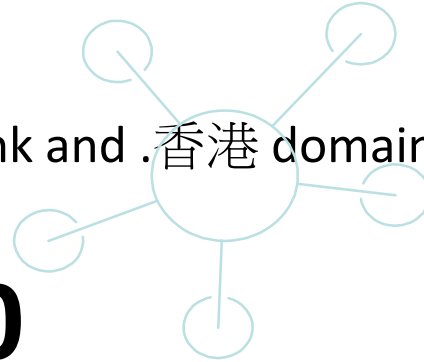


HKIRC

 HKIRC is a not-profit-distributing company limited by guarantee set up in December 2001, and designated by the Government of the HKSAR to manage and administer all Internet domain names under .hk and .香港 country-code top level domain names

 As of 1 Sep 2018, the total registration of .hk and .香港 domain names:

283,490





Security and .hk

- 🔒 HKIRC always strives to provide reliable, robust and secure services
- 🔒 Maintaining customer confidence and trust is important for .hk
- 🔒 Customers are now more security-aware, and the demand for secure internet related services is growing



“Authentication”

- Domain Name Authentication
 - “DNSSEC”
- Website Authentication
 - “https” or “SSL/TLS Cert”



Domain Name System

DNS



What is a Domain Name System?

- **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network
- “Phone book” for the Internet
- For example, **www.police.gov.hk** translates to **54.239.216.35** (IPv4) and **2600:9000:2012:d400:2:e4f8:8cc0:93a1** (IPv6)



Where are Domain Names used?

- Website URL

<https://www.hkirc.hk/GO/DNSSEC>

- Email address

info@hkirc.hk

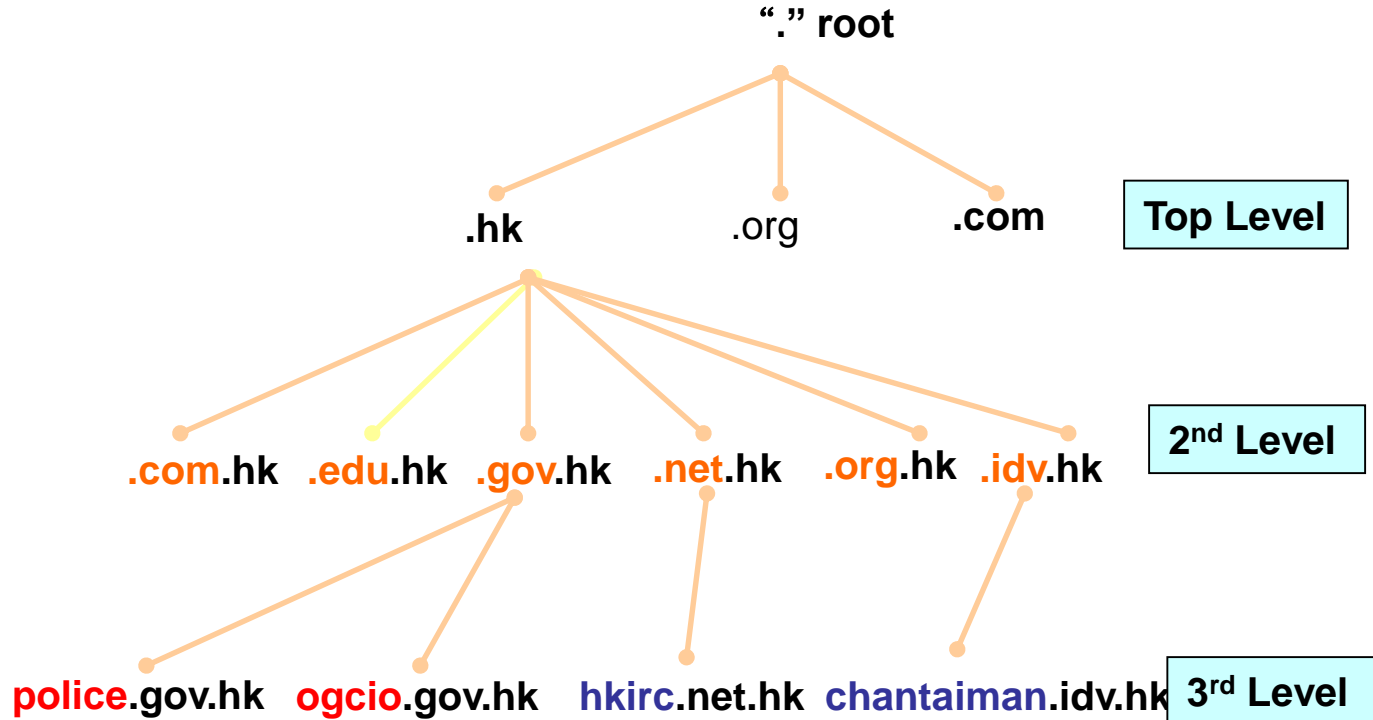


Levels of Domain Name

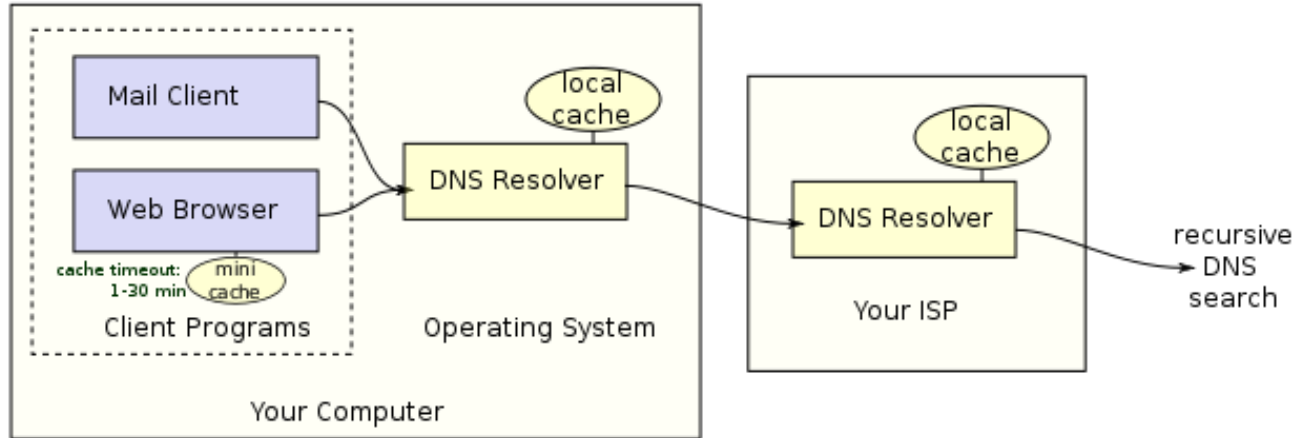
- `www.hkirc.hk.`
 - root = `.`
 - top level = `hk.`
 - 2nd level = `hkirc.hk.`
 - 3rd level = `www.hkirc.hk.`
- There could be more lower levels (sub-domain names)



Domain Name Hierarchy

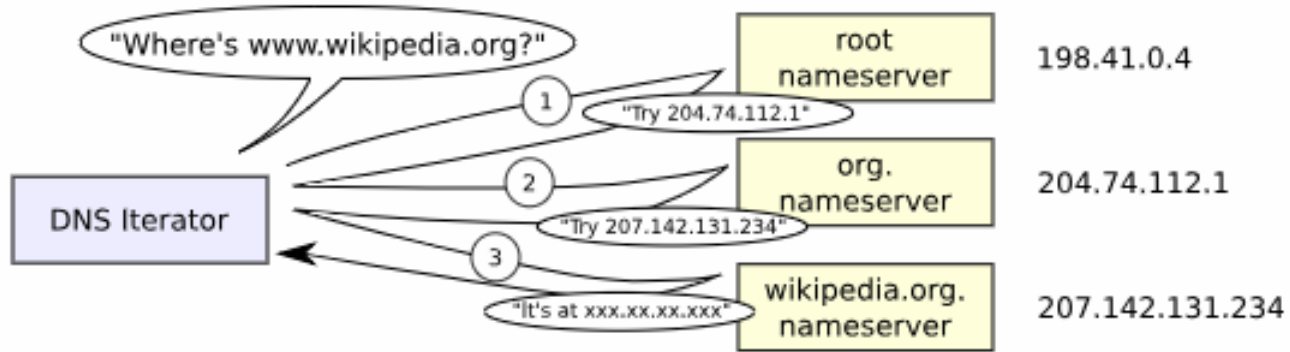


How it works



- Source: Wikipedia

How it works



- Source: Wikipedia



Why DNS is vulnerable?

- DNS was designed in the **early days** of Internet
- The DNS clients **do not check the authenticity** of the DNS answer
- Vulnerable to **man-in-the-middle (MITM) attacks**
- Much bigger impact if the Client is also a Server (i.e. **Cache poisoning** to a Cache resolver for an ISP)



Why we need to protect DNS?

DNS

- Denial of services and data access

Website (E-commerce) traffic diversion

- Theft of customer information
- Loss of revenue / reputation

Email traffic diversion

- Leakage of confidential information

DNS attacks news

SECURITY

Security expert: DNS attacks are happening

IOActive researcher Dan Kaminsky says people are looking for unpatched DNS systems and some attacks are due to a fatal vulnerability with the DNS Web address lookup system.

BY ELINOR MILLS / AUGUST 21, 2008 2:25 PM PDT



A fatal flaw with the DNS (Domain Name System) is being exploited in Internet attacks and more attacks are likely, the security researcher who discovered the flaw said on Thursday.

"I do think we are going to see attacks. I think we have been seeing attacks already going on in the field," said Dan Kaminsky, director of penetration testing for IOActive, who warned the industry about the DNS vulnerability nearly five months ago. "We're doing everything we can to mitigate and reduce its incidence."

Kaminsky mentioned a DNS-related incident with China Netcom (possibly the incident [reported by the ZD Net Zero Day blog](#)), but said it wasn't clear



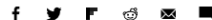
Dan Kaminsky

SECURITY

Anonymous claims DNS attacks against Symantec, Apple, Microsoft

Anonymous Sri Lanka says that it breached the DNS servers of several major companies, including Symantec, Apple, Facebook, Skype, and Cisco.

BY LANCE WHITNEY / AUGUST 31, 2011 9:40 AM PDT



The Sri Lankan branch of Anonymous claims to have hacked into the DNS servers of Symantec, Apple, Facebook, Microsoft, and several other large organizations over the past few days.

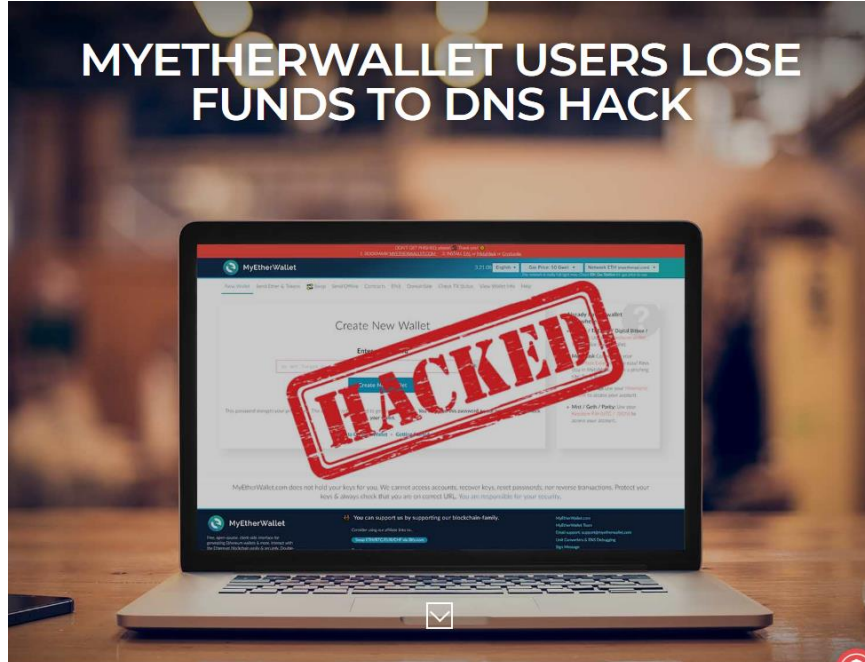
Posting the news and records of its exploits on [Pastebin](#), the group is taking credit for launching "DNS Cache Snooping" attacks against its victims.



DNS cache snooping is the process whereby hackers can query a DNS server to find out which domain names are being resolved into IP addresses.

[DNS cache poisoning](#) is a method through which hackers are able to insert malicious and fake records into the cache of DNS servers. As a result, the hackers can then spoof a response to a DNS query, forcing users to go to a phony Web site instead of the real one.

USD150k Ethereum Coins Stolen



OSATO AVAN-NOMAYO · APRIL 24, 2018 · 6:30 PM

FEATURED COMPANIES



Security

AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet

Audacious BGP seizure of Route 53 IP addys followed by crypto-cyber-heist

By Shaun Nichols in San Francisco 24 Apr 2018 at 19:04

42

SHARE ▼





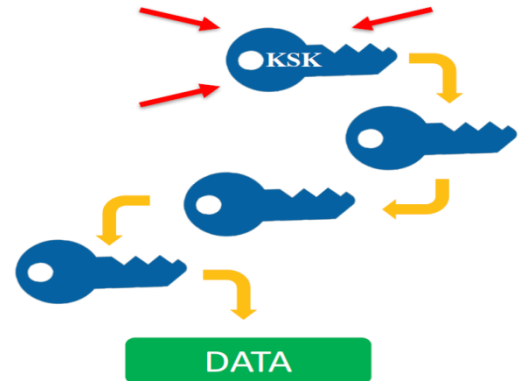
Domain Name System Security Extensions

DNSSEC

DNSSEC Solution




Domain Name System Security Extensions (DNSSEC) :

- DNSSEC uses **digital signatures** to assure that information is correct and came from the right place.
- DNSSEC can assure users they are **reaching the right location**.
- DNSSEC provides cryptographic information that can be used to verify that DNS information:
 - came from the proper source and
 - it was not changed enroute
- It builds a Chain of Trust:
 - Each level signs the key of the next level
 - Until the chain is complete



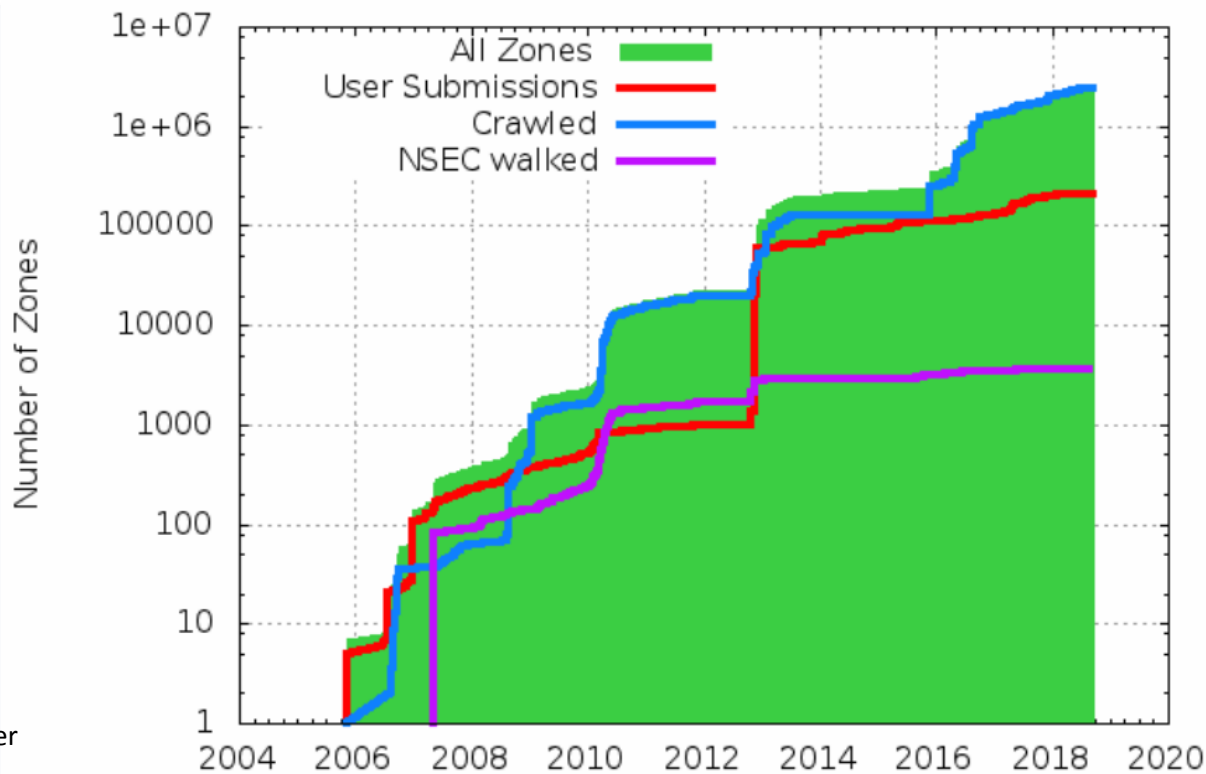
Key Benefits of Using DNSSEC

Results:

- Provide an **extra level of security** to improve reliability, trustworthy and quality of the DNS 
- Help ensure that internet users will be **directed to the expected website** or service when they enter a domain name into their browser 
- Safeguard the internet environment and **strengthen trust in the Internet** as a whole 

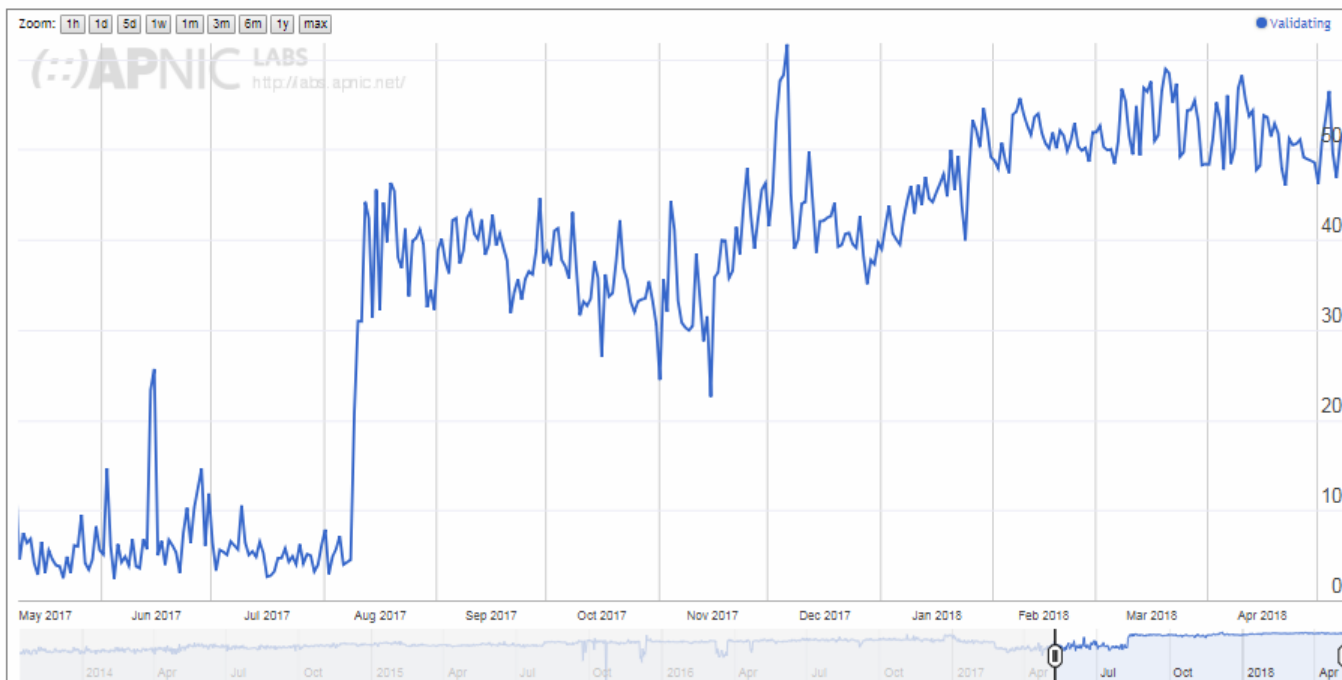


Internet DNSSEC enabled zones: 2,072,588



Verisign
SecSpider

DNSSEC Validation in Hong Kong : 52.78%

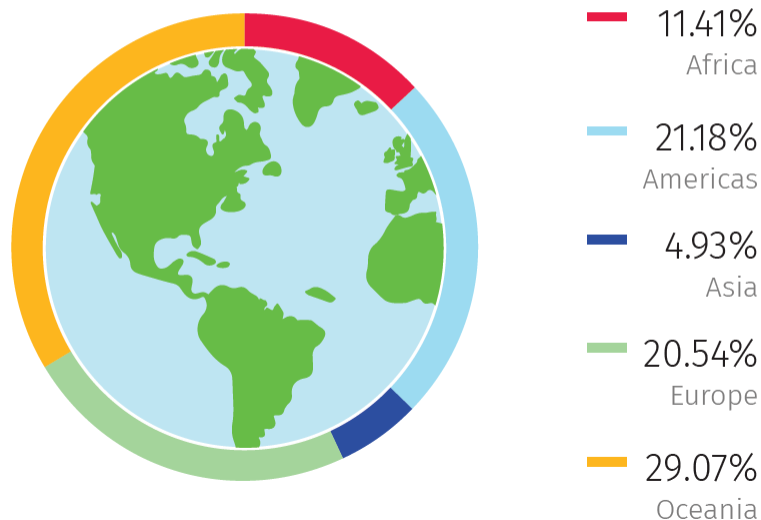


stats.labs.apnic.net/dnssec/HK (Apr 2018)

DNSSEC Validation in Hong Kong : 52.78%

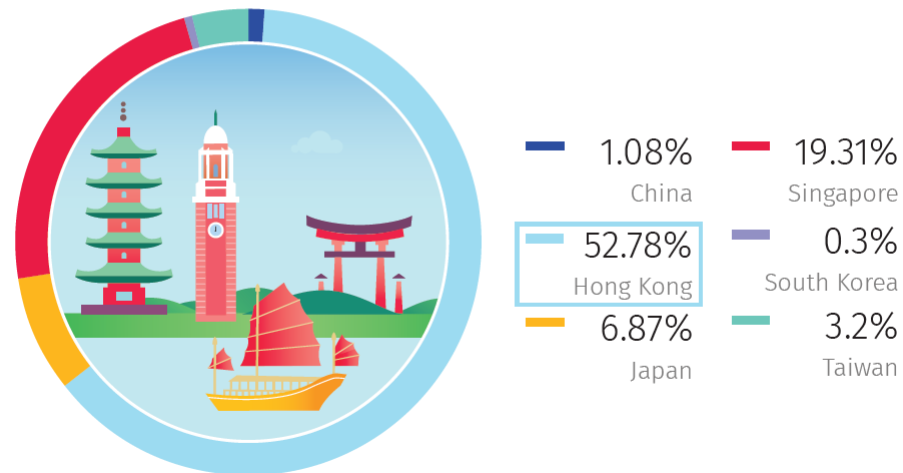
DNSSEC Validation in the World

As of 19 April 2018

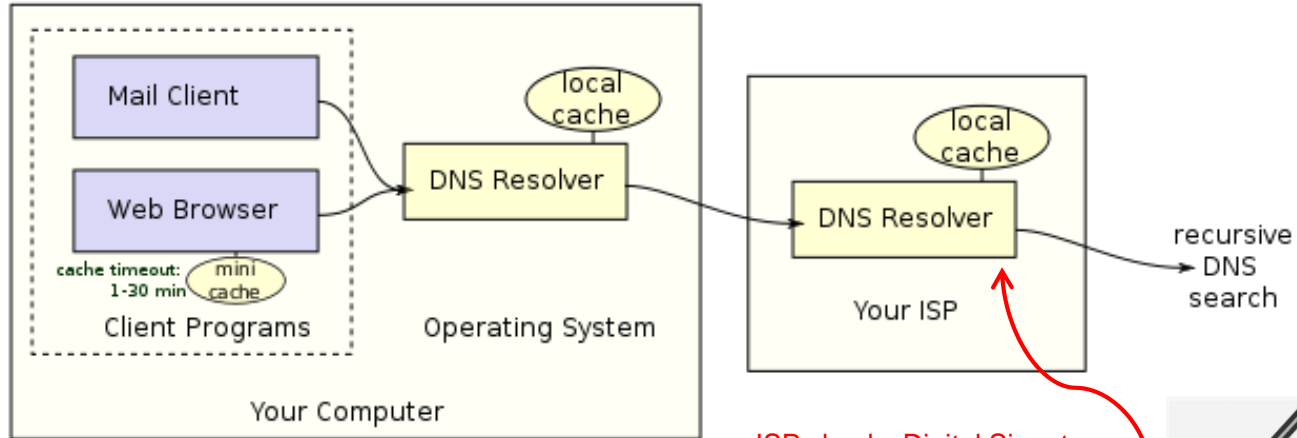


DNSSEC Validation in Asia

As of 19 April 2018



How it works



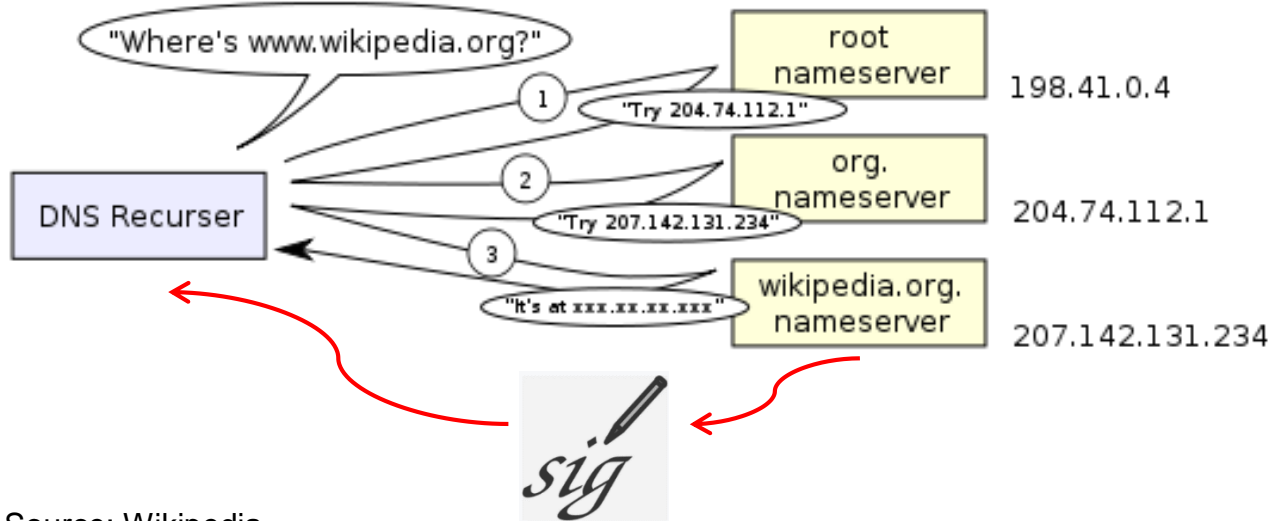
- Source: Wikipedia

ISP checks Digital Signature

- If ok, pass to computer
- If not ok, protect the computer and block access



How it works



- Source: Wikipedia



What to do to enable DNSSEC?

DNS Hosting

- Digitally sign domain names in name servers
- Build DNSSEC “chain-of-trust” - by submitting your public key info (DS) to parent zone

Internet Access

- Enable DNSSEC validation in DNS resolvers
- Ready for the ICANN KSK rollover - by installing both old KSK-2010 and new KSK-2017, enable auto KSK installation (RFC5011)

DNSSEC – enabling guide

- DNS hosting
 - Example Architecture and Design
 - Example Configuration
- Internet Access
 - DNS validation in DNS resolver
- Testing tools
- Implementation considerations

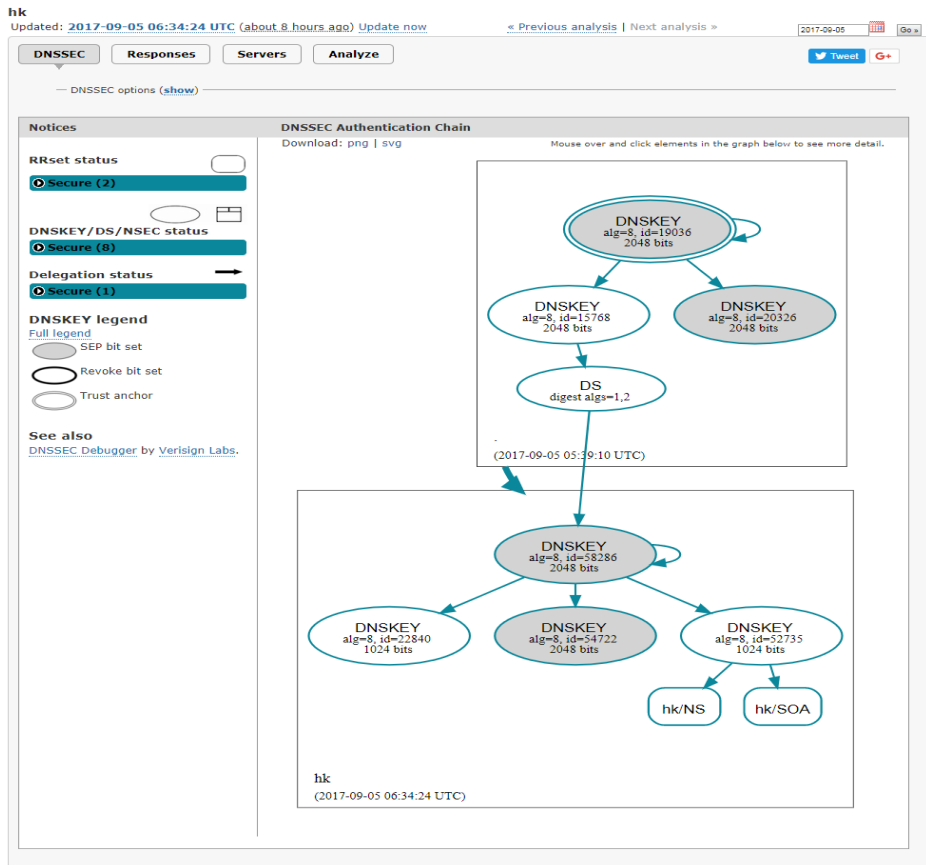




DNSSEC Signing – Testing Tools

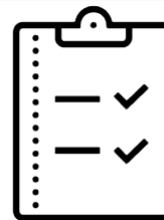
- Web tools to check DNSSEC signing:

- <http://dnssec-debugger.verisignlabs.com>
- <http://dnsviz.net>
- <https://internet.nl/>
- <https://www.zonemaster.fr>



DNSSEC Validation Deployment and Testing

- Multiple resolvers? Turn on validation one-by-one and monitor the effect
- HKIRC had set up 3 examples to facilitate DNSSEC resolvers testing



State	Testing Domain	Explanations
Insecure	disabled.dnssec.hkirc.hk	not DNSSEC enabled
Secure	enabled.dnssec.hkirc.hk	DNSSEC enabled and verification is successful
Bogus	failed.dnssec.hkirc.hk	DNSSEC enabled and verification is failed

Work Together for a Safer Place

- DNSSEC service for .hk domain names has been made **available since January 2018**
- Number of DNSSEC enabled .hk increasing at an average rate of **11.3%** per month
- Over **1,400 Government websites** have DNSSEC enabled.





Hypertext Transfer Protocol Secure

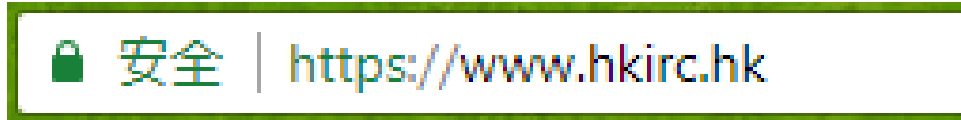
HTTPS

What is https?

- Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP) for secure communication over a computer network
- Data is encrypted using Transport Layer Security (TLS), or formerly, its predecessor, Secure Sockets Layer (SSL).

What can https do?

- Encrypt data in transit, prevent data theft and snooping
- Authenticate a website
- When protected https, browser display 'https' with a lock icon





Who will need https?

- All websites need https
 - Personal data
 - HK PCPD Privacy Ordinance
 - EU General Data Protection Regulation (GDPR)
 - E-commerce and transaction
 - Username and password
 - Credit card number



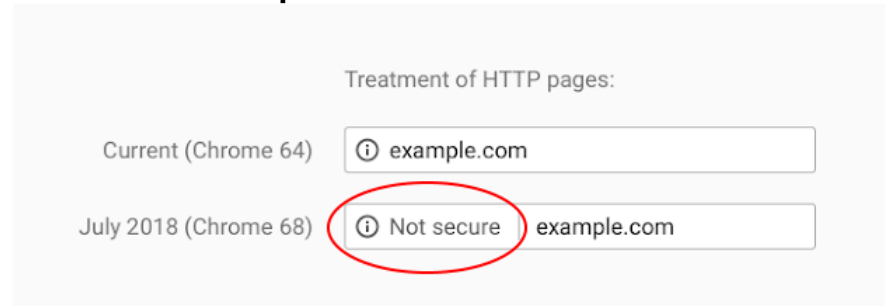
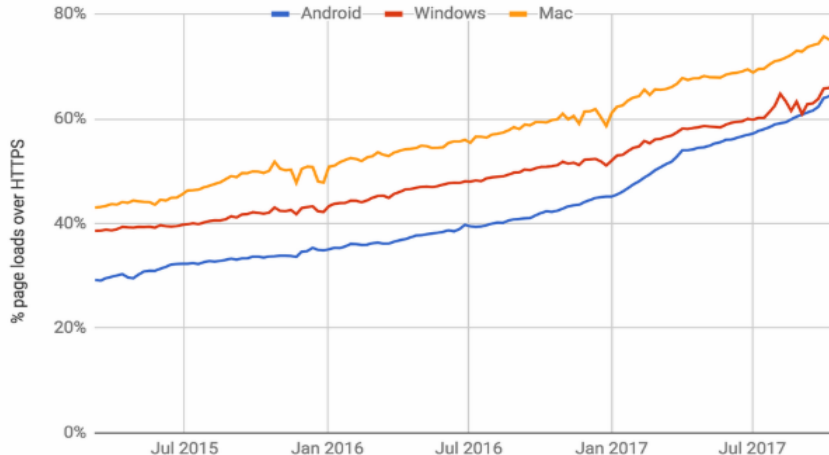
Tipping point of https

51.8%

68%

- “Over 50% of Top Global Sites (1 mil.) Now on HTTPS” - *Scott Helme*

- 68% of Chrome traffic on Android and Windows was https encrypted
- Google Chrome 68
 - no https = “Not secure”



“Why No HTTPS” website



Hong Kong

The Most Popular Websites Loaded Insecurely

Each of the following 50 websites is sorted by [Alexa rank](#) and loads over an insecure connection without redirecting to a secure, encrypted connection.

Alexa Rank	Website
------------	---------

1,159	a [REDACTED]
-------	------------------------------

2,182	e [REDACTED]
-------	------------------------------

2,807	o [REDACTED]
-------	------------------------------


4,976	n [REDACTED]
-------	------------------------------

5,184	c [REDACTED]
-------	------------------------------

How much?



- Range from Free of Charge to a few thousands
- Various types of SSL Cert
 - Domain Validated SSL
 - Organization Validated SSL
 - Extended Validation SSL



 Your Company www.yourcompany.hk

Chrome



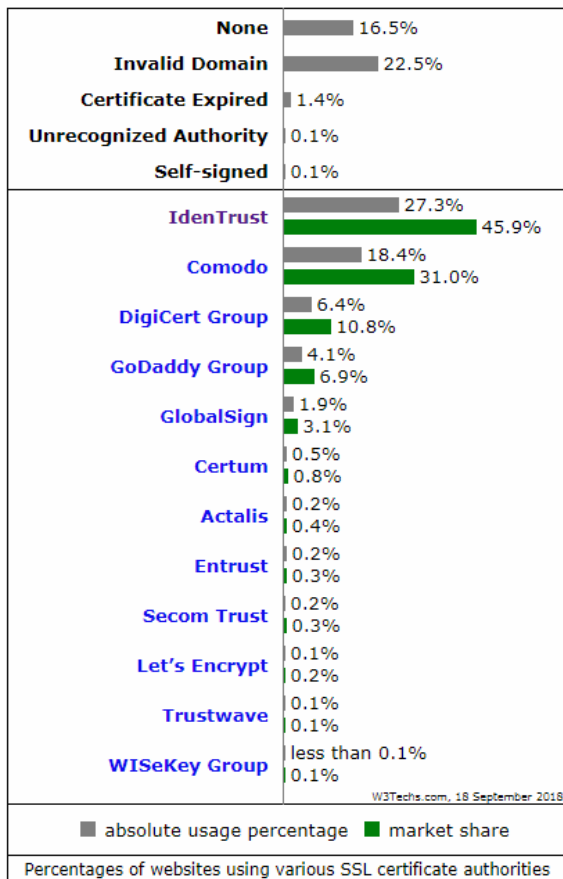
  Your Company www.yourcompany.hk

Firefox

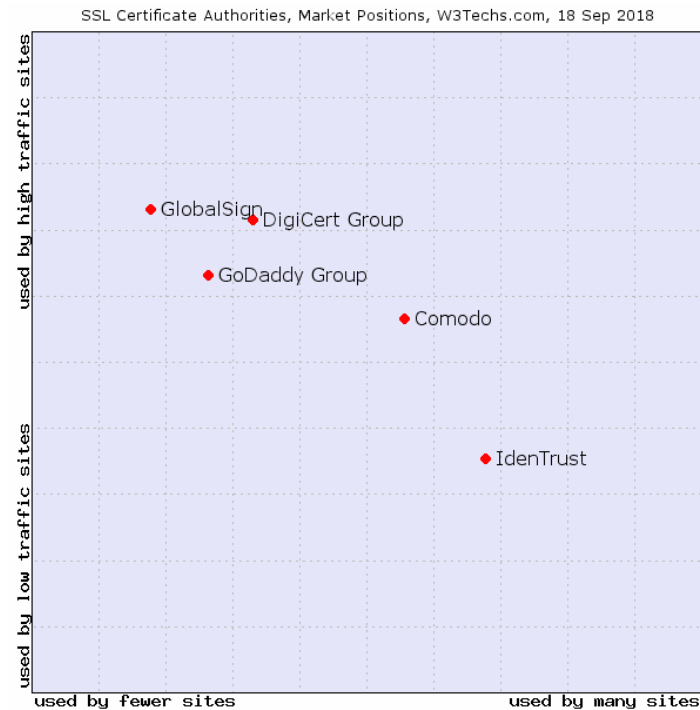


Your Company  www.yourcompany.hk

Safari



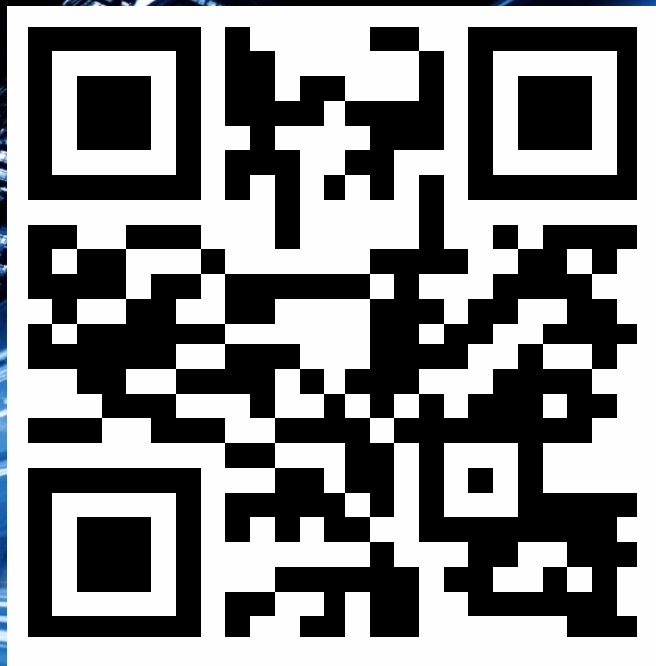
CA market share (W3Techs)





Let's Get Started!

<https://www.hkirc.hk/GO/DNSSEC>





Additional Info

- HKIRC DNSSEC info page
<https://www.hkirc.hk/GO/DNSSEC>
- RFC6781 - DNSSEC Operational Practices, Version 2:
<https://tools.ietf.org/rfc/rfc6781.txt>
- NIST, Secure Domain Name System (DNS) Deployment Guide:
<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf>
- DNSSEC Operations: Setting the Parameters: <http://www.dnssec-deployment.org/wp-content/uploads/sites/2/2012/02/Setting-the-Parameters-20091124032.pdf>

Additional Info

- DNSSEC Signing Testing Tools
 - <http://dnssec-debugger.verisignlabs.com>
 - <http://dnsviz.net>
 - <https://internet.nl/>
 - <https://www.zonemaster.fr>

Additional Info

- DNSSEC validation testing domain names
 - <http://disabled.dnssec.hkirc.hk>
 - <http://enabled.dnssec.hkirc.hk>
 - <http://failed.dnssec.hkirc.hk>



Thank you!

My City
My Domain

