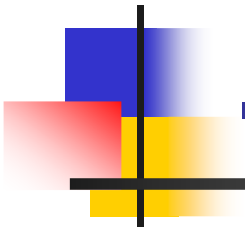


.TW DNSSEC trial experience

Nai-Wen Hsu
TWNIC

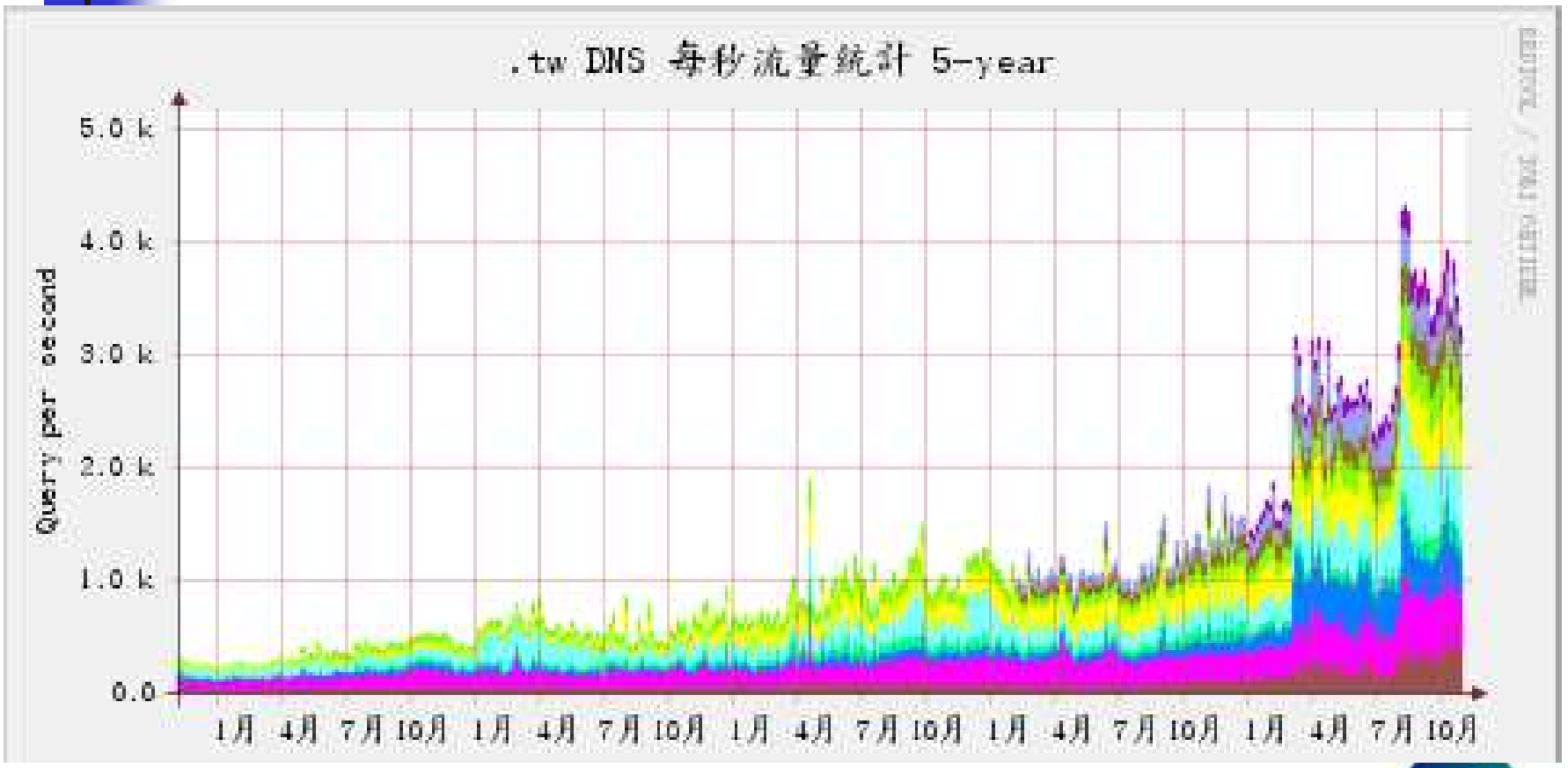
Cairo ICANN

Content

- Background
- DNSSEC trial system
- Performance
- Something need to improve
- Time schedule

www.twnic.net.tw

.TW DNS Query Traffic



www.twnic.net.tw

Why we need DNSSEC

- msn.com.tw
- DNS cache poisoning and vulnerability

Real Case - msn.com.tw

- Before 6-Sep-07 msn.com.tw DNS
  - dns.cpmsft.net
    - it is a typo, should be dns.cp.msft.net
  - dns1.cp.msft.net
  - dns1.tk.msft.net
  - dns1.dc.msft.net
  - dns3.uk.msft.net

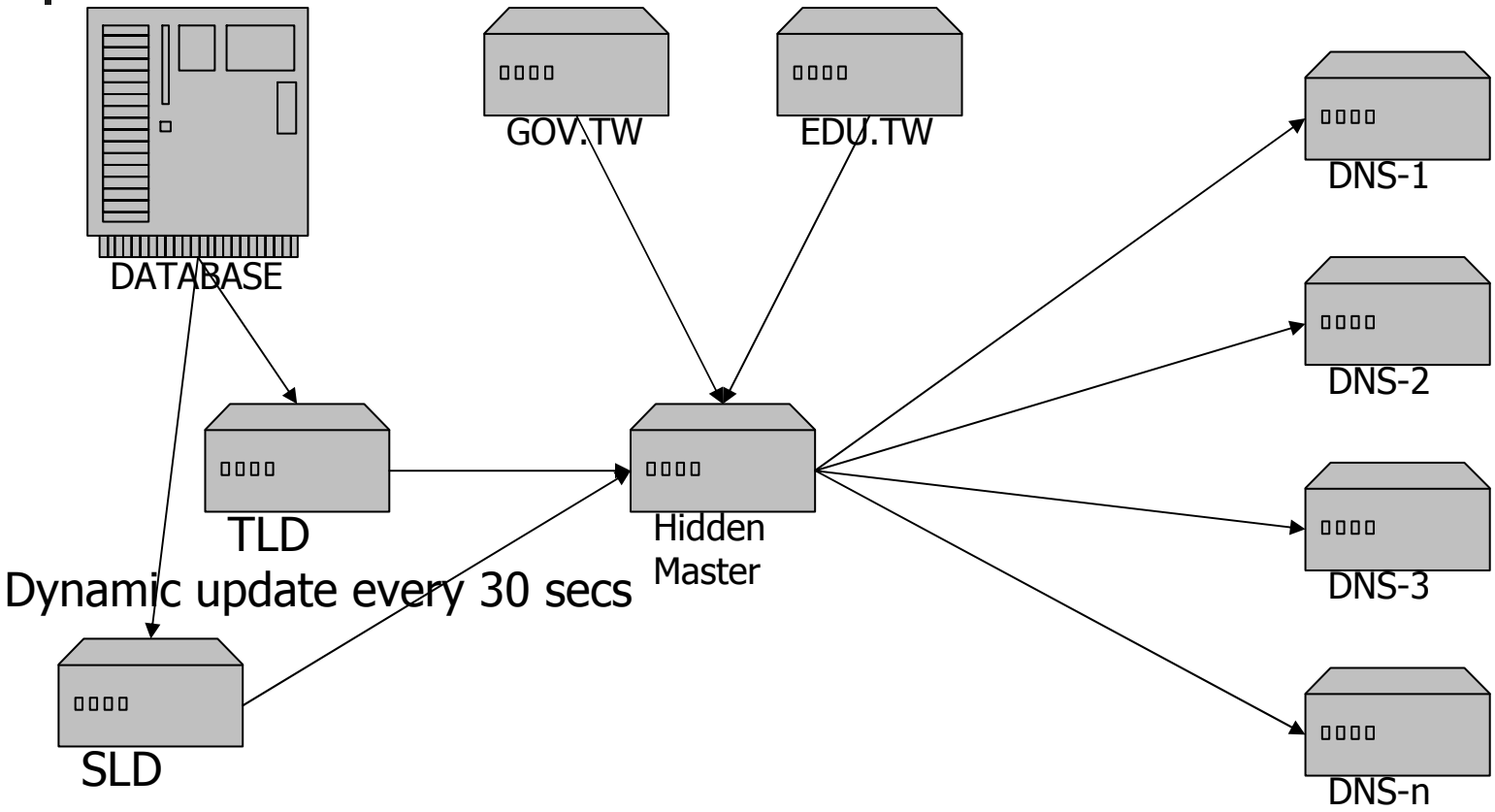
msn.com.tw

- The error last for many years, because DNS resolver will try next server if one is no response
- Until someone found the error and register cpmsft.net, setup a DNS to hijack www.msn.com.tw traffic
- Detail information
  - http://www.julianhaight.com/msnhack.html

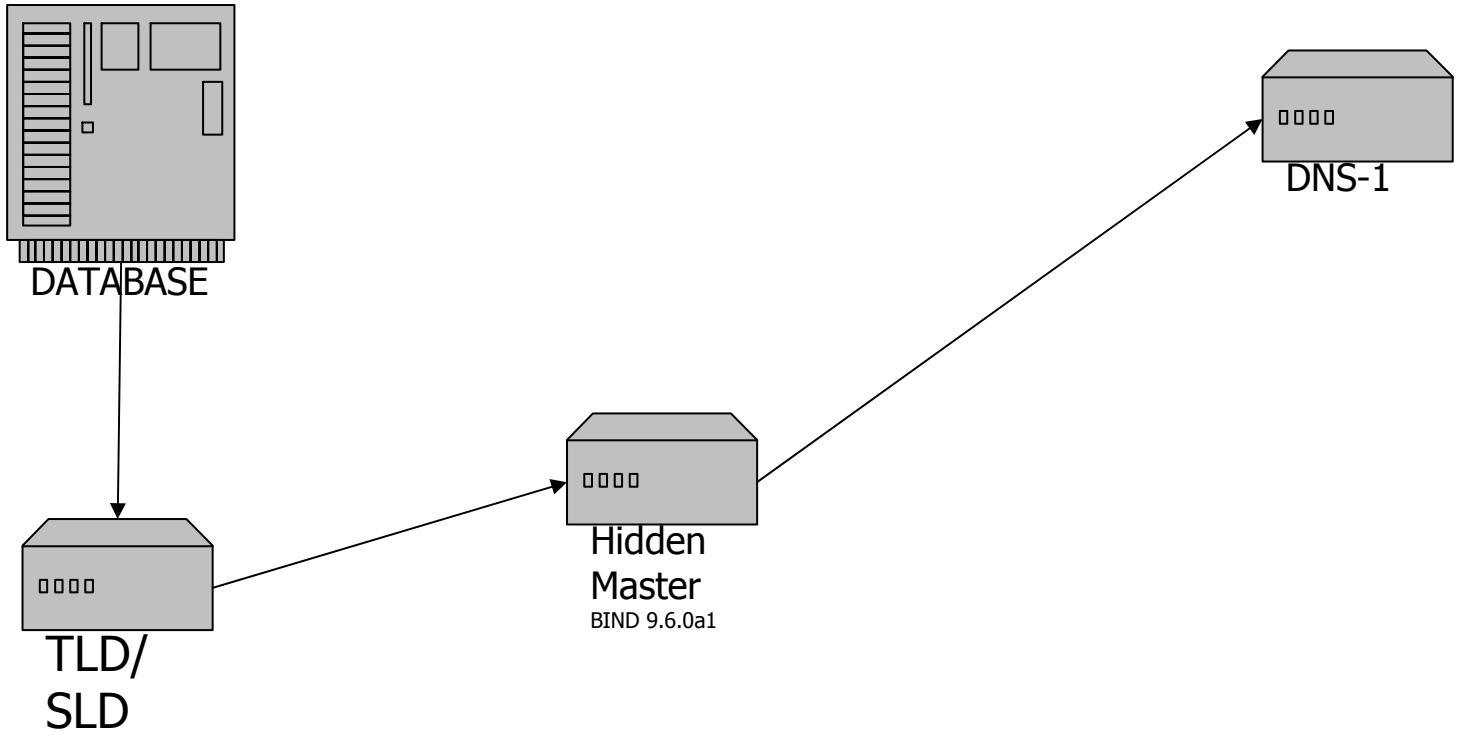
DNS cache poisoning

- Vulnerability Note VU#800113
  - Multiple DNS implementations vulnerable to cache poisoning
  - Insufficient transaction ID space
    - It leads to a ‘birthday attack’
- VU#484649
- VU#252735
- VU#927905

DNS server structure



DNSSEC trial system



www.twnic.net.tw

Key component of DNSSEC trial system

- DNS server: BIND 9.6.0a1 (ISC)
- Key Management: maintkeydb (RIPENCC)
- Key generator: dnssec-keygen (ISC)
- Zone file signer: dnssec-signzone (ISC)

DNSSEC zone generation

- 4 dual-core CPUs server
- Parallel generate zone files from database every 1 hour

www.twnic.net.tw

Key rollover schedule

- Key Sign Key rollover every 1 year
- Zone Sign Key rollover every 1 month
  - There are 8 zones in TWNIC, rollover 1 ZSK every 3 or 4 days

Performance (BIND 9.6.0a1)

	NSEC3	NSEC	Without DNSSEC
Create zone files	25min26sec	21min42sec	2min
Zone file size	115M	97M	20M
Query time	-	6.02 ms	3.47 ms

Something need to improve

- Key management
  - Automatic key rollover
  - Manually change key for security
  - Key distribution
- Dynamic update
  - Performance issue, it take a long time to update whole zone file

Key maintenance

- When key change, you must distribute the public key to end user
- How to distribute the public key
  - DNSSEC Lookaside Validation [RFC4431]
  - Root server enable DNSSEC

Incremental update

- It take too long to update whole zone file
- Incremental update is a solution to solve the performance issue
- We will enable incremental update on DNSSEC trial system in the near feature

Time schedule

- Open trial if
  - BIND 9.6 beta release
- We expect to implement DNSSEC on .TW zone in one or two years when
  - Root servers enable DNSSEC
  - BIND 9.6 production release

www.twnic.net.tw

Thanks
Any Question?

www.twnic.net.tw