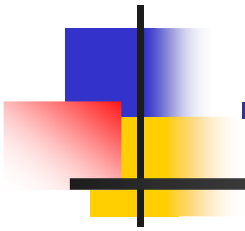


.TW DNSSEC trial experience

Nai-Wen Hsu
TWNIC
2007 ICANN LA meeting

Content

- Why TWNIC want to implement DNSSEC
- Pro and con of DNSSEC
- Time schedule

www.twnic.net.tw

Why need DNSSEC

- msn.com.tw
- DNS Poisoning and BIND vulnerability

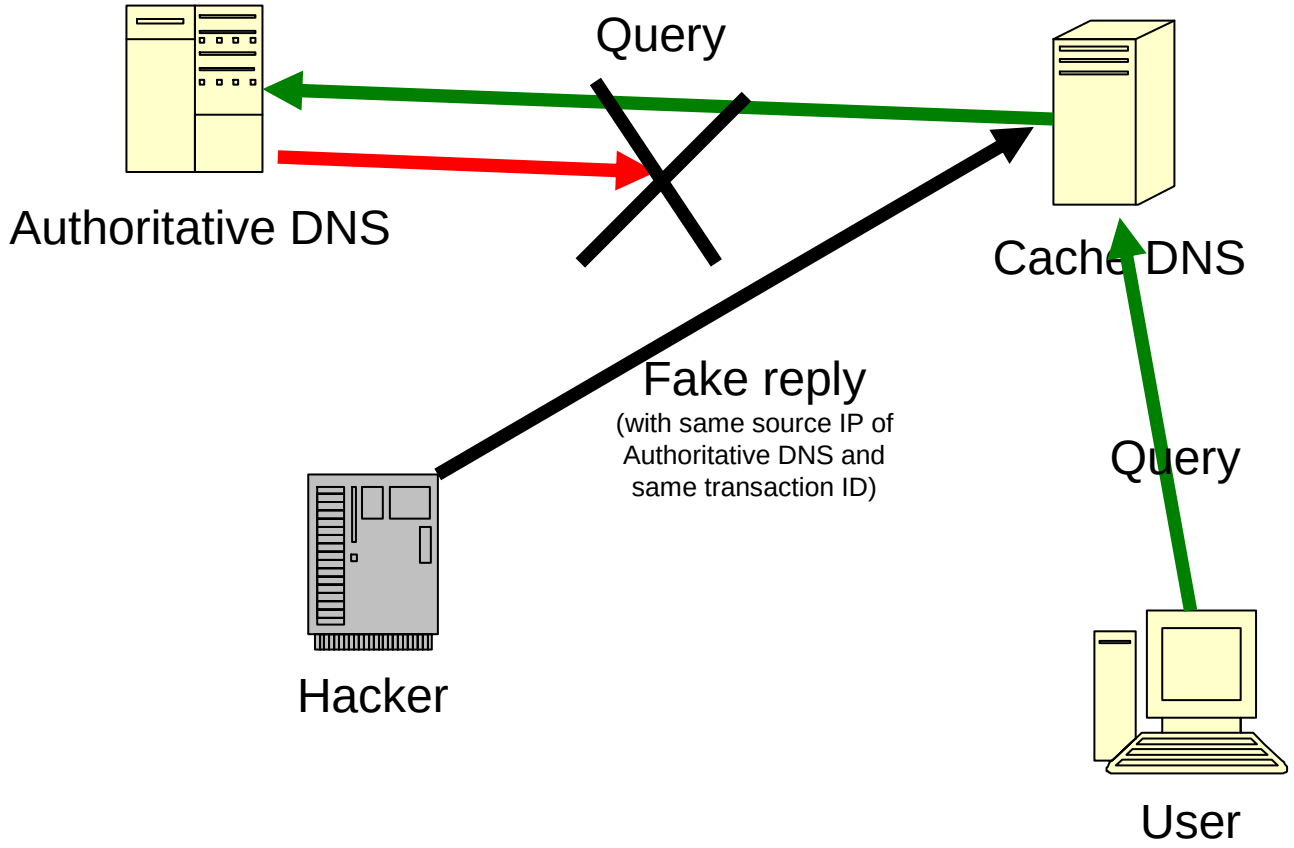
Real Case - msn.com.tw

- Before 6-Sep-07 msn.com.tw DNS
  - dns.cpmsft.net
    - it is 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



DNS cache poisoning

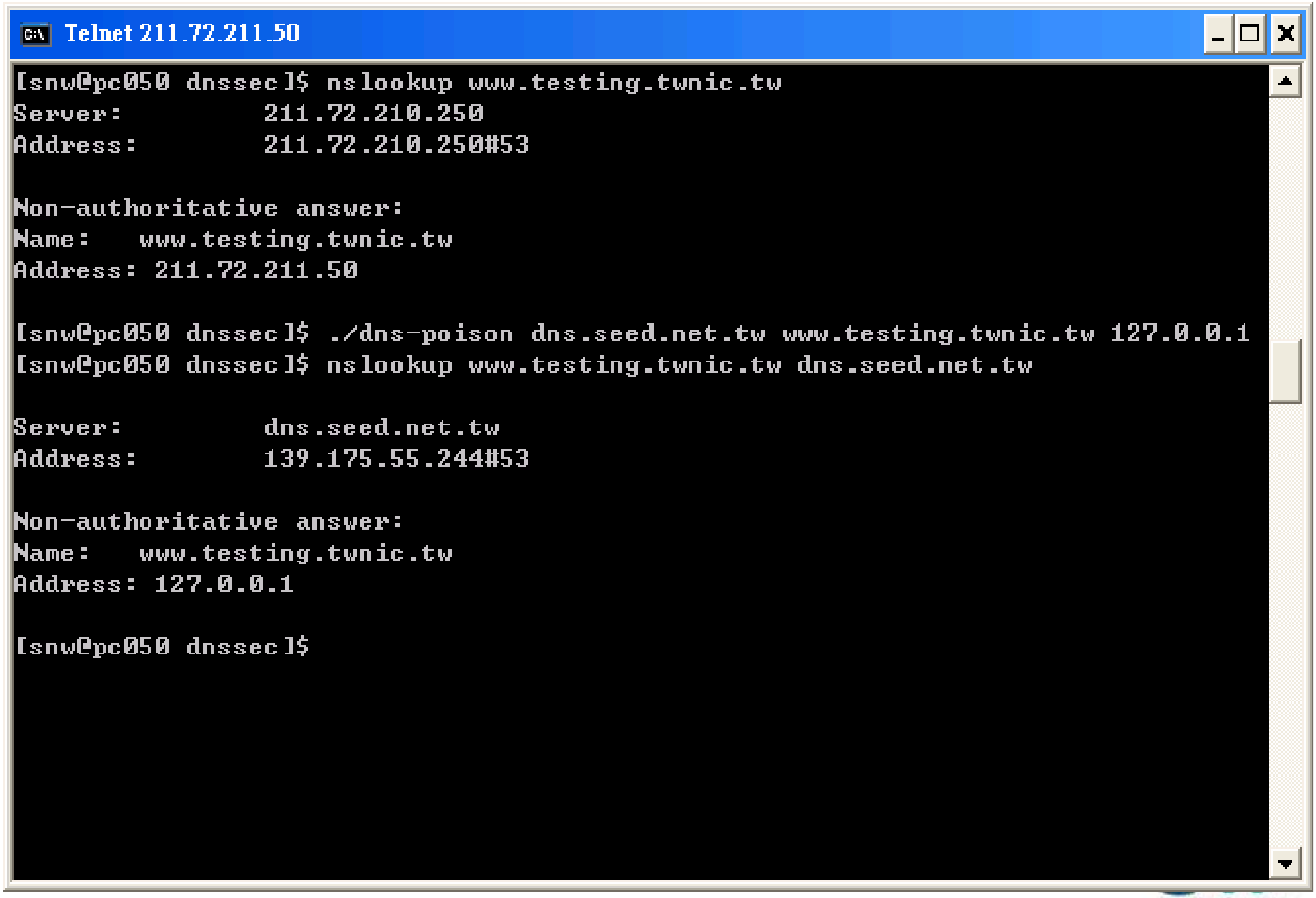
- DNS protocol use transaction ID to verify authenticity
- Transaction ID is 16 bits
  - n spoofed replies for one query probability of success is n / 65535
- Is it secure?

Birthday Attack

- How many people in an office that two or more share the same birthday with probability is greater than 50%
  - ANS: 23
  - Simply calculate 1- P(n)
  - P: probability of n people not having the same birthday
  - 1-(365-0/365)*(365-1/365)*…*(365-(n-1))/365

DNS Cache Poisoning

- DNS transaction ID: 1~65535
- Send 302 questions and 302 replies then you have the probability of 50% success
- Send 550 questions and 550 replies then you have the probability of 90% success
- Send 950 questions and 950 replies then you have the probability of 99.9%


Telnet 211.72.211.50
[snw@pc050 dnssec]$ nslookup www.testing.twnic.tw
Server: 211.72.210.250
Address: 211.72.210.250#53
Non-authoritative answer:
Name: www.testing.twnic.tw
Address: 211.72.211.50
[snw@pc050 dnssec]$ ./dns-poison dns.seed.net.tw www.testing.twnic.tw 127.0.0.1
[snw@pc050 dnssec]$ nslookup www.testing.twnic.tw dns.seed.net.tw
Server: dns.seed.net.tw
Address: 139.175.55.244#53
Non-authoritative answer:
Name: www.testing.twnic.tw
Address: 127.0.0.1
[snw@pc050 dnssec]$

BIND vulnerability

- CVE-2007-2926 [2007.07.24]
  - BIND 9: cryptographically weak query IDs
- CVE-2007-2930 [2007.08.29]
  - BIND 8: cryptographically weak query IDs
- ➔The transaction ID of BIND is predictable

SANS Top-20 Internet Security Attack Targets

- **Cross-Platform Applications**
  - C1. Web Applications
  - C2. Database Software
  - C3. P2P File Sharing Applications
  - C4. Instant Messaging
  - C5. Media Players
  - C6. DNS Servers
  - C7. Backup Software
  - C8. Security, Enterprise, and Directory Management Servers

What does DNSSEC protect?

- Data spoofing and corruption
- Man in the middle attack
  - Each Resource Record in DNS server with a digital signature
  - Resolver verifies the signature, if it is correct, response to the end user's application, otherwise not

What DNSSEC does NOT do

- It does not provide confidentiality of DNS responses
- it does not protect against DDOS attacks
- It does not provide authorization

How DNSSEC protect zone data

- RFC4035 introduce 4 RR for DNSSEC
  - DNSKEY: contain the public key of a zone
  - RRSIG: every RRset except RRSIG signed with private key and store in RRSIG
  - NSEC: every name in zone must with NSEC RR that contain the next name and resource types of the name
  - DS: when child zone is signed, DS reference a public key in child zone to verify RRSIG

Non-DNSSEC vs DNSSEC

	With DNSSEC	Without DNSSEC
Create zone files	21min42sec	2min
Zone file size	97M	20M
Query time	6.02 ms	3.47 ms
Start named	24.6s	6.3s

Some issues with DNSSEC

- Key maintenance
- Root servers enable DNSSEC
- Zone walking

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
- How does the root servers' key get to end user and change

Key rollover

- RFC 4986: Requirements Related to DNS Security (DNSSEC) Trust Anchor Rollover
- RFC 5011: Automatic Updates of DNS Security (DNSSEC) Trust Anchors

Zone walking

- An authoritative denial of existence of a given domain name delivers as a proof the next existing domain name
- NSEC RR always point to the next RR in the zone
  - se. NSEC 0-0.se.
  - 0-0.se. NSEC 0-0-0.se.
  - 0-0-0.se. NSEC 0-0-1.se.

Zone walking

- Anyone can load whole zone file via NSEC one by one
- It is a security issue
  - Attacker/Hacker is easy to identifying the target
  - Spamer is easy to collect spam-list
- It is a privacy issue
  - Domain name→Whois→Personal information

Zone walking

- NSEC3
  - draft-ietf-dnsext-nsec3-12 DNSSEC Hashed Authenticated Denial of Existence
  - DNS server can send an "NSEC3" record instead of an NSEC record when a record is not found

Time schedule

- We expect to implement DNSSEC on .TW zone in one or two years
  - NSEC3 publish as RFC
  - Root servers enable DNSSEC

www.twnic.net.tw

Time schedule

	Root servers enable DNSSEC	key rollover and distribution	Zone walking	End user applications
TWNIC test internal				
Open trial		X	X	
Release as service	X	X	X	

www.twnic.net.tw

Thanks
Any Question?

www.twnic.net.tw