DNSSEC
對未來網路安全的挑戰

TWNIC 許乃文

內容

- DNS簡介
- 什麼是DNSSEC/為什麼要DNSSEC
- DNSSEC原理
- DNSSEC面臨的問題
- DNSSEC的幾個觀念的澄清
- 目前推動現況

DNS簡介

- Domain Name System:一個分散、可靠、快速、Client/Server架構、可大量佈建、分層負責的資料庫查詢系統
- 全球上億部的DNS運作中，成為Internet最重要的基礎
- 新的社交網站導致大量的DNS查詢
  - 一個單一的MySpace頁面就可能產生200到300次DNS查詢
  - 一個帶有廣告的新聞網站可能產生10到15次DNS查詢

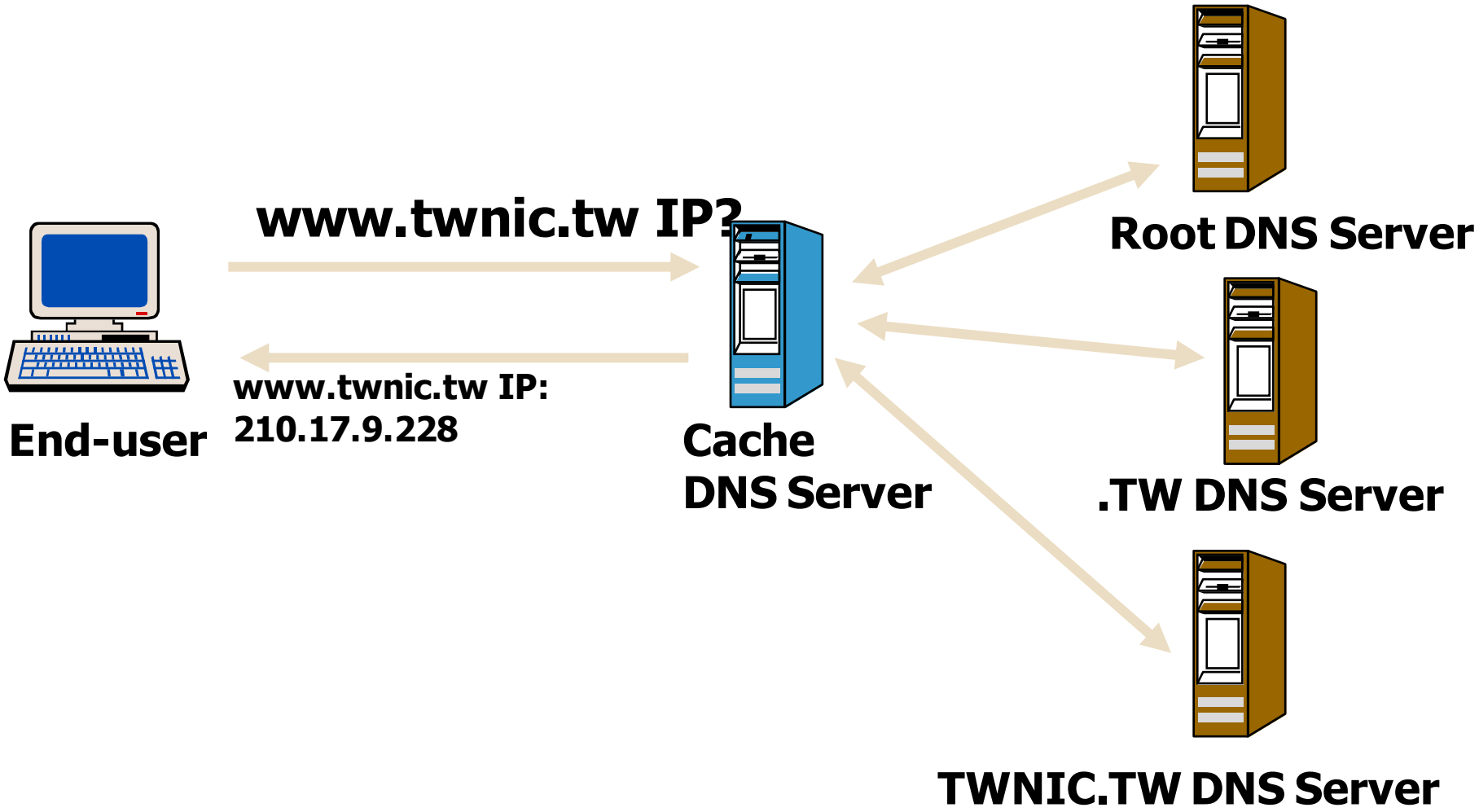
DNS弱點

- 僅用ID作為交易認證（0-65535）
  - DNS cache poisoning
- 假的DNS server
  - Men in the middle attack
- Domain hijacking
  - DNS指向被竄改

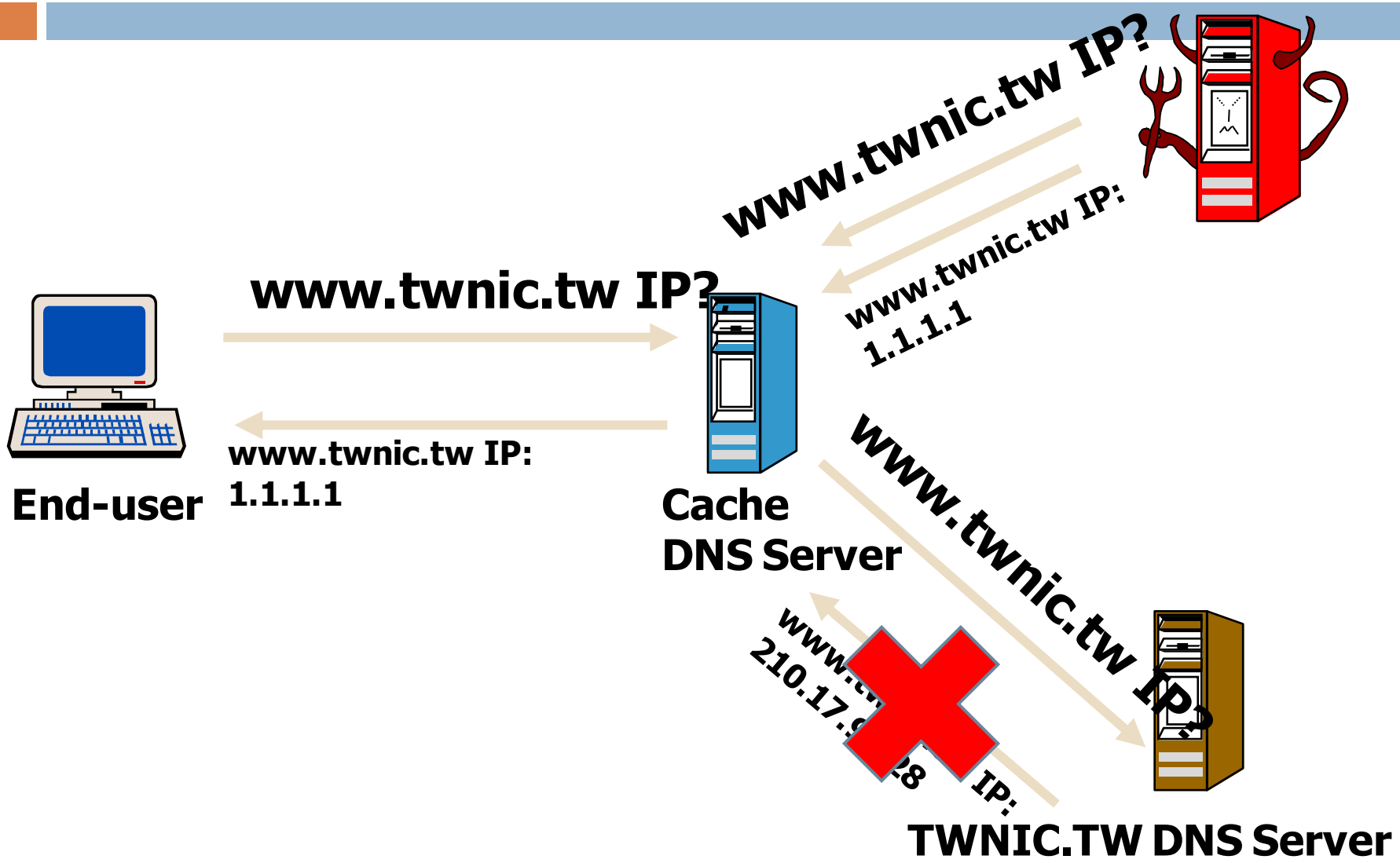
為何要DNSSEC

- 原本DNS的協定就沒有注重在安全上的問題，僅有簡單的安全機制，例如DNS spoofing是很容易的事
- DNS協定因先天存在缺失，導致DNS資料正確性受到嚴重威脅
- 2001年起IETF開始制定DNSSEC標準來解決這個問題

正常的DNS查詢


www.twnic.tw IP?
www.twnic.tw IP:
210.17.9.228
End-user
Cache
DNS Server
Root DNS Server
.TW DNS Server
TWNIC.TW DNS Server

DNS cache poisoning



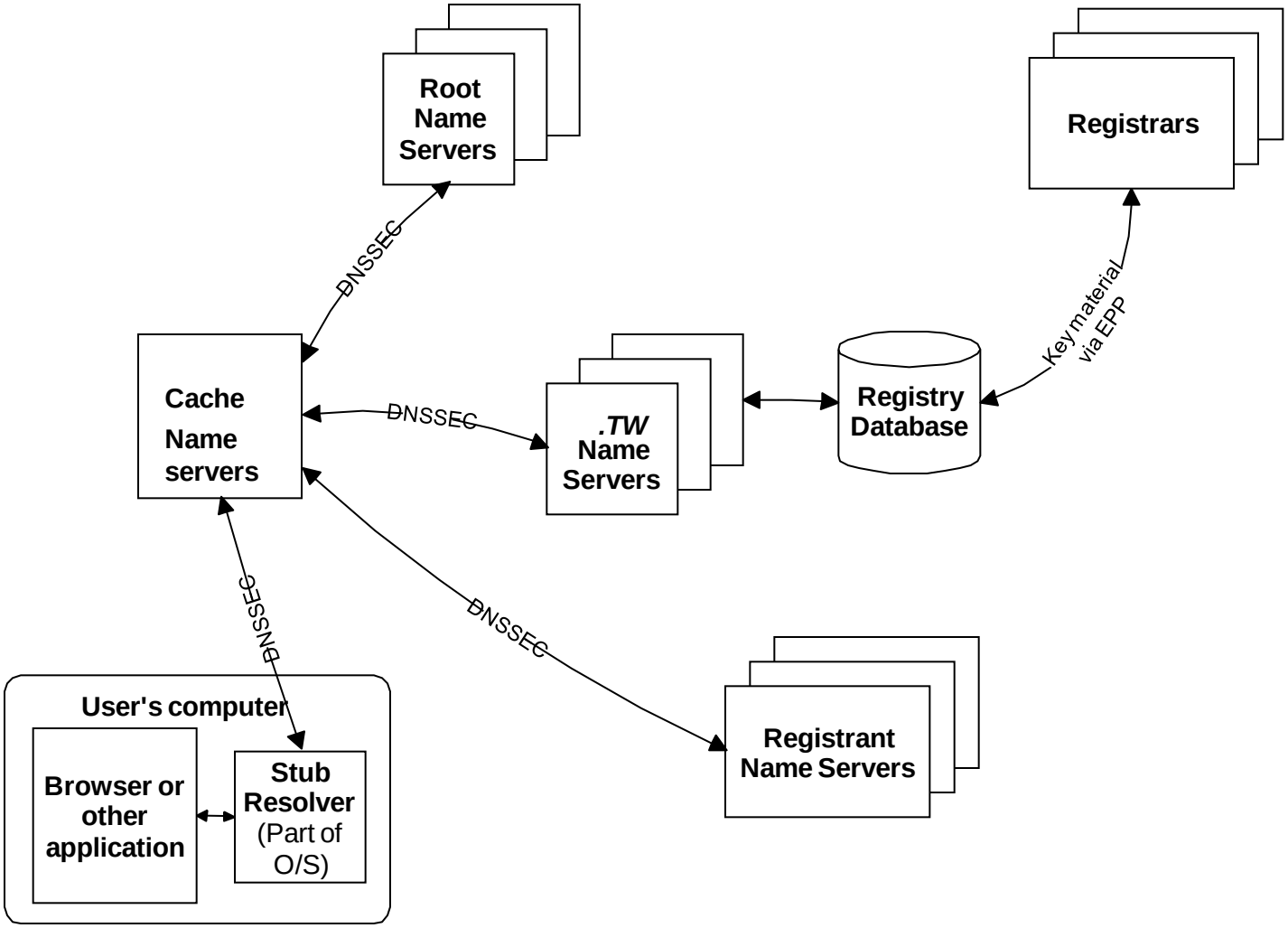
生日攻擊法

- 當一個辦公室有多少人時會有多個人的生日是在同一天的機率超過50%?
  - 答案：23人
  - 計算方式：1-P(n)
  - 1-(365-0/365)*(365-1/365)*...*(365-(n-1))/365

DNS cache poisoning

- 送 302 查詢和 302 回應則攻擊命中率 > 50%
- 送 550 查詢和 550 回應則攻擊命中率 > 90%
- 送 950 查詢和 950 回應則攻擊命中率 > 99.9%
- BIND 8及BIND 9早期版本的transaction ID是可以預測的

DNSSEC運作原理


Root Name Servers
Registrars
DNSSEC
Cache Name servers
DNSSEC
.TW Name Servers
Registry Database
Key material via EPP
DNSSEC
DNSSEC
User's computer
Browser or other application
Stub Resolver (Part of O/S)
Registrant Name Servers

DNSSEC的弱點

- Protocol:
  - NSEC: data leak (NSEC3已改善)
  - RRSIG: create zone file效率
  - Packet Size: 查詢/傳輸效率
  - 解析效率
- Implement:
  - Key management
  - 軟體支援時程(作業系統、應用程式、IP分享器...)
  - 對DDoS等的攻擊存活率

效率

	DNSSEC with Key rollover	With DNSSEC	Without DNSSEC
Create zone files	40min20sec	21min42sec	2min
Zone file size	176M	97M	20M
Query time	-	6.02 ms	3.47 ms
Start named	39.1s	24.6s	6.3s

Packet Size

- $ dig @a.dns.tw. tw. ns
  - ;; SERVER: 2001:cd8:800::8#53(2001:cd8:800::8)
  - ;; WHEN: Tue Mar 26 08:15:36 2013
  - ;; MSG SIZE rcvd: 499

- $ dig @a.dns.tw. tw. ns +dnssec
  - ;; SERVER: 2001:cd8:800::8#53(2001:cd8:800::8)
  - ;; WHEN: Tue Mar 26 08:16:11 2013
  - ;; MSG SIZE rcvd: 3130

DNSSEC的幾個迷思(1)

- DNSSEC將DNS封包作加密，確保DNS封包傳輸的正確性
  - 事實上是DNSSEC沒有作加密碼，還是明碼傳送，但有額外傳送簽章資料讓查詢者驗證資料之完整性
- DNSSEC讓DNS server本身更安全
  - 事實上是DNS server為了要提供DNSSEC需要更大的運算能力及頻寬，如上頁封包大小的統計，攻擊者針對啟用DNSSEC的DNS server只要用六分之一的封包數達到相同的DoS攻擊結果

DNSSEC的幾個迷思(2)

- 有了DNSSEC後能阻擋大部份的網路攻擊
  - 事實上是DNSSEC僅能確保DNS封包的正確性，對其他的網路攻擊毫無幫助。你大部份碰到的SPAM或網路釣魚是因為DNS查詢結果錯誤嗎?
  - 除了DNS解析結果正確性有保障外，其餘的網路攻擊行為依然存在

目前全球DNSSEC推動現況

- 全球共有317個頂級域名
- 有102個頂級域名已啟用DNSSEC
  - 13個gTLD
  - 10個測試TLD
  - 79個ccTLD

台灣地區推動現況

- 2011年11月.TW/.台灣域名啟用DNSSEC
- 2012年6月第二層域名啟用DNSSEC
- 2012年10月各註冊商開放用戶設定DNSSEC
  - 至目前共有51個域名啟用DNSSEC
- 2013年成立DNSSEC推動委員會

為什麼要推動DNSSEC

- 在目前沒有Client內建支援的情況下值得推動DNSSEC嗎?
  - 不是值不值作的問題，而是該不該作的問題
  - 現在中文域名很普遍，但在2003年開放註冊時還沒有瀏覽器支援(支援中文域名的IE7到2007年才出現)

Q & A