การอบรมเชิงปฏิบัติการ
การปรับปรุงระบบ DNS ให้รองรับ DNSSEC

นายชยา ลิมจิตติ <Chaya.L@Chula.ac.th>
สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย

๒๑ กรกฎาคม ๒๕๖๐ มหาวิทยาลัยราชภัฏรำไพพรรณี

DNS เชื่อถือได้ ?

- ตัวอย่างการโจมตี

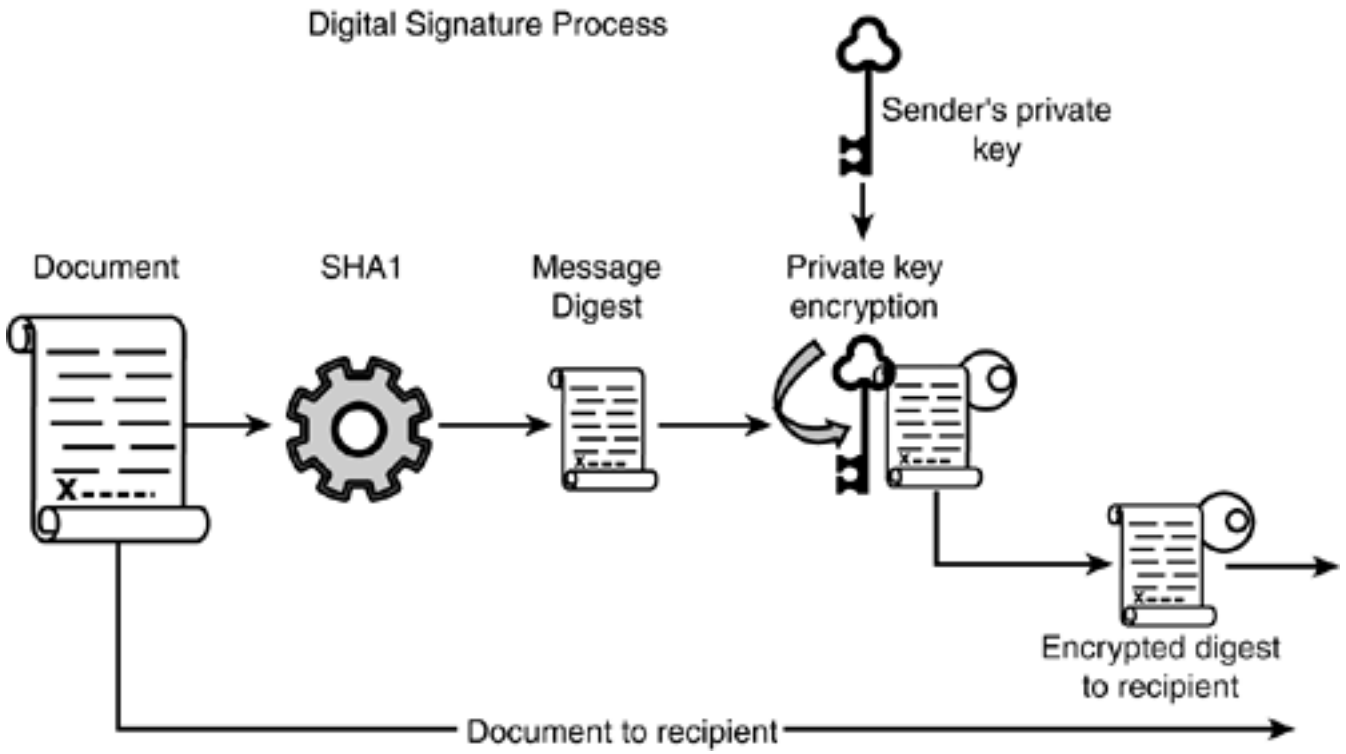
แนะนำ DNSSEC (1)

- DNS Security Extension
- เพิ่มความสามารถในการตรวจสอบการคงสภาพของข้อมูลที่มาจาก authoritative server (I ใน CIA)
- ลดปัญหาที่เกิดจาก DNS Spoofing, cache poising เช่น Kaminsky attack

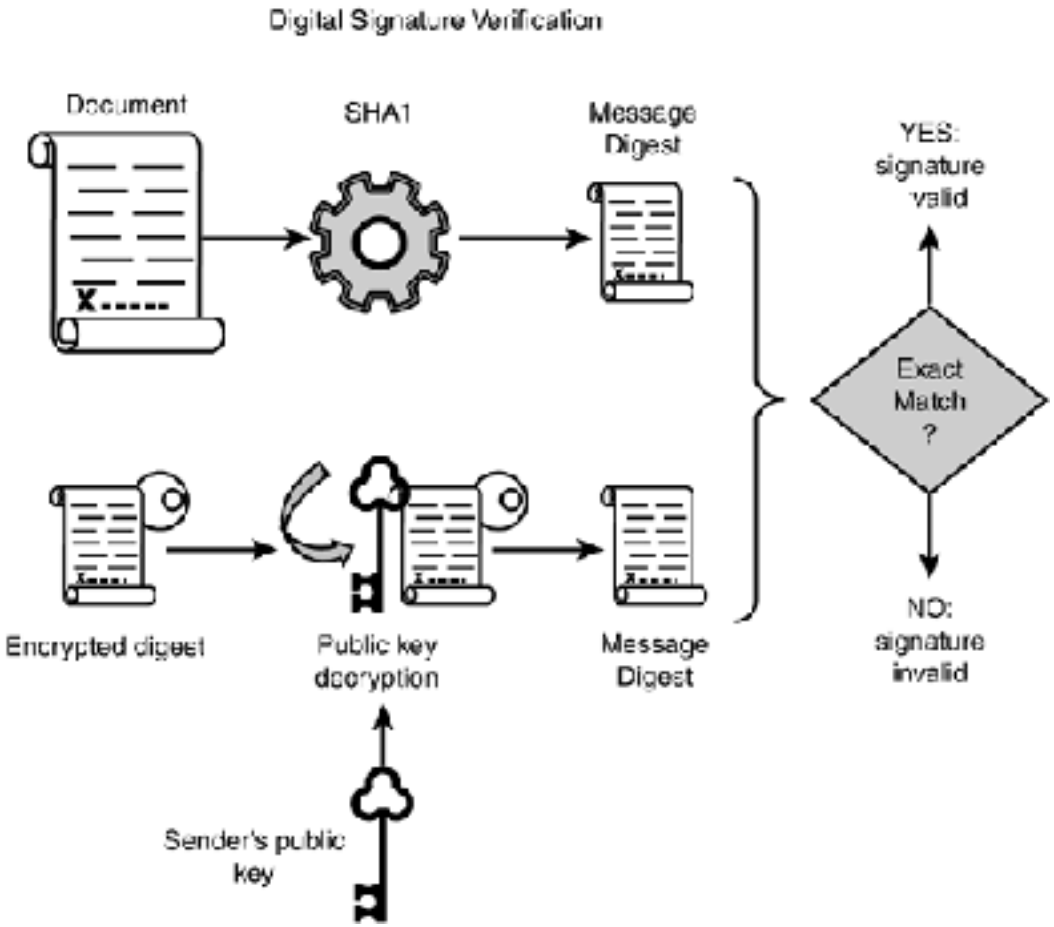
แนะนำ DNSSEC (2)

- แต่ละ zone ประกอบด้วย private key และ public key
- ผู้ดูแล zone สร้าง “ลายเซ็นต์”ของ zone โดยใช้ private key
- recursive name server ตรวจสอบ zone โดยใช้ public key
- ประกาศ public key ไว้ในข้อมูลของ DNS
- ใช้ zone delegation path เพื่อสร้าง “chain of trust” ของ public key

การสร้างลายเซ็นต์



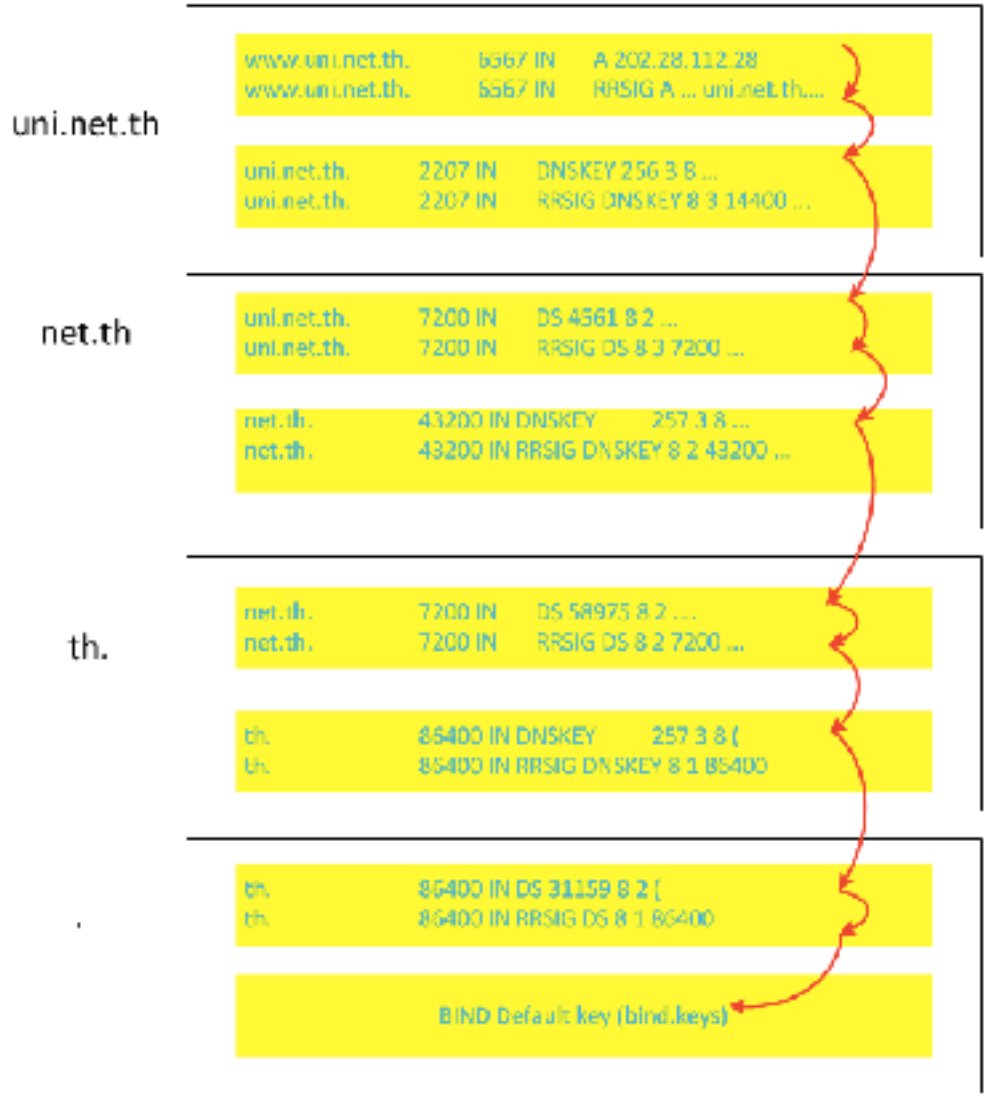
การตรวจสอบ


Digital Signature Verification
Document
SHA1
Message Digest
YES: signature valid
Exact Match ?
NO: signature invalid
Encrypted digest
Public key decryption
Message Digest
Sender's public key

การทำงานของ DNSSEC

- ตัวอย่างการป้องกัน

การทำงานของDNSSEC



DNSSEC: สิ่งที่ต้องเตรียมตัว

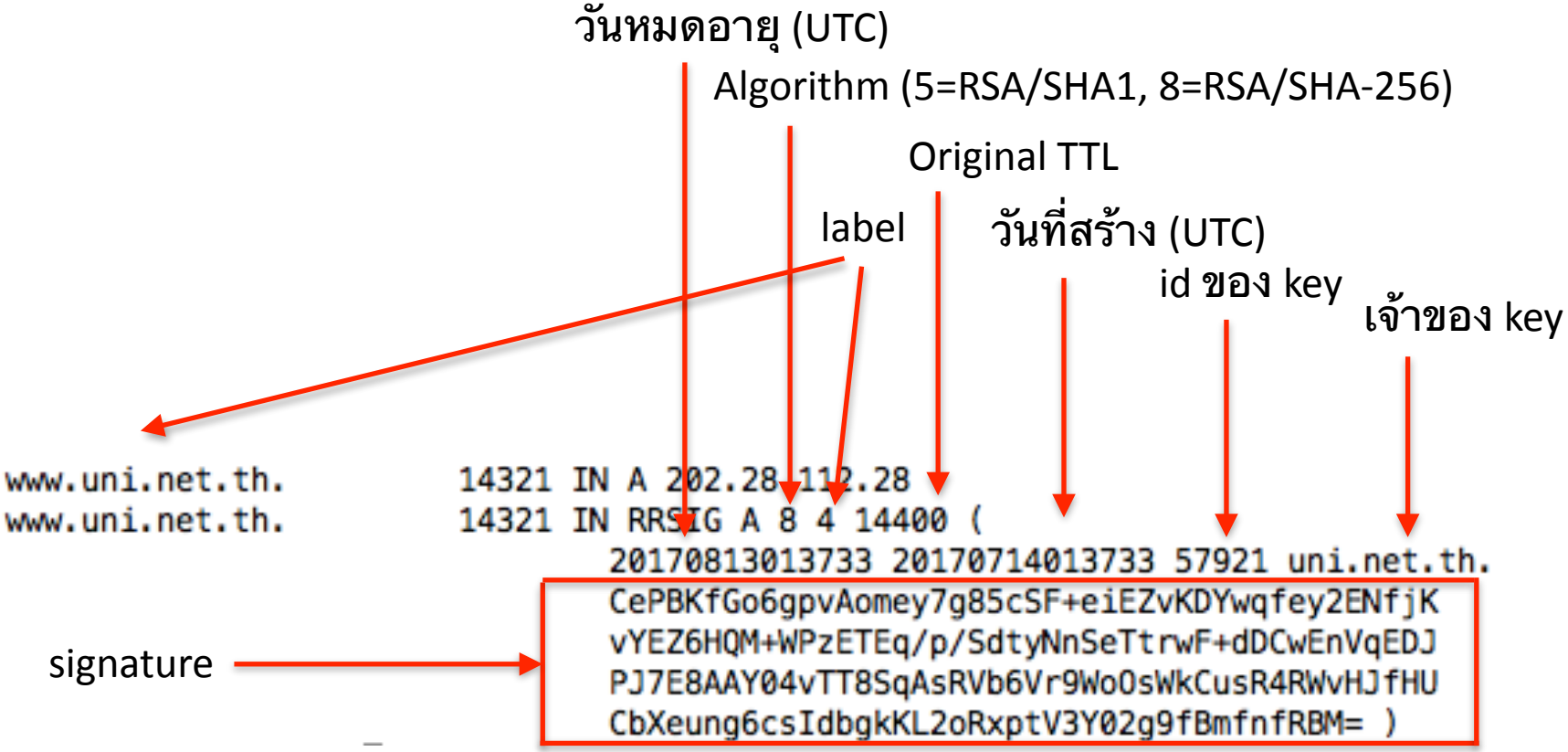
- ระบบเครือข่าย
  - Firewall/IPS ต้องรองรับ UDP 4096 bytes
  - มั่นใจว่าอนุญาต TCP 53 และ UDP 53
- ปรับเปลี่ยนโปรแกรม DNS ให้รองรับ DNSSEC
  - BIND ตั้งแต่ 9 ขึ้นไป
- System Entropy
  - haveged
- เรียนรู้ DNSSEC พร้อมวิธีตรวจสอบและแก้ไขปัญหา
  - dig

DNSSEC RR

RRSIG	DNSSEC Signature
DNSKEY	zone publicly
DS	Delegation Signer
NSEC	Next Secure record (proof of non-existence)
NSEC3	enhanced version of NSEC

RRSIG record

- signature ของ www.uni.net.th IN A



DNSKEY

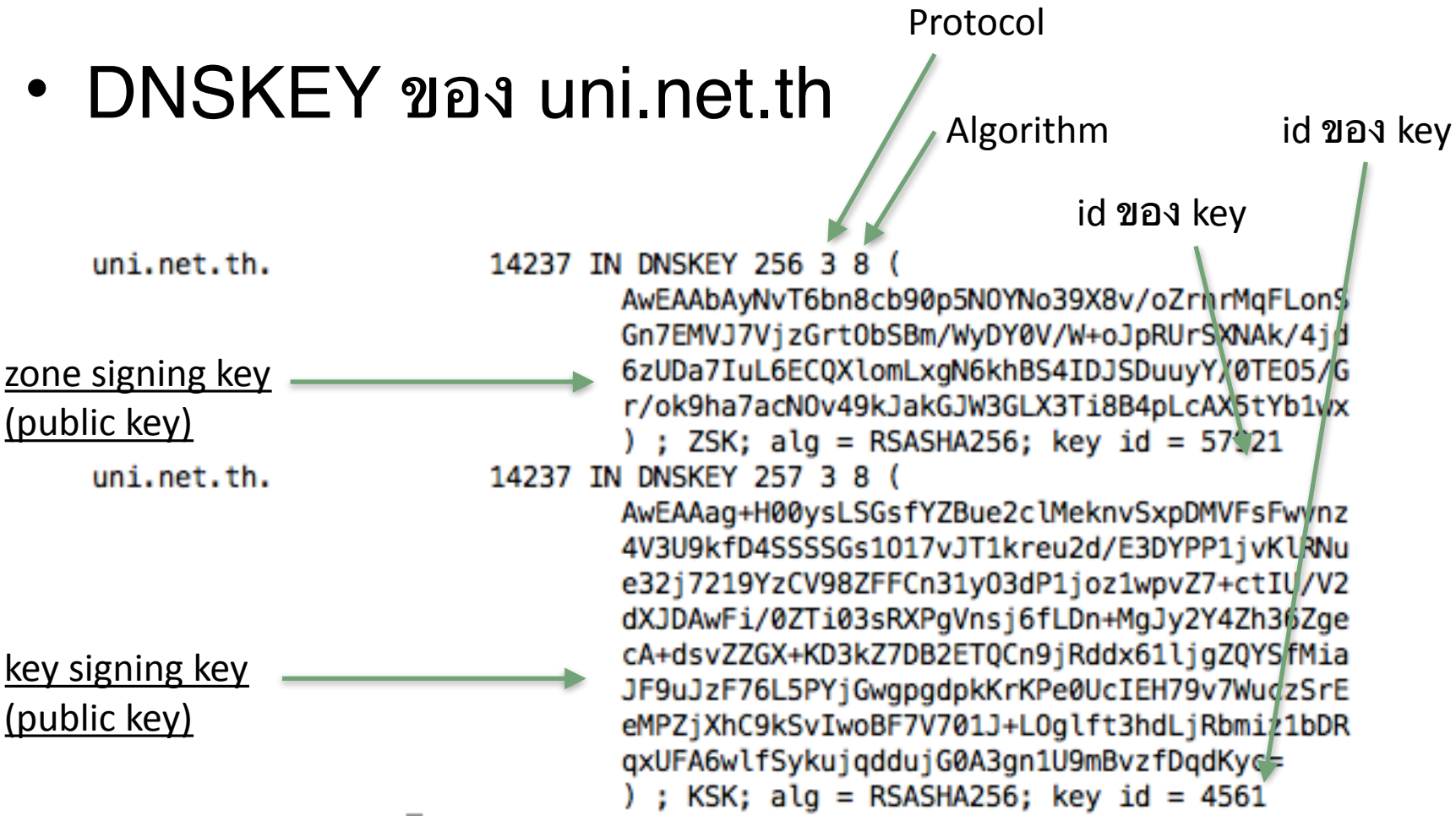
- ใช้กุญแจคู่ 2 ชุด
- Key Signing Key (KSK)
  - ใช้เพื่อลายเซ็นต์สำหรับรับรอง public key ของ ZSK (RRSIG ของ DNSKEY)
  - ประกาศ public key ของ KSK ไว้ใน DNS เพื่อตรวจสอบ ZSK
- Zone Signing Key
  - ใช้เพื่อสร้าง RRSIG ของแต่ละ RR
  - ประกาศ public key ของ ZSK ไว้ใน DNS เพื่อตรวจสอบ RRSIG

DNSKEY record (1)

- Flags 257=KSK, 256=ZSK
- Protocol = 3 (DNSSEC)
- Algorithm
  - 0 - reserved
  - 1 - RSA/MD5
  - 2 - Diffie/Hellman
  - 4 - reserved
  - 5 - RSA/SHA-1
  - 8 - RSA/SHA-256

DNSKEY record (2)

- DNSKEY ของ uni.net.th



DS record

- ตัวอย่าง DS ของ uni.net.th ที่เก็บไว้ที่ parent

```
uni.net.th.             7200 IN DS 4561 8 2 (
                                4E2C43A0B0EAB3A92A822F73C016284CA2B68CDC58BE
                                B49DD6BBEE4FC9645FC4 )
uni.net.th.             7200 IN DS 4561 8 1 (
                                250431D7083E42FF25CBE4891A3DCA5BE549700A )
```

NXDOMAIN กับ DNSSEC

- ต้องรับรองได้ว่าชื่อนั้นไม่มีอยู่จริง
- ต้องป้องกันการหลอกว่าชื่อนั้นไม่มีอยู่จริง

NSEC (1)

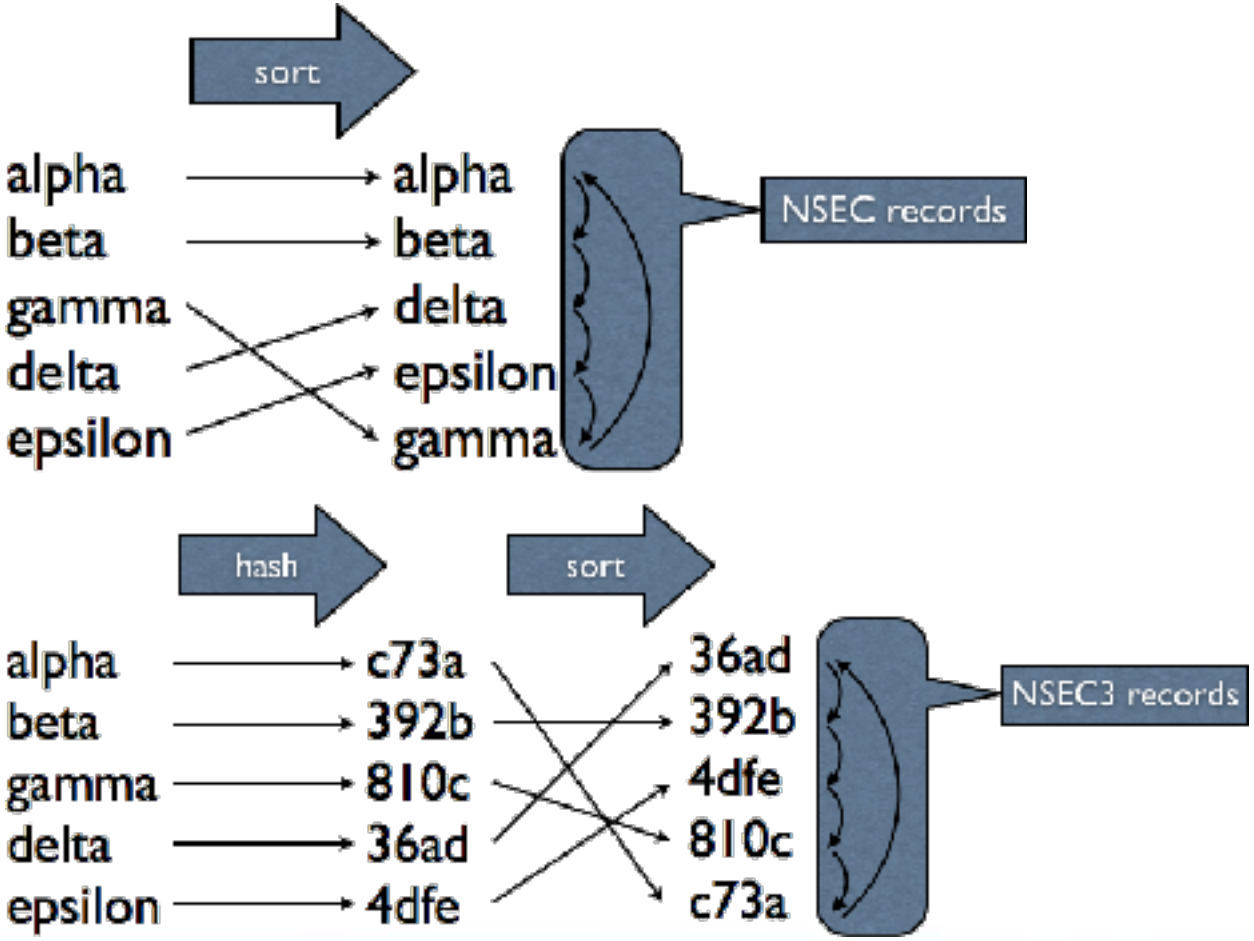
- เรียงลำดับโดเมนตามตัวอักษร
  - a.example.com IN A, AAAA, RRSIG
  - c.example.com
- NSEC record
  - a.example.com TTL IN NSEC c.example.com A AAAA RRSIG
  - บอกว่าระหว่าง a กับ c ไม่มีอะไรอยู่
- พิสูจน์ได้ว่าไม่มี b.example.com

NSEC (2)

- $ dig *.u2xx.ac.th +dnssec
  - หาชื่อแรกใน zone
- สามารถหาชื่อทั้งหมดใน zone ได้
- คล้ายๆ zone transfer
- NSEC3 แก้ปัญหานี้

NSEC3

- ชื่อใน zone จะถูก “hashed” และ “salted"



การเปลี่ยน ZSK และ KSK

- ZSK และ KSK เปรียบได้กับรหัสผ่านของ zone
- ZSK และ KSK จะถูกใช้เพื่อสร้าง RRSIG อยู่เป็นระยะๆ
- มีความเสี่ยงที่จะหา private key ได้เมื่อถูกใช้เป็นระยะเวลานาน
- ควรจะเปลี่ยนเป็นระยะๆ
- อายุของ ZSK และ KSK เป็นเรื่องนโยบาย ไม่ใช่เรื่องทางเทคนิค

การเปลี่ยน ZSK

- 1 เดือนก่อนเปลี่ยน
  - เปลี่ยนเวลาของ ZSK ปัจจุบัน
  - สร้าง ZSK ใหม่
  - ประกาศ DNSKEY (ของ ZSK ใหม่)
- วันที่เปลี่ยน
  - สร้าง RRSIG โดยใช้ ZSK ใหม่
- 1 เดือนหลังเปลี่ยน
  - ลบ DNSKEY เก่าออกจาก zone
  - สร้างลายเซ็นต์ของ DNSKEY โดยใช้ KSK

หน้าที่ผู้ดูแล

หน้าที่โปรแกรม

การเปลี่ยน KSK

- 1 เดือนก่อนเปลี่ยน
  - เปลี่ยนเวลาของ ZSK ปัจจุบัน
  - สร้าง KSK และ DS ใหม่
  - ประกาศ DS ที่ parent
- ณ วันที่เปลี่ยน
  - ใช้ KSK ใหม่สร้าง RRSIG ของ DNSKEY
  - ประกาศ RRSIG ใหม่
  - ลบ RRSIG เก่า
- 1 เดือนหลังเปลี่ยน
  - ลบ KSK DNSKEY เก่าออกจาก zone
  - ลบ DS เก่าออกจาก zone

หน้าที่ผู้ดูแล

หน้าที่โปรแกรม

หน้าที่ผู้ดูแล

ปัญหาที่พบบ่อยๆ

- ต้องการทำ DNSSEC แต่
  - ไม่ได้เพิ่ม DS ที่ parent
- RRSIG หมายอายุ
- ต้องการยกเลิก DNSSEC แต่
  - ไม่ได้ยกเลิก DNSSEC ที่ parent
- เครือข่ายไม่ยอมรับ UDP ขนาด 4096

เรียนรู้ DNSSEC ผ่าน dig

- $ dig www.uni.net.th
- $ dig www.uni.net.th +dnssec +multiline
- $ dig www.isc.org a +dnssec +multiline
- $ dig uni.net.th dnskey +multiline
- $ dig @ns.thnic.net uni.net.th ds +multiline

ปรับ BIND ให้เป็น DNSSEC

- $ sudo dnssec-keygen -a RSASHA256 -b 1024 -3 u2xx.ac.th
- $ sudo dnssec-keygen -a RSASHA256 -b 2048 -3 -fk u2xx.ac.th
- zone statement ของโปรแกรม BIND
  - key-directory "/etc/namedb/keys";
  - auto-dnssec maintain;
  - inline-signing yes;