ยินดีต้อนรับสู่
CYBER SECURITY WORKSHOP

OPENDNSSEC PART 2

Bangkok
8-9 May 2019

The material in these slides is based on
OpenDNSSEC course material from Berry van Halderen

CONF.XML

Configuration contains

RepositoryList (which HSMs)

Common

Enforcer

Signer

```
<Configuration>
    <RepositoryList>
      …
    </RepositoryList>
    <Common> … </Common>
    <Enforcer> … </Enforcer>
    <Signer> … </Signer>
</Configuration>
```

Repository List

Defines where private keys live

- ✘ You need at least one but can have more (separate ZSK/KSK)
- ✘ HSM interface available
- ✘ Each private key repository is listed as an <repository> element
- ✘ SoftHSM if you do not have the ~~money~~ hardware

```
<RepositoryList>
  <Repository name="SoftHSM">
     <Module>/usr/lib/libsofthsm2.so</Module>
     <TokenLabel>OpenDNSSEC</TokenLabel>
     <PIN>1234</PIN>
  <Repository>
```

Having multiple Repositories

Off-line KSK when not needed

Place signing of keyset (using KSK)

And regular zone signing (ZSK) in different locations

- Long validity period signatures keyset
- Zone needs updating -> short period remainder

Choice of algorithm

- ✘ Crypto improves over time
- ✘ also matter of preference

  - ✘ RSAMD5, DSA, RSASHA1, DSA-NSEC3-SHA1,.. -- legacy
  - ✘ RSASHA256 -- the current
  - ✘ RSASHA512 -- future?
  - ✘ ECC-GOST -- Russia?
  - ✘ ECDSAP256SHA256, ECDSAP384SHA384 -- upcoming
  - ✘ ED25519,ED448 – emerging

Key rollover

Crypto improves over time

Keys may still be stolen

When to roll over

1. Crypto works better when rolling keys
2. When keys stolen or better crypto
3. Just as a procedure regulary

Key states

TTL of data in DNS caches need to be taken into account.
Why?

Other propagation delays and timings.

Key states

1. Generate
2. Publish
3. Ready
4. Active
5. Retired
6. Revoked

Key Rollover methods

Know the state of your keys and signatures

1. Hidden
2. Rumoured
3. Omnipresent
4. Retentive

1.x compatible vs. 2.0 key list

```
$ ods-enforcer key list
Zone:        Keytype: State:  Date of next transition:
example.com  KSK      publish 2016-04-15 00:22:18
example.com  ZSK      ready   2016-04-15 00:22:18


$ ods-enforcer key list -d
Zone:        Key role: DS:    DNSKEY:  RRSIGDNSKEY: RRSIG:      Pub: Act:
example.com  KSK       hidden rumoured rumoured     NA           1    1
example.com  ZSK       NA     rumoured NA           omnipresent 1    1
```

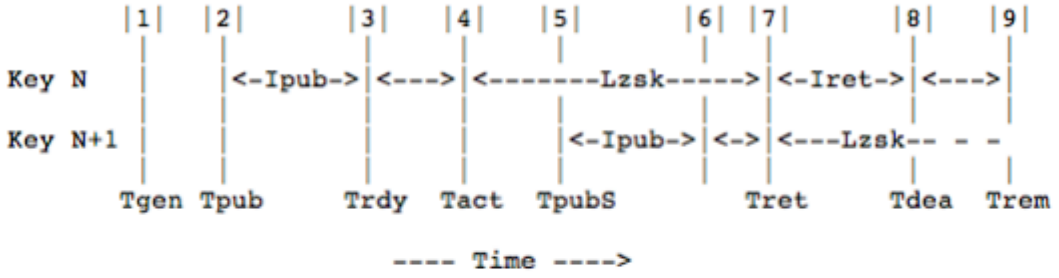
ZSK Method	KSK Method	Description
Pre-Publication	N/A	Publish DNSKEY before the RRSIG
Double-Signature	**Double-Signature**	Publish DNSKEY and RRSIG at the same time. For a KSK, this happens before the DS is published
Double-RRSIG	N/A	Publish RRSIG before the DNSKEY
N/A	Double-DS	Publish DS before DNSKEY
N/A	Double-RRset	Publish DNSKEY and DS in parallel.

Rollover methods

Part 8: Using OpenDNSSEC

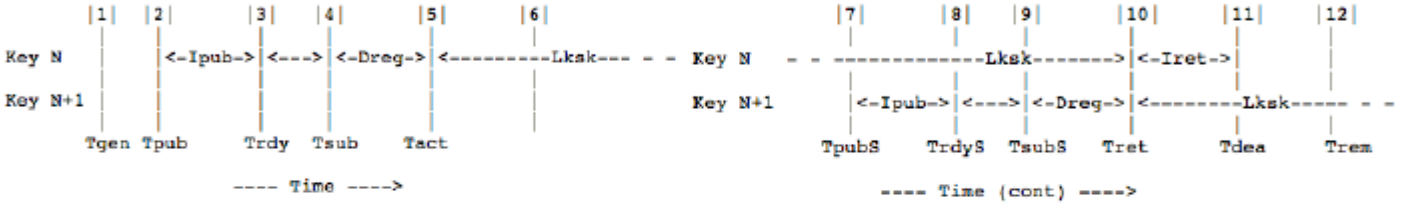
http://bangkok.lol/

Pre-Publication ZSK rollover



- First key: Ipub = Dprp + min(TTLsoa, SOAmin)
- Future keys: Ipub = Dprp + TTLkey
- TpubS <= Tact + Lzsk - Ipub
- Iret = Dsgn + Dprp + TTLsig

Double-Signature KSK rollover



- Ipub = Dprp + TTLkey
- TpubS <= Tact + Lksk - Dreg - Ipub
- Iret = DprpP + TTLds

Configration conf.xml highlights

Enforcer/Datastore

Enforcer/ManualKeyGeneration

Enforcer/AutomaticKeyGenerationPeriod

Enforcer/RolloverNotificationPeriod

Enforcer/DelegationSignerSubmitCommand

Signer/Threads

Signer/NotifyCommand

KASP

Values in default policies are sane starting values

Signatures/Resign
Signatures/Refresh
Signatures/Validity/Default
Signatures/Validity/Denial
Signatures/Jitter
Signatures/InceptionOffset
Signatures/MaxZoneTTL

Denial/NSEC3/OptOut
Denial/NSEC3/Resalt
Denial/NSEC3/Hash

Keys/TTL
Keys/RetireSafety
Keys/PublishSafety
Keys/Purge
Keys/KSK/Lifetime

Zone/PropagationDelay
Zone/SOA/TTL
Zone/SOA/Minimum
Zone/SOA/Serial

Zone/PropagationDelay
Zone/SOA/TTL
Zone/SOA/Minimum
Zone/SOA/Serial

Parent/PropagationDelay
Parent/DS/TTL
Parent/SOA/TTL
Parent/SOA/Minimum

SOA

Always have valid signatures in zone

Zone should expire before signatures expire

SOA Expire < signature refresh period

ods-kaspcheck

Rollover specials

- ✘ Emergency roll-over (rollover when in rollover procedure)
- ✘ Algorithm rollover
  - ○ Requires signatures to be published before DNSKEY

Features

- ✘ Combined signing keys

Migrating

- ✘ Exporting keys and importing them
- ✘ Publish DNSKEY in old sign environment
- ✘ Go insecure

Updating DS

- ✘ Manually
- ✘ Use delegationSignerSubmitCommand
- ✘ Future CDS / CDNSKEY RFC7344

Never give ds-seen without verifying.

Monitoring

OpenDNSSEC, NSD, Bind, all are stable, but integration will break:

- ✘ Signer up and running
- ✘ Signature expiration nearing unexpectedly
- ✘ Zone updates get through

Prepare for when things to wrong

- ✘ Backup not just keys, also var/lib/opendnssec and kasp.conf

Recommendations

Roll KSK at least yearly (or not at all and prepare to go unsigned)

Roll ZSK every 3 months

SHA256, RSASHA256 not yet ECDSA

Key size 1024 / 2048

NSEC / NSEC3 ? OptOut when number of DS is low.