ยินดีต้อนรับสู่
CYBER SECURITY WORKSHOP

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

Bangkok
8-9 May 2019

```
$ORIGIN groupX.odslab.se.
$TTL 60
@       SOA nsX.odslab.se. test.odslab.se. (
                    2011062100 ; serial
                    360        ; refresh (6 minutes)
                    360        ; retry (6 minutes)
                    1800       ; expire (30 minutes)
                    60         ; minimum (1 minute)
                )
@       NS    nsX.odslab.se.
www     CNAME nsX.odslab.se.
```

Unsigned zone file

```
groupX.odslab.se.       60 IN SOA nsx.odslab.se. test.odslab.se. (
                        2011062145 ; serial
                        360        ; refresh (6 minutes)
                        360        ; retry (6 minutes)
                        1800       ; expire (30 minutes)
                        60         ; minimum (1 minute)
                        )
groupX.odslab.se.       60 IN RRSIG SOA 8 3 60 20110628103724 (
                        20110628083552 44494 groupx.odslab.se.
                        HJ5lIdcdwJTJ1SjYd5N/Gk1Ctq2u2VfXAVIF49em/jdm
                        pAlJnejkw8AfbUTjdcXRUH6cQ2XIHobjgEJEpWRM9G/W
                        W7DYJZmdo6o09YrMexTLCZLcq6eyjTpS8TmwmconuNEN
                        FiCkBztqgHlyw0Teq9sw/1E0UVwGHKgd0S0v8Nw= )
groupX.odslab.se.       60 IN NS nsx.odslab.se.
groupX.odslab.se.       60 IN RRSIG NS 8 3 60 20110628103609 (
                        20110628083552 44494 groupx.odslab.se.
                        KJYxcz25nv0mRSZDHkh0YXPBrZ0+78bVsT7FD4A9G29m
                        JsHpkpfzjZ/Bee+lqw2ZGIJRmMfyRtQQon7oCa2Z9xe9
                        L/D9KQzPzZb2CMrOxG/usZZ+LtwYuNJb0H12BJhk1j15
                        fBN6aEsyhw+hiV9ibobzqHe5bMnxaa9IfMscVlc= )
groupX.odslab.se.       120 IN DNSKEY 256 3 8 (
                        AwEAAasvOuyeTp5kIaw/fwPyQncY06YMnJ70lczC5GCx
                        veUNQXLhihm+tV/1TvkMd5GHq/ebjTPSR6mqB/jTs7CH
                        /iNhprxdnhllVW7PjFpC5tDfF1HyDM97q8A+41nBmiB4
                        S2JR1qOGmeoiU2BP2uyT1v3lKJPDm08GwmPTTX8fi3LV
                        ) ; key id = 44494
groupX.odslab.se.       120 IN DNSKEY 257 3 8 (
                        AwEAAc6Wk/UqaEMaytXNL2y25I0Z8UuubnkrufaJEERw
                        ni0bHaNGMscp5I52O7ScR6L70DJS46S9bA4k8mbcRNPA
                        V1DOQVz1kPTTNt45XzYQ7ymQJyobQdPtVq8TXtaFPiFP
                        S7nz7qaR/HVNRVNRp4H51ajsqh4LCX+J99tJX+rk61JR
                        tbnHVv2POUiuZNFqZLOkbzGtNRb14UvoRQi5q+tjV/ow
                        cUkn8tljQGPpTe/ELImUT+MrftnY6m8jvq0+qhd2o/12
                        6XEcVBuDB+UGrhFcU72HmeKfQRMtCuGZhmMOcOymPcDJ
                        120NkBqgj28Cu/4Kr44DMTu4q2ax07dD0fSyHqM=
                        ) ; key id = 62246
groupX.odslab.se.       120 IN RRSIG DNSKEY 8 3 120 20110628103715 (
                        20110628083552 62246 groupx.odslab.se.
                        Tw32FON95e84g0FYxyXuJnDQWTdAELaVhq4RVoRAJRWx
                        1AgkZk/XQRUforjd/qNNjrIA2+a9wwrvLNokRB6xzSTR
                        bwx199Mu8Xj9p9Q8CbzCvbvHPtRqFqf6Mto9jjlUaZK4
                        N1NQWq/qfsLvkvxRpdE4q9Xac3b7lTPuylQSovvARRDv
                        4rJ4zmBdomdQHjtwOuQ4GeVfpgRqFCqaBHFK8D20Kmjk
                        56a7rbeGUNt5hNWjQfyzJNfvulFAdCTNDRbikms7YQMw
                        j6msmzRS8Zj+I1BbmkuGRwxVxNF/caD9fuz4NhyOCGRP
                        JmRTBIwk+XcybA6vK5ofnrRTCSSoJ0t4+g== )
groupX.odslab.se.       60 IN NSEC3PARAM 1 0 5 3A5BF749D1330DE3
groupX.odslab.se.       60 IN RRSIG NSEC3PARAM 8 3 60 20110628103502 (
                        20110628083552 44494 groupx.odslab.se.
                        GvylAOrm6dENvVUke1CkJHmjB5WlmbvIsFdvm2p2MfZa
                        magUJHJDsT6RJjIyRlvc+6TJjADDHGpvr6ILLnWySFRb
                        9efAn/SDt060NJYsU6emv5iAh/TRbo7gRUNtokm1TAds
                        5rZ187cOoJyqQ05qBSTVo8wCcFlHS6+htEt+vQs= )
www.groupX.odslab.se.   60 IN CNAME nsx.odslab.se.
www.groupX.odslab.se.   60 IN RRSIG CNAME 8 4 60 20110628103414 (
                        20110628083552 44494 groupx.odslab.se.
                        BAs7KPVdwoPeC9ian/N00dV20R62sSjbQS65rGhREOGF
                        ToRqd6wRpd8ChNSNrJNn7ycH61m2j71NhE00fsMLA1T6
                        vxGNVcK6IeR+7Vpu4bgnE93jq8fJTftaiR22bYN1+Y9Q
                        Y7PNNFcm20PmoqVmilmtJdpn+YNjUJ5a+Riwojo= )
7oreblsb9elhfqfp53bqqde6bcdm5eo3.groupx.odslab.se. 60 IN NSEC3 1 0 5 3A5BF749D1330DE3
OTANAROMKJB00QC2G6K2IT2GU2SB4DOA CNAME RRSIG
7oreblsb9elhfqfp53bqqde6bcdm5eo3.groupx.odslab.se. 60 IN RRSIG NSEC3 8 4 60
20110628103552 (
                        20110628083552 44494 groupx.odslab.se.
                        azU2yRsLQNKANwyTxosI4hwf6JPfV5XKNdPtQxGprShE
                        w6N/sDG9QzMJjlQrPW82rY2SY17xGJMBGdfsGVBZJJQ4
                        nXBmenjT5Grm9k/a0hyOnYYAHzoq4isV5fLDYrHRaf/u
                        uvoFs90vJIN4OMbENJUrHGsCsJRzps/kD/aR+Dw= )
otanaromkjb00qc2g6k2it2gu2sb4doa.groupx.odslab.se. 60 IN NSEC3 1 0 5 3A5BF749D1330DE3
7OREBLSB9ELHFQFP53BQQDE6BCDM5EO3 NS SOA RRSIG DNSKEY NSEC3PARAM
otanaromkjb00qc2g6k2it2gu2sb4doa.groupx.odslab.se. 60 IN RRSIG NSEC3 8 4 60
20110628103526 (
                        20110628083552 44494 groupx.odslab.se.
                        QLlN/6Cj1kO6O9P9/AntqRFHMANJ8PUI253ROEfN9DGP
                        P2Er/7dd+jlv2sqEmIYx/GVXySr4RafgmB+k0fwEU+JY
                        TjmfkLUOD6O9DOQ/RqNtLp5HFR6TLMZx07VdPr9vE2ql
                        5UIUQjIPT2+aQR3Dd/QMq26ysRGqOApGH/wkq6Y= )
```

Signed zone file

DNSSEC extra requirements

Procedure to make changes to key infrastructure

- Add, remove, swap key usage

Signatures expire, and need refreshing

DNSSEC extra status

- ✘ Insecure
- ✘ Secure
- ✘ BOGUS
- ✘ …

A whole new dimension

Past: Goofing up –> your slaves would keep you up

DNSSEC: not doing in means going out of existence

Past: static

DNSSEC: constant maintaining the zone.

OpenDNSSEC

OpenDNSSEC Whay, Why, Who

OpenDNSSEC is a zone signer that automates the process of keeping trackof DNSSEC keys and the signing of zones

- ✘ Many DNSSEC Tools missing
  - ○ key management
  - ○ policy handling
  - ○ hardware acceleration
- ✘ DNSSEC should be easy to deploy
- ✘ Increase DNSSEC users and add experience from previous deployments

OpenDNSSEC - Who

OpenDNSSEC goals

- ✘ Open Source software with BSD license
- ✘ Simple to integrate into existing infrastructure
- ✘ Key storage and hardware acceleration using PKCS#11
- ✘ Anticipate OpenDNSSEC deployed between hidden and public master invisible as bump-in-the-wire.

Components of OpenDNSSEC

- ✘ Key and Signing Policy (KASP)
- ✘ Enforcer (handling policy, key handling)
- ✘ Signing (signing the zone based on enforcer instructions)
- ✘ HSM (hardware accelerated PKCS#11 crypto, or SoftHSM)

Key and Signing Policy (KASP)

- ✘ How to sign a zone is described by a policy
- ✘ Allows choice of key strengths, algorithm, key and signature lifetimes, NSEC/NSEC3, etc.
- ✘ One policy per zone, or some zones sharing policies

Enforcer

- ✘ Management of Keys (manages creation, disposal)
- ✘ Keeps track of timing and key rolling
- ✘ Select which keys need to sign
- ✘ Handles changes in policy

Signer

- ✘ Automatic signing of the zones
  - ○ can re-use signatures that are not too old
  - ○ can spread signature expiration over time (jitter)
- ✘ Maintains NSEC/NSEC3 chain
- ✘ Updates SOA serial number

Hardware Security Module

- ✘ Performs actual crypto
- ✘ Therefor keys only live inside HSM
- ✘ Often security must, but also a good abstraction

Everything can be rebuild – except your keys

Input and Output adapters

- ✘ Acts as nameserver
- ✘ Both incoming and outgoing:
  - ○ AXFR
  - ○ IXFR
  - ○ Notify
- ✘ Any nameserver can be used (BIND, NSD, ...))
- ✘ Automation to reload zone

Configuration And Parameters

Configuration of OpenDNSSEC

Very configurable

- conf.xml -- used for overall configuration of the system
- kasp.xml -- defines the various policies for signing zones
- addns.xml -- defines In- and Output adapter parameters (e.g. TSIG).

Time definition in OpenDNSSEC

"P1M3DT1H30M10S" ISO8601

P[n]Y[n]M[n]DT[n]H[n]M[n]S

- ✘ Configuration of OpenDNSSEC about durations (periods) not absolute times.
- ✘ No clue about Gregorian Calendar (P1Y == P365D)

Pitfall: P5M PT5M

A world of difference (actually 13391700s).

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>
```

Sideline: SoftHSM

- ✘ PKCS#11 is the industry API to HSMs;
- ✘ Private keys are assumed to be stored in HSM;
- ✘ The SoftHSM is distributed separately and independently from OpenDNSSEC (but in co-operation);
- ✘ for those who do not have HSM (most users);
- ✘ HSMs can be tricky, read documentation about capacity, backups, sessions;

Part 7: SoftHSM

http://bangkok.lol/