



## 3 days of DNSSEC Technical Workshop – Implementation and Deployment

### General description

This DNSSEC Workshop is a classroom style course with lecture and hands-on labs. Limited seating. It is designed for Network and SysAdmin veterans who need to know how to deploy DNSSEC for their organization. Students are expected to be familiar with the UNIX environment (file structure, basic utilities) and with text editing in UNIX (vi or nano editor). A basic knowledge of TCP/IP addressing is also helpful but not required.

The training will follow our public training class content mentioned on our website:  
<http://www.menandmice.com/support-training/training/dnssec-workshop/>

### Syllabus

- DNS Fundamentals 101
  - A quick recap of DNS Fundamentals
  - DNS Namespace
  - Delegation
  - Nameserver
  - DNS Message Format
  - Name Resolution
  - Caching
  - DNS Practice
  - Resource Records
- DNSSEC Theory and History
  - What is wrong with the good old DNS?
  - Spoofing
  - Man in the Middle Attacks
  - Betrayal of a trusted name server
  - Attack on authoritative data
  - The danger of Denial of Service Attacks
- DNSSEC Introduction



- DNS and DNSSEC History
- TSIG and DNSSEC
- Basics of Public Key Cryptography
- DNSSEC Technical Overview
- DNSSEC Record Types
  - DNSKEY (DNS Key Material)
  - RRSIG (Resource Record Signature)
  - NSEC (Next Secure)
  - DS (Delegation Signer)
- Zone Signing Key (ZSK) and Key Signing Key (KSK)
- the DNSSEC chain of trust
- DNSSEC Infrastructure Requirements
- Signing tools
  - Authoritative DNS Servers
  - Caching/Resolving DNS Servers
  - Middleboxes (Firewalls, Load-Balancer, NAT ...)
  - Application Requirements
- DNSSEC Deployment
  - DNSSEC signing with BIND 9.6-ESV
  - creating keys
  - Adding keys to a zone
  - Signing a zone
  - Test the setup
  - Getting DS record in the parent zone
  - Resigning a zone
  - Maintenance: Signature Expiration
  - Lab: DNSSEC zone signing
- DNSSEC with BIND 9.7+
  - Managing key timing values
  - DNSSEC automation
  - Dynamic zones and DNSSEC



- Managing zone content with nsupdate
- Lab: DNSSEC with BIND 9.7+
- DNSSEC Validation
  - DNSSEC in DNS Messages
  - The AD and CD flags
  - DNSSEC Name resolution
  - DNSSEC Lookaside Validation (DLV)
  - Validating DNSSEC in the Internet
  - DNSSEC validation in Web-Browsers (Firefox, IE, Chrome)
- A validating caching only configuration for BIND 9
  - BIND as a caching server
  - Named.conf setup (ACL, rndc, statistics channel)
  - Getting the root-anchor
  - Verifying the root zones key
  - DNSSEC validation setup (BIND 9.6-ESV)
  - DNSSEC validation setup (BIND 9.7.0+)
  - Lab: DNSSEC validation with BIND
- Signing zones with NSEC3
  - The NSEC3 Record
  - NSEC3 zone signing
  - Salt and Iterations
  - NSEC3 opt-out
- DNSSEC Key rollover
  - The need of key rollover
  - Key rollover with pre-publication
  - Key rollover with double-signing
  - Emergency key rollovers
  - Algorithm Rollover
  - Switching DNS Operators
    - Operator rollover (cooperative)
    - Operator rollover (non-cooperative)



- Lab: ZSK and KSK rollover
- DNSSEC tools and troubleshooting
  - DNSSEC troubleshooting with DIG
  - Lab: find the cause of DNSSEC lookup failures
  - Other DNSSEC tools (drill, unbound-host, dnssec-tools, zonecheck, OpenDNSSEC)
  - DNSSEC monitoring tools
- DNSSEC in BIND 9.8 and 9.9
- Hardware Security Modules (HSM)
  - The role of a HSM
  - Selection criteria for HSM
  - SoftHSM – an HSM Emulator
  - Using BIND with SoftHSM

### List of Labs in the 3 day DNSSEC Workshop:

1) a basic DNS setup that we use for later DNSSEC work (also to clarify understanding of clean DNS delegation required for DNSSEC)

- setting up a basic DNS authoritative infrastructure (a BIND 9.9.x DNS server with an authoritative zone)
- setting up a delegation to a child zone
- setting up a child zone received from the parent domain

2) DNSSEC signing with BIND 9.6 functional level (NSEC)

- generating keys with dnssec-keygen
- publishing the public keys in DNS
- signing the zone using dnssec-signzone
- loading the signed zone
- submitting the DS record to the parent operator
- zone edits, re-sign the zone, reload the zone
- testing DNSSEC "ad" flag

3) DNSSEC signing with NSEC3

- using dnssec-signzone to sign a zone with NSEC3

4) DNSSEC signing with BIND 9.7 functional level (dynamic zones)

- using the zone signing automation with BIND 9.7 dynamic zones
- generating keys with timing values
- generating a DS record from key material
- submitting the DS record



- delegating a DNSSEC signed zone
- receiving a DS record as a DNSSEC signed parent zone from a downstream client
- publishing the clients DS record in the DNS zone

#### 5) DNSSEC troubleshooting

- using "dig" and "date" for manual DNSSEC troubleshooting
- using "drill" to troubleshoot "chain-of-trust" issues
- using "unbound-host" for DNSSEC troubleshooting

#### 5) DNSSEC signing with BIND 9.9 functional level (static zone in-line signing)

- signing a child zone with in-line signing
- working with signed and un-signed zones and BIND 9.4

#### 6) ZSK key-rollover

- manual ZSK pre-publication key rollover

#### 7) KSK key-rollover

- manual KSK double-signing key rollover

#### 8) OpenDNSSEC (optional on your request)

- installing OpenDNSSEC
- adapting a DNSSEC signing policy
- adding zone to OpenDNSSEC
- checking the ZSK/KSK rollover
- exporting a DS record
- marking a zone as "DS-seen"

## DNSSEC Consulting

### 1 day discussion for DNSSEC deployment for the .VN domain name in Vietnam

Please let us know if you already have special questions or topic you would like to discuss. This will help the trainer in his preparation to give you the best possible answers and solutions.