

DNSSEC

Underleverantör: IP-Solutions

Datum

- 3-4 okt
Stockholm

DNSSEC är det säkerhetstillägg som möjliggör att man kan verifiera att de svar man får ur DNS är äkta och inte ”spoofade” (dvs. förfalskade). DNSSEC är en bakåtkompatibel vidareutveckling av DNS som varit ”på gång” under många år och nu övergår i produktionsdrift. Denna kurs innehåller en fullständig genomgång av DNSSEC och dess användning.

- hotbild, designkrav, alternativ och lösning
- protokollutvidgning
- nya krav på och betydelse av kommunikation mellan föräldrar och barn
- verktyg för att förenkla och automatisera införande och drift av DNSSEC

Målgrupp

Denna kurs siktar parallellt på flera olika målgrupper. Dels givetvis på de som praktiskt skall utforma, administrera och förvalta DNSSEC som tjänst, dvs nätverkstekniker, nätverks- och DNS-administratörer. Men även beslutsfattare, IT-strateger, konsulter, säkerhetsfolk och andra som vill ha en djupare förståelse för hur DNSSEC fungerar och hänger ihop, och på vilka sätt det kommer att påverka framtida DNS-hantering men också ge nya möjligheter för framtida systemutveckling.

Förkunskaper

Goda kunskaper om DNS-teknik och funktion.

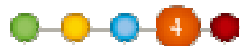
Övrigt

Denna kurs finns som schemalagd utbildning och presentationen ges på svenska eller engelska. Under kursen blandas teoretiska presentationer med praktiska övningar. Vi kan även hålla denna kurs företagsintern. Kontakta oss för att få reda på hur vi kan hjälpa er med anpassade kurser.

Längd

2 dagar

Svårighetsgrad



Agenda

Quick repetition of traditional DNS Principles behind the DNS protocol:

- autonomy, coherence, redundancy

Packet format:

- The different parts of the DNS message and their usage

Name server implementations

- BIND (both authoritative and recursive server)
- NSD (authoritative-only server)
- Unbound (recursive-only server)
- Other implementations
- Differences, pros and cons

Lab Exercise: Compilation and installation of the DNS software Role separation for name servers:

- inevitable when deploying DNSSEC
- different implementation alternatives
- usage together with TSIG
- pitfalls

TSIG: signing DNS transactions

- Symmetric encryption
- Symmetric algorithms: HMAC-SHA1, HMAC-SHA256
- Securing zone transfers (server-server)
- Securing queries (client-server)
- BIND: TSIG Configuration in named.conf:
 - key, server and masters directives
- NSD: TSIG Configuration in nsd.conf:
 - key: attributes and the use of the NOKEY keyword
- Securing the transport vs securing the data

Lab Exercise: Using TSIG between master and slave

- Configuration
- Need for synchronized clocks
- Debugging

EDNS(0):

- framework for DNS protocol extensions
- usage of the OPT pseudo-RR
- fields in the DNS packet that are expanded via EDNS(0) and their use

Introduction to DNSSEC

- Background, threat scenario, the Kaminsky attack, etc
- Walkthrough of the concepts

DNSSEC: Validation of signed DNS data

- “Trusted keys” and validation of data
- What does “security apex” mean?
- What should happen when data doesn’t validate?

Lab Exercise: Configuration of a validating resolver DNSSEC: Publication of signed DNS data

- Asymmetric encryption with public keys
- Asymmetric algorithms: RSA, DSA
- KSK and ZSK: different operational uses for keys

DNSSEC: Protocol extensions and new record types:

- RRSIG: digital signature of DNS records
- DNSKEY: publik key stored and distributed via DNS
- DS: identification of the "KSK" in use

DNSSEC low-level tools:

- dnssec-keygen to create keys
- dnssec-signzone to sign zones

Lab Exercise: Publishing a DNSSEC signed zone

- Create the configuration
- Generate the keys and add them to the zone
- DNSSEC Zone Signing

DNSSEC Key Rollover: Replacing old keys with new keys

- Policy management
- Delegation Signer and parent interaction
- Parent/child interaction with examples
- Tools to simplify DNSSEC management

Lab Exercise: The DS record and interacting with your parent

- Closing the signature chain from the parent
- Verification of the signature chain
- Debugging

Resolver issues

- Suitable API
- Securing the "last mile"
- The requirement for a "clear path"

Lab Exercise: Key Rollover of ZSK and KSK

- Logging

DNSSEC Protocol extension: ADE (Authenticated Denial of Existence)

- Why is ADE so important?
- NSEC: Filling out the empty space to facilitate ADE
- NSEC3: When zone contents must not be listed
- Lab Exercise: NSEC3

DNSSEC high-level tools

- ZKT
 - Lab: ZKT
- OpenDNSSEC
 - Lab: OpenDNSSEC
- Others

International outlook:

- Signing different Top-Level domains
- Signing the root zone
- Development and and adjustment of different systems for DNSSEC

Summary

End of course