DNSSEC key management

Splitting of key management teams

CZ.NIC
Jaromír Talíř / *jaromir.talir@nic.cz*
24.10.2012

CZ DOMAIN REGISTRY

Agenda

- Current state – ZKT and online keys
- HSM testing
- Splitting into two DNSSEC teams
- Extended key management ceremony
- Conclusion

Current state

- ZKT – DNSSEC Zone Key Tools
  - Wrapper around Bind tools (dnssec-keygen, dnssec-signzone)
- Using filesystem storage, keys are online
- KSK rotates manually as needed
  - Passed only once last year with algorithm change
- ZSK rotates automatically every 2 month
  - Requires to have both KSK and ZSK online
- Administered by single DNS zone management team

HSM testing

- Sun/Oracle SCA6000
- Solaris or RedHat drivers, patched versions for Ubuntu
- Cancelled support from Oracle
- PKCS11 support in Bind
  - Patched version of OpenSSL
  - Patched version of Bind to use PKCS11 directly
- Maintaining patched versions is a nightmare
  - Upgrades are complicated

Splitting of management teams

- KSK compromise identified as biggest risk
- Responsibility for KSK passed to CSIRT security team
  - Knowledgeable team for security issues
  - HW: notebook, TPM/smartcard tested
  - KSK kept offline in safe inside notebook + backups
- DNS zone management team keeps responsibility for ZSK
  - No access to HW with KSK

Extended DNSSEC ceremony

- Planned to be done twice a year
- ZSK team pregenerates ZSK keys for given period
- ZSK's are grouped to DNSKEY RRSet
  - Based on time intervals with key rotation incorporated
  - KSK added
  - KSK+ZSK1, KSK+ZSK1+ZSK2, KSK+ZSK2, KSK+ZSK2+ZSK3....
- Result is PGP signed and passed to KSK team
- KSK team signs each RRSet and extends it with RRSIGs
- Result is PGP signed and passed back to ZSK team

Conclusion

- Advantages
  - Better security
- Disadvantages
  - No tools – back to shell scripts
  - More manual work – exchange of signing requests
- Plan
  - Evaluation is in process within ENUM domain – 0.2.4.e164.arpa
  - CZ will follow based on experiences

Questions ?

jaromir.talir@nic.cz

CZ DOMAIN REGISTRY