HSMs and DNSSEC

John Dickinson

Michele (Mike) Hjörleifsson

AEP Networks, Inc.

john.dickinson@aepnetworks.com | mikeh@aepnetworks.com

HSM Intro

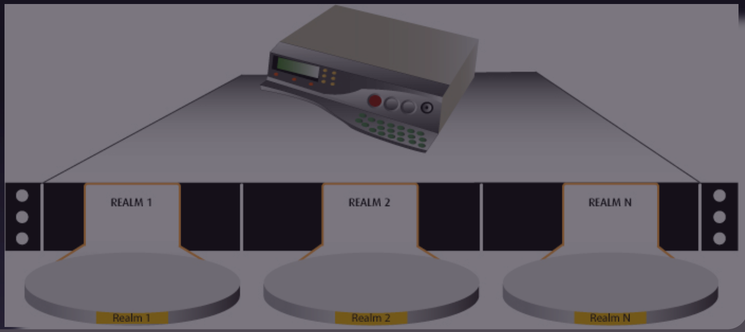
- What is an HSM ?
  - Do we really need to protect keys ?
  - Cryptography profiles
- Why use an HSM ?
  - Cost of loss vs. Cost of protection
  - Random number generation / PC v Appliance

HSM Intro

- Overall Features ?
  - Role Based Security
  - Tamper Profile
- HSM vs Others
  - SSL Accelerator
  - SmartCard
  - CryptoBoundry vs. True HSM

HSM Intro

- FIPS
  - Level 2, Level 3, Level 4
  - Why Level 4
- Benefits of Network Based Level 4
  - Physical security requirement
  - Shared device
    - Independent but equal



Using an HSM

PKCS#11 directly

- Comes with the HSM
- Platform independent
- Understands managing keys in HSM
- Provides functions to perform crypto operations
- All the crypto you need to write DNSSEC code
- Difficult to learn
- Not widely known

Using an HSM

- OpenSSL using an engine
  - PKCS #11 engine (e.g. OpenSC)
  - Proprietary engine
  - Can not manage keys
  - Can only use them
  - Documentation can be hard to follow
  - Many API's (Need to use EVP)
- No “correct” way!

Using an HSM

Even within a single application there is no consensus on how access hardware

For example OpenSSH 4.7.p1

- Smartcard support using libsectok
- Smartcard support using OpenSC
- Enable OpenSSL (hardware) ENGINE support
- Patches from Alon Bar-Lev use pkcs#11 directly
- http://alon.barlev.googlepages.com/open-source

Using an HSM

There is a need for more language support

There is no Perl module for either the OpenSSL EVI API or PKCS#11

http://blog.nominet.org.uk/tech/2007/04/22/using-perls-inlinec-to-call-openssls-evp-and-engine-libraries/

Using an HSM

DNSSEC

- First generation of tools store private keys in an unencrypted file!
- Trying to add HSM functionality can be hard
- All the tools use OpenSSL
- Did not use EVP API
- Tools use their own code to handle the keys

Using an HSM

Lots of work going on to add HSM support to DNSSEC tools

- Nominet
  - http://public.oarci.net/files/dnsops-2007/Dickinson-Crypto.pdf
- Rick Lamb
  - Patches to bind 9.4
- ISC
- NLNet Labs
  - Beta code available for ldns and ldns-signzone
- http://keihatsu.kirei.se/trac/dnssec/wiki/HSM

Using an HSM

It does work!

DNSSEC can be done with an HSM right now.

It will only get easier!