Software For Cryptech Alpha

Rob Austein <sra@hactrn.net>

Berlin
July 2016

Overview

- Firmware: Pre-built images suitable for flashing onto your HSM
- Software: Code that runs on your computer to talk to the HSM
- Binary packages for Debian (Jessie) and Ubuntu (Xenial)
- Source package for OSX (Homebrew)
- Repositories so you can `apt-get install` or `brew install`
- All source available, packaging is just a convenience

Firmware

- Output of Verilog synthesis and ARM cross-compilation
- Compressed tarball, same on any host (runs on none of them)
- Includes PGP-signed manifest, which includes SHA-256 digests
- Firmware upgrade script understands tarball format
- Firmware upgrade script does not yet check signature (sorry)

Software

PKCS #11 library `.../lib/libcryptech-pkcs11.*`

HSM port probe `.../bin/cryptech_probe`

HSM firmware upgrade `.../bin/cryptech_upload`

HSM console tool `.../bin/cryptech_miniterm`

libcryptech-pkcs11

- PKCS #11 implemented as Cryptech RPC protocol client
- SHA-1, SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512)
- RSA (1024–8192 bit) and EDSA (P-256, P-384, P-521)
- Plain signature and verification
- Signature and verification combined with hashing
- Default configuration hashes in `libcryptech-pkcs11`, not over RPC, but you can change this at compile time.
- Uses environment variables set by `cryptech_probe`

cryptech_probe

- Pokes at likely-looking USB ports to figure out what's connected
- Sets environment variables, like `ssh-agent`
- Don't read this script if you've eaten recently
- Run thusly:

  ```
  eval `cryptech_probe`
  ```

  or

  ```
  eval `cryptech_probe -v`
  ```

cryptech_upload

- Uses environment variables set by `cryptech_probe`
- Use `–firmware` to upload ARM image from firmware tarball
- Use `–fpga` to upload FPGA bitstream from firmware tarball

cryptech_miniterm

- Uses environment variables set by `cryptech_probe`
- Connects to HSM console using toy terminal emulator from PySerial
- Feel free to use some other terminal emulator (*e.g.*, `picocom`)

Installing from APT (Debian Jessie and Ubuntu Xenial)

Configure

```
$ base=http://apt.cryptech.is
$ key_url=$base/apt-gpg-key.asc
$ src_url=$base/sources.$(lsb_release -cs).list
$ src_apt=/etc/apt/sources.list.d/cryptech.list
$ wget -O - $key_url | sudo apt-key add -
$ sudo wget -q -O $src_apt $src_url
$ sudo apt-get update
$ sudo apt-get install cryptech-alpha
```

Update

```
$ sudo apt-get update
$ sudo apt-get upgrade
```

Installing from Homebrew (OSX)

Configure

```
$ url=https://brew.cryptech.is/tap
$ brew tap cryptech/sw $url
$ brew update
$ brew install cryptech-alpha
```

Update

```
$ brew update
$ brew upgrade
$ brew cleanup
```