Introduction to Hardware Security Modules

Joseph Birr-Pixton
@jpixton
http://jbp.io/

Intro to HSMs

1. What's a HSM?

Intro to HSMs

1. What's a HSM?
2. Who buys them?

Intro to HSMs

1. What's a HSM?
2. Who buys them?
3. What do they do?

Intro to HSMs

1. What's a HSM?
2. Who buys them?
3. What do they do?
4. And not do?

Intro to HSMs

1. What's a HSM?
2. Who buys them?
3. What do they do?
4. And not do?
5. 'Fun' with standards

Introduction

Who the hell am I?

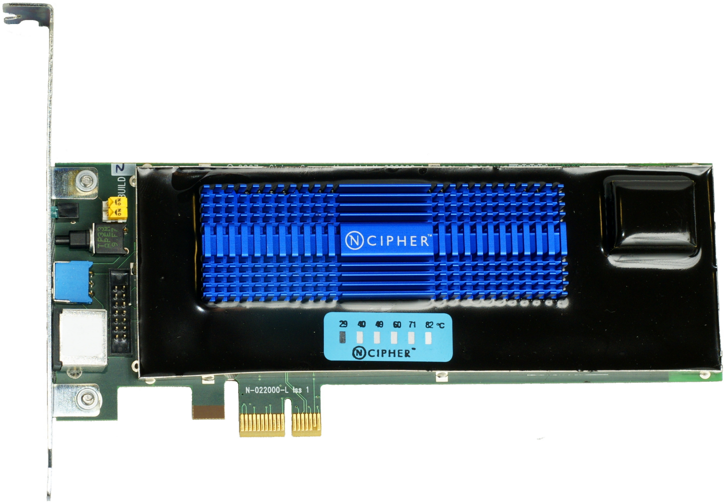
- Wrote software and firmware for nCipher 2005-2012.

Introduction

Who the hell am I?

- Wrote software and firmware for nCipher 2005-2012.
- nCipher acquired by Thales 2008.

WTF is an HSM?



WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.

WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.
- Often with a commercial or custom crypto accelerator.

WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.
- Often with a commercial or custom crypto accelerator.
- A communications path to talk to the thing (PCI, PCIe, ethernet, USB, etc.)

WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.
- Often with a commercial or custom crypto accelerator.
- A communications path to talk to the thing (PCI, PCIe, ethernet, USB, etc.)
- Hardware typically has physical protection:

WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.
- Often with a commercial or custom crypto accelerator.
- A communications path to talk to the thing (PCI, PCIe, ethernet, USB, etc.)
- Hardware typically has physical protection:
  - *Tamper evident* hardware usually potted in epoxy-based compound.

WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.
- Often with a commercial or custom crypto accelerator.
- A communications path to talk to the thing (PCI, PCIe, ethernet, USB, etc.)
- Hardware typically has physical protection:
  - *Tamper evident* hardware usually potted in epoxy-based compound.
  - *Tamper reactive* hardware usually enclosed in tamper sensing membrane, with active response circuitry within.

WTF is an HSM?

- Usually built from general purpose CPU, RAM, non-volatile storage.
- Often with a commercial or custom crypto accelerator.
- A communications path to talk to the thing (PCI, PCIe, ethernet, USB, etc.)
- Hardware typically has physical protection:
  - *Tamper evident* hardware usually potted in epoxy-based compound.
  - *Tamper reactive* hardware usually enclosed in tamper sensing membrane, with active response circuitry within.
- Tamper reactive hardware rare in HSMs; more common in things in adversarial environments like payments terminals.

Who buys them?

Payments HSMs:

- Single-purpose.

Who buys them?

Payments HSMs:

- Single-purpose.
- Implement various financial crypto standards, but rarely anything else.

Who buys them?

Payments HSMs:

- Single-purpose.
- Implement various financial crypto standards, but rarely anything else.
- Sold entirely to banks, payments processors, financial services.

Who buys them?

Payments HSMs:

- Single-purpose.
- Implement various financial crypto standards, but rarely anything else.
- Sold entirely to banks, payments processors, financial services.

General purpose HSMs:

- Standard, sometimes modern crypto.

Who buys them?

Payments HSMs:

- Single-purpose.
- Implement various financial crypto standards, but rarely anything else.
- Sold entirely to banks, payments processors, financial services.

General purpose HSMs:

- Standard, sometimes modern crypto.
- Integration with standard APIs (OpenSSL, PKCS#11, Microsoft CNG, etc.)

Who buys them?

Payments HSMs:

- Single-purpose.
- Implement various financial crypto standards, but rarely anything else.
- Sold entirely to banks, payments processors, financial services.

General purpose HSMs:

- Standard, sometimes modern crypto.
- Integration with standard APIs (OpenSSL, PKCS#11, Microsoft CNG, etc.)
- Sold to governments and industry.

What do they do?

- Well, crypto...

What do they do?

- Well, crypto…
- But mainly: key management.

What do they do?

- Well, crypto...
- But mainly: key management. Like:
  - Dual control: 'any 3 of these 5 people can use the key'

What do they do?

- Well, crypto...
- But mainly: key management. Like:
  - Dual control: 'any 3 of these 5 people can use the key'
  - Complex key policies: 'this RSA key can only decrypt using OAEP'

What do they do?

- Well, crypto...
- But mainly: key management. Like:
  - Dual control: 'any 3 of these 5 people can use the key'
  - Complex key policies: 'this RSA key can only decrypt using OAEP'
  - Providing a decent way to back up key material

What don’t they do?

- HSMs don’t know best; they do what they’re told

What don’t they do?

- HSMs don’t know best; they do what they’re told
  - Compromised hosts are a common overall problem with systems containing HSMs.

What don't they do?

- HSMs don't know best; they do what they're told
  - Compromised hosts are a common overall problem with systems containing HSMs.

DigiNotar®
A VASCO COMPANY

What don't they do?

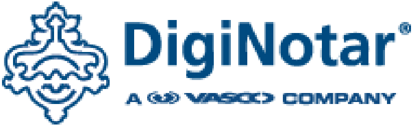
- HSMs don't know best; they do what they're told
  - Compromised hosts are a common overall problem with systems containing HSMs.

    DigiNotar®

    A VASCO COMPANY
  - Understanding and expressing the policy you want is an ongoing problem.

What don’t they do?

- HSMs don’t know best; they do what they’re told
  - Compromised hosts are a common overall problem with systems containing HSMs.

  - Understanding and expressing the policy you want is an ongoing problem.
- Don’t do crypto any quicker (in general) than software running on a modern CPU.

What don’t they do?

- HSMs don’t know best; they do what they’re told
  - Compromised hosts are a common overall problem with systems containing HSMs.

    DigiNotar®

    A VASCO COMPANY
  - Understanding and expressing the policy you want is an ongoing problem.
- Don’t do crypto any quicker (in general) than software running on a modern CPU.
- Don’t fix a system using rubbish crypto (RC4, unauthenticated block cipher modes, RSA PKCS#1 encryption, MD5/SHA1 signatures, ...)

‘Fun’ with standards

- Most (75%?) of custom is driven by ‘compliance.’

‘Fun’ with standards

- Most (75%?) of custom is driven by ‘compliance.’
- Other customers are eager/paranoid security folks.

‘Fun’ with standards

- Most (75%?) of custom is driven by ‘compliance.’
- Other customers are eager/paranoid security folks.

- FIPS 140-2 is the main standard for HSMs (and software crypto modules).

‘Fun’ with standards

- Most (75%?) of custom is driven by ‘compliance.’
- Other customers are eager/paranoid security folks.

- FIPS 140-2 is the main standard for HSMs (and software crypto modules).
- Implemented crypto standards come from NIST, IEEE, ANSI, KISA, etc. usually at request of customers.

‘Fun’ with standards

- Most (75%?) of custom is driven by ‘compliance.’
- Other customers are eager/paranoid security folks.
- FIPS 140-2 is the main standard for HSMs (and software crypto modules).
- Implemented crypto standards come from NIST, IEEE, ANSI, KISA, etc. usually at request of customers.
  - Some requests are ‘interesting.’

Fin

Questions?

Twitter: @jpixton
Web: http://jbp.io/