Introduction to Hardware Security Modules

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

Contents

1. Intro.

Introduction

Who the hell am I?

Introduction

Who the hell am I?

1. Wrote software and firmware for nCipher 2005-2012.

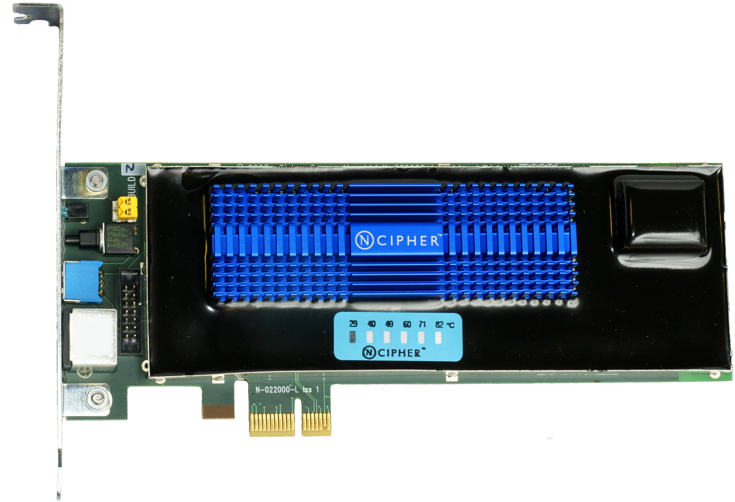
Introduction

Who the hell am I?

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

WTF is an HSM?

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.
- Some 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.
- Some 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.
- Some 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.
- Some 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.

Fin

Questions?