Hardware security modules

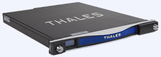
A brief introduction

Fabian Schierok
fabian.schierok@udo.edu

August 23, 2024

1 What is a HSM?

- Hardware Security Modules (HSMs) are physical devices that provide tools for a secure encryption.
- They come in different form factors for different applications.
- Most people carry a HSM in their pocket every day, in form of a credit/debit card.



An example of a HSM for installation in a server rack from Thales[1].

A very portable HSM from Yubico[2].

[1] Thales Group. *Hardware-Sicherheitsmodule*. 2024. URL: https://cpl.thalesgroup.com/de/encryption/hardware-security-modules

[2] Yubico. *YubiHSM 2 FIPS*. 2024. URL: https://www.yubico.com/de/product/yubihsm-2-series/yubihsm-2-fips

2 Why use a HSM?

- An encryption is only as private as the key used to encrypt it.
- HSMs provide a secure environment for key generation, storage and management.
- Using dedicated and specialized hardware has many advantages:
  - Faster encryption/decryption
  - Better power efficiency
  - Fewer attack vectors
  - Less knowledge required to use them

3 What is in a HSM?

The industry is secretive about the exact details of their HSMs, but some common features are:

Secure key storage: A taper resistant storage for keys. Only the HSM can access it.

True random number generators: A source of true randomness for key generation.

Secure execution environment: The brain of the HSM, where all the math happens.

Physical security: A suite of physical security measures to prevent tampering, for example temperature sensors or vibration sensors.

Secure communication: A secure channel to communicate with the HSM. It shields the HSM against some types of attacks, for example the heard-bleed exploit.

4.1 How could one attack a HSM?

Through the communication channel and audited software, there should be no logical way to attack a HSM. However, there are some physical attacks that could be attempted:

- Power monitoring
- Cold boot
- Probing
- RNG seeding

4.2 Power monitoring

Attack

When a key is used in binary form, the encryption boils down to ”if bit is 1, do this, if bit is 0, do that”. When ”this” and ”that” have different power consumption, an attacker could monitor the power consumption of the HSM and deduce the key.

Defense

The power consumption must be decoupled from the operations performed. Possible solutions are:

- Insert random delays
- Add dummy operations
- Add noise or smooth the power consumption

4.3 Cold boot

Attack

After powering off the HSM, the RAM is still readable for a short period of time. This time can be extended by cooling the RAM.

Defense

The RAM must be cleared when the HSM is powered off. Possible solutions are:

- Use of a battery to ensure a proper shutdown
- The RAM must be securely overwritten
- Ensure self destruction at extreme low temperatures

4.4 Probing

Attack

An attacker could probe the HSM with a needle and measure the voltage on the needle. This could give the attacker information about the internal workings of the HSM.

Defense

The HSM must detect physical intrusion. Possible solutions are:

- Encase the HSM in a harden shell
- Use a vibration sensor to detect probing
- Surround the HSM with a mesh that will short-circuit the HSM when probed

4.5 RNG seeding

Attack

If the RNG of the HSM is depending on some outside influence, an attacker could manipulate the RNG and predict the keys generated by the HSM.

Defense

The RNG must be truly random. Possible sources are:

- Decay of a radioactive isotope
- brownian motion
- Use of a quantum RNG

”The Wall of Entropy” by CloudFlare[3].

[3] CloudFlare. *How do lava lamps help with Internet encryption?* 2024. URL: https://www.cloudflare.com/en-gb/learning/ssl/lava-lamp-encryption/

Fabian Schierok

Essen, August 23, 2024

fabian.schierok@udo.edu