Hardware Security Modules

Jan GOETTE, Mori Lab/Humboldt University of Berlin

May 2019

What? *and* Why?

- **An HSM...**
  1. is a hardware component
  2. is providing some form of API (fully programmable/key mgmt/etc.)
  3. actively erases secrets when tampered with
  4. generally contains a battery and is alwasy-on
- **An HSM is not a smartcard**

HSM

- Always powered
- Active tamper detection

Smartcard

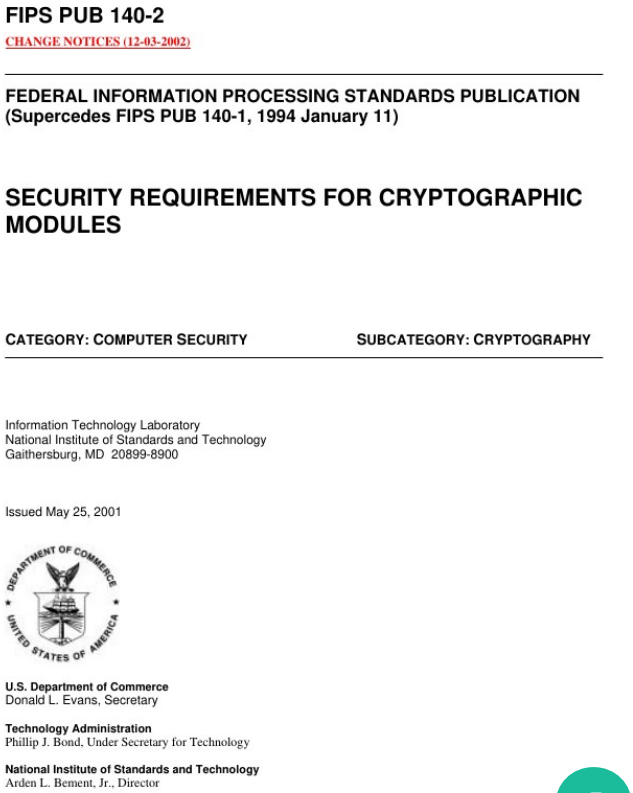
- Powered off most of the time
- Active tamper detection

Usage scenarios

- **CA keys (TLS/code signing)**
  - Asymmetric signing keys
- **Credit card data**
  - Symmetric keys (encryption and authentication)
- **Smart meters**
  - Asymmetric keys (client certificates)
  - Measurement circuitry
- **Misguided attempts at VPN**
  - Symmetric keys
- **Digital Restriction Management**
  - Symmetric keys
- **Electronic ID documents**
  - Asymmetric signing keys
  - potentially private data sometime in the future

Relevant Standards

- **FIPS 140-2 (US govt)**
  - US government standard for cryptographic modules
- **PCI DSS (PCI SSC)**
  - “Payment Card Industry Security Standards Council”
  - Formed by Visa, MasterCard, American Express, Discover, JCB
  - Defines requirements to merchants for processing CC payments
- **In both cases: Few concrete criteria, mostly to cert lab**



FIPS PUB 140-2

CHANGE NOTICES (12-03-2002)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Issued May 25, 2001

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director

FIPS 140-2

- US government standard for crypto-graphic modules
- Four levels, only level 4 is meaningful!
- Active countermeasures, security envelope

→ See: `https://en.wikipedia.org/wiki/FIPS_140-2`

PCI DSS

- “Payment Card Industry Data Security Standard”
- Enforcement also through fines
- Contains requirements for hard- and software involved in CC data processing
- Most interesting: Requirements to HSMs
- Standard open, but overly vague.
  Specific requirements are not public.

→ See: `https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard`

Commercial products

- Thales, Rohde&Schwarz, IBM, Utimaco,...
- Main form factors: Card terminal, PCI(e) card, 1HU rackmount
- From full CPU access to high-level crypto API
- Processing power
  in O(smartphone ARM processor)

Common defense techniques

- **Security-by-obscurity (industry favorite!)**
- Switches
- Meshes: the only effective technique
- Potting makes meshes more effective
- Light/vibration sensors
- Temperature sensors may be necessary

Common defense techniques

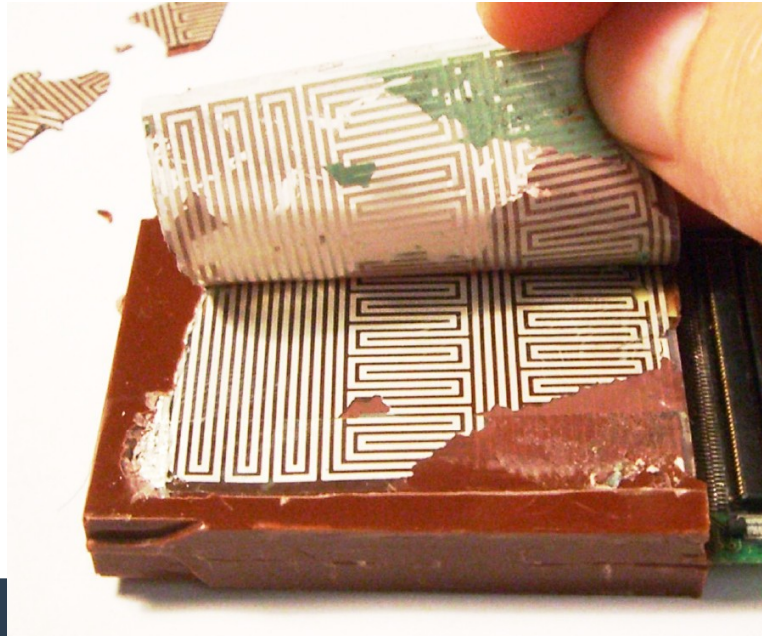
- Security-by-obscurity (industry favorite!)
- Switches
- Meshes: the only effective technique
- Potting makes meshes more effective
- Light/vibration sensors
- Temperature sensors may be necessary

Common defense techniques

- Security-by-obscurity (industry favorite!)
- Switches
- **Meshes: the only effective technique**
- Potting makes meshes more effective
- Light/vibration sensors
- Temperature sensors may be necessary

Common defense techniques

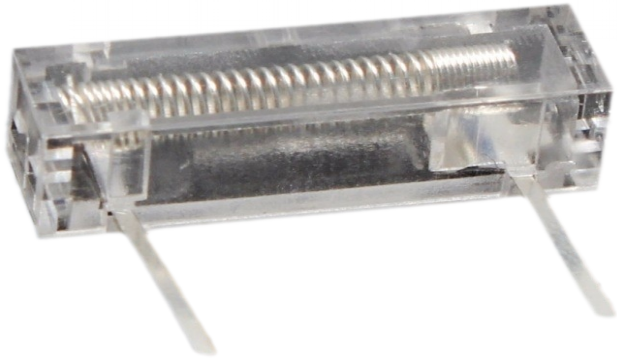
- Security-by-obscurity (industry favorite!)
- Switches
- Meshes: the only effective technique
- **Potting makes meshes more effective**
- Light/vibration sensors
- Temperature sensors may be necessary



Common defense techniques

- Security-by-obscurity (industry favorite!)
- Switches
- Meshes: the only effective technique
- Potting makes meshes more effective

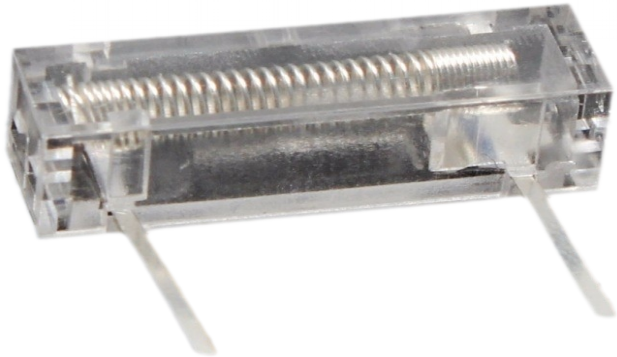
- **Light/vibration sensors**
- Temperature sensors may be necessary



Common defense techniques

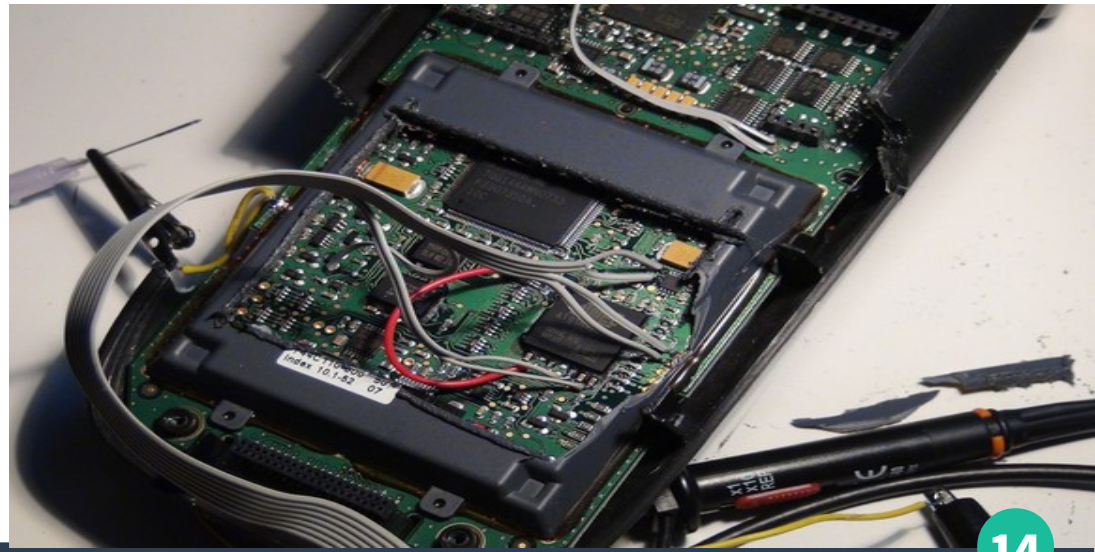
- Security-by-obscurity (industry favorite!)
- Switches
- Meshes: the only effective technique
- Potting makes meshes more effective

- Light/vibration sensors
- Temperature sensors may be necessary



Practical attacks

- **Cold boot, SRAM remanence**
  - Turn off, then scrape remains of data out of memory
- **Drilling/lasers**
  - Mesh at best provides upper bound at size of probe
  - Good meshes: several hundred µm
- **Disabling the monitoring circuit**
- **Bypassing the mesh**



Usage scenarios

Good fit

- Instant Messaging encryption
- email encryption & authentication
- Secure Boot/HW root of trust

→ **Limited attack budget, robust system**
(limited scope of attack)

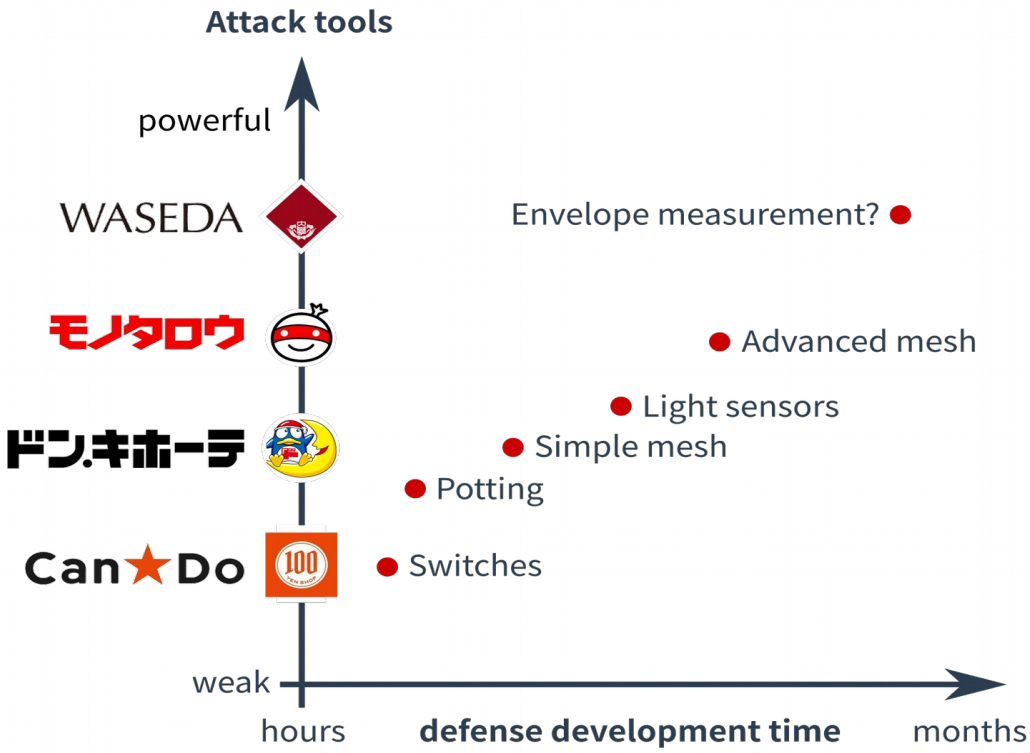
Bad fit

- Certificate authorities
- DRM

→ **Unbounded attack budget, fragile system**
(one successful attack suffices)

Take-aways?

- Even a very good HSM only adds to the cost of a **one-off attack 10k US$ to 100k$**.
- Be careful who you listen to. **Lots of wrong information** around! (ex.: anything that speaks USB is in general not an HSM!)
- Consider actually **solving the underlying algorithmic problem instead** of using band-aids.
- Designing your own **HSM is not complicated** if you know what to look out for!
- HSMs are **only useful in very specific scenarios**!



Questions

Research Ideas!

Research directions

- **Open source HSM reference design** to serve as a research reference standard
  - General architecture
  - Mesh construction with small-lab resources
- **Novel tamper detection techniques**
  - Acoustic: MEMS/Piezo microphones
  - Envelope measurement (Radar/Optics/Ultrasonic acoustics)
  - Use triboluminescence for mechanical tamper detection

Take-aways?

- Even a very good HSM only adds to the cost of a **one-off attack 10k US$ to 100k$**.
- Be careful who you listen to. **Lots of wrong information** around! (ex.: anything that speaks USB is in general not an HSM!)
- Consider actually **solving the underlying algorithmic problem instead** of using band-aids.
- Designing your own **HSM is not complicated** if you know what to look out for!
- HSMs are **only useful in very specific scenarios**!

Image sources

- **Title page image: Central Midori Demmel Group website**
  - https://cdn2.hubspot.net/hubfs/2386245/header1.jpg
- **Red smartcard: USA Today - Many retailers haven't met deadline for chip-card readers**
  - https://www.usatoday.com/story/money/business/2015/10/01/chip-credit-debit-card-readers-october-1/73140516/
- **PCIe HSM: TSSL product page for Gemalto Safenet ProtectServer SSL http://www.tssl.com/tsslweb/wp-content/uploads/2014/11/product_safenet_luna_pcie1200x800.png**
  - http://www.tssl.com/project/luna-pci-e/
- **MyNumber cards: RBB Today**
  - https://www.rbbtoday.com/imgs/p/RqJIzsl7cmxG8-cARbeaqilNLEDQQ0JFREdG/496199.jpg
- **FIPS PUB 140-2: US NIST FIPS PUB 140-2**
  - http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- **FIPS LOGO: US NIST FIPS Logo form**
  - https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402LogoForm.pdf
- **Black security mesh: PCWorld - ORWL PC: The most secure home computer ever**
  - https://www.pcworld.com/article/3118264/orwl-pc-the-most-secure-home-computer-ever.html
  - https://images.techhive.com/images/article/2016/09/dsc09431-100681691-orig.jpg
- **Black expoxy: AET Sp. z o.o. Sp.k.**
  - https://en.aet.com.pl/RESINS-AND-VARNISHES
  - https://en.aet.com.pl/portals/0/images/1%20%C5%BCywica.jpg
- **Ingenico HSM (brown epoxy): Saar Drimer, Steven J. Murdoch, Ross Anderson - Security Failures in Smart Card Payment Systems: Tampering the Tamper-Proof, 25th Chaos Communication Congress, Berlin, Germany, 2730 December 2008**
  - https://murdoch.is/talks/
  - https://murdoch.is/talks/ccc08tamper.pdf
- **Light sensor: ModuleFans Aliexpress store, Guangdong, China**
  - https://www.aliexpress.com/store/612195
  - https://www.aliexpress.com/item//32673563904.html
- **Vibration sensor: DIKAVS Aliexpress store, Guangdong, China**
  - https://www.aliexpress.com/store/1552478
  - https://www.aliexpress.com/item//32686838884.html
- **Verifone HSM hack: Security Research Labs GmbH, Berlin, Germany**
  - https://srlabs.de