Surveying the Physical Landscape

What do we mean by “physical security”?

Some might think about this …

Or this …

Or …

For this presentation, we mean protection from attackers with physical access to a device.

Case study: FIPS 140-2 minimum requirements

	All Embodiments	Single Chip	Multi-chip Embedded	Multi-chip Standalone
Level 1	Production grade, passivation	No additional requirements	Enclosure, cover (if applicable)	Enclosure
Level 2	Tamper evidence, opacity	Opaque tamper evident coating	Opaque tamper evident material / enclosure Tamper seals or pick resistant locks for doors or removable covers	
Level 3	Penetration resistance; Maintenance access tamper response.	Hard coating, or strong removal/penetration resistant enclosure	Hard opaque encapsulating material or penetration resistant enclosure Removal attempts cause serious damage	
Level 4	Temperature, voltage protections or testing	Chemical agent characterization	Tamper detection/response envelope with tamper response and zeroization circuitry	

What is meant by terms like "hard" or "strong"?
What is the FIPS 140-2 intent?

FIPS 140-2 interpretation of physical security

Implementation Guidance articles

- Level 2 opacity and probing for modules with fans, vent holes, slits
- Testing tamper evident seals
- Hard coating test methods (defines “hard”)
  - Tests over temperature range … but … no milling, drilling, grinding
- Level 3 + EFP/EFT

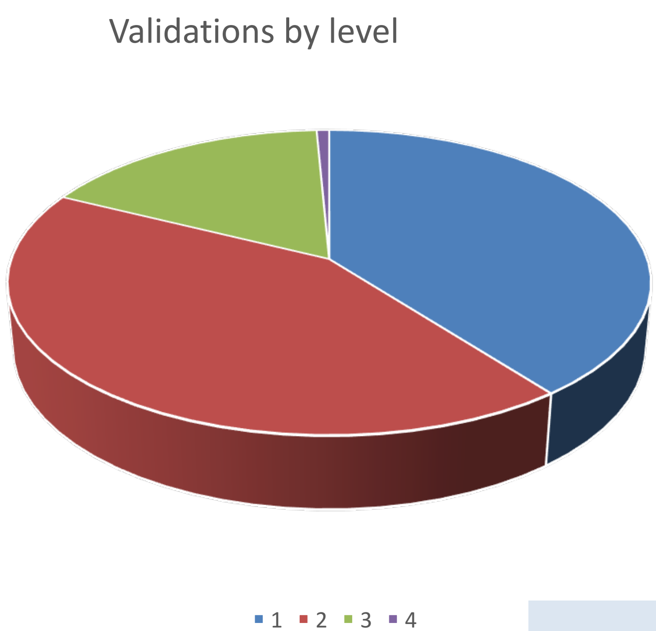
- IG 5.3 Physical security assumptions describes each level in terms of:
  - Protection provided, user assumptions and value
  - Attack type, characterization and testing assumptions

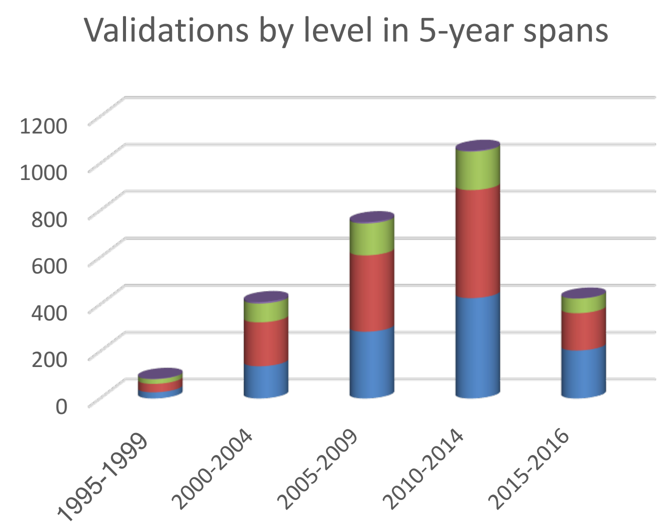
FIPS 140-2 physical security assumptions

	Protection provided User assumptions and value	Attack Type, characterization, assumptions
L1	**No protection or value.** User assumptions: correct function; used for scenarios with negligible data value	***Passive attack***; no prior access assumed. No tools and materials are assumed.
L2	**Awareness of tamper; no visible components.** Used for scenarios with low data value	***Active attack***; no prior access assumed. Readily available, low cost tools, materials Low attack time
L3	**Prevent (or … resist?) direct entry or probing.** Used for scenarios with moderate data value	***Moderately aggressive attack****;* prior access, basic knowledge of module assumed Moderate attack time
L4	**Module is tamper resistant against all physical attacks defined in the standard** Used for scenarios with high data value	***Aggressive attack****;* prior access, advanced knowledge of module, specialized tools No time restriction on attack

FIPS 140-2 is a 2001 standard .. How does that hold up today?
What do we see in practice?

FIPS 140-2 validation trends





	L1	L2	L3	L4	
1995-1999	26	36	20	2	84
2000-2004	137	187	80	7	411
2005-2009	284	325	136	6	751
2010-2014	427	460	164	4	1055
2015-2016	204	159	62	1	426
Subtotal	1078	1167	462	20	

2245 of 2727 validations are L1, L2

- *Negligible or low data value*
- *Tamper evidence and opacity*
- *Minimal testing*
- *Note: Some L4 physical security test occurs at Overall 2,3*

How do other standards approach physical security?

- In the majority of cases, PP based Common Criteria evaluations assume the device is physically secure.
  - When that physical security is not assumed, all data at rest must be encrypted.
- EAL based CC schemes and PCI use a costing model
  - Each asset must be protected to a threshold of how many “points” an attack would expend to perform a successful attack, where the points vary based on the asset (e.g. 26 points for PINs, 35 points for keys, etc.).
  - The points are assigned for each part of the attack: Time to perform the attack, expertise needed, type of information needed, etc.

How has hardware changed since 2001?

Paleo Physical Security

Single chip
- Feature sizes / geometry
- System on chip
- Multiple processors
- Security subsystems
- Crypto co-processors
- Security "annealing"
- Active shields
- Sensing and response

PCBs - less exposed circuitry
- Greater use of SoC
- *Lower* component counts for PCBs
- Flip chip, ball grids make access harder
- Heat sinks
- Chip-on-chip / 3-D packaging

Enclosures
- Rackmount devices are still the same size, shape, most are "air-breathing"
- Rise of virtualization, cloud computing
- Migration of boxes into bunkers

The DIY movement
- More open source (including IP cores)
- Cheaper tools
- More published information (e.g. teardowns)

FIPS 140-2 Physical Security Relevance & Value

- The value of 140-2 tamper evidence and opacity is diminishing
- In some scenarios, tamper evidence doesn't make sense
  - Single-chip (especially die boundary) practicality of inspection
  - Some IoT scenarios (like car-to-car) practicality of inspection
- In some scenarios, a defense in depth approach makes more sense
  - Identity card scenario and USB scenario
- Tamper response is higher value than tamper evidence
  - … but few devices support it
  - Some programs seeking tamper response with notification
- Prevalence of DIY tools, methods and information aids attackers
- FIPS 140-2 segregation of "other attacks" muddies assurance waters

- What about ISO 19790 / ISO 24759?
  - Re physical security, only incremental updates to FIPS 140-2

Evolution of attacks and protections

- Not surprisingly, more evolution has occurred at the IC level
- Tarnowski demonstration of IC attacks (2009 Blackhat)
  - Requires a lot of devices, skill and time
  - Diversification of secrets affects hack value
  - Active shields became more sophisticated
  - Features keep getting smaller
- Opacity considerations
  - Thermal imaging arguably better to understand IC design
  - Synthesized logic increases difficulty of pinpointing structures
- Emergence of more generalized fault resistant architectures
- Side channel awareness and countermeasures
- Hardware noise sources for better randomness

"…the potential for software security to overtake and end the reign of hardware in the cryptographic module space."

This statement is intended to provoke thought.

A shift in threat models combined with increasing complexity

- Impact of cloud services and virtualization …
- Mobile or IoT devices, SE, exposed network equipment require protections

- Software and firmware are easier to modify in place …
- Hardware is typically not updated once deployed.
  - Yet … the ease of SW/FW modification presents it's own issues.
  - Hardware root of trust still has a place.

- Some hardware protections (e.g. tamper evidence) are low-value
- An adequate noise source is a necessary element of key generation.

The focus is shifting to software security, but hardware security still has value.

- A defense-in-depth (AKA a layered defense) strategy has value.
- Strong physical /logical protections of crucial secrets has value.

THANK YOU.