Design tricks for great products at FIPS-140-2 Level 2 and 3

Robert W. Baldwin, Plus Five Consulting, Inc.

Abstract

This presentation may be downloaded from:
http://www.plusfive.com/reports.html or
RSA Conference site over next few months.

Abstract

Competition in the market for FIPS-140-2 validated products is intense, especially at Levels 2 and 3. Come learn about design tricks that allow your products to have compelling features and be easy to use without adding months to the FIPS-140-2 validation cycle.

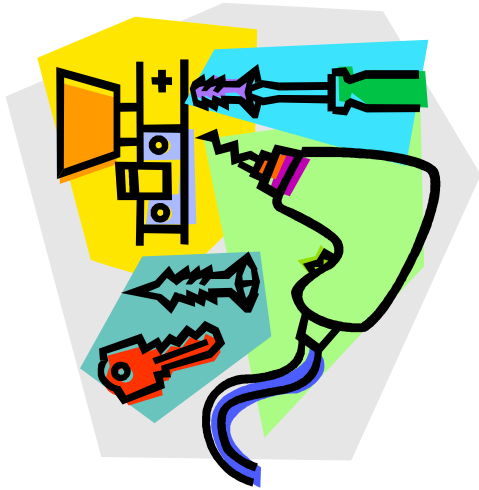
Dr. Baldwin has culled these “best practices” from years of helping vendors design FIPS-140 products.

The “Tricky” FIPS-140-2 Problems

- Physical Security
- Cooling and Safety Compliance
- Tamper Evidence and Response
- Testing Tricks
- Simplifying Device Initialization and Administration
- Integration with Enterprise Authentication

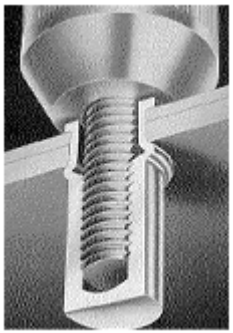
Physical Security

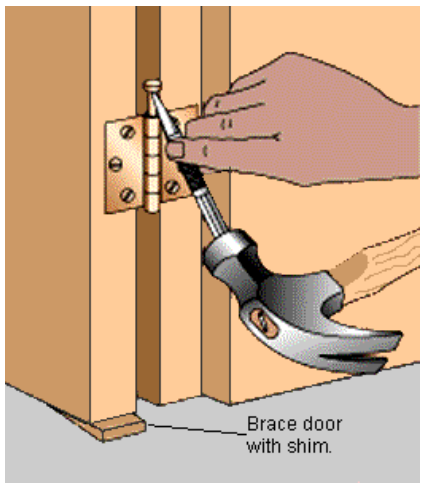
- Must be opaque.
  - Makes it harder to attackers to locate parts.
  - No line-of-sight from outside to active electronics
  - OK to see power supply
- Thwart probing
  - Rule of thumb: Cannot insert a 30 gauge wire
  - Tip: have tight overlapping seams
  - Tip: avoid gaps around connectors and faceplates
- Right angle bends in airflow protect against probing
  - Also helps with line-of-sight



Physical Security

- Flexing the metal (or plastic) box is allowed
- Removing connectors and plugs is allowed
- Removing Fasteners, Screws, Hinges, Clips, Snap-ins is allowed
- Tip: Blind nuts thwart unscrewing attacks





Snap-in connectors can be pried-out to expose components

Resist the Appeal of Potting

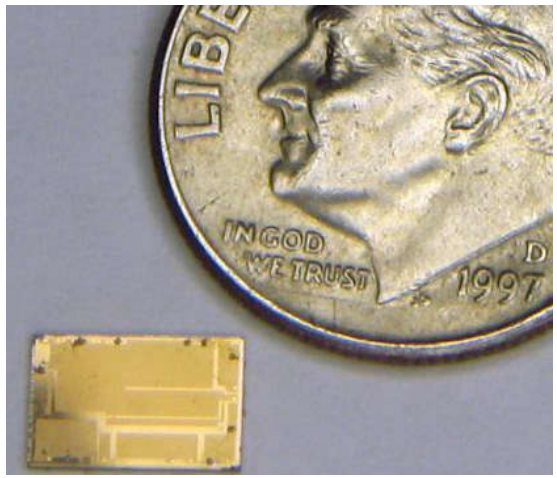
- Potting seems like a good solution (no battery, no holes)
- Post QA repair very hard
- Messy and time consuming
- Some potting can be cracked off with hot or cold bath

However:

- Without potting, need battery.
- Battery backup and zeroize feature is available as an inexpensive chip from Texas Instruments.

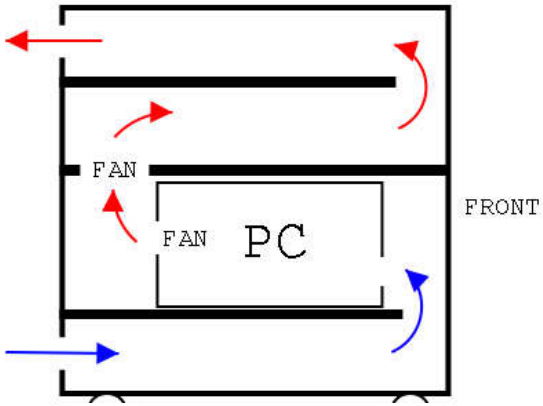
Keep Packaging Simple

- Box with cover, or fully self contained
- Understand threat model
  - No drilling or cutting the casing
  - No evident damage to case

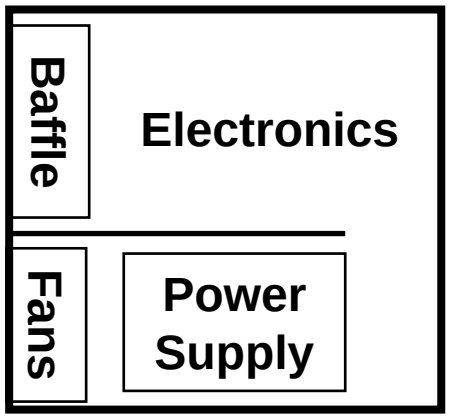


Cooling

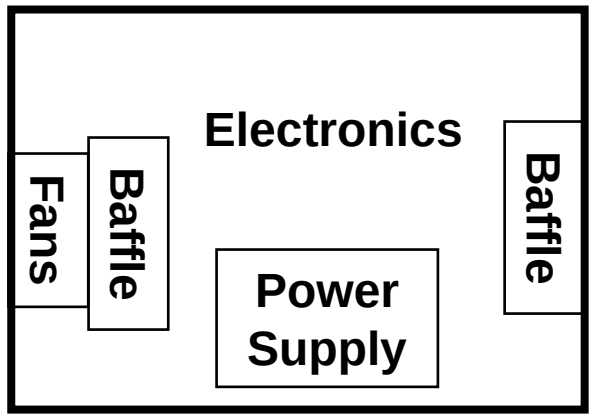
- Stopping fan to insert probe is allowed attack at Level 3
- Include extra airflow space in original design
- Measure temperatures early in mechanical design
- Common baffle configurations:



Extreme Retrofit



U-shaped air flow

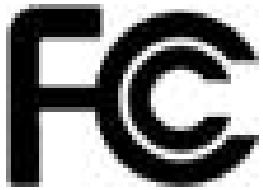


Pass through air flow

Baffle assemblies must include right angle bends

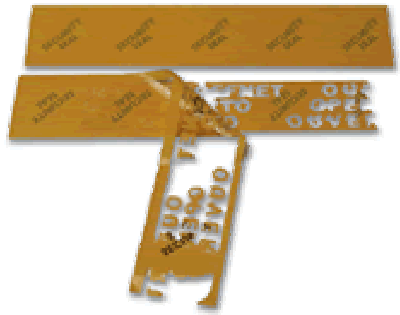
Safety Compliance

- Power safety rules vary widely throughout the world
- External power supplies may help solve Safety and Heat problems
- FCC Part 15 Subsection B (commercial) easier once product has Level 3 physical security
  - Due to shielding provided by metal parts complying with Level 3



Tamper Evidence

- Level 2: Tamper evidence only.
  - Details of stickers & paints are critical
  - Lab can use solvents and knife-edges to test seals
  - Tamper evidence is inexpensive to replicate once it is approved



Tamper Evidence Tips

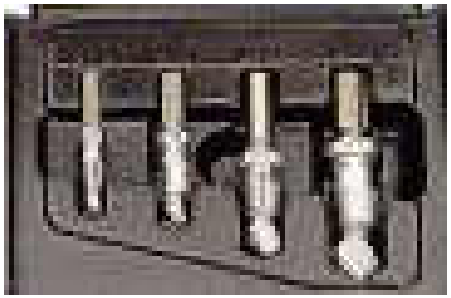
- Overlap seams of box
- Use just one seal if possible
- Inset nuts and spot welding good

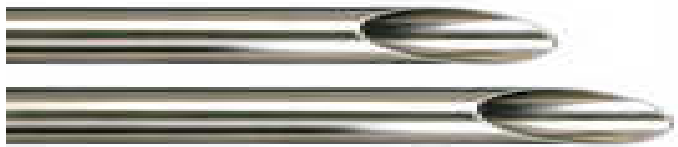
Tamper Evidence and Response

- Locks treated as removable covers
  - Level 3: Must zeroize when opened, then re-initialize after closed
- Level 3: Tamper detection and Zeroization – even if power off
  - Trick: Use single key to encrypt all other keys and passwords, then just need to zeroize that single key
  - Trick: No need to encrypt public keys
  - Trick: One HMAC-SHA-1 integrity check for whole configuration
- Texas Instruments sells $3 Clock & NVRAM with zeroize pin
  - http://focus.ti.com/docs/prod/folders/print/bq3287a.html

Tamper Evidence and Response

- Level 3 “FIPS game” played more seriously
  - Insert pry-bars that don’t permanently bend the case
  - Drill out screws that can be replaced
  - Custom-bent thin pipe used to spray glue on tamper switches
  - Expanding foam can hold down many switches





Tamper Evidence and Response

- Must avoid accidental Zeroization
  - Result can be expensive dead device needing factory service.
- Dangers can come from switches
  - Vibration or impact or air pressure
  - Trick: Use only one switch and deeply overlap product covers

- Danger can come from operators
  - Device must support a Zeroize command, so operator error could kill the product

Tamper Detection versus Logging

- FIPS-140-2 concept of tampering:
  - Device stops providing cryptographic services
  - Device zeroizes ALL unencrypted keys and passwords
  - Result: Dead product returned to factory

- Digital Cinema concept of logging:
  - Device stops providing cryptographic services
  - Must be able to prove tampering happened long after the fact
  - Administrative step is required to re-start cryptographic services
- Trick: Provide service to zeroize the logging key.
  - Generate new logging key. Record date-time and key hash.

Testing Tricks

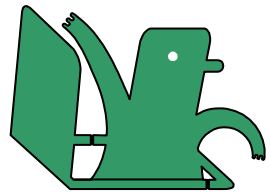
- NIST Algorithm Testing
  - Fast path to product visibility

NIST CMVP

- NIST requires custom tests. Hundreds of pages long.
  - Purchase an Algorithm Test Harness (e.g., from Plus Five)
  - Test Harness implements Monte Carlo and other tests
  - Use for correctness testing.
  - Use source code of harness to clarify meaning of NIST tests
- Corporate officer must certify results are from your real product.
  - Sample details: If CBC mode done by your product, you cannot use the ECB mode of the test harness to emulate CBC mode.

Testing Tricks

- Product must include instrumentation for FIPS-140 Operational Testing
  - OK to have test build to exercise operational tests that are described in the Derived Test Requirements Document
  - Must be able to confirm that testing features are not in real product



- Tools needed to speed Operational Testing
  - Cause every FIPS-140 error state (DRNG failure, self-test failure)
  - Set and Get all keys (test key mismatch, confirm zeroization)
  - Change Key-Entity association (trick: scripted breakpoints)
- Create Op Test Plan with help from Developers
  - Validation Lab reviews plan for completeness.
  - Over testing can avoid long delays.
  - Perform dry run one week before Validation Lab arrives.

Simplifying Device Initialization

- Level 3: Strict rules for Key Entry and Output
  - How get first key without hassles of such a device?
  - How avoid need for separate key loading device?
- Trick: Pre-load TLS key-pair and certificate during manufacturing
  - Device protects unencrypted keys and PINs with TLS
  - Enables key management over network
  - Recommend manufacturing modules with unique key-pairs
  - Allow Enterprise to replace these key-pairs and certificates
- Pre-loaded Passwords (if used)
  - Administer via TLS. Good to mark passwords as pre-expired.

Simplifying Device Administration

- Important services to support for a cluster of devices
  - Enroll new device in existing administrative cluster
  - Move device to a different administrative cluster
- Trick: Text file tables copied to initialize new or moved devices
  - For network distribution, use TLS
  - Each device has unique key-pair and certificates
  - Can use operator-specific passwords over TLS

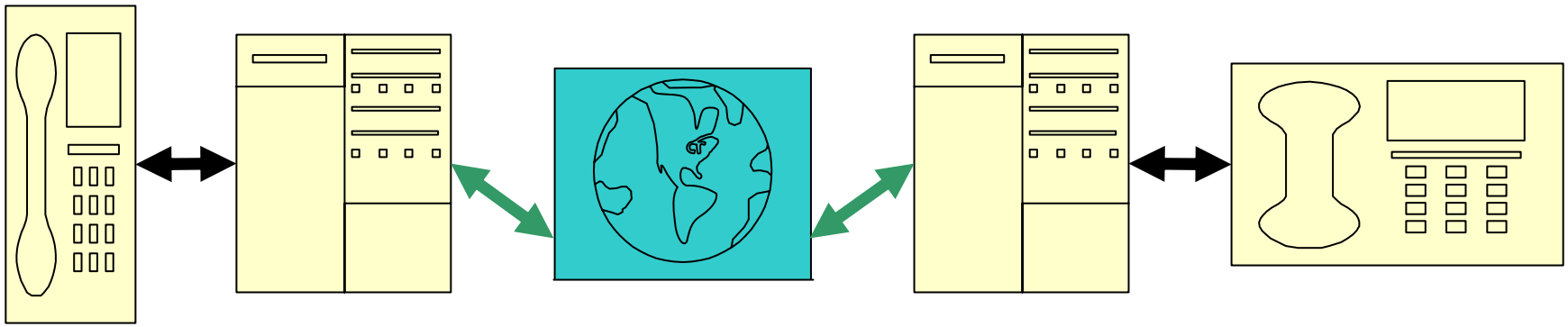
Simplifying Device Administration

- For physical distribution must comply with Level 3 Key Entry & Output rules
  - USB token
  - Smart card
  - Custom key loader

- Key splitting algorithms can simplify I/O of keys as multiple parts
- Trick: Load one high-entropy cluster-specific key
- Use cluster-specific key to protect and manage keys, passwords, PINs, roles and configuration options

Integration with Enterprise Authentication

- Example: Secure VoIP Hardware Product for an Enterprise
  - Unencrypted call starts via desktop software connecting over network to *Secure VoIP Hardware Product* and then on to other instances of the product located worldwide, and finally an unencrypted call is delivered to the destination user.



Hardware Product encrypts external VoIP connections

Integration with Enterprise Authentication

- Enterprise user authentication is HARD problem.
  - Each enterprise solves it slightly differently.
- Trick: Don't put the enterprise users in the FIPS-140-2 access model.
  - Each instance of the *Product* is authenticated via TLS & certificates.
  - The IT administrators are identified to the *Product* and authenticated via TLS with user certificates.
  - Enterprise user authentication data (Kerberos or NTLM) is treated as encrypted data passed over TLS sessions between instances of the *Product*.
  - Must carefully word the documentation on Key to Entity association.

Summary

There are best-practices tricks that can simplify:

- Physical Security
- Cooling and Safety Compliance
- Tamper Evidence and Response
- Testing Tricks
- Simplifying Device Initialization and Administration
- Integration with Enterprise Authentication