Fault Induction and Environmental Failure Testing

NIST CMVP
Physical Security Conference

Travis Spann

September 16, 2005

05-998-R-0064 Version 1.0

Table of Contents

List of Figures

1 Introduction

Fault induction is a process by which a device (and for the purpose of this discussion, in particular a cryptographic module) is forced to miscalculate defined operations, skip over required operations (such as password verification or self-tests), and exhibit other erroneous behaviors enabling the attacker (or tester) to gain access to sensitive data or unauthorized control of the device. Many regard fault induction as a new cutting edge technique. Terms such as covert attacks, side channel analysis add to a mystique surrounding this area of research. In reality, fault induction has been widely used by IC manufacturers, QA testing laboratories, and military entities as part of the normal manufacturing and QA testing process. Fault induction was originally used to test products during development to verify that functions could be performed over a wide range of operational parameters (e.g., temperature, voltage, shock, vibration, clock speed, electro-magnetic, etc.). By testing the cryptographic module within a variety of operational conditions, the testers would find single point failures that resulted in aberrated behavior that could lead to compromise of the system. An incremental process of inducing faults provides a process by which the tester can trace where problems are in the cryptographic module implementation, and then provide guidance and suggestion to the design and production team for redesign or process improvement. It's important to note that the design itself may not be flawed, rather the manufacturing and assembly process itself may have introduced weaknesses into the end product. From a historical perspective, asynchronous and analog components may have been more susceptible to fault induction attacks because of how the circuits worked due to higher correlation between voltage, temperature, and performance. Most of the focus for fault induction has been placed on single-chip cryptographic modules (such as smart cards), although this should not be the only focus area (or main focus area). Multi-chip devices are also susceptible to attack, and the concept we must remind ourselves is that an attacker will always go for the weakest point in the infrastructure.

2 Environmental Failure Testing (EFT)

The FIPS 140-2 standard includes Environmental Failure Testing (EFT) which combines several types of fault induction attacks into Level 4 testing requirements. It is important not to confuse Environmental Failure Protections (EFP) with EFT. With EFP, the cryptographic module contains active mechanisms to monitor and respond to fluctuations (accidental or induced) outside normal operating ranges for temperature and voltage. It is much easier to perform EFP testing because a set of thresholds are known (e.g. known range where the tamper response mechanisms will activate). Since the tester can determine where a module will fail, it's easier to collect the data. With EFT a series of tests are performed to ensure that fluctuations outside normal operating ranges for temperature and voltage will not compromise security of cryptographic module; however, the point at which the cryptographic module will fail is unknown so more scrutiny is required.

2.1 Testing Methodology

A simplified attack model for EFT can be summarized as follows: The attacker will obtain as much design information as possible, through data sheets, white papers, marketing literature, employees of the module vendor, etc. The attacker will create a specialized attack based upon the cryptographic module characteristics and he will leverage any analysis performed by other entities to place emphasis on known areas of weakness (e.g., a known faulty part). Physical samples of the cryptographic modules will also need to be obtained. There are many places where this type of attack could be performed including: universities, IC manufacturing facility, competing vendor facility, government, qualified laboratory, "Hired Hands" (e.g., ex military, Intel, etc.). The expected threat agents would be skilled or semi-skilled individuals with an electrical engineering and/or computer engineering/computer science background.

The FIPS 140-2 EFT testing methodology can be summarized as follows: The FIPS PUB 140-2 specifies that the "*temperature range to be tested shall be from -100° to +200° Celsius (-150° to +400° Fahrenheit). The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that causes the zeroization of the electronic devices or circuitry to the smallest positive voltage (with respect to ground) that causes the zeroization of the electronic devices or circuitry, including reversing the polarity of the voltages.*" The tester creates a series of matrices and graphs of operational parameters for temperature and voltages through analysis of component data sheets and other supporting documentation to create test cases such as the examples below:

Test #	**Temperature**	**Voltage**
1	Nominal temperature	Voltage low threshold
2	Nominal temperature	Exceed voltage low threshold
3	Nominal temperature	Voltage high threshold
4	Temperature low threshold	Nominal voltage
5	Temperature low threshold	Voltage low threshold
6	Temperature low threshold	Exceed voltage low threshold
7	Exceed temperature low threshold	Nominal voltage
8	Nominal temperature	Nominal voltage
9	Nominal temperature	Nominal voltage
10	Temperature low threshold	Voltage high threshold
11	Temperature low threshold	Exceed voltage high threshold
12	Nominal temperature	Exceed voltage high threshold
13	Temperature high threshold	Nominal voltage
14	Temperature high threshold	Voltage low threshold
15	Temperature high threshold	Exceed voltage low threshold
16	Temperature high threshold	Voltage high threshold
17	Temperature high threshold	Exceed voltage high threshold
18	Exceed temperature high threshold	Nominal voltage

Figure 1 - Environmental Conditions

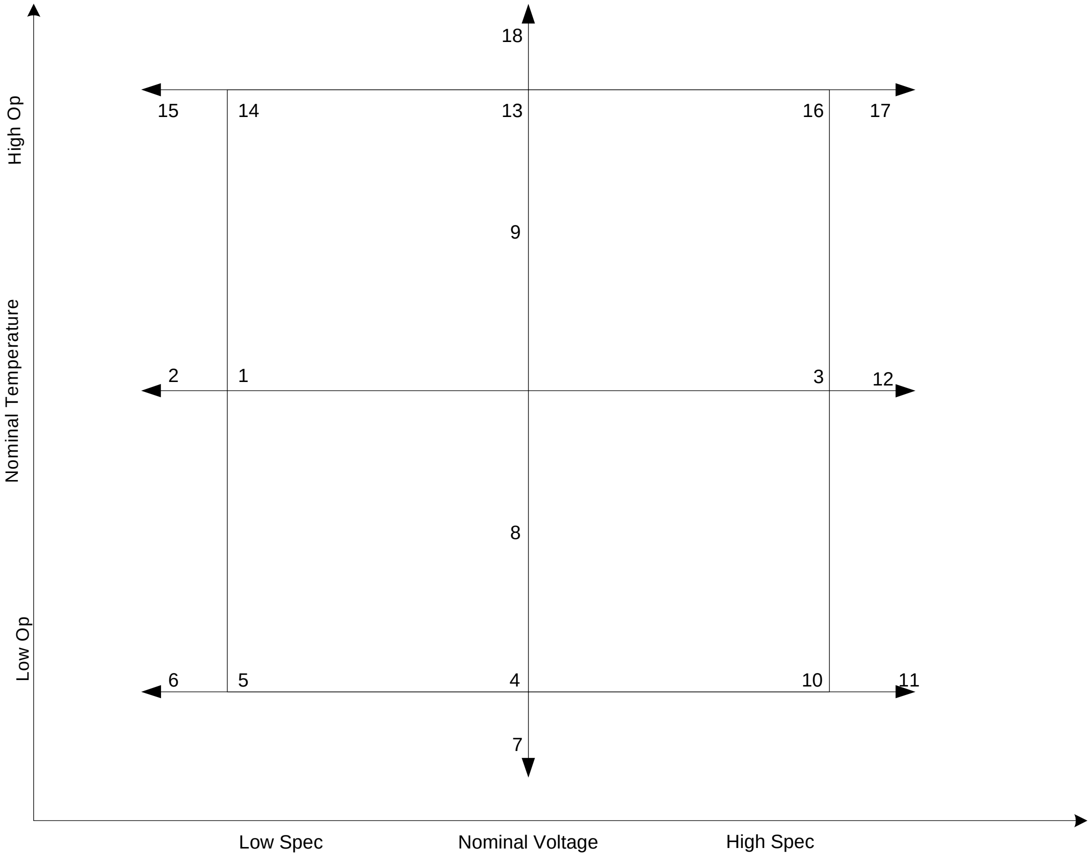

Figure 2 - EFP/EFT Testing Graph

The operational parameters defined in Figure 1 above would be plotted on charts and graphs as shown in Figure 2. The component within the cryptographic module that is most likely to fail first is used to gauge the normal operating ranges of the device under test. The tester then begins to test the cryptographic module by configuring the environment to a series of nominal settings and verifies that the module is operational. The component that is most likely to fail first is used to gauge the normal operating ranges of the device under test. The tester induces slight fluctuations in temperature and voltages and records all of the test points as shown in the example below:

Test #	Description	Temp (Celsius)	Voltage	Expected Test Results	Observed Test Results
1	Nominal temp/voltage near low threshold	0	5.75 volts	Module OK	Module OK
1	Nominal temp/voltage near low threshold	8	5.73 volts	Module OK	Module OK
1	Nominal temp/voltage near low threshold	20	5.64 volts	Module OK	Module OK
1	Nominal temp/voltage near low threshold	55	5.61 volts	Module OK	Module OK

Figure 3 – Example of EFT Test Data (normal operational parameters)

When the tester is confident that the module behaves as specified under these normal conditions, he begins his fault induction by extending the module outside its normal operating ranges (e.g. high temp, low temp, high volt, low volt, etc.). The test point data is recorded in a similar fashion as shown in the example below:

Test #	Description	Temp (Celsius)	Voltage	Expected Test Results	Observed Test Results
6	Temp near low threshold/voltage below low threshold	-8	4.4 volts	Module to shutdown	Module processor halt; shutdown.
6	Temp near low threshold/voltage below low threshold	-7	4.6 volts	Module to enter Critical Failure State	Module entered Critical Failure State; output status of failure
6	Temp near low threshold/voltage below low threshold	-7	4.4 volts	Module to shutdown	Module processor halt; shutdown

Figure 4 – Example of EFT Test Data (outside normal operational parameters)

In many cases, these tests will lead to destruction of the hardware, so the tester must be prepared with enough hardware samples. Often times, acquisition of test modules is difficult because of low quantities on an initial product run or prototype devices, and the high cost for vendor may be somewhat prohibitive. Experience and intuition shows that the combination of high temperature and high voltage tests are the most destructive. In many cases, it is difficult to find environmental chambers that will go down to –100°C so the tester needs to be well prepared prior to testing.

During the EFT testing, the tester will continuously monitor all of the physical ports and logical interfaces supported by the cryptographic module (such as through the use of PCI bus analyzer, hyper terminal, Ethereal, logic scope, etc.). This enables the tester to detect erroneous device behavior. In addition, the tester will be able to verify that no data leakage occurs (e.g. no improperly formatted data, status, etc.). The testing setup can be rather complicated because the cryptographic module is connected to various probes and analyzers, all of which need to be run through the side of the environmental chamber.

2.2 Test Equipment

A generic testing setup could be summarized as follows:

- Environmental chamber: used to modify the cryptographic module's temperature; notice the monitoring equipment extending out of the chamber's side.

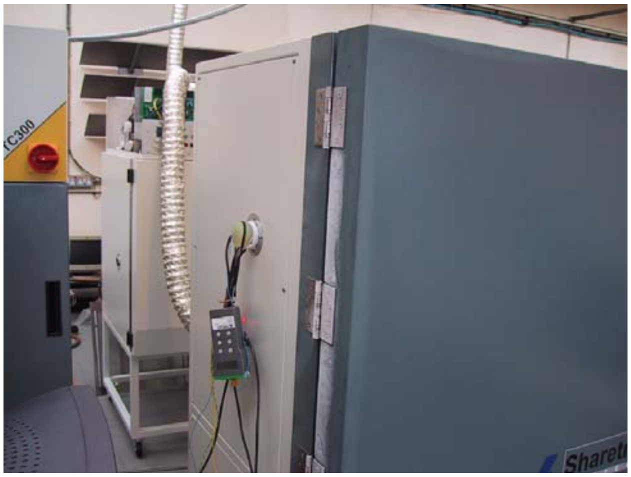

Figure 5 – Chamber Equipment

- Peripheral chamber equipment: liquid nitrogen may be required to bring the temperature down to cold extremes; notice the frozen condensation on the pipes.

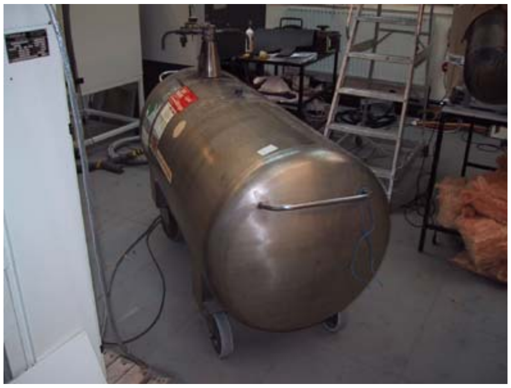

Figure 6 – Chamber Equipment

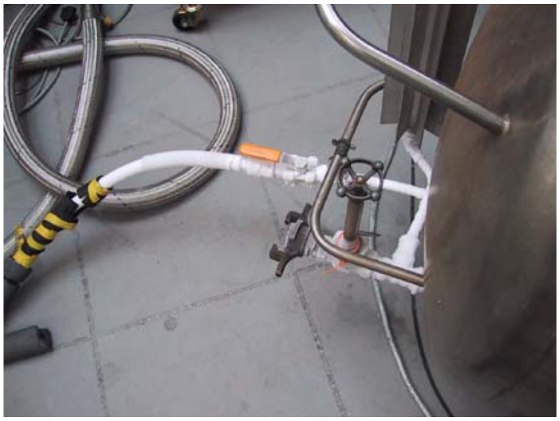

Figure 7 – Chamber Equipment

- Power related equipment: power supply used to modify the power available to the cryptographic module; multimeter used for measuring voltages and resistance.

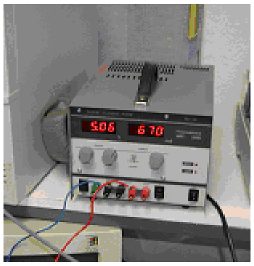

Figure 8 – Power Supply

Figure 9 - Multimeter

- Monitoring equipment: a wide variety of monitoring equipment can be used to observe, monitor, and record the activity on each of the physical interfaces supported by the cryptographic module.

Figure 10 - PCI Bus Analyzer

Figure 11 - Serial Bus Analyzer

Figure 12 - Smart card Analyzer

(PCI Bus Analyzer Photo obtained from http://www.corelis.com/products/PCI_Analyzers.htm)
(Serial Bus Analyzer photo obtained from http://www.yokogawa.com/tm/dl/serialbus/tm-serialbus_03.htm)
(Smart Card Analyzer photo obtained from http://www.securetech-corp.com/class3150.html)

- Cryptographic module under test: the tester will have access to the production grade version of the module and in many cases, additional test jigs are used to enable more convenient access to memory and internal signals for testing purposes.

Before using any of the equipment for the tests cases, the tester must first determine that the testing equipment works correctly. Otherwise, the data gathered could be flawed. The tester initially performs preliminary tests to exercise the testing equipment such as running a sequence of known commands and inputs, and reviewing the log files and other status outputs. In addition, the tester reviews a log of the equipment calibration and may take additional measures to ensure proper setup.

2.3 Testing Conditions

Exercising cryptographic modules under such extreme conditions can lead to hazardous conditions for the testers. Emphasis should be placed on the safety of EFT tests during the laboratory accreditation process and during the testing process itself. As an example, in one test case, a cryptographic module with an internal lithium battery was being heated to nearly 180°Celsius. This resulted in the module literally exploding inside of the temperature chamber, damaging the testing apparatus beyond repair and ruining the environmental chamber to some degree. Another example is that in order to bring an environmental chamber down to –100 degrees, another test case required retrofitting the chamber to support the input from a 100 liter tank of liquid nitrogen; additional ventilation had to be added to the warehouse where the chamber was kept to prevent the exhaust from the asphyxiating the testers. Often times, the higher temperatures and higher voltages lead to melted components and in some cases, requiring excessive cooling time before the modules and testing equipment can be handled. With these examples in mind, some interesting questions that need to be asked are: Is the facility where the tests are being performed properly insured to perform that type of testing? What do you do when the module explodes and someone gets hurt? Who is liable? To prevent negligence during testing, a few simple safety measures should be in place during all EFT tests:

- Face masks (in some cases, a respirator) for smoke and other exhaust
- Thick gloves to protect hands against hot or freezing components
- Smock for body protection against melted parts
- Eye goggles
- Eye wash station

3 Published Attacks

Following is a brief overview of some of the published fault induction attacks:

- Optical Fault Induction Attacks: the IC is irradiated with light to modify bits in CMOS memory; from a FIPS 140-2 perspective this would provide the ability to modify executable code and keys in an unauthorized manner. [http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/faultpap3.pdf]
- Spike Attacks: Voltage transients on power supply, that could lead to alteration of program execution; from a FIPS 140-2 perspective a successful attack could violate the limited operational environment (e.g. untrusted and incorrect program execution). [http://www.silicon-trust.com/pdf/secure_9/15_ifx_laackmann.pdf]

- Glitch Attacks: Modifications of clock signal that could lead to skipping over required operations; from a FIPS 140-2 perspective this could lead to violations of required identification/authentication, self-tests, proper error handling. [http://www.silicon-trust.com/pdf/secure_9/15_ifx_laackmann.pdf]
- Eddy Current for Magnetic Analysis with Active Sensor (ECMAAS): Electromagnetic induction via electrical coils; "Attacks on the PIN (personal identification number) check of a GSM SIM card give the attacker the possibility to extract protected data from the card without knowledge of the PIN." [http://www.silicon-trust.com/pdf/secure_9/15_ifx_laackmann.pdf]
- Conducting temperature attacks: Modification of ambient temperature may provide the ability to alter contents of RAM or "freeze" the data into memory even once power has been removed; from a FIPS 140-2 perspective this could provide the ability to manipulate sensitive data and also prevent zeroization in the event of memory "freezing." [http://www.silicon-trust.com/pdf/secure_9/15_ifx_laackmann.pdf]
- Thermal Induced Voltage Alteration TIVA: Local Temperature alteration due to laser irradiation can lead to irregular behavior in module components; from a FIPS 140-2 perspective, at minimum, this could constitute violations of the defined Finite State Machine. [http://www.silicon-trust.com/pdf/secure_9/15_ifx_laackmann.pdf]
- Single Event Effect Attacks: Alpha particle radiation could lead to modification of data in memory; this would have similar implications to those already noted above. [http://www.silicon-trust.com/pdf/secure_9/15_ifx_laackmann.pdf]

Looking forward to the FIPS 140-3, absolute thresholds for temperature may not be the most effective or valid approach to testing. In many cases, the cryptographic module may become volatile and unstable leading to dangerous conditions for the tester. Emphasis on safety should be placed in the testing standard, requiring additional research and verification by the tester regarding the chemical and mechanical characteristics of the components materials. This would help to ensure that the unstable conditions could be anticipated and appropriate safety measures implemented to support the testing. In lieu of an absolute operating range, emphasis could instead be placed on a specification of certain ranges beyond the normal operating parameters (e.g., a certain number of degrees/volts above and below normal ranges).

4 Conclusion

In conclusion, this paper has provided a brief overview of fault induction with emphasis on environmental failure testing. The intent has been to open the door for discussion on these topics and shed light onto an area of testing somewhat surrounded by mystery. With advances in technology, more sophisticated designs and attack methodologies arise; the FIPS standards need to keep up pace with such advancements. With this in mind, the EFT tests could be broken into multiple levels of security (e.g. Level 3 and Level 4); the lower level emphasizing testing of cryptographic modules more thoroughly within normal operational ranges, and the higher level placing more emphasis on exercising the module outside of intended operational ranges. Currently the environmental tests are only performed at Level 4, leaving a very large gap in the assurance associated with performance of the cryptographic module at the lower levels of security. With EFP, the cryptographic module has physical security mechanisms to respond to environmental conditions thus it is appropriate to test EFP mechanisms under the Area 5 – Physical Security section of FIPS 140-2 (e.g. the tester is testing a particular physical security mechanism). Whereas with EFT, the module is shown to provide a level of resistance to environmental attacks despite having particular mechanisms to thwart the attacks. For this reason, consideration should be placed on moving the EFT tests into the Area 11 - “Mitigation of Other Attacks” section. In addition to the voltage and temperature fault induction tests, other fault induction tests (such as those mentioned above) should be added and specification of how to perform the tests should be detailed in the FIPS 140-3 derived test requirements. It’s an interesting dynamic when one considers the cost of performing these attacks vs. the value of the information being compromised. It is well known that it is much cheaper to attack the product than to protect it. In short, more money and effort need to be spent on design, development, and verification to increase security.