As originally published in the SMTA Proceedings.

TAMPER PROOF, TAMPER EVIDENT ENCRYPTION TECHNOLOGY

Phil Isaacs,[1] Thomas Morris Jr.,[2] and Michael J. Fisher[2]
IBM Corporation
[1]Rochester, MN, USA
[2]Poughkeepsie, NY, USA
pisaacs@us.ibm.com

Keith Cuthbert[3]
W. L. Gore & Associates
Dundee, Scotland

ABSTRACT

Hardly a week goes by where there isn't a report of cyber-crime having occurred. So much so that there is a special branch of the FBI established to address the many forms of Cyber-Crime. While the internet is convenient for many regular on-line activities, for example: Information searches, goods purchasing, sales, airline and hotel reservations, banking, bill-pay, driving directions and telephone/address look-up. It is the ease at which this information is so readily available that makes it vulnerable to attack.

One solution would be to completely isolate the computer applications. However, most applications cannot perform their function in isolation. In order to prevent cyber crimes from occurring on server level products, IBM and Gore[1] have collaborated on a state-of-the-art physical security package to protect the hardware components of a cryptographic coprocessor module.[2] [3] This package meets the highest level of physical security requirements contained in the U.S. Government Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules- (Level 4), and supports the overall attainment of FIPS 140-2 (Level 4) for the cryptographic coprocessor. This is the highest level of encryption technology which is allowed outside of the government or military. The packaging technology includes tamper response where any attempt at physically gaining access would render the cryptographic module useless.

This paper will provide an overview of the protection features of the assembly and the manufacturing processes used to manufacture the product.

Key words: Encryption, Tamper proof, Tamper evident, FIPS 140-2

INTRODUCTION

Encryption alone is no longer adequate to protect sensitive data. Imagine having your encryption keys breached without knowing it happened. Storing data in electronic form may be convenient, but it is also susceptible to stealth attacks. In order to perform cryptographic functions (encrypt, decrypt, sign, authentication) a computer system requires access to cryptographic keys and other security relevant data in a clear format. It is evident by getting access to such security relevant data in clear format a hacker can easily get access to the data being protected and also impersonate other authorities. Continuous technology improvements are affording unscrupulous individuals with opportunities to unravel encrypted data. The way to prevent this is to generate and never expose the most important cryptographic key outside an enclosure capable of detecting and responding to any type of physical tamper.

One can find many approaches to tamper prevention, tamper detection and appropriate reaction. Often these approaches are concepts. Some of the concepts are as simple as a passive circuit pattern with no electrical connection, which can be monitored for any physical intrusion by change or distortion in the monitored electro-magnetic field.[4] Others use capacitive networks or fringe capacitance to create a sensor device.[5] There are also quite sophisticated approaches such as using quantum mechanics to create a non-repeatable encryption key.[6] Sensors can be made from a variety of materials: Semi-conductors, metallic traces, organic traces, etc.[7] The approach selected for this product is a sensor with an organic trace network constantly monitored for any attempted intrusion into the package. This technology has been proven successful in previous products.[8] This paper focuses on the hardware design and the manufacturing process used to make this product.

Tamper Detection and Response

Data stored in electronic form such as electronic components when left unprotected can be susceptible to access without detection. Simply wrapping the components in a physical enclosure hampers component access, but does not prevent data retrieval. The use of a thick impenetrable envelope is not practical and can not be considered secure by itself. The enclosure needs to do more than visually signify that an intrusion has taken place. An after-the-fact

indicator of data breach means the data has already been compromised. The enclosure must detect and respond at the time of the intrusion.

Our two companies have partnered in the development of a secure environment that supports the physical security requirements of Federal Information Processing Standard 140-2 (FIPS 140-2) certification.[9] This solution is currently in use in the PCI express Cryptographic Coprocessor.[10]

The methodology behind this secure solution is the use of a multilayered random pattern mesh sensor incorporated with response circuitry. Tamper Respondent Sensor[11] [12] technology is wrapped around the security sensitive components (i.e. secure module). This wrapping shields against physical intrusion such as puncture, chemical attack, and laser penetration.

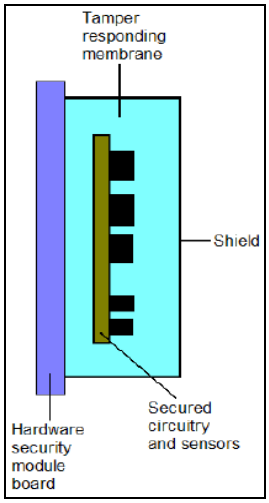

Figure 1: Secure Module Diagram

Utilizing the concepts of a Wheatstone Bridge and comparator logic, the resistance of each "leg" of the sensor mesh is constantly monitored for deviation against a known base value. The tamper sensors, control electronics and small key memory (part of BBRAM) are highly integrated in a small tamper detection and response module (DS3645[13]). This tamper detection module provides higher overall reliability including more reliable tamper validation thus preventing false tamper incidents. The employment of a tamper module versus discrete electronics results in a lower battery back up current drain. It also better enables the housing of the tamper subsystem within the confines of the secure enclosure.

The IBM 4765 coprocessor is shipped from the factory with a certified device key which is stored in the card's battery back up protected memory. The electronic key digitally signs test messages to confirm that the coprocessor is genuine and that no tampering has occurred. The coprocessor cannot operate without this device key. If any of the secure module's tamper sensors are triggered by tampering or accident, the coprocessor erases (zeroizes) all data in the protected memory destroying the device key. This renders the coprocessor permanently inoperable with no recovery.

A change in the mesh sensor characteristics triggers an imbalance in the tamper circuitry. When a physical or laser penetration is attempted the resistance of the sensor mesh conductive ink track changes the resistance. The response module senses this imbalance and invokes the immediate erasure of the high speed erase battery backed up memory (3KB BBRAM) eliminating all security sensitive data (i.e. coprocessor critical keys and certification). The 3KB BBRAM hardware controller embeds a function that offloads the firmware task of flipping the data in order to avoid imprinting data. A chemical attack (reagents and solvents) causes the conductive ink track to "dissolve" changing the "leg" resistance resulting in a similar detected imbalance. Attempts to unwrap the adhesive mesh sensor causes permanent changes to the characteristics of the ink tracks also resulting in a detected imbalance.

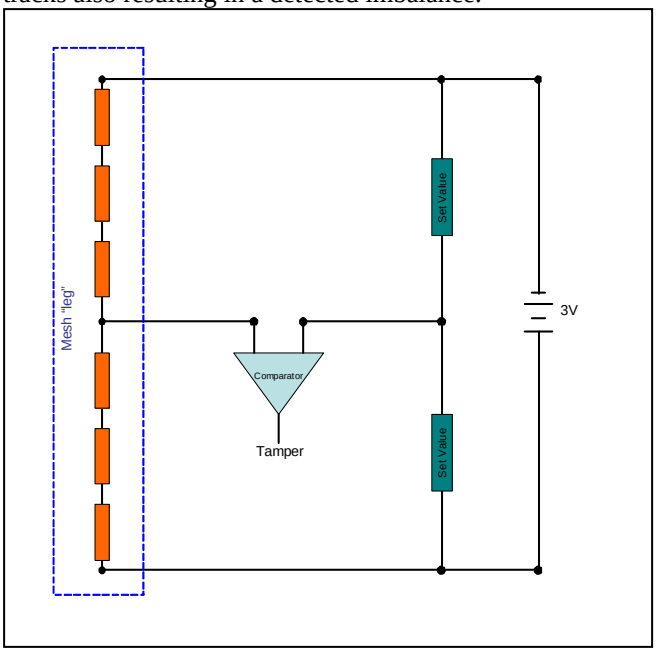

Figure 2: Tamper Circuit Schematic

The data stored in this secure memory is encrypted for added security with a key stored in the small key memory of the DS3645 Security Manager. Once the sensitive data is erased, the IBM 4765 is placed into diagnostic mode and left in a permanently inoperable state.

A pair of batteries mounted on the coprocessor board ensures the tamper subsystem is always active even when the IBM 4765 is not in a powered on machine. Removal of these batteries outside the authorized battery replacement process will trigger a tamper event.

Tamper Respondent Technology

The current Cryptographic card uses the Tamper Respondent Technology. This technology defends the

physical security boundary of the module by creating a "tamper respondent" envelope. Protection is provided by an organic, flexible sheet sensor which enfolds the electronic package creating an enclosure with no direct entry points.

Conductive ink traces are deposited onto an organic substrate. The electrical state of the sensor changes if an ink trace is broken, triggering tamper respondent mechanisms, such as zeroing encryption key memory. An opaque outer resin coating prevents attackers from optically seeing the traces. The traces are also invisible to X-rays, further thwarting analysis. In its finished form, entry into the module without circuit damage and detection is extremely improbable.

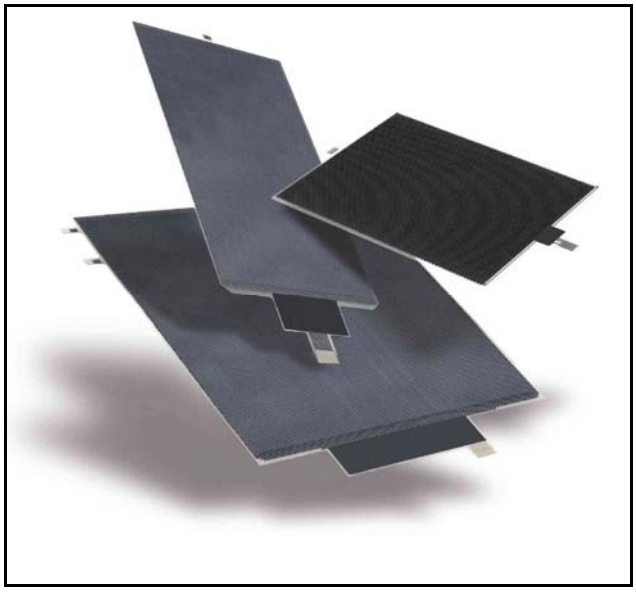

Figure 3: Tamper Respondent Sensors

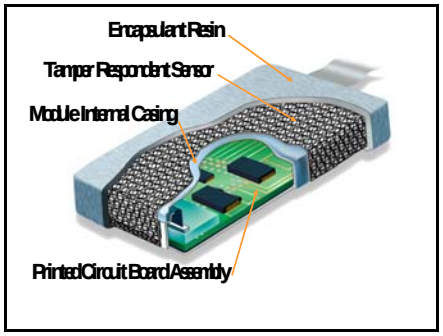

Figure 4: Tamper Respondent Secure Encapsulated Module

Electrically, the sensor consists of a resistive network which is constantly monitored by a detector circuit inside of the package. When a trace breaks, it triggers a fast and unrecoverable change in electrical state**.**

This sensor network is validated in the Cryptographic Module to FIPS 140-2 (Level 4) physical security. Tamper Respondent Technology in this application has undergone a number of validations to FIPS 140-2 (Level 4).

Manufacturing Encapsulation Process

In the following section we will describe the manufacturing process and key process controls used to assemble the tamper proof hardware assembly.[14]

Manufacturing Process and Storage Environments

All processing operations must be performed in a temperature and humidity controlled environment.

Encapsulation Process Steps

1. Electronic Card Assembly and Test, ECAT Card Primary Enclosure
2. Tamper Proof Sensor Folding and Cure
3. Resin Encapsulation

ECAT Card Primary Enclosure

Insert the signal flex cable assembly and the Power Flex cable assembly into the daughter card mating connectors.

Figure 5: Flex Cable Plug

The two flex cables must be pre-folded creating an upward right angle with respect to the daughter card plane. This operation is meant to facilitate the enclosure of the daughter card and flex cable assemblies into the inner cover while sliding the cables through slots in the top cover.

Figure 6: Flex Cable Pre-Bending

Remove the blue plastic release sheets from the 2 thermal pads in the inner bottom cover and lay the daughter card down in this cover with the flex cables up, aligning the 5 card holes with the 5 rivets in the cover.

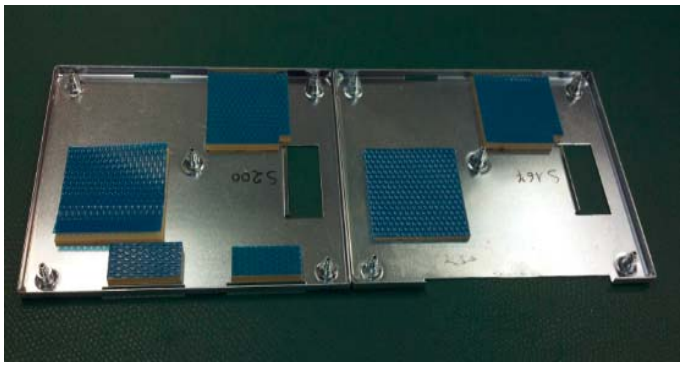

Figure 7: Inner Covers with Thermal Pad Release Sheets.

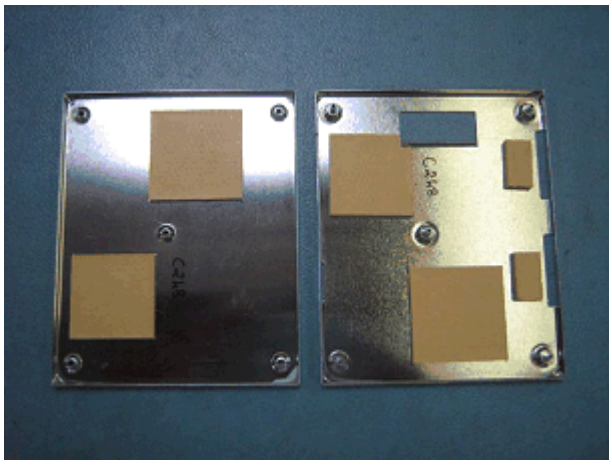

Figure 8: Inner Covers without Thermal Pad Protectors

Remove the blue plastic release sheets from the 4 thermal pads in the inner top cover and place the top cover aligning to the rivets below while passing the 2 Flex cables through the cover cable slots to fully enclose the daughter card inside the inner cover.

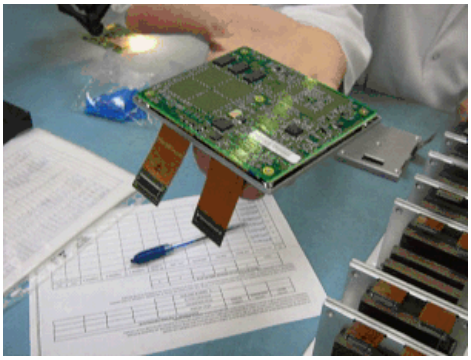

Figure 9: Card Assembly placed into Inner Cover

The resulting assemblies are placed inside the pre-riveting holding tools to avoid inner covers becoming loose while moving pre-riveted assemblies around the manufacturing floor.

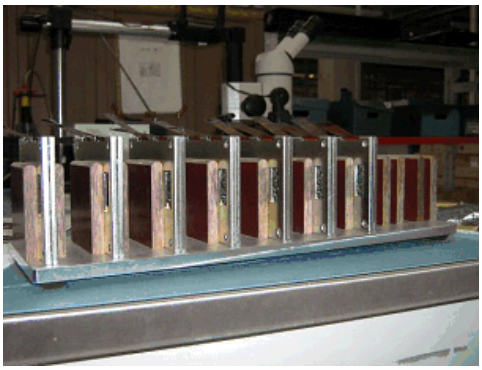

Figure 10: Pre-Riveting Holding Tools

Customized tooling is used to form the rivets on the inner cover assembly. The package is placed into a pre-load fixture and automatically shuttled under a press head with rivet forming punches.

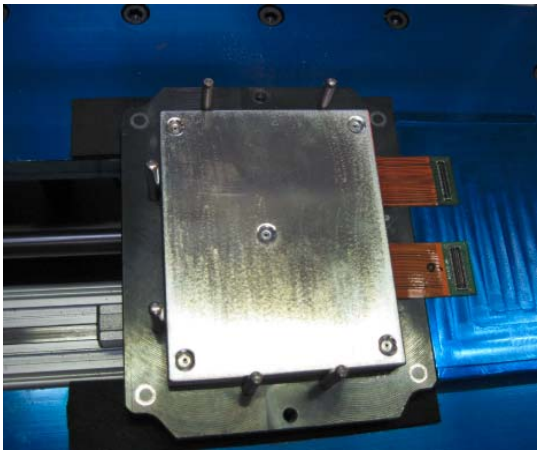

Figure 11: Riveting Alignment Aids

Critical to function measurements of the inner can assembly are as follows:

Rivet Attributes

- Max assembly thickness
- Minimum diameter of rivet head
- Lack of cracking, breaking and burrs

Cover Attributes

- Top and bottom inner covers outline alignment.
- Cover surfaces are free of burrs and sharp edges
- Cover assembly planarity
- Total covers thickness
- Good Flex cable to daughter card interconnection by electrically testing connection.

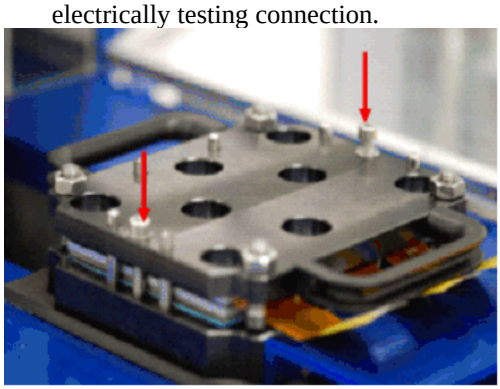

Figure 12: Riveting Pre-load Fixture

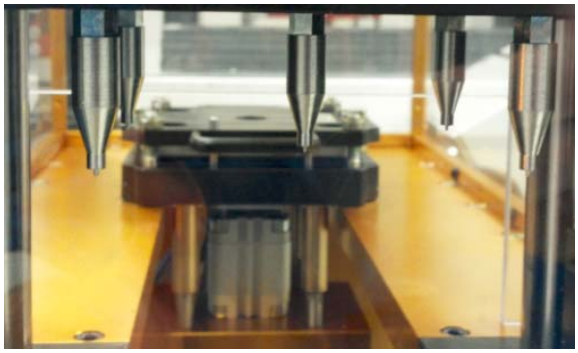

Figure 13: Rivet Forming Punches

The inner cover assembly is cleaned with IPA, handled with low ionic gloves and should be processed immediately after cleaning.

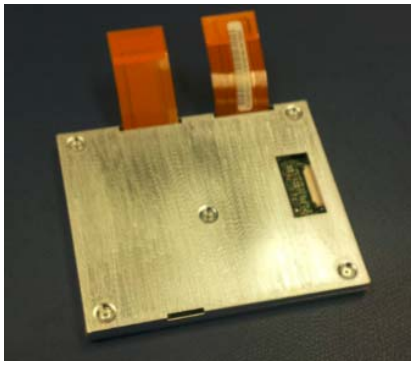

Figure 14: Completed Inner Assembly

TAMPER PROOF SENSOR FOLDING AND CURE

Tamper Sensor Preparation

The tamper sensor is pre-tested prior to application for critical function electrical and mechanical measurements.

Tamper Respondent Sensor Folding

1. Blow off the tamper respondent sensor with nitrogen under ionized flow.

Figure 15: Tamper Proof Sensor

2. Remove the release layer
3. Align on the folding tool with the adhesive side up

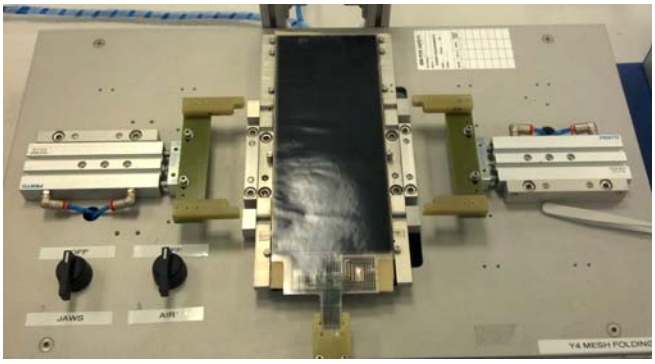

Figure 16: Sensor Folding Equipment

4. Place the inner can onto the tamper respondent sensor using the guides.
5. Press the inner can onto the tamper respondent sensor to activate the pressure sensitive adhesive.
6. Fold the first fold which contains the tamper respondent sensor leads using the folding apparatus.
7. Insert the tamper respondent sensor I/O cable into the PCBA sensor connector.

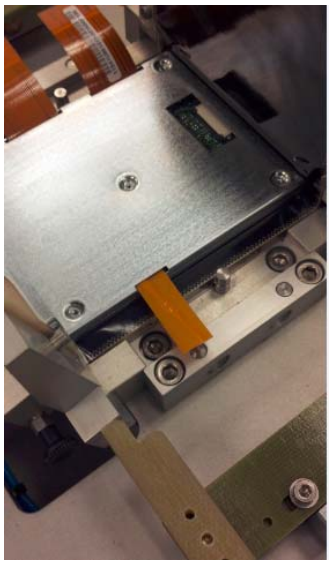

Figure 17: Inner Assembly Placement

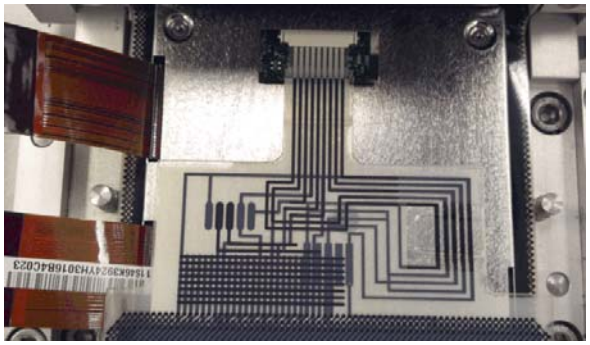

Figure 18: Sensor Plug into ECAT Card

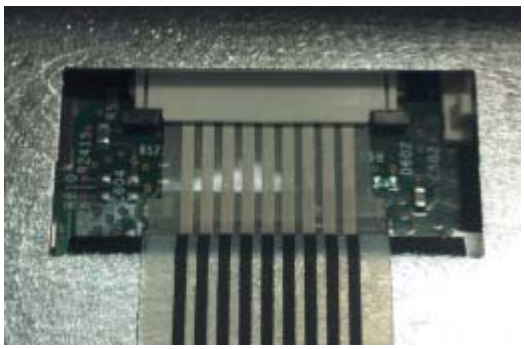

Figure 19: Sensor Alignment into ECAT Card

8. Fold the tamper respondent sensor around the inner cover to complete the first folding.

Figure 20: First Fold of Tamper respondent sensor on Inner Cover

9. Tamper respondent sensor folding continues on the two package sides where there are the flex cables on one side and the vent on the opposite side

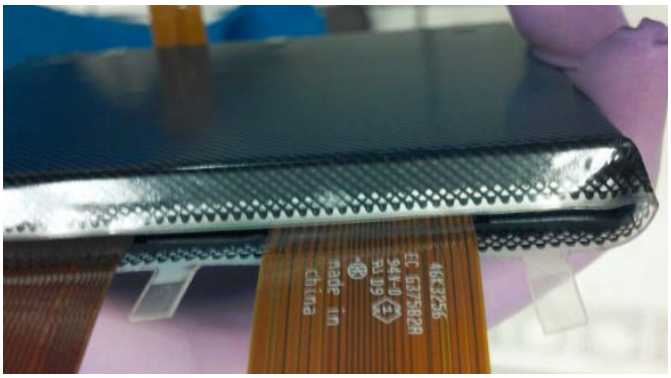

Figure 21: Edge Fold on Ribbon Cable

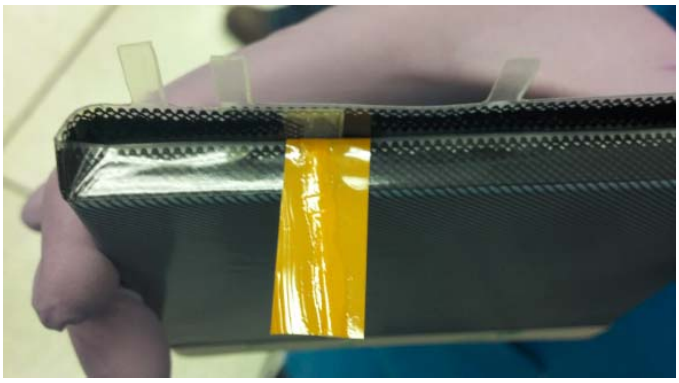

Figure 22: Edge Fold on Vent Side

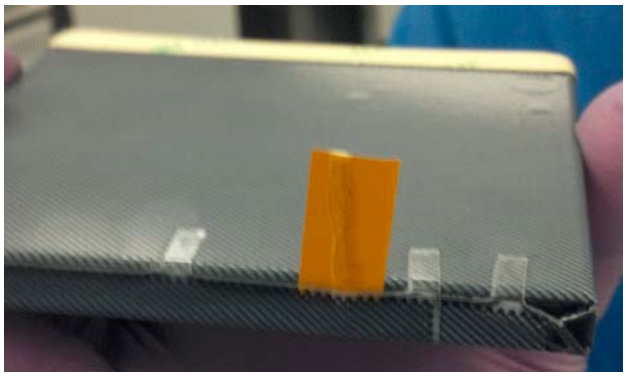

Figure 23: Completed Fold on Vent Side

10. Inspect for cracks, scratches, creases, bubbles and any gaps in the sensor.
11. Place the folded assembly into the holding tool.

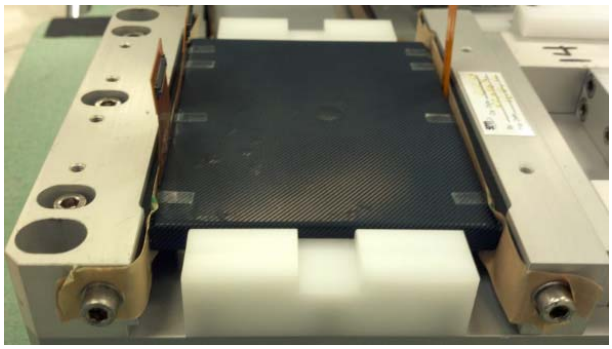

Figure 24: Holding Tool

Tamper Respondent Sensor Holding/Curing

The assembly is held in the holding fixture just after the folding operation. The package, retained in the fixture, must be cured for 1 hour at 60°C. The package is encapsulated in resin within 24 hours after curing.

RESIN ENCAPSULATION

Process Indicators and Process Controls

Water in the polyol component can lead to bubbles or foaming in the polyurethane, PU, resin. Such bubbles can also occur when the curing PU mixture is allowed to pick up water during processing. Thus water content must be controlled. Transfer of polyol needs to be done under nitrogen with controlled pressure (to avoid over pressurizing the shipping container).

Transfer of isocyanate also needs to be done under nitrogen with controlled pressure to avoid over pressurizing the shipping container. The environment in which the dispense operation occurs must have an RH maximum of 30%. Properties of the fully cured PU must be determined after change of either polyol or isocyanate and periodically during manufacturing. Whether in the tool production or back up tanks, the Polyol and the Isocyanate must be stirred constantly.

The mixing ratio of Isocyanate to Polyol is from 0.91 to 0.99:1 by weight. Defects in the cured resin such as swirls, areas of inhomogeneity, wet or soft spots are not allowed. When starting a new encapsulation lot, a sample of the PU resin will be taken from the dispense tool for the purpose of obtaining a time to gel point determination, G'/G". The gel point must fall between the values of 70 to 125 minutes.

First Resin Dispense

Dispense 4 shots of mixed Resin Polyurethane into the outer cover using a long plastic mixing nozzle. This operation must be performed in a dry environment such as a Dry Hood through which either dry nitrogen or dry air flows to keep the humidity level below 30%. The polyurethane should not be allowed to be stationary in the static mixer nozzle for longer than 2 minutes. The nozzle must be replaced frequently in order to assure good polyurethane mixing. The resin must fully cover the bottom of the outer cover.

Assembly Package Positioning With Template Alignment

After dispense insert the Crypto card package in the outer cover with the cables oriented toward the longer outer cover side. The assembly is manually centered into the outer cover. The thickness of the resin around the enclosure must be maintained.

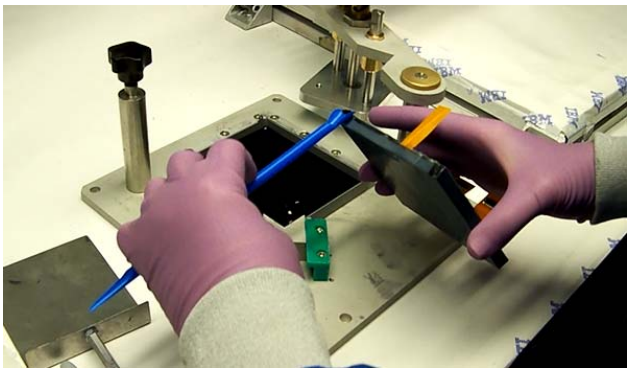

Figure 25: Applying Resin to Package Corners

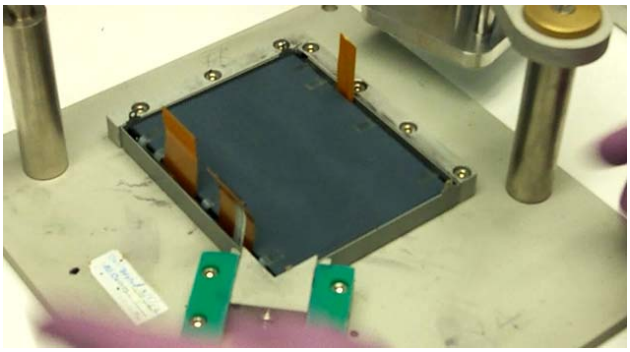

Figure 26: Positioning of Package within Outer Cover

Second Resin Dispense
Dispense 4 shots of mixed Resin Polyurethane over the assembly. Put the part in a Dry Hood. No part of the assembly should be visible after this resin dispense.

Figure 27: Fully Encapsulated Module

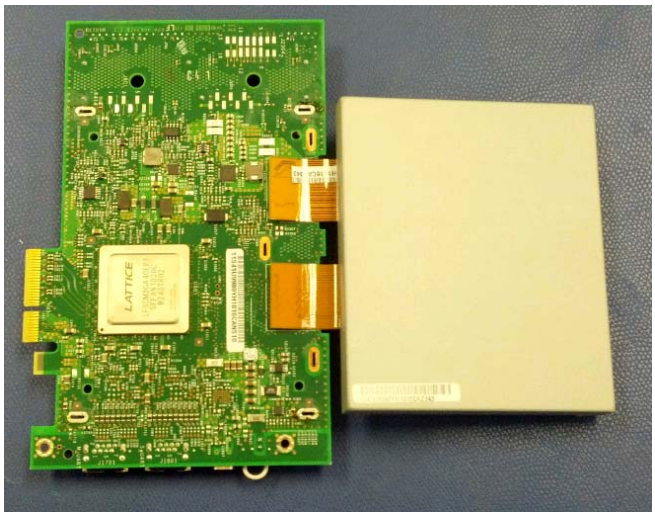

Figure 28: Encapsulated Module Connected with PCIe Assembly

Figure 29: Finished Cryptographic Module assembled to PCIe Card

Second Polymerization (Cure)
The resin polyurethane must be cured in a nitrogen oven using the following parameters:

- Cure PU for one hour at 25 C.
- Ramp to 50 C and cure for 70 minutes.

Vent Trim
Trim the vent to within 0.5 mm above the level of the resin.

Secure Module Encapsulation Visual Inspection
The resin must completely cover the folded sensor, no uncovered area is allowed. Separation between resin and cover is not allowed. The resin must be below or equal to 0.5 mm below the cover edge. The cured resin must be shiny and show only minimal bubbles.

Quality and Reliability
There are several process steps included as package verification quality gates. They can be found in Table 1. In addition to the in-line quality tests the package has passed a series of stress tests to assure the package will last a lifetime consistent with the requirements of high end, mission critical server products.

Table 1: Quality Gates

Item	Test	Criteria
1	Receiving Inspection of the Sensor and circuit verification	Dimensions
2	Resin	Chemical analysis
3	Visual Insp. of the Sensor prior to folding	Damage & contamination
4	VI Sensor after folding	Proper folding
5	Electrical verification of sensor after folding	Sensor circuits
6	Electrical verification after sensor cure	Current circuits
7	PU Material Properties	Stoichiometry & cure
8	VI after PU dispense	Physical appearance
9	Electrical verification after resin	Sensor circuits
10	VI after Crypto to PCI merge	Solder defects
11	PCI compliance	Thickness gage
12	Burn-in	Functional Test

SUMMARY

The combination of a sensor mesh and monitoring circuitry provides an environment that protects sensitive data from cyber theft. It is manufactureable and reliable both in preventing undesired access and its longevity in the field.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the following contributors: Assistance provided by Vincenzo Condorelli, Nihad Hadzic, and William Santiago Fernandez of IBM Poughkeepsie, NY toward the content of this paper. We would also like to acknowledge the team who have worked on this project: Dave Allan, Ed White, Frank Orapello, Jason Wertz, Jim Wilcox, Jing Zhang, Mitch Ferrill, Nandu Ranadive, Norm Curry, Stu Lake and Tim Donahue.

REFERENCES

1. Gore is a trademark of the W. L. Gore & Associates, Inc. Newark, DE.

2. T. W. Arnold, C. Buscaglia, F. Chan, V. Conderelli, J. Dayka, W. Santiago-Fernandez, N. Hadzic, M. D. Hocker, M. Jordan, T. E. Morris, Jr. and K. Werner, " IBM 4765 Cryptographic Co-Processor," IBM Journal of Research and Development, Vol. 56 No. ½, pp. 10:1-10:13.

3. Arnold, T., Dames, A., Hocker, M. D., Marik, N., Pellicciotti, A. and Werner, K., "Cryptographic system enhancements for the IBM System z9", IBM Journal of research and Development, Volume 51 Number 1.2. web site: http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=5388699&punumber=5288520

4. Woodard, S. E.., Functional Electrical Sensors as Single Component Electrically Open Circuits Having No Electrical Connections, IEEE Transactions on Instrumentation and Measurement, Vol. 59. No. 12, December 2010, pp. 3206-3213.

5. Eren, H. and Sandor, Lucas D., "Fringe-Effect Capacitive Proximity Sensors for Tamper Proof Enclosures," Proceedings of Sensors for Industry Conference, Feb. 8, 2005, pp. 22-26.

6. Liebholz, Stephen W., "Solutions for the grand Challenges of Information Security: Protection Against Rogue Insiders, Dynamic Compartmentalization and True Quantum Encryption." Proceedings from 2007 IEEE Conference on Technologies for Homeland Security, pp. 129-132.

7. Paul, P., Moore, S. and Tam, S., "Tamper Protection for Security Devices." from the proceedings of the 2008 Symposium on Bio-inspired Learning and Intelligent Systems for Security, pp. 92-96.

8. Isaacs, P., Buscaglia, C., Feger, C., Pearsall, K., Wolf, H., Cesana, M., Moscheni, G., Cuthbert, K. and Hunter, S., "Packaging and Processing of a State-of-the-Art Encryption Technology." From proceedings of 2007 IMAPS Symposium, San Jose.

9. National Institute of Standards and Technology Cryptographic Module Validation Program (CMVP). website: http:/csrc.nist.gov/groups/STM/cmvp/index/html.

10. IBM 4765 PCIe Cryptographic Coprocessor Installation Manual. web site: http://www-03.ibm.com/security/cryptogards/pciecc/pdf/4765install.pdf.

11. Tamper Respondent Mesh is a trademark of the W. L. Gore &Associates, Inc. Newark, DE.

12 Gore Anti-Tamper Physical Security for Electronic Hardware. web site: http://www.gore.com/en_xx/products/electronic/anti-tamper/anti-tamper-respondent.html.

13. Maxim Integrated DeepCover™ Security Manager (DS3645). web site: http://www.maximintegrated.com/datasheet/index.mvp/id/5424.

14. IBM Engineering Specification, PCIe Cryptographic Coprocessor Secure Module Assembly Requirements, written by IBM and SEM, Services for Electronic Manufacturing, Milano, Italy.