INFOGARD

Security Assurance
Independence. Integrity. Trust.

Physical Security 101

NIST CMVP
Physical Security Conference

Tom Caddy

September 15, 2005

05-998-R-0059 Version 1.0

Table of Contents

List of Figures

1 Objective

This paper has been drafted to provide a backdrop for physical security as it pertains to cryptographic modules. It is structured with following top level subject areas:

- Introduction
- Physical Security Threats
- Physical Security as a subsystem
- Physical Security Specification Challenges
- Roles/Constituents
- Physical Security vs. Module Lifecycle
- Conclusion

2 Introduction

Physical Security is a first line of defense for any device or system. The FIPS 140-2 concept of a crypto module is that it needs to have the ability to protect itself to an ever increasing degree as the security level increases from Level 1 to Level 4.

Security in these terms may include the following factors depending on security level:

- Reliability
- Integrity
- Access Control
- Disclosure

On a Microsoft web site describing threats, they have the following statement:

> *It should be very clear that compromised physical security always means that all security layers have been compromised. All security discussed in this solution is based on the assumption that physical security has been addressed. Without physical security, no other security measures can be considered effective.*

This is a powerful statement from a software provider, but it's very true. Physical security is at the root of access control; if physical access control cannot be maintained then all other security can be significantly weakened or lost.

3 Physical Security Threats

The module may have different threat models, which would affect the physical security requirements for secure operation. The two most basic threat profiles are:

1. The module owner/user is motivated to have the module secure (i.e., low threat environment)

2. The module owner/user is motivated to compromise the module (i.e., high threat environment)

There are also other situations that may be a combination of the above.

3.1 Low Threat Environment

The most common scenario, especially for level one and two modules is that both the Crypto-Officer and the module user are both interested in the module correctly performing both its logical functionality as well as its security functionality. Therefore, the operator can make use of tamper evidence and can be expected to correctly use the module and take notice if it is not working correctly. Typically in these situations, a module would only be available to the attacker for a limited period of time before the conscientious owner returned to take personal custody of the module.

As an example, an email encryption product is used on your personal PC. The user is motivated to use the module correctly because he is trying to protect his own information from disclosure. The primary local threat is someone modifying the system or software without his or her knowledge so evidence of tampering can be desirable and useful. This tamper evidence may be either physical with tamper labels or logical as evidenced by power up self-tests such as the software firmware integrity required check.

3.2 High Threat Environment

We often have crypto modules or systems with crypto modules in them that are designed for high threat environments. These devices protect critical information, often funds or financial transactions, but may also be personal privacy data, authentication data, or cryptographic key material. It is often the person who is in control of the module that would benefit most by the compromise of the module. Therefore, they have virtually unlimited time and availability to perform the attack.

A vending machine is an example. It contains product and money that the person operating the machine has not personal stake in the security.

3.3 External Environment

Many times the environment outside the crypto module greatly affects the level of physical security required at the cryptographic module boundary. Our experience would indicate this is often a significant factor for the end user and regulator in their overall security model, especially if there are financial implications. For example, a server may be put into a “vault” that affords the necessary physical protections. However, providing the necessary physical protections, like the “vault” can sometimes provide a false sense of security, since the critical aspects of the module are still exposed to employee accidental or malicious attack. Insider attacks both solo and in collusion with another party make up the majority of compromises (in some published estimates up to 80%). This reinforces the concept of having the smallest crypto boundary possible as it provides the best end-to-end protection by minimizing the areas clear text information is accessible.

3.4 Security Policy

The concept of the FIPS 140-2 security policy is important to mention at this point. As the primary FIPS 140-2 unique document and the only CMVP public document it is extremely important to the end user. Each implementing agency has a department security policy and by providing a FIPS 140-2 cryptographic module security policy, enables the department CIO to compare the two and assess if the module will satisfy the security level and requirements as specified. Figure 1 depicts this important process.

Department CIO compares features and details to ensure that module is consistent with ALL aspects of the department Security Policy

Figure 1 - Security Policy Comparison

4 Physical Security as a Sub-system

Physical security at Levels 2, 3 and 4 are required to implement physical security systems that are dependant on a variety of technologies all working together as an integrated system. The goal of the system (depending on level) is to provide the following three objectives:

- Tamper Evidence
- Tamper Resistance
- Tamper Response

A pertinent reference for these objectives is ISO 13491-1 Banking – Secure cryptographic devices (retail) Part 1, Appendix A, which has a very applicable tutorial on the balance of tamper resistance, tamper detection/response, and tamper evidence.

Although tamper evidence, resistance, and response seem to be easy concepts, they can require complex, state of the art technology in the areas of materials, adhesives, solvents, and physics, as well as the more obvious mechanical and electrical attributes working synergistically together.

For a robust security design, all variables are important to consider, including the aesthetics of the products. For example, the enclosure texture can reduce the effectiveness of tamper label adhesive to nil. The enclosure texture provides reduced surface area for the label to adhere to, while at the same time, can allow solvents to have full access to the underside of the label.

Each of these important areas (tamper evidence, resistance, and response) will be examined in closer detail.

4.1 Tamper Evidence

Tamper evidence has three primary purposes:

- Trust warning that is obvious to any user
- Forensic which can be used for prosecution
- Warranty used for vendor protection

FIPS 140-2 envisioned that tamper evidence would be a warning to a non-hostile user that the module may not be able to be trusted. As such, the tamper evidence needs to be an obvious indicator that is recognized by the average user, rather than only by the module vendor or expert. This type of tamper evidence can be of limited value in some situations such as high threat environments or in cases where the module is embedded in another product and not typically visible.

Tamper evidence has been critical in some cases to establish cases for prosecution of criminals. This category of tamper evidence can go into significant technical depth to establish criminal intent. In typical cases, there may be no obvious evidence, but only subtle, real bits of visible obscure evidence. This category is not applicable to FIPS 140-2 evaluations, but is typically used by other regulators such as the USPS. It should be noted that for some situations, designing a module that has a very high probability of producing solid forensic evidence which can be used in court, could be a high priority.

Even in non-security devices, it is not atypical to have tamper detection measures designed into products to provide vendors warranty protection. Often times, these measures can protect them from illegitimate claims, impacting costs reputation and possible loss of intellectual property.

4.2 Tamper Resistance

Tamper resistance is one of the most critical lines of defense. It is far more important to have security that is preventative (tamper resistance) rather then reactive (tamper detection/response) or responsive (tamper evidence). Therefore, this can be a critical aspect of attaining an appropriate level of security.

Many factors work together to establish tamper resistance, some of which are specifically required by FIPS 140-2 such as obscurity or opaqueness to hide the underlying circuitry and pick resistant locks, others are not able to be specified such as the materials used.

The materials used and how they are fitted together make a significant difference in how effective the security is and how tamper resistant the device is. To accomplish the goals, it typically requires strong coordination between the various engineering disciplines mentioned earlier in this paper.

One example is the effectiveness of adhesives or potting which can vary drastically depending on substrates it is applied to and the environment it is subjected to. Most adhesives have dramatically different adhesion properties when applied to different types of plastic or to metal. They also have different strengths depending on the stress mode (sheer vs. tension) which can make a difference of where they are used in the structure. Shelf life, cleanliness and curing processes can also affect the strength of the adhesive in the final product as well as the environment temperature and light conditions as many adhesives (and plastics) degrade with elevated temperatures and exposure to UV light.

4.3 Tamper Detection

Ideally, tamper detection is never needed and is the last line of defense as it always results in a denial of service situation, which could be the real goal of the attacker. It is important as the final defense that the module has a robust system of not only detecting if the crypto boundary has been compromised, but also that the zeroization is immediate, complete and effective.

Zeroization and the circuits that detect and perform that function are typically not complicated electrically, but the specification of tolerances, operating windows and functionality can render the detection to be so sensitive that it is always false triggering or alternatively, is so insensitive that it is ineffective at performing the mission in all, but the nominal case.

Similar to tamper resistance, the materials chosen and the specific mechanical and electrical design have a significant effect on the robustness of the security. Each material choice and design trade-off has security strengths and weaknesses, and must be carefully understood in order to make cost effective and security effective decisions for the product. In most cases, cost is a significant driver in how much security can really be afforded in that particular application.

4.4 Multiple Discipline Technology

One of the most difficult challenges of a robust physical security design is the multitude of disciplines that may need to be involved and must be seamlessly integrated to provide a robust and appropriate solution. As the level of security increases, the number and the sophistication of these disciplines increase significantly. These disciplines need to be part of the design team and also the evaluation team (laboratory) and in many cases to comparable levels of skill. Some of the probable disciplines that are necessary include:

- Mechanical Engineering; Technician: Practitioner
    - Stress and strength of mechanical systems
- Chemical Engineering; Technician: Practitioner
    - Adhesion
    - Solvents
- Materials Engineering; Technician: Practitioner
    - Strength of materials
- Electrical Engineering; Technician: Practitioner
    - Analog Circuits
    - Digital Circuits
    - Electromagnetic
    - RF and emissions
- Physics; Technician: Practitioner

  - Thermal
  - Optical
  - Audio
- Security Engineering; Technician: Practitioner
  - Integration of the all the disciplines to attain the security objective
  - Understanding of vulnerability and risk assessment

As with any complex system, the effectiveness of the system is the attention to details.

SECURITY IS ALL ABOUT DETAILS

This concept is particularly relevant to physical security. Often, the weakest points of systems are at interfaces, this applies to virtually all designs that are modularized, and is particularly evident when technology transitions are also present. Crypto module physical security is the same way with often the weakest point being where components physically come together and attached by a fastener or adhesive, and also when there are technology interfaces between different disciplines of the design team.

5 Physical Security Specification Challenges

5.1 Standard Challenge

How does a standard such as FIPS 140-2 describe physical security requirements and furthermore multiple levels of security?

In many respects, the real objective of increasing the levels of physical security is to have an ever increasing "*level of effort*" to implement a successful attack on the module. The level of effort is a function of several factors:

- Time required to conduct the attack
- Time to develop specific attack methods, tools, and skills. This is sometimes referred to "non-recurring" labor.
- Formal education of the attacker
- Skill and practice of the attacker
- The availability of capital equipment and expert or unique resources as required
- Risk of failure or probability that the attack will not be successful

Figure 2 shows how the level of effort to conduct a successful attack would increase as the desired security level increases.

In general, all attacks begin with a survey to find the potential weakest points and then to develop an attack plan to maximize the probability of success. The weakest element is likely to be what a real live attack would focus on and not necessarily the FIPS specified features or test methods.

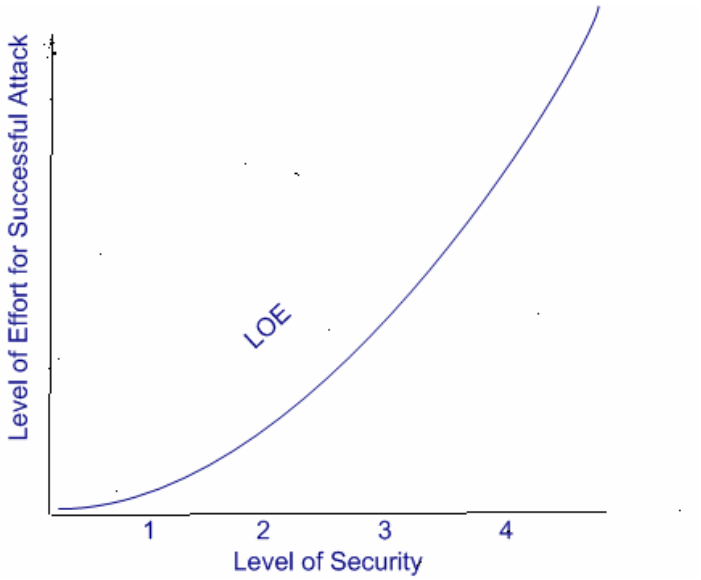

Figure 2 - Level of Effort

When FIPS 140-1 was developed, a choice was made to define characteristics that at the time would, in theory, require increasing levels of effort as the security level specified increased. This decision drove the testing toward compliance of the design to the specified features and not toward a vulnerability assessment and mitigation program. As such, it is entirely possible for modules to be compliant and yet be extremely vulnerable. An important question is; at what point does the allowance of extreme vulnerabilities no longer serve the needs of the end user, even though the module has been validated? In addition, is it possible for the standard or DTR to be augmented to resolve this dilemma?

The table below summarizes the basic concepts specified in FIPS 140-2 and is not intended to be 100% comprehensive or to address the variations described for the various embodiments. The purpose of including this table is to provide a brief glimpse at how the specification of features adds security and "*level of effort*" for the specific potential threats/vulnerabilities envisioned when FIPS 140-1 was drafted.

Security Level 1	* Production grade hardware	*Production Grade Hardware* promotes a level of product quality and reliability that enable the user to trust the module is likely to operate correctly. This reliability as opposed to least expensive grade of products (i.e., toys).
Security Level 2	* Production hardware *Plus* * Tamper Evidence * Opaque to visible spectrum * Pick Resistant Locks on Doors and Covers	*Tamper Evidence* provides a mechanism for the user to have an opportunity to observe that the module may not be trustworthy and subsequently take appropriate action. *Opaque* provides a deterrent to being

		able to, collect information about the module, target an attack or direct a probe to be able to collect data that may compromise the module. *Pick Resistant Locks* provides a deterrent to being able to gain ready access to the hardware, providing a level of tamper resistance.
Security Level 3	* Production hardware *Plus* * Tamper Evidence *Plus* * Opaque to visible spectrum *Plus* * Vents obstructed * Hard Epoxy Potting *or* * Tamper Detection and Response - covers and doors	*Hard Epoxy Potting* combines tamper evidence along with tamper resistance in that it requires time and experience for the attacker to remove the epoxy without damaging the underlying circuitry. The hardness of the potting can have a direct effect on how hard it is to push a tool through the potting that could probe for signals. *Vents* or other openings can be used as access points to probe or sense internal signals to either capture text or data from an existing session or to compromise CSPs that could affect current and future sessions. *Tamper Detection* for covers or doors provides a level of tamper resistance that reduces the probability of a successful attack. *Tamper Response* is the action taken when tamper or a threat is detected. This includes zeroization of the CSP's.
Security Level 4	* Production hardware *Plus* * Tamper Evidence *Plus* * Opaque to visible spectrum *Plus* * Tamper detection and response – envelope *Plus* * EFP/EFT	*Tamper Envelope* provides a mechanism to detect any breach in the cryptographic boundary. This is a significant increase over sensing covers and doors. *EFP/EFT* provides a protection from inducing faults via temperature techniques.

Figure 3 - FIPS 140-2 Levels

As a comparison, we have observed and worked with other approaches dealing with this challenge.

1. Establish a minimum cost (level of effort) that it would take to compromise the module. This approach includes guidelines on how to estimate the cost which

includes all the factors that may play a role in the cost, including equipment, labor and material. Additional notes to mention is that the program is currently not limited to only the function of compromising the crypto boundary, but also having a mechanism that would electrically/logically compromise the module. Another aspect is returning the module to operational state, which does allow the use of substitute/replacement parts (which in real life is valid probability).

2. Secondly, we have worked in environments where the expected approach was more along the lines of a risk assessment. From a concept perspective, this is similar to basic concepts in the NIST FISMA program, which is currently targeted to address system security rather then module security. Virtually all the same IT security principles apply to both. This approach is more of a vulnerability assessment and then comparison to the amount of security required vs. defining features. This approach provides information on the weakest elements and allows the overall security and risk to be managed vs. compliance to a set of features that may or may not be comprehensive or to have the most relevant factors. On the other hand, it does not provide as easy of an environment to manage the laboratory and validation process.
3. Lastly, we have seen a combination of the two approaches used. Typically, FIPS 140-2 Level 3 requirements may be imposed, but then the regulator also wants to be provided information that would allow them to understand if the realized security has vulnerabilities that are not caught with FIPS 140-2 and may not meet the intent of their security requirements. At that point, a decision is made between the lab and the regulator if the vulnerability is really an issue in that case or can be accepted as meeting the intent and security threshold.

This strategy of defining the physical security features vs. defining the level of physical security has both positive implications, as well as, negative implications. On the positive side:

- It provides the vendors with clear features that must be present in their product designs. This provides a straightforward set of requirements for the designers to plan and include into their designs.
- It provides clear feature for the laboratory to use and evaluate during testing, and for CMVP during the review of reports.
- It provides a range of solutions that are likely to provide a progression of stronger and stronger physical security as the level increases.

The challenges in the strategy, which was established in the early nineties when FIPS 140-1 was being drafted, include:

- The realized effectiveness or quality of the design and materials are not easily specified and therefore taken into account. This is a challenge due largely to the wide range of disciplines that a developer and a laboratory need to have proficiency in when implementing a higher security level product. Our observations indicate that the specific design and material choices have a dramatic effect on the realized physical security of the product. The effectiveness and

quality of the design is left to the laboratory to determine, which is appropriate, but can also allow for significant variations in security depending on if the laboratory would actually be able to be considered qualified and skilled in all the disciplines mentioned in the introduction, to a point that it could be a "highly motivated attacker" as some threat sources (Figure 6) could be described.

Figure 4 below shows the addition of some quality ranges to the level of effort shown in Figure 3. Note that it is feasible for the realized security to be no better than the anticipated typical level of lower level. If lower effectiveness choices are made, then there are a variety of potential risks that may be implicitly accepted.

- Security, if one level is necessary (department security policy), but in actual fact, it is lower level threats that may be able to compromise the module.
- It could be risky to maintain security over the entire product life, both in terms of the number of years the product is produced and sold, as well as, the installed life, as the tendency is to degrade over time.

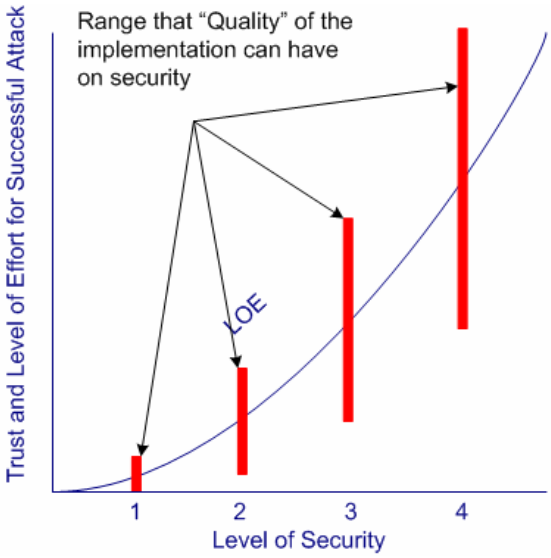

Figure 4 - The effect of "Quality" on realized Physical Security

- Flexibility of the designer to meet the intent without getting caught up in specific compliance language; thereby reducing innovation to create new solutions intended to meet physical security expectations. How long will the concepts from the 80's and 90's be the only or best approach to solve the physical security goals?
- Manufacturing tolerances can have dramatic effect on the performance of a physical security system. Items that are handmade and custom fitted may have acceptable tolerances while later in the manufacturing process, component tolerances or assembly variations can render some features as virtually useless.

- What are the boundaries of the testing? For example, the actual capture of signals and compromise is out of scope as these sections of the standard are focused on physical security barriers not on the capture or compromise of the available logic. This is important in order to contain the evaluation costs, but a question most often asked by vendors is "now that you have gotten through the cryptographic boundary what can you really do". As portrayed in the statement by Microsoft, included in the introduction, it may not be important to proceed as there are really no access controls once the physical security is compromised.

This approach has worked well for the CMVP so far because the laboratories evaluating the product has specific features to look for that will support increasing levels of physical security. There has been a small community of laboratories that work closely with NIST to have a reasonable understanding of the intent as well as the language. The challenge is that the "effectiveness" of the security feature can have a dramatic effect on the ability of the feature to provide the security envisioned, and how the standard can better specify both the feature and the effectiveness of the feature.

5.2 Evaluation Laboratory (Test) Challenge

How should FIPS 140-2, the derived test requirements (DTR) and the Implementation Guidance documents describe physical security testing requirements? What tests would really assess if a module's physical security features and characteristics function as intended and in compliance with the vision and intention of the FIPS 140-2 standard?

The CMVP program faces a multitude of challenges in determining the best strategy to test or evaluate modules for compliance. The first difficulty is not only assessing if a feature exists, but also if the effectiveness, quality and functionality of the feature are sufficient to meet the intent.

To promote consistency between labs, the CMVP program has established some testing ground rules. This has helped in implementing common test methods, but has created areas where the test methods are not comparable to a real attacker. One example has been that at Level 3, processes using drills are not considered a valid test; however in some cases, modules with tamper detection switches can be accessed in a couple of minutes using a drill to defeat the tamper detection switches.

Just as one design does not work for all vendors and crypto modules, one test process or test method does not adequately test the security effectiveness of the device under test. Actual attackers use innovation to find the easiest and best way to defeat a module. It is difficult to have repeatable processes when a significant amount of innovation is introduced. Therefore, the FIPS 140-2 program is challenged to come up with test guidance that enables some level of common sense innovation while also maintaining consistency for each evaluation and for each lab.

For Levels 3 and 4 with a determined attacker as a probable threat, the scenario is one in which the attacker has significant time and resources to utilize in attaining their goal. However, the laboratory needs to use methods and techniques to leverage their assessment as the budget to perform the testing may only be 10 or 20 percent of what a real attacker may have available.

6 Roles/Constituents

A multitude of relationships can be present on a particular project or product line, see Figure 5. Effective security, especially physical security (access control) is often implemented in a layered approach of which the crypto module is the final defense and in other cases, it may be the one and only defense.

NIST has been mandated and chartered to develop and maintain the FIPS 140-2 standard to support the needs of the federal government. The value of the process is to enable the end users of the devices to have security that is interoperable and trusted. As the CMVP community proceeds with the evolution of FIPS 140-2 to FIPS 140-3, the expectations of final end users should be given serious consideration in spite of the fact that they may have limited direct input into the standard.

Both the environments that the crypto modules are used in and the threats to the systems are dynamic and ever changing; therefore, it is unlikely that all of the same reasoning and logic that was applicable in FIPS 140-1 (early nineties) and FIPS 140-2 (late nineties) is still the optimum for the next generation of FIPS 140-3 end users. On the other hand, the CMVP program and the vendors have a motivation to keep the program stable and minimize the changes. The challenge will be to find the best balance between change and stability.

Figure 5 depicts the major (typical) constituents and the interfaces they typically have. In some cases, the module owner/user has little or not contact with NIST or the laboratory, and in other cases there may be a closer working relationship.

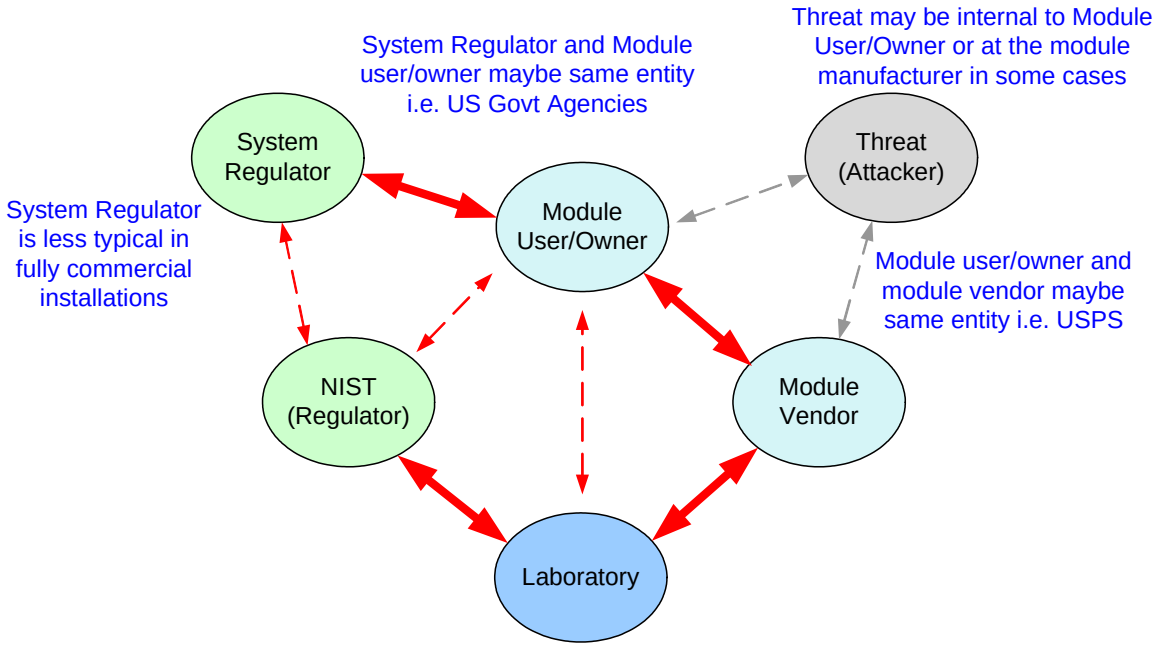

Figure 5 – Typical crypto module constituents

One topic that should be noted with respect to the risk/threat of a module is that at some point, it is possible for the system regulator or the module owner to have a loss associated

with the insecurity of a device. The loss can range from significant, such as the physical compromises that have cost vendors and owners considerable money to re-key their entire systems, to catastrophic, where it can cost jobs, careers or even legal implications.

As we engage in reviewing physical security requirements, the entire team needs to heavily weigh the needs of the end users in comparison to the laboratory, CMVP, or vendor's direct motivations.

6.1 Attackers

Physical security is intended to thwart the efforts of persons attempting to compromise the module. Many organizations have categorized attackers, for this discussion the profiles from SP 800-30 will be used, and are summarized in Figure 6.

Threat Source	***Motivation***	***Threat Actions***
Hacker; Cracker	• Challenge • Ego • Rebellion	• Hacking • Social Engineering • System Intrusion, break-ins • Unauthorized system access
Computer Criminal	• Destruction of information • Illegal Information disclosure • Monetary gain • Unauthorized data alteration	• Computer Crime (e.g. cyber stalking) • Fraudulent act (e.g. replay, impersonation, interception) • Information bribery • Spoofing • System Intrusion
Terrorist	• Blackmail • Destruction • Exploitation • Revenge	• Bomb/terrorism • Information warfare • System Attack (e.g. distributed denial of service) • System penetration • System tampering
Industrial Espionage (Companies, foreign governments, other government interests)	• Competitive advantage • Economic espionage	• Economic exploitation • Information theft • Intrusion on Personal Privacy • Social Engineering • System Penetration • Unauthorized system access (access to classified, proprietary and/or technology related information)
Insiders	• Curiosity • Ego • Intelligence • Monetary Gain	• Assault on an employee • Blackmail • Browsing proprietary information

Threat Source	Motivation	Threat Actions
	• Revenge • Unintentional errors and omissions (e.g. data entry error, programming error)	• Computer abuse • Fraud and Theft • Information bribary • Input of falsified, corrupted data • Malicious code (e.g. virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

Figure 6 - Threat profiles from SP 800-30 Risk Management Guide for IT Systems

In analyzing the various threat sources listed in Figure 6, it becomes apparent that the threats have a wide range of ability to carry out an attack. From the lower end, such as a single student with somewhat limited financial and time available to the other extreme, where a well-funded project is dedicated to compromising the module.

One example of a well-funded project is the attack on the security systems protecting satellite TV programming. One of the primary organizations interested in attacking the satellite TV system were the South American drug lords. The drug lords had a personal desire to have the programming and signals wherever they were located and could not afford to take the risk of signing up for the service. Thus, as you can imagine, there were no practical limits on the equipment cost, time or talent required to accomplish the task. A side benefit, of course, was once they had broken the system, it enabled them to then start up another illegal business entity (pirated satellite signals).

In summary, the attackers can have a lot of different motivations and may very well have more resources available to defeat the module than the design or test teams in building the module. FIPS 140-2 and the associated standards and processes can provide leverage to stand up to significant threats, if careful attention is given to the details.

7 Physical Security vs. Module Life Cycle

Currently FIPS 140-2 covers only the operational phases of the crypto module's lifecycle (see Figure 7 below). Although this is satisfactory for most end users, it is insufficient for some of those end users that operate in high threat environments. In high threat environments, physical security features need to commence protecting the module while it is in final manufacturing and testing phases as well as initialization, personalization, distribution and finally at the end of life phase.

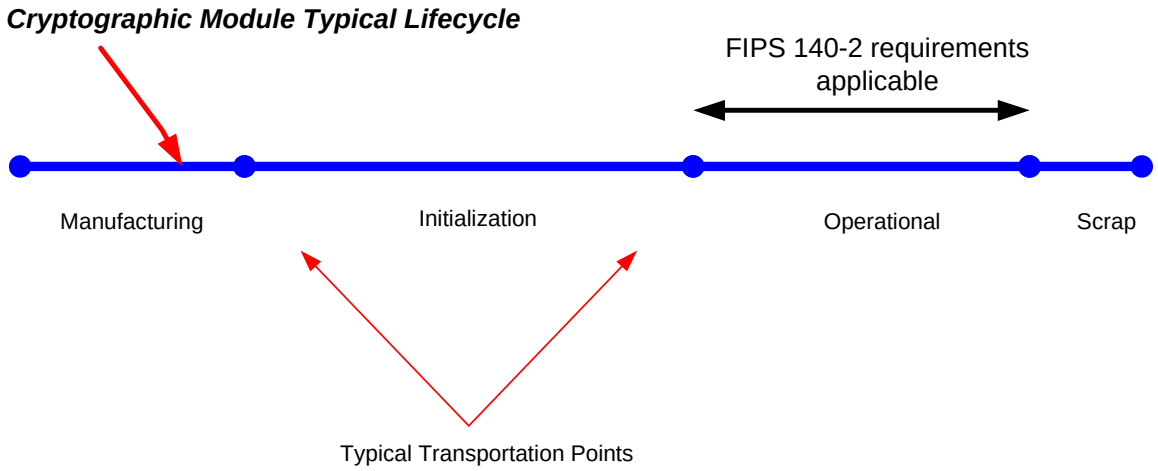

Figure 7 – Entire module lifecycle vs. FIPS 140-2

The extended protection timeframe is necessary to protect the integrity from threats that may exist in the environments the module is in during those phases. For example, risk of loss of critical common keys, authentication parameters, source code or specific data may require extensive effort and impact to re-key the system and re-establish security, which maybe in addition to the impact of the loss itself. In some cases, this has end user impact, while in others, the risk is to the vendor that is outsourcing manufacturing.

End users need to realize that if more than "off the shelf" security is needed, then additional testing beyond the current FIPS 140-2 crypto module lifecycle is required. In the future, FIPS 140-3 could add the flexibility for the security policy to state the relevant phases and the specification could be augmented to support what is needed for the situation versus only a predefined window of time.

As outsourcing design and manufacturing becomes more prevalent, trust becomes a major issue. It is possible with today's economic development pressures that the crypto module manufacturer may not be a trusted entity. This situation brings new challenges as different entities have different levels of legal, management, or technical process controls. This phenomenon brings a unique set of threat and lifecycle scenarios that are dependant on multi-layered security, including physical security in many cases. Two examples of this situation include voting machines and postal meters.

8 Conclusion

Physical security is a complicated system that involves a wide range of engineering disciplines. Often physical security design is not considered a critical factor in the product design early enough in the process to have the appropriate security designed in with minimal cost and schedule impact. It can be a significant error to underestimate the challenges of implementing and achieving a high level of security, especially the level, which we as security professionals would trust with our most precious information.

FIPS 140-3 is a great opportunity to work together and make the standard better for end users (the real beneficiaries) and vendors as well as improve the evaluation and validation processes implemented by evaluation laboratories and NIST respectively.

9 References

FIPS 140-2

http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/ipsecapd.mspx

Special Publication 800-30 - Risk Management Guide for Information Technology Systems