INFOGARD

Security Assurance
*Independence. Integrity. Trust.*

# FIPS 140-2
# Physical Security Attack Scenarios

NIST CMVP
Physical Security Conference

Mark Shin

**September 15, 2005**

*05-998-R-0060 Version 1.0*

# Table of Contents

1 Abstract ..... 3
2 Introduction ..... 3
3 Physical Security Features ..... 4
3.1 Potting Encapsulation ..... 4
3.1.1 Potting Encapsulation Security Feature Overview ..... 4
3.1.2 Potting Encapsulation Attack Scenarios ..... 4
3.2 Enclosures and Tamper Switches ..... 5
3.2.1 Enclosure and Tamper Switch Security Feature Overview ..... 5
3.2.2 Enclosure and Tamper Switch Attack Scenarios ..... 6
3.3 Enclosures and Tamper Wrappers ..... 6
3.3.1 Enclosure and Tamper Wrapper Security Feature Overview ..... 6
3.3.2 Enclosure and Tamper Wrapper Attack Scenarios ..... 7
4 Conclusion ..... 9

# 1 Abstract

This general, informative paper describes various attacks and vulnerabilities that security modules have experienced. The attack examples presented will be used to provide an orientation of how physical security is a necessary element of securing a module to protect the module's use and function. Some of the attack examples provided are illustrative of those that may have occurred in the payment card or postal industries.

A range of tools, methods and techniques often implemented by attackers will be described. The appropriate tools used by attackers typically vary by embodiment and level of security. Thus, this discussion will include a graduated attack approach based on embodiment, level of security and security target.

This paper will educate end users to assist them in determining what level of security they should choose when selecting a security module or if they should augment their current security environment to more effectively manage security module risk. In addition, the topic of this paper will help assist regulators, designers and evaluators on how to more effectively perform their roles.

# 2 Introduction

The physical security characteristics and mechanisms integrated in cryptographic modules (security or cryptographic) are an independent system that should effectively protect against potential penetration attacks deemed reasonable and appropriate for their given deployment environment. As the deployment environment becomes more hostile, the integrity of the (security or cryptographic) module relies heavily on the detection and possible prevention of unauthorized physical access; this has become a prime objective of FIPS 140-2 Level 3 and Level 4 physical security requirements.

The dependability of cryptographic modules is reliant upon all of the elements and the interactions of the physical security system. The components that devise the physical security system must work together in unison and be of comparable strength. If any component of the system is weak or works ineffectively with any of the other components, then that component has the potential of causing an overall physical security system weakness. Attackers typically research and investigate these system weaknesses and tailor an exploit to take advantage of this vulnerability to compromise cryptographic module.

This paper will describe some of the commonly used FIPS 140-2 Level 3-4 physical security features and various attack methods and tools devised and used by InfoGard Laboratories to compromise security modules during FIPS 140-1 / 140-2 Levels 3 and 4 cryptographic modules validations.

This paper will not discuss or disclose specific proprietary designs, but rather common security features.

# 3 Physical Security Features

Cryptographic modules designed to meet FIPS 140-2 Levels 3 or 4 physical security requirements are, in many ways, designed with similar types of physical security features. The three most commonly used protections include: encapsulation by potting, enclosure protected via switch, and enclosure protected via tamper wrapper. The following sections will give a brief introduction to each of these protection features, benefits of the protection feature, successful attacks executed against the protection feature, and examples of the tools used during the attack.

## 3.1 Potting Encapsulation

### *3.1.1 Potting Encapsulation Security Feature Overview*

Potting encapsulation of the module circuitry is a common protection feature seen in FIPS 140-2 Levels 3 and 4 cryptographic modules. Encapsulation potting is best described as surrounding the cryptographic boundary with a hard, opacic material. FIPS 140-2 Level 3 security requirements indicate that it is sufficient to protect the cryptographic module with this option provided that the potting material adheres to certain physical characteristics: opacity (or inability to see through the potting material), visible tamper evidence if removed, and "hard" after properly cured. No other electrical, mechanical, or physical security components are required at the FIPS 140-2 Level 3, if this option is chosen.

FIPS 140-2 Level 4 modules also allow for potting encapsulation, but require additional security features such as "envelope protection" and "tamper detection and response circuitry". These types of mechanisms, when employed with a potting material typically require a tamper wrapper of some sort (discussed later).

One of the major benefits of potting encapsulation is its design simplicity. Adopting this protection feature allows the designer to forgo incorporating additional active circuitry to monitor tamper.

### *3.1.2 Potting Encapsulation Attack Scenarios*

Potting materials, such as epoxy, are typically susceptible to two methods of attack: heat and solvents. It should be noted, however, that both of these attack methods are currently beyond the scope of FIPS 140-2 Level 3 and only relevant for Level 4 modules. InfoGard's experience is that bypassing or compromising the encapsulation material alone is a trivial task.

#### 3.1.2.1 Heat Exposure

Potting materials have a high temperature threshold where the epoxy will no longer be reliable. The reaction will differ per encapsulation material; however, epoxy can generally be removed without causing serious damage to the underlying circuitry. These high temperature thresholds can easily be found in the material datasheet, where it specifies the recommended operating range. The common reaction to heat is that the potting material either becomes extremely soft such that a knife can easily cut through the material; or the material begins to burn, crumbling off when lightly brushed with a copper brush. The heat can be applied in a variety of ways. Common tools used include:

- High temperature heat gun

- Soldering iron with a variable temperature controller

#### 3.1.2.2 Solvent Exposure

Potting materials are typically susceptible to a variety of solvents that are commonly available in the market. Available solvents range from those designed specifically to remove potting materials such as epoxy to common household cleaners that have small concentrations of sulfuric acid. The required solvents are readily available and do not require special handling skills.

Generally, it takes less than 4 hours of exposure to the solvent to observe a compromise of the potting encapsulation material; however, to remove large portions of potting material takes approximately 16 hours.

## 3.2 Enclosures and Tamper Switches

### *3.2.1 Enclosure and Tamper Switch Security Feature Overview*

The most common mechanisms used to protect modules with metallic and/or plastic enclosures are tamper switches. Tamper switches prevent unauthorized access by detecting an opening of the module's cover and/or doors. Upon detection, the module responds by zeroizing all plaintext critical security parameters; thus, leaving the module and its information virtually without value.

There are a variety of different switch technologies, with each exhibiting unique security characteristics:

- *Micro-switches* are the most basic switch. These types of switches are engaged when the module's enclosure (covers and/or doors) are closed and force is applied. When the enclosure is opened, the switch releases, which in turn causes a tamper event.
- *Pressure contacts* function in a similar manner as the micro-switch. With this approach, there are typically two conductive pads designed on a PCB board (rather than a separate component). When the module's covers/doors are closed, the two pads become shorted typically by a conductive membrane (commonly seen in keypads). When the enclosure is opened, the conductive membrane no longer provides the conductive link between the two pads, creating an open circuit, and causing the module to respond with a tamper event.
- *Reed switches* respond to the polarity of a magnetic source in close proximity. Typically, the module's enclosure is fixed with a magnet to engage a reed switch, which is mounted on the module's PCB. When the enclosure is opened, the magnetic source moves further apart from the reed switch, eventually causing a tamper event.

The benefits that tamper switch protection include ease of manufacturing and incorporating both tamper and response detection.

It should be noted that the limitations (e.g., no drilling, milling, grinding, or dissolving) imposed on CMVP laboratories make tamper switches, by themselves, acceptable solutions for FIPS 140-2 Level 3 cryptographic modules. However, the testing limitations are removed on FIPS 140-2 Level 4 modules so in order to achieve compliance, these modules would require additional security features.

### *3.2.2 Enclosure and Tamper Switch Attack Scenarios*

In many cases, tamper switches are extremely easy to defeat. The challenge of defeating a tamper switch largely depends on whether or not the objective is to limit or have no visible evidence of tamper.

Beyond FIPS 140-2, other programs such as those imposed on pin entry devices and postal security devices, realize that the end user may be the individual or organization that is most interested in compromising the module. As such, an overseeing officer such as a Crypto-Officer, may not exist to visually inspect the module to see if a tamper event has occurred. In these scenarios, the dependency of the module to protect itself would, in general, be that much more critical.

Standard micro-switches are generally more susceptible to common attacks because of the mechanical aspect of engaging the switch. Such attacks include: utilizing a custom tool to hold the switch down as the enclosure is opened, applying glue to the actuator of the switch to keep it engaged, and filling the whole chassis with a material that would keep the switch engaged (e.g., a foam insulator).

Pressure contacts, which are typically found in modules with keypads, are somewhat more difficult to attack, since they require slightly more force to keep engaged. The objective to defeat pressure contacts is to gain access to the contacts and apply conductive ink, shorting the contacts pads, and making the device believe that the conductive membranes were never released. Depending on the size of the accessible area, a thin hypodermic needle with conductive ink could be used to assist with this type of attack.

Reed switches require a different set of techniques due to the inherent characteristics of the switch. Reed switches are engaged with the use of a magnetic charge so they can be defeated by inducing an outside magnetic source. To successfully defeat a reed switch, the polarity of the existing magnet must first be determined (i.e., with the use of a compass). Once the polarity is determined, a strong magnetic force is introduced directly over the location of the reed switch prior to opening the enclosure; this will avoid the introduction of a magnet with the opposite polarity, which may cause a tamper event.

## 3.3 Enclosures and Tamper Wrappers

### *3.3.1 Enclosure and Tamper Wrapper Security Feature Overview*

Modules attempting to provide protection features against drilling attacks typically rely on a tamper wrapper solution. A tamper wrapper is a flexible film that has conductive traces on it, used to fully enclose the cryptographic module. Depending on the material of the tamper wrapper and the characteristics it exhibits, the tamper wrapper also provides security features that could protect against a variety of other attacks, including chemicals, heat, cutting, grinding, and drilling.

Other tamper wrapper characteristics that determine the strength of the physical security include the penetration prevention, which depends on the number of tamper layers within the film, width and distance between traces, visibility of the traces, and composition of the material traces. Tamper wrappers that exhibit high impedance characteristics are typically harder to defeat

because of their ability to monitor a change in voltage potential due to physical attack or outside characteristics such as heat. Tamper thresholds are defined in a manner to balance security sensitivity and are reliable (i.e., prevention of false tampers).

The security of the module with a tamper wrapper solution also relies on the folding and wrapping methodology. Areas that are not covered by the wrapper could be exploited, depending on the size of the hole and the accessibility of the opening. The ability to unwrap the tamper wrapper is also a concern. This would be dependent on the adhesive or bonding material (e.g., epoxy or resin) used to ensure that one could not unfold the wrapper sufficiently enough to create an opening.

### *3.3.2 Enclosure and Tamper Wrapper Attack Scenarios*

Tamper envelope implementations are generally more difficult to defeat, requiring more time, precision, and creativity to devise and execute a plan successfully. The following sections provide a summary of basic needs and attack processes against such protection features.

#### 3.3.2.1 Visibility

The effectiveness of an opaque enclosure is one critical area in higher end physical security devices. Without visibility of the traces, it is nearly impossible to bypass and defeat the tamper traces. Visibility can be achieved through a variety of mechanism, but the object is the same: remove or thin the outer enclosure or layer that is directly above the traces. Some ways to achieve this is through the use, or a combination, of:

- Precise drilling tools
- Milling tools
- Chemical exposure
- Sandblasters
- Electrical blasters
- Heat exposure

Covert mechanism can also be used to expose the traces so that an attack can be mounted. These methods generally require more creativity and planning, and will more than likely be depending on the module design and material. Such mechanisms may include:

- X-Ray
- Statically charge the conductive traces
- Heat dissipation

#### 3.3.2.2 Accessibility

After the traces are visible, they must be physically accessible before going any further. This step requires care since the encapsulation or enclosure material is generally bonded to the wrapper traces directly. This prevents the ability to easily access large areas on the wrapper. Often, the accessible areas are multiple openings of no larger than 200 – 400 microns in diameter; this type of process is necessary to prevent an entire tamper trace from being removed.

These holes would be exploited by using them to short multiple areas within the wrapper in an effort to create an area on the tamper film that is disabled.

Tools that are commonly used would include drilling, melting, or piercing tools. However, if a solvent exists that removes the outer enclosure or encapsulation material, but does not adversely affect the tamper wrapper, that would be the most optimal solution.

The size of the disabled area will depend on the detection circuit. If the detection circuit acts in a digital manner, then the voltage potential across two or more points are not monitored allow us to remove the largest possible area that is accessible. However, if the detection circuit monitors the voltage potential of two or more points, then a pre-calculation must be performed to determine the maximum area that can be disable and still be within the tamper detection threshold. This threshold varies greatly from module to module; however, it is not uncommon to have a threshold as large as 35% from the norm since product reliability (i.e., prevention of false tampers) is as critical as the security during product development.

#### 3.3.2.3 Attacks on copper based tamper wrapper solutions

A variety of methods have been used to attack cryptographic modules that are protected with copper based tamper wrapper solutions. Modules that are protected with low impedance tamper wrappers are generally easier to defeat. These wrappers are commonly composed of copper traces imposed on a thin single layer PCB. Copper traces are relatively durable against mechanical, chemical, and high temperature based attacks. Once the traces are accessible, they are also relatively easy to bypass, either by unwrapping the tamper wrapper or by penetrating the wrapper after shorting traces with tools such as solder.

#### 3.3.2.4 Attacks on conductive ink based tamper wrapper solutions

There are also solutions that use tamper wrappers that are more sensitive than copper based wrappers, such as conductive ink. These types of wrapper solutions can be supported with a similar tamper circuitry as seen in copper traces, which is more of a digital detection mechanism, or if the wrapper exhibits high impedance characteristics, it could be designed with circuitry that detects a change in the voltage potential. Regardless, these solutions are generally more sensitive against chemical, mechanical, and heat attacks.

In these solutions, visibility and accessibility are crucial steps before critical security parameters can be extracted and a successful attack is mounted. Preventing visibility and accessibility are generally depending on the compatibility of the outer material used to enclosure the wrapper solution, and the conductive ink. Some examples of the outer material may include metallic enclosures, plastic enclosures, and an encapsulation material such as epoxy. Once visibility and accessibility have been realized, the vast majority of the cryptographic modules tested have been successfully defeated.

# 4 Conclusion

Physical security is an independent system. Every material used, process employed, and design detail may be important for it to be capable of reliably fulfilling the role intended. Deficiencies in any of these areas may result in weaknesses that could be exploited when deployed. It is important to understand the type of physical protection features, and the potential weaknesses that may exist as they all affect the over all security.