TECHNICAL SPECIFICATION

ISO/IEC TS 30104

First edition
2015-05-15

Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements

Technologies de l'information — Techniques de sécurité — Attaques de sécurité physique, techniques d'atténuation et exigences de sécurité

Reference number
ISO/IEC TS 30104:2015(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT), see the following URL: Foreword — Supplementary information.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Security techniques*.

Introduction

The protection of sensitive information does not rely solely on the implementation of software mechanisms employing cryptographic techniques, but also relies significantly on appropriate hardware implemented security devices that employ tamper detection and protection of critical security parameters (e.g. cryptographic keys, authentication data, etc.).

This is especially relevant for devices that may be installed, deployed or operated in hostile, untrusted, or non-secure environments, or for devices that contain high-value data assets.

An attacker may not be motivated by the economic value or the successful access to sensitive information, but simply the challenge of compromising a design or system that has been advertised as "secure". The challenge to break the design gives such an attacker instant fame and recognition amongst peer groups.

Currently, much of the information in this area originates from disparate sources, may not be presented consistently, and may not address appropriate evaluation and testing techniques.

Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements

1 Scope

Physical security mechanisms are employed by cryptographic modules where the protection of the modules sensitive security parameters is desired. This Technical Specification addresses how security assurance can be stated for products where the risk of the security environment requires the support of such mechanisms. This Technical Specification addresses the following topics:

— a survey of physical security attacks directed against different types of hardware embodiments including a description of known physical attacks, ranging from simple attacks that require minimal skill or resources, to complex attacks that require trained, technical people and considerable resources;

— guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks; and

— guidance on the evaluation or testing of hardware tamper protection mechanisms and references to current standards and test programs that address hardware tamper evaluation and testing.

The information in this Technical Specification is useful for product developers designing hardware security implementations, and testing or evaluation of the final product. The intent is to identify protection methods and attack methods in terms of complexity, cost and risk to the assets being protected. In this way cost effective protection can be produced across a wide range of systems and needs.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790 and ISO/IEC 24759 apply and are duplicated here for reference.

NOTE Definitions followed by a reference in square brackets are taken verbatim from ISO/IEC 19790:2012 or ISO/IEC 24759:2014 All other terms and definitions are adapted from those in ISO/IEC 19790:2012 or ISO/IEC 24759:2014.

3.1
compromise
unauthorised disclosure, modification, substitution, or use of critical security parameters or the unauthorised modification or substitution of public security parameters

[SOURCE: ISO/IEC 19790:2012, 3.13]

3.2
conformal coating
material that may be applied in layers or in various thicknesses that adhere directly to the electronic components or printed circuit boards and provide a hard coating that deters machining, probing, energy or chemical attacks

3.3
critical security parameter
CSP
security related information whose disclosure or modification can compromise the security of a cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.18]

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

Note 1 to entry: A CSP can be plaintext or encrypted.

3.4
cryptographic boundary
explicitly defined perimeter that establishes the boundary of all components (i.e. set of hardware, software, or firmware) of the cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.21]

3.5
cryptographic module
module
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

3.6
differential power analysis
DPA
analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

[SOURCE: ISO/IEC 19790:2012, 3.29]

3.7
environmental failure protection
EFP
use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions outside of the module's normal operating range

[SOURCE: ISO/IEC 19790:2012, 3.39]

3.8
environmental failure testing
EFT
use of specific methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions outside of the module's normal operating range

[SOURCE: ISO/IEC 19790:2012, 3.40]

3.9
firmware
executable code of a cryptographic module that is stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution while operating in a non-modifiable or limited operational environment

[SOURCE: ISO/IEC 19790:2012, 3.45]

EXAMPLE Storage hardware can include but is not limited to PROM, EEPROM, FLASH, solid state memory, hard drives, etc.

3.10
hardware
physical equipment/components within the cryptographic boundary used to process programs and data

[SOURCE: ISO/IEC 19790:2012, 3.50]

3.11
passivation
effect of a reactive process in semiconductor junctions, surfaces or components and integrated circuits constructed to include means of detection and protection

[SOURCE: ISO/IEC 19790:2012, 3.87]

EXAMPLE Silicon dioxide or phosphorus glass.

Note 1 to entry: Passivation can modify the behaviour of the circuit. Passivation material is technology dependant

3.12
physical protection
safeguarding of a cryptographic module, CSPs and PSPs using physical means

[SOURCE: ISO/IEC 19790:2012, 3.90]

3.13
production-grade
product, component or software that has been tested to meet operational specifications

[SOURCE: ISO/IEC 19790:2012, 3.95]

3.14
physical security invasive attacks
attacks that involve a physical alteration to the implementation that may also cause an operating aberration different from normal operation

3.15
physical security non-invasive attacks
attacks that do not involve a physical alteration to the implementation cause an operating aberration different from normal operation

3.16
removable cover
physical means which permits an intentionally designed non-damaging access to the physical contents of a cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.101]

3.17
sensitive security parameters
SSP
critical security parameters (CSP) and public security parameters (PSP)

[SOURCE: ISO/IEC 19790:2012, 3.110]

3.18
simple power analysis
SPA
direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), in relation to the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

[SOURCE: ISO/IEC 19790:2012, 3.114]

3.19
software
executable code of a cryptographic module that is stored on erasable media which can be dynamically written and modified during execution while operating in a modifiable operational environment

[SOURCE: ISO/IEC 19790:2012, 3.116]

EXAMPLE Erasable media can include but not limited to solid state memory, hard drives, etc.

3.20
tamper detection
automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module

[SOURCE: ISO/IEC 19790:2012, 3.125]

3.21
tamper evidence
observable indication that an attempt has been made to compromise the security of a cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.126]

3.22
tamper response
automatic action taken by a cryptographic module when tamper detection has occurred

[SOURCE: ISO/IEC 19790:2012, 3.127]

3.23
TEMPEST
codename by the US National Security Agency to secure electronic communications equipment from compromising emanations, which, if intercepted and analysed, may disclose the information transmitted, received, handled, or otherwise processed

3.24
timing analysis
TA
analysis of the variations of the response or execution time of an operation in a security function, which may reveal knowledge of or about a security parameter such as a cryptographic key or PIN

3.25
zeroisation
method of destruction of stored data and unprotected SSPs to prevent retrieval and reuse

[SOURCE: ISO/IEC 19790:2012, 3.134]

4 Symbols and abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 19790 or ISO/IEC 24759 apply and are duplicated here for reference.

EDC Error Detection Code

EFP Environmental Failure Protection

EFT Environmental Failure Testing

EME Electro-Magnetic Emanation

HDL Hardware Description Language

IC Integrated Circuit

PROM Programmable Read-Only Memory

RAM Random Access Memory

ROM Read-Only Memory

5 Physical security

Traditionally the term 'physical security' has been used to describe protection of material assets such as cash, jewellery, bonds, etc. from fire, water damage, theft, or similar perils. However on-going concerns in computer security have caused physical security to take on a new meaning: technologies and protocols used to safeguard information against physical attack. This information can be anything from a spreadsheet work file to cryptographic keys which are used to protect other files. This information can be stolen without being physically removed from where it is kept. If information can be accessed, it can simply be copied.

Physical security is a barrier placed around a computing system to deter unauthorized physical access. Physical access can be accomplished by either invasive or non-invasive techniques. This concept is complementary to both logical and environmental security. Logical security describes the mechanisms by which operating systems, security protocols and other software prevent unauthorized access to data. Environmental security describes the procedures that limit or prevent unauthorised physical access of a computing system by virtue of location such as guards, cameras, fences, structures, etc. Operational security depends on both the environmental security attributes that the computing system or device will operate and on the physical and logical security attributes of the computing system itself.

It may be reasonable for an individual to have access to a location (environmental security) and not to have access to the information stored on a computing system in that environment (physical and logical security). Physical security is increasingly important because advances in technology have reduced the footprint of what historically were large and complex computing systems to both smaller and mobile devices (e.g. tablet computing devices, smart phones and mobile memory tokens). These historically

complex and compute intensive systems, and their system unique applications with large data storage mechanisms, are transitioning out of environmentally secure computer rooms and into less secure offices and homes. They are being migrated on to distributed, cloud-based data platforms and mobile devices where the physical location of the data may be uncertain. If the environment of the deployed computing system provided a measured level of protection, then the level of physical protection of the computing system itself may reduce to a simple tamper detection mechanism (e.g. to detect an insider attack) or where it is not necessary at all. Whereas sensitive information held on a portable device such as a smart card, smart phone or similar device, if lost or misplaced, would require much stronger physical protection. At the same time, the value of the cryptographic critical security parameters (e.g. cryptographic keys) and similar sensitive security parameters which provide access control to data on these computing systems is increasing as centralization decreases. The motivation to attack computing systems is increasing because the rewards for doing so are increasing.

For physical security to be effective the following criteria must be met: in the event of an attack, there should be a low probability of success and a high probability of detection either during the attack, or subsequent to penetration.

Physical security systems to protect sensitive data can make unauthorised access to the data difficult, as a bank vault makes stealing cash a daunting task (tamper resistant). They can trigger mechanisms to thwart the attack, much like an alarm system (tamper detection). They can make an attempted attack apparent so that subsequent inspection will show an attack had been attempted (tamper evident).

Physical security systems can be defined as providing protection against either *invasive* or *non-invasive* attacks. Physical security *invasive attacks* are attacks that involve a physical alteration to the implementation that may also cause an operating aberration different from normal operation. Physical security *non-invasive attacks* are attacks that do not involve a physical alteration to the implementation or cause an operating aberration different from normal operation.

Classification systems have been proposed, accepted and put into use that evaluate or test computing systems according to criteria that measure the difficulty of mounting a successful attack. However many of the methods for evaluation and testing may not lead to comparable results due to the lack of defined evaluation or test methods, scope of the applied methods or the consistency and competence of the evaluators or testers. This had led to the advancement of physical security and evaluation and testing standards; these standards have become accepted as they provide a baseline of repeatable, consistent and comparable results while at the same time the standards are being rigorously and publicly evaluated. These standards led organizations and national bodies to develop evaluation and testing programs to certify or validate implementations to this baseline level of assurance.

6 Physical security invasive mechanisms

6.1 Overview

A variety of physical security techniques are currently employed to protect hardware implementations. The physical security mechanisms must address a wide range of different technology implementations, use environments and attack scenarios. This field is increasingly recognized in the commercial market as users, both business and private individuals, request such features as they have become increasingly aware of the need to protect their sensitive information. Governments have been working on this problem for decades as applied to the protection of information for both unclassified and classified domains. The amount of sensitive, but unclassified, information that governments must protect can be vast, as includes (but is not limited to) health records, tax records, law enforcement records, business records (e.g. procurements or bids), communications, transaction records, and voter information. National and International standards have been developed to address various levels of physical security assurance which in many cases coincide with the use of cryptographic protocols which require the protection of the critical security parameters (e.g. cryptographic keys, access credentials, etc.). The ways and means described here are not an exhaustive list, nor are they represented as ultimate methods.

Development is continuing in both the protection methods and the attack methods. Any evaluation or testing of appropriateness of a physical security system is time dependent and must be repeated periodically. For example ISO standards are re-evaluated at five-year intervals.

6.2 Tamper proof

Tamper proof systems are largely theoretical and unachievable as an implementation. Practical methods to analyse and test a system against all known attacks and possible emergent attacks are prohibitively costly and time consuming as there are no clear metrics to determine if the system is truly tamper proof. Such systems are only tamper proof until a successful attack is devised and accomplished.

6.3 Tamper resistant

Tamper resistant systems take the "bank vault" approach. This type of system is typified by the outer case design of an automated teller machine. Thick steel or other robust materials are utilized to slow down the attack by requiring powerful tools and great effort to breach the system. This type of system can be used in many environments and sometimes has the advantage of being so physically heavy (as in automated teller machines), that it resists theft by sheer weight. However on-going thefts of automated teller machines by thieves using towing chains and four-wheel drive vehicles indicate that ATMs relying solely on this type of protection are no longer sufficiently tamper resistant. A system that is only tamper resistant has the disadvantage that the owner may not be aware of the loss until the break-in is discovered. An attacker may be able to replace any material that had been removed or altered to remove evidence of an attack.

Tamper resistant physical security is usually the easiest to apply. Steel cases and locks are well-known technologies and are easily manufactured. Weight and bulk can be a problem or benefit, depending on the application.

Complexity or size can be another variety of tamper resistance. Single chip implementations of secure devices have a certain level of physical security due to the small size of the features and the complexity involved in determining which part of a circuit performs which function. However this has become a race between defenders and attackers as the equipment and skills needed to work with semiconductor devices at the microscopic level are becoming commonly available at universities and technology centres. As technologies and circuit densities continue to improve, current layout and placement techniques make discernment of the circuit details even more difficult.

6.4 Tamper detection

Tamper detection systems use the burglar alarm approach. The defence is the detection of the intrusion followed by a response to protect the asset. In the case of attended systems the response may consist of sounding an alarm.

Erasure or destruction of secret data are sometimes employed to prevent theft in the case of isolated systems which cannot depend on outside response. Tamper detection systems do not depend on robust construction or weight to guard an asset. Therefore, they are good for portable systems or other systems where size and bulk are a disadvantage.

6.5 Tamper evident

Tamper evident systems are designed to ensure that if a break-in occurs, evidence of the break-in is left behind. This is usually accomplished by chemical or chemical/mechanical means, such as a white paint that 'bleeds' red when cut or scratched, or tape or seals that show evidence of removal. This approach can be very sensitive to even the smallest of penetrations. Frangible (brittle, breakable) covers or seals are other methods using currently available technology.

These systems are not designed to prevent an attack or to respond to the indication that one is in progress. Their job is to ensure that the fact of a break-in will remain known and can be ascertained at

a later time. An audit policy must exist, and be adhered to, for a tamper evident system to be effective; otherwise it may not be known if, or when, the system was breached.

NOTE If no one looks for the evidence of tampering, that evidence will never be found.

6.6 Additional physical security considerations

6.6.1 Summary

Some of the properties of specific methods of physical security in the prior sub-clauses were included with the introduction of each type. Additional points are considered in the following sub-clauses. Each system must be examined to determine the correct protection mechanism.

6.6.2 Size and weight

The size and weight implications of a potential physical security design must be considered in the light of the application. Thick steel would not be a good idea for a portable system. A lightweight system would not be effective for an automated teller machine, as it would allow the system to be carried away more easily.

6.6.3 Mixed and Layered Systems

In many cases a security system can be made substantially more secure by using more than one layer and more than one kind of system.

For example, a typical safety deposit vault has steel walls, an alarm system, and a high quality vault lock. These methods might seem sufficient, but the individual safety deposit boxes have significant locks as well. The individual locks serve two purposes. They provide a second layer of general security by requiring an attacker to break into each box individually after breaking into the vault. The locks on the individual boxes also serve as an additional authorization/authentication process which requires an individual to possess the correct key to open the box.

In many cases tamper response is coupled with a tamper resistant design. If the attacker appears to be making progress in thwarting the tamper envelope, the device would respond by zeroising internal sensitive security parameters or data before the envelope is compromised.

Similarly, a layer of tamper evident security placed over a layer of tamper resistance or tamper response can prevent an attack, which might be attempted over a period of days. A regular audit may turn up indications of tampering before the system is fully breached and allow additional measures to be taken before the attack is completed.

Multiple layers of security also make the attack more difficult in general. The requirement for two different kinds of tools, skills, etc., may not make the two-layered system twice as difficult to attack, but it does increase the difficulty.

7 Physical security invasive attacks and defences

7.1 Overview

The following sub-clauses describe different methods of invasive physical attacks that may be attempted upon computing systems, as well as the defence mechanisms that can be useful in deterring or detecting such attacks. Examples will explore existing and contemplated attack mechanisms, and the corresponding defence mechanisms that are being brought into commercial use now, or are being considered for the near future.

7.2 Attacks

This section deals with mechanisms that range from the generally known types of attacks to those that used to be considered unusual. The attacks described in this section, and the defences described in the following section, may far exceed the typical levels of skills and resources available to the common attacker. However, the skill level of the common attacker is increasing and as data value increases (e.g. Internet commerce) these defensive techniques should be considered and become a standard part of common business practice. Many of these techniques are now required to meet certain government requirements (e.g. FIPS 140-2, ISO/IEC 19790, etc.). The business community is also beginning to embrace these same government requirements as a means of assurance (Payment Card Industry, Digital Cinema Initiative, et al.) and demonstrable due diligence.

7.2.1 Attack mechanisms

7.2.1.1 Internal Probe attacks

The purpose of a probe attack is to directly attach conductors to the circuit(s) so that information can be obtained from, and/or changes injected into, the system under attack.

7.2.1.2 Probing

7.2.1.2.1 Passive probes

These are common oscilloscope or logic analyser probes. They may be used to watch and record information contained in circuits. When used with a logic analyser, a trigger condition may be set such that the attacker waits for a predetermined event and then begins recording.

The term passive probe is somewhat of a misnomer in that so-called passive probes may be terminated in active circuitry, which gives them very high input impedance. This may prevent their detection by, or interference with, the circuit being attacked.

7.2.1.2.2 Active or injector probes

Active probes are generally used in conjunction with passive probes. Using a pattern generator or similar device, these probes can inject signals or information into an active system. These are common electronic development tools.

7.2.1.2.3 Pico-probes

Pico-probes (and micro-probes) can be utilized as either a passive probe or an active probe. Pico-probes are very tiny and are used to directly probe the surfaces of integrated circuits.

7.2.1.2.4 Energy probes

Energy probes can be electron beams, ion beams, or focused beams of light. Depending on the technology being attacked, energy probes can read or write the contents of semiconductor storage, or change control signals. Ion beam deposition has been used to successfully reconnect fuse links, to return product level smart cards to their debug-state where access to key storage registers, etc., was permitted.

7.2.2 Machining methods

7.2.2.1 Machining

The purpose of machining is to cut or remove material and also includes within this context drilling. A cover or potting material is machined to access circuitry beneath the potting or cover. Once the covering is removed, a probe attack, as described above, can proceed.

If the system is protected by physical security, the intent is to perform the machining operation without tripping a sensor or leaving evidence. After the covering material is removed, the sensor is then disabled or bypassed so that a probing attack may proceed.

If the system is protected by a tamper evident system, there may be an attempt to cover the evidence after the attack is complete.

The list of machining methods includes chemical and energy methods of material removal, as well as traditional machining methods.

7.2.2.2 Manual material removal

Manual material removal is commonly referred to as the 'brain surgery' attack. In this scenario an attacker using a knife, or other tool, attempts to remove material from a potted or sealed container while stopping short of tripping a sensor. This attack is much more effective than might be thought. If the attacker is dexterous and has good hand-eye coordination, extremely delicate work can be accomplished.

7.2.2.3 Mechanical machining

This method removes much material, very precisely, in the shortest time. Its disadvantages lie in the fact that there is little or no feedback. This frequently causes cuts that are too deep. If the cutter is conductive, it may be detected by the tamper detector. However with the use of a capacitance detection device, the depth to the buried sensor can sometimes be determined very accurately.

7.2.2.4 Water machining

Water machining is a very precise method for material removal. The 'cutter' can be nonconductive (if the water is pure), does not dull, and is very effective for all but very soft materials. Its chief disadvantage is that water machining equipment is typically very large.

However, in situations where cost and size are a concern, but time is not, a directed slow, steady, drip of water will effectively cut through many materials given sufficient time.

7.2.2.5 Laser machining

This technique has many of the same advantages as water. One disadvantage of laser machining is that the process may generate a great deal of heat. The laser must be tuned for the material of interest, e.g. EXCIMER (Ultra Violet) lasers are excellent for ablating organic materials (such as epoxy).

7.2.2.6 Chemical machining

Almost any material can be dissolved. Jet Etch and similar commercial tools are very good for removing coatings and potting material cleanly. These techniques work by using a high-pressure, very precise spray of a solvent or acid to dissolve away the material.

The solvent or acid may be heated to increase effectiveness. The main disadvantage is the potentially high conductivity of highly ionic cutting liquids, which may cause short circuits.

7.2.2.7 Sandblasting

A sandblasting system can be used very effectively for removing small amounts a material in a very controlled manner. If the sand/air ratio is decreased, such that very little sand is used, a micron level depth of cut can be achieved.

NOTE The term 'sand' is used loosely, many materials from sand, to glass micro beads to silicon carbide granules can all be used as the abrasive.

7.2.3 Shaped charge technology

Shaped charge technology has become so commonly available that precision welding and cutting sample kits are available promote the technology.

These techniques have the advantages of being very accurate and being extremely fast. The penetration speed can approach 25,000 ft/sec. with pinpoint accuracy at a distance of several inches. At these hypersonic speeds, a package can be penetrated and circuits disabled before they can respond. For example, a memory zeroing circuit can be disabled before the energy can be removed from the memory. This could give the attacker from a few seconds to a minute to finish entering a package and to reapply power to the memory before its contents decay.

7.2.4 Energy attacks

7.2.4.1 Energy mechanisms

These attacks are both of the contact and non-contact variety. However even the non-contact attacks usually require close access to the system.

7.2.4.2 Radiation imprinting

By irradiating CMOS RAM in the X-Ray band (and possibly other bands), the contents can be 'burned in' such that power down or over-write will fail to erase the contents.

The basic imprinting attack uses radiation to imprint the CMOS RAM used to store cryptographic keys or other secret data, and then the unit can be physically breached without regard for power down or rewrite mechanisms. The RAM may then be read at leisure.

7.2.4.3 Temperature imprinting

CMOS RAM will retain its contents with the power removed for seconds to hours when the temperature of the RAM is lowered. This effect starts at just below freezing. The lower the temperature, the longer the memory contents will typically remain. Over-writing will erase the contents.

7.2.4.4 High Voltage Imprinting

High Voltage Imprinting by 'spiking' CMOS RAM with short duration, high-voltage pulses, it may be possible to imprint the contents in a manner similar to radiation imprinting.

7.2.4.5 High or low voltage

By changing Vcc to abnormally high or low values, erratic behaviour may be induced in many circuits. The erratic behaviour may include the processor misinterpreting instructions, erase or over-write circuitry failing, or memory retaining data when not desired.

7.2.4.6 Clock glitching

By lengthening or shortening the clock pulses to a clocked circuit such as a microprocessor, its operation can be subverted. Instructions or tests can be skipped or generally erratic operation can be induced. This is a well-known attack and has been used on simple devices like smart cards very effectively.

7.2.4.7 Circuit disruption

Strong electromagnetic interference may cause disruption in noise-diode type random number generators and computing circuits. Intense RF fields are easily created using microwave ovens.

7.2.4.8 Electron beam read/write

The electron beam of a conventional scanning electron microscope can be used to read, and possibly write, individual bits in an EPROM, EEPROM, or RAM. To do this the surface of the chip must be exposed first, usually via chemical machining. This is a very powerful attack once the chip is exposed since buried, normally non-readable, keys and secrets can possibly be stolen and/or modified.

7.2.4.9 IR LASER read/write

Silicon is transparent at IR frequencies. Because of this, it is possible to read and write storage cells in a computing device by using an IR LASER directed through the bulk silicon side of the chip. By going through the bulk side there is no need to jet etch or otherwise remove the device's passivation.

7.2.4.10 Imaging technologies

Any of the current imaging technologies including X-Ray, tomography, ultrasound, etc. can all be used to visualize the contents of a sealed or potted package. This can assist the attacker by pinpointing areas of vulnerability, identifying printed circuit card layout, showing part placement, and possibly identifying specific parts. This also includes visual examination through constructed ventilation openings such as vents or fans.

7.2.5 Environmental conditions

7.2.5.1 Environmental operation

Electrical devices and circuitry are designed to operate within a particular range of environmental conditions. Operation outside the specified normal operating ranges can cause unpredictable operation or failure of device. Methods employed to protect a device or provide tamper evidence can be susceptible to varying environmental conditions.

7.2.5.2 Voltage and temperature device failure

Varying the operational voltage or temperature outside the normal operating ranges at both the low and high end limits, can be used to force the device to transition into an unpredictable state. Operating the device in this unpredictable state can compromise the security of the device.

7.2.5.3 Temperature augmentation

Varying the operational temperature can be used to compromise other protection mechanisms such as potting materials or adhesives used in tamper evident seals. High temperatures can cause potting materials or adhesives to become soft or pliable if not cured properly or designed to maintain hardness or adhesive strength. Low temperatures can cause potting materials or adhesives to become brittle. Varying the environmental temperature combined with other methods such as machining can result in a successful attack.

7.3 Defences

7.3.1 Overview

The detection methods below fall into three categories: preventing intrusion, detecting intrusion, detection of non-invasive energy attacks (cold, radiation, etc.). After detection, there are various methods of response. Each method must be examined when choosing the design point. For example, a design that calls for a low temperature sensor must take into account the temperatures which the unit could be exposed to while in transport.

7.3.2 Tamper resistant

7.3.2.1 Overview

These types of systems resist attacks either by the selection of materials that are hard to penetrate, or by the materials thickness. Another approach is to attach the device to the tamper barrier so firmly that the attempt to separate the layers, or to penetrate the protection, results in the destruction of the protected device.

7.3.2.2 Hard enclosures

An enclosure that is constructed of a hard material deters machining, probing, energy or chemical attacks. Examples of enclosure constructed of steel or other hard metal or ceramic materials. This may include technologies such as reinforced carbon fibre composites or reinforced aramid fibres.

7.3.2.3 Conformal coatings

Conformal coatings are materials that may be applied in layers or in various thicknesses that adhere directly to the electronic components or printed circuit boards. Typically they are applied to protect the components or printed circuit boards from moisture, fungus, dust, corrosion, abrasion and other environmental stresses. To deter physical attacks or determining design implementation details, a hard opaque conformal coating is applied that deters machining, probing, energy or chemical attacks in addition to design implementation details. They can be applied by dipping, spraying, or simple flow coating methods. These include various epoxies or epoxies doped with material that provides enhanced abrasiveness or hardness.

7.3.2.4 Single chip coatings

This technique is used to prevent attack on the single chip level (e.g. pico-probing). The surface of the chip may not be probed with the coating in place and these coatings are applied so that removal will damage the chip beyond reclamation.

7.3.2.5 Insulator based substrates

To prevent an attacker from compromising a protective coating by using an IR LASER technique, the bulk silicon must be replaced with a material that is not transparent at useful frequencies. Silicon/Metal Oxide (SiMOX), Silicon-on-Sapphire (SOS), or other silicon-on-insulator technologies, combined with advanced passivation represent the highest level of passive, single chip, protection. One must still carefully evaluate the possibility of using surface grinding techniques to thin the substrate to the point of transparency.

7.3.2.6 Special semiconductor topographies

To prevent scanning electron microscope or pico-probing attacks, even in the presence of chemical machining or other techniques that can remove coatings, a chip can be designed so as not to expose critical structures without removing active layers of the device. This technique has become common for performance reasons as well as security. Simulated annealing as a placement method has become common along with other similar techniques that render the layout of the device virtually random from a gross organizational viewpoint.

7.3.2.7 Opacity

Opacity is the degree to which light is not allowed to travel through a material. To deter visual examination of the construction of a device, the enclosure or conformal coating should be of a material that is opaque.

7.3.3 Tamper evident

7.3.3.1 Overview

Tamper evident systems are not designed to prevent attack or entry into the protected area. They are designed such that entry will leave evidence to be discovered during physical audit.

7.3.3.2 Brittle packages

The device is sealed in a package that is made of ceramic, glass, or another frangible material. If an attempt is made to enter the package, it cracks or shatters, leaving evidence.

7.3.3.3 Crazed aluminium

The package is made from aluminium or other similar material, which has been heated (usually above 1000 °F or 500 °C) and quenched. This heat treating causes a myriad of shallow, web-like cracks to appear on the surface. These cracks, like a fingerprint, are unique to each piece. The case can be photographed and subsequently audited using the photograph and optical comparison devices.

7.3.3.4 Stressed glass

Metal, or metal oxide, lines can be printed on glass, in a manner similar to a printed circuit board sensor. Contacts to the glass can be made using elastomeric 'Zebra' connectors. Stressed glass can be obtained that is virtually impenetrable without the glass breaking. This method is very good for large flat surfaces, or possibly, for secure doors.

7.3.3.5 Polished packages

Similar to crazed aluminium the package is inspected for changes in surface appearance. In this case any mark at all represents an attempted breach.

7.3.3.6 Bleeding paint

Paint of one colour is mixed with micro-balloons containing paint of a contrasting colour. If the surface is marred, the other colour 'bleeds' onto the surface. The surface quality is the auditable characteristic.

7.3.3.7 Holographic and other tamper detection tapes and labels

The surface of tape, with a very firm adhesive, is printed with a holographic image similar to the kind used on credit cards. This kind of tape is moderately difficult to forge, and it is constructed so that attempts to remove it will damage it (the tape may be scored to promote tearing when removal is attempted). This is good for checking to see if doors or covers have been illicitly opened.

There is also a wide assortment of tamper detection labels available from many different companies. Some are designed with multiple adhesives such that removing the label will cause patterns or words (such a 'VOID', or 'TAMPERED') to appear in the label. Some are designed, as mentioned above, to easily tear when removed.

In any case, the most difficult task in choosing a tamper evidence label is to match the adhesive to the material that the label is placed on. With orange oil based solvents available (in additional to all of the familiar solvents that are more toxic and less effective in many cases), it is difficult to choose a label that is not removable and replaceable without detection.

7.3.3.8 One-time strain gauges

A strain gauge is a device used to measure the strain of an object. The most common type of strain gauge consists of an insulating flexible backing which supports a metallic foil pattern. The gauge is attached

to the enclosure by a suitable adhesive and if the enclosure is deformed, the foil is deformed, causing its electrical resistance to change which can be measured.

7.3.3.9 One-time photosensitive materials

A material that is sensitive to various wavelengths of light. If a device is constructed to operate in an area of a known light exposure different from what it may be exposed to while attacked, this can be recorded or alter the appearance of the material.

7.3.3.10 Gas analysis

7.3.3.10.1 Overview

The gas composition that is injected within an enclosure can be monitored or later measured if the enclosure were compromised during an attack.

7.3.3.10.2 One-time pressure gauge

The interior of an enclosure can be manufactured with an under- or over-pressure atmosphere which can be measured if compromised (i.e. loss of pressure or loss of vacuum).

7.3.3.10.3 One-time composition change

The interior of an enclosure can be manufactured with a unique gaseous composition (i.e. filled with an inert gas) which can be measured if compromised (i.e. introduction of oxygen). The measure can be by a material that will change colour or structure when the composition changes.

7.3.3.11 Dosage sensors

These sensors store the total radiation dose over time. Total dose is the best indicator of imprinting in CMOS SRAM. Unfortunately, at this time there are no available dosage sensors which are small, low cost, low power, and directly readable.

7.3.3.12 RFID polling

An RFID tag is embedded within the enclosure or device which can be polled to determine if the physical location has changed or the device is replaced with an unknown but seemingly similar device.

7.3.3.13 Painting of recognizable patterns

The application or painting to the case or chassis screws of metallic coatings or paints with visible, recognizable patterns (e.g. swirls of metal particles). The surface quality is the auditable characteristic if the paint is marred in a manner that the patterns are blemished or unrecognizable.

7.3.4 Tamper detection sensor technology

7.3.4.1 Overview

Tamper detection sensor technology covers a wide variety of types, like the tamper evident devices above. Each type of tamper detection sensor is designed to detect a particular type of attack or intrusion and trigger a response in real time.

7.3.4.2 Voltage sensors

Voltage sensors are useful in almost any design that requires proper power delivery for correct operation. Both high and low voltage can be a deliberate or accidental attack. To guarantee correct operation of circuits all power supplies should be monitored. Any excursion outside of nominal operating range

should be considered an attack, and response should be engaged. References for monitors should be independent of power supply variations.

7.3.4.3 Probe sensors

Probe sensors form a large family of active tamper barriers. Individual designs may feature tamper resistance or evidence, as well as tamper detection for additional security. Some designs are more or less costly, or heavy, or manufacturable, than others.

When applied to tamper sensing barriers or detector membranes, this technique is becoming very difficult from a load detection perspective. It is nearly impossible to detect the electrical load that a modern FET probe places on the circuit that it is measuring. Therefore electrical probe detectors must be sensitive enough and/or have features small enough that they are difficult to manipulate. This is required to detect probes that are very small, or have almost undetectable electrical loading.

Whether the probe is passing through air via a vent, an opening in the case or through an active tamper sensing barrier or membrane; mechanisms that detect the physical passage of the probe are much more likely to be successful. These may be optical (scanning for an obstruction), mechanical (detecting force applied), electrical (breaking a conductor, capacitive, inductive) or ultrasonic/microwave detractors (such as used in security alarms to detect presence of moving objects).

At lower levels of security, passive barriers such as baffles placed in ventilation paths, that require one or more significant path changes, may be sufficient to deter an attack. Lips or dead ends may be employed along with the baffles to prevent using a flexible probe to 'slide around the corners'.

7.3.4.4 Wire Sensors

Thin wire wrapped around the package to be protected and then potted forms the intrusion sensor. Ideally the wire should have a high resistance so the wire can be used as a distributed resistance, so small changes can be detected as well as opens and shorts. If the wire is folded back over itself, or wound as multiple parallel strands, the sensitivity is increased because two adjacent wires may be electrically distant. So shorting two wires gives a larger signal than would two adjacent strands on a continuous wrap. The insulation on the wire should be as similar to the potting material as possible in both appearance and chemistry. This makes machining more difficult because no hints as to the whereabouts of the wire are given. Chemical attacks are made more difficult because of the difficulty of dissolving the potting without dissolving the insulation and causing shorts. It is also an advantage if the wire is made from a material which is difficult to attach to.

7.3.4.5 Printed circuit board sensors

A sensor similar to the wire sensor above can be made for a much lower cost by printing the wiring onto a printed circuit board. However, the regular spacing of the lines and the usual copper conducting material give somewhat less security. This is due to the ease with which the conductors may be isolated, owing to the regularity of a rigid printed circuit board. Once a conductor is located, it is very easy to attach another wire to it for the purpose of giving the tamper detection circuitry false information. However, with good potting material and small lines, this design gives moderate security.

7.3.4.6 Flexible printed circuit sensors

This design incorporates the best features of the previous two. The flexible surface helps break up the regularity of the surface planes. The lines can be made of silk-screened conductive paste, which allows high resistance. It is even better to use lines made from a conductively doped version of the same material used for final potting. The realm of package shapes is wider because the package can be ``gift wrapped' with the material, then potted. Also, the narrow screened lines will be much more difficult to find without breaking. Multiple layers can be used for additional security.

7.3.4.7 Stressed glass with piezo-electric sensor

Using the same glass as in the previous example, this sensor uses a piezo-electric element to signal the breakage of the glass. The force of stressed glass breaking is enough to induce a large signal from a piezoelectric device attached to the inside of the glass.

7.3.4.8 Piezo-electric sheet

Plastic piezo-electric sheets can be used as probe barriers. If an area protected by a piezoelectric sheet is probed or punctured, an electric charge is generated proportional to the force applied. This charge can be measured and used to activate tamper response circuitry. There are problems with this application because of sensitivity to pressure and vibration, both making the design too sensitive to environmental conditions, and potentially insensitive to slow puncture attacks.

7.3.4.9 Bulk multiple scattering

This sensor uses the scattering properties of coherent light through bulk materials to create a very sensitive probe sensor based on measuring the optical speckle pattern.

7.3.4.10 Motion sensors

These sensors are typically used to sense motion in an area or box. They often need to be used in pairs because each type can sometimes cause a false positive or can miss under unusual conditions. An infrared sensor can trip falsely when the first rays of the sun fall on the protected package through a window.

7.3.4.11 Ultrasonic sensors

Ultrasonic sensors average a picture of the protected space via ultra-sonic projection and reflection. They can be very effective at detecting intrusion into a space, but can have false positives due to air currents, external vibrations, etc. Even in small spaces, such as the interior of a package or secure PC case, heat can cause sufficient air movement to be detectable. Ventilation fans can also trigger ultrasonic sensors.

For both attack and defence purposes, ultrasound-based imaging techniques can be used to visualize internal structures or the composition of an object. Ultrasound images are made by sending a pulse of ultrasound into the object using an ultrasound transducer (probe). The sound reflects and echoes off parts of the object; this echo is recorded and displayed as an image to the operator. The attack uses the information to visualize the interior of the secure area to formulate an attack, the defence attempts to 'see' the probe as it enters the protected space so that a response may be made.

An ultrasonic sensor can detect attempts to discern the topology of protected areas via external ultrasound probing, while monitoring the area for physical intrusion at the same time.

7.3.4.12 Microwave

Microwave sensors are similar in performance to ultrasonic sensors, with many of the same strengths and weaknesses, but operate at a higher frequency. The material of the walls of the protected area has to be taken into account with this type of system since some non-metallic materials can be transparent at these frequencies. This can cause false positives due to activity outside of the protected region.

7.3.4.13 Infrared

This sensor is not typically sensitive to air currents or the like, but these systems have been known to trip due to light (and heat) changes due to sunrise through windows when the averaging is too sensitive. They are most useful for detecting warm bodies, people, animals, etc. A tool at ambient temperature will probably not be noticed unless it was moved to suddenly block an infrared radiating source that the sensor already 'sees.'

7.3.4.14 Acceleration sensors

These sensors are used to detect movement or vibration. Their primary uses are to prevent theft, and to detect drilling or hammering.

7.3.4.15 Solid state

This sensor detects a beam of light reflected by mirrors that are attached to flexible mounts, or a piezo-electric device and a small mass. They are quite sensitive and reliable.

7.3.4.16 Micro-switches

Micro-switch motion sensors use mercury or pendulums to detect motion. They are lower in cost than solid state devices, but are less sensitive, and are more prone to failures. However, a liquid mercury switch can be reliable and virtually without wear.

7.3.4.17 Radiation sensors

Radiation sensors are used to detect attempts at radiation imprinting. These sensors are most important for remotely located systems which could be taken into a laboratory and attacked.

7.3.4.18 Flux sensors

Flux sensors sense the real-time radiation intensity. The advantage of this type of circuit is that it can be very low cost. The disadvantage is that this sensor has no cumulative memory (total dose measurement).

If the data are invariant over a long period of time, low levels of radiation (below the sense point) can imprint the data. Given the power and cost budget for typical physical security systems, integrating the flux reading is too costly. So a compromise must be struck as to flux level trip point vs. minimum time to imprinting.

Phototransistors can be very effective radiation flux sensors. The circuit is the same as is used for light measurement; however a higher gain is typically required. The typical problems with this circuit are that the sensitivity in the radiation band of interest is usually not specified by the manufacturer and must be determined by testing, and that the sensors tend to degrade with time and exposure to radiation.

One method that can make phototransistor flux sensors more sensitive is to use a chemical down converter, such as the fluorescent material used in X-Ray enhancement screens. This material glows in the visible band when struck by higher energy flux. If the chem-optical output can be matched to the sensitivity spectrum of the phototransistor a great sensitivity enhancement can be obtained.

7.3.4.19 Temperature sensors

Temperature sensors are well-known and readily available at all cost performance points.

7.3.5 Tamper responding

7.3.5.1 Overview

The methods of tamper response technology discussed here are means of removing data from memory circuits or devices which contain sensitive information. Currently, the most common method of storing such information is in RAM, DRAM, FLASH, hard drives or other volatile or non-volatile read/write mechanism because the retention is reliable and the erasure is reasonably so.

7.3.5.2 RAM power drop

This is the most straightforward method of data erasure. If aided by a crowbar circuit that supplies a very low impedance path from Vcc to ground, it is reliable if imprinting protection (temperature sensing and

radiation sensing) has been employed. Since there is a tendency for RAM contents to imprint over time, any information that is to be stored in RAM for long periods should be regularly scrambled, inverted, or otherwise changed to prevent imprinting.

7.3.5.3 Memory overwrite

This method has had the widest acceptance in government specifications; however in a catastrophic condition it is difficult to guarantee that reliable power will be available to operate the over-write circuit. The common method is to over-write some number of times with all 0s, then all 1's. In an attempt to counter more advanced data recovery techniques, specific overwrite patterns and multiple passes have often been prescribed. These may be generic patterns intended to eradicate any trace signatures, for example, the seven-pass pattern: 0xF6, 0x00, 0xFF, random, 0x00, 0xFF, random. However it has not been shown that this multiple overwrite increases the effectiveness. It would also take even longer to complete the overwrite since the random data would have to be generated.

7.3.5.4 Degaussing

Degaussing is the removal or reduction of a magnetic field of a disk or drive, using a device called a degausser that has been designed for the media being erased. Applied to magnetic media, degaussing may purge an entire media element quickly and effectively.

Degaussing often renders hard disks inoperable, as it erases low-level formatting that is only done at the factory during manufacturing. It is possible, however, to return the drive to a functional state by having it serviced at the manufacturer.

7.3.5.5 Physical destruction

7.3.5.5.1 Overview

This is the only method of data erasure that is completely reliable.

7.3.5.5.2 Chemical reaction

One method of destruction that can be accomplished with a minimum of overt violence and would barely be detectable at the surface of a metal hybrid package is the use of thermite. Nonetheless, this method is typically reserved for the most sensitive circumstances. Thermite is the typical destruction agent of choice, since once the 'irreversible chemical reaction' has started, it is virtually impossible to stop, and anything in contact is incinerated.

7.3.5.5.3 Grinding and Shredding

These methods physically grind or shred the physical components into scrap material. These include hard drive shredders which can also shred small electronic devices such as cell phones, smartphones, PDA's, etc., micro-shredding of electronic components.

7.3.5.5.4 Incineration

Incineration is the physical destruction of the electronic components utilizing high temperatures which will liquefy or vaporize the material. For magnetic media, raising its temperature above the Curie point (at which a ferromagnetic or a ferrimagnetic material becomes paramagnetic) resulting in the destruction of the magnetization.

8 Physical security non-invasive mechanisms

8.1 Overview

This is a field that is increasingly recognized as requiring attention due for example to the proliferation of sophisticated portable devices that contain sensitive information that may be easily lost or misplaced. For example smart cards may be used for payment schemes and include banking and transaction information, user health records, military service information and access credentials. Smart phones and the proliferation of easily downloadable applications are available to encompass and manage almost all aspects of a user's electronic activities. Therefore standards are being developed, both national and international, to address various levels of physical security non-invasive assurance. The ways and means described here are not an exhaustive list, nor are they represented as ultimate methods.

8.2 Mixed and Layered Systems

In many cases a security system can be made substantially more secure by using more than one layer and more than one kind of system. A portable device should be designed for protection against both physically invasive and non-invasive attacks. The attacker will focus on that aspect of the design that yields the most promise for success.

9 Physical security non-invasive attacks and defences

9.1 Overview

Physical security *non-invasive* attacks attempt to compromise a computing system by acquiring knowledge of the module's protected information without physically modifying, invading the device or causing an operating aberration different from normal operation. The following sub-clauses describe different methods of non-invasive physical attacks that may be attempted upon computing systems, as well as the defence mechanisms that can be useful in deterring or detecting such attacks.

9.2 Attacks

9.2.1 Overview

This section deals with methods to obtain sensitive security information either by gathering information while coupled to the devices power interface or via electromagnetic emanations. In either case the device is unaware that information is being gathered to be analysed to acquire internal sensitive security parameters. The attacks described in this section, and the defences described in the following section, may far exceed the typical levels of skills and resources available to the common attacker. However, the skill level of the common attacker is increasing, and as data value increases (e.g. Internet commerce), these defensive techniques should be considered and become a standard part of common business practice.

9.2.2 External Probe attacks

9.2.2.1 Correlation power analysis

An extended variant of the basic differential power analysis, which uses a more precise power model such as the hamming weight or hamming distance model, detecting the highest correlation between measured power consumption and calculated power based on the model with each guessed key.

9.2.2.2 Differential power analysis

An analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques on a large number of measured power consumption values for the purpose of extracting the keys used in a cryptographic algorithm. Power

models are generated based on assumptions about the targeted key and tested against measurements. The highest correlation reveals the key.

9.2.2.3 Simple power analysis

A direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.

9.2.3 External EME attacks

9.2.3.1 Differential electro-magnetic analysis

An analysis of the electro-magnetic emanation or the variations of the proximity magnetic field due to the electrical activity on a cryptographic module, using the same statistical techniques on the measured data and for the same purpose as those for differential power analysis.

9.2.3.2 Simple electro-magnetic analysis

An analysis of the electro-magnetic emanation or the variations of the proximity magnetic field due to the electrical activity on a cryptographic module, using the same inspection techniques on the measured data and for the same purpose as those for simple power analysis.

This is a passive attack. Electromagnetic emanations from a computer, or other electronic device, can be detected at a distance and decoded to determine contents or behaviour. The distance can be many hundreds to a thousand feet or more. Power supply current profiles can also be measured to determine circuit activity. Most information on TEMPEST was government classified in the interests of national security. However some of the material has become declassified and is now available on the Internet. It is well known, and has been demonstrated, that a video display or serial communication line can be tapped at distances of hundreds of feet. Recently more aspects of TEMPEST technology have been independently invented/discovered in the commercial sector. Smart cards have been successfully attacked by means of studying their power supply current and RF emanations, and others have developed new approaches to using this method.

9.2.4 Timing analysis

An analysis of the variations of the response or execution time of a matching function or an operation in a cryptographic algorithm, which may reveal knowledge of or about a critical security parameter such as a PIN or cryptographic key.

9.3 Defences

Recently there has been published literature that describes various methods to design or construct a device, process data or execute algorithms (e.g. cryptographic) that deter non-invasive attack techniques in the form of power analysis or side channel attacks. Attention to the how conditional branches are determined, power consumption variations in multipliers, algorithmic modifications such that the cryptographic operations occur on data that is related to the actual value by some mathematical relationship that survives the cryptographic operation, EME shielding, or approaches that involve blinding parameters to randomize their value. Other examples include:

— Dual rail hardware implementation

— Masking techniques

— Randomization of the operations

— Constant delay implementation

10 Operating Envelope Concept

One of the main problems encountered while implementing physically secure systems is the prevention of the class of attacks that cause erratic operation. This can occur when the operating point is pushed to the boundaries of the operating range. For example, running the circuit at either marginally high or low supply voltages may cause erratic operation of the circuit such that secret information could be leaked. If one considers the possibility of adjusting both temperature and voltage, the problem can become even more complex.

Manufacturers define the operating range of the components that they make, but often the specification is incomplete. It can be incomplete because no one ever intended the part to be used in some particular way, and the manufacturer, justifiably, doesn't want to deal with the problem. In general, designers can design circuits that stay within prescribed limits and the circuit functions properly. For example, if the circuit is run at too high a temperature while at too low a supply voltage, the condition is undefined. This may open the system to attack.

It is the physical security designer's responsibility to determine the safe operating envelope of the circuit under all conditions, and to provide safeguards to detect conditions outside of the acceptable operating envelope. If these conditions are detected the response circuitry must protect the secret data. This is the basic idea behind the environmental failure protection requirement in ISO/IEC 19790. If conditions leave the safe operating envelope in a non-catastrophic manner (e.g. Vcc drop during power down), the system should be stopped (or held reset). If system's conditions exit the safe operating envelope in a catastrophic manner (e.g. ambient temperature exceeding safe operating range), the critical data should be erased and the system should be prevented from operating.

Secure designs should also employ good engineering practice to prevent improper clock signals from reaching sensitive circuits by use of phased lock loops (PLLs), or similar techniques. Power analysis attacks should be prevented by designing in adequate power filtering to reduce information leakage.

11 Development, delivery and operation considerations

11.1 Introduction

Physical security mechanisms are intended to prevent a successful attack by employing tamper resistance, tamper response or tamper detection. As implementations and technologies employed become more sophisticated, the attacker continues to learn and conceive of new approaches and have greater access to sophisticated tools and method. The internet provides a forum for the collaborative exchange of ideas and sharing of information and insights but also access to many vendors or forums to procure tools (e.g. online auctions), share methods (e.g. social networking) and research the design of implementations (e.g. user guides, maintenance manuals, repair schematics, etc.).

As attackers employ and leverage these available mechanisms, the following development, delivery and operation topics are addressed to mitigate their success.

11.2 Development

11.2.1 Functional test and debug

During module development, testing and manufacturing, mechanisms (e.g. test probe access points, logic or array built-in self-test pins, firmware break points,etc.) may be incorporated to aid in diagnostics. Before a module is released from manufacturing, these mechanisms need to be removed, inhibited or the construction of the module designed such that they are not available to an attacker. If not, the attacker could use these mechanisms to exploit and circumvent any physical protection mechanisms.

11.2.2 Security testing

Test modules are expensive and thus there may be reluctance to perform adequate destructive testing to verify the security characteristics employed. An attacker can often purchase or acquire the same

modules and is free to try many different attack approaches to see which route offers the best chances of compromise through trial and error. Once the attack method is optimised, the attacker is able to successfully attack an operational device (found or stolen) that contains actual sensitive information (e.g. a smart card). Manufacturer testing may appear to be expensive to validate the security mechanisms of a module. However, once a module is deployed, a single successful attack may result in the recall or cessation of use of all delivered modules or a catastrophic financial impact or lost of product or manufacturer reputation.

11.2.3 Environmental testing

A particular epoxy may be used to seal a module and is carefully tested at nominal ambient temperature for hardness. However in actual use, a module may be deployed or shipped at temperatures that are significantly different then the tested ambient temperature. For example, a security token (e.g. USB memory device) may be left on the dashboard of the car on a hot summer day. The significant temperature difference may cause the epoxy to soften such that the epoxy no longer provides the intended security protection. A module should be tested, and the tested ranges documented, so that the user can determine if the module's security mechanisms will work properly at the environmental conditions the user expects it to be deployed with sensitive information. Testing should be done in regard to temperature, humidity, vibration, etc. during both operational use and during expected shipping and storage.

11.2.4 Factory installed keys or security parameters

A module may be designed that utilizes factory installed cryptographic keys or security parameters (e.g. seed values, initialisation values, etc.). These keys or security parameters may control the secure access to the device or to control physical security mechanisms. The protection and secrecy of factory installed keys or security parameters are critical once the module is shipped to the end user. However it is also critical to protect and maintain the secrecy during the internal manufacturing processes. If an attacker can gain access to these values due to poor manufacturing security controls and procedures, then knowledge of these keys or security parameters could be used to comprise deployed or operational devices. The manufacturer may have internal processes and mechanisms in place, but must ensure that they are rigidly controlled and enforced during the manufacturing and delivery process. This may require periodic auditing, employee screening, or access controlled secure areas when this information may be vulnerable.

11.3 Delivery

11.3.1 Documentation

Development of a module includes the detailed generation and publishing of documentation to support manufacturing, customer support, field repair, maintenance or customer setup and operation. The documentation may provide design specifications, schematics, internal drawings or illustrations and information on the physical security mechanisms. Typically this documentation may be included with the shipped product or available from the manufacturer's website for viewing or downloading. An attacker will also have access to these details of the design and operation that could assist in the method or approach to an attack. For example if a module is designed to be opaque to deter visual inspection, yet repair or maintenance documents provided for download include explicit internal drawings or illustrations, this intended design characteristic is of no deterrence. The location of tamper switches, the identification of a repair or replacement part, will give the attacker a wealth of information to examine. The manufacturer should take particular care in the development of such supporting documentation and its publishing or access to prevent the inadvertent compromise of the physical security mechanisms employed. This includes the coordination of the document developers and a final comprehensive review of the total set of documentation before published and released. The document team developing the repair or maintenance procedure documents may be unaware that these details compromise the design intentions that the module security developers developed.

11.3.2 Packaging

During the delivery or shipment of a module, consideration of how the module is packaged may be considered to ensure that the module is not examined, modified, or compromised during delivery. The modules design or manufacture may be that it requires the intended operator or recipient of the module to perform the final assembly and security set up. During shipment, when the module is unassembled, it could be compromised in a manner that the intended operator or recipient may not be aware of. Mechanisms should be employed in the packaging of the module or its sub-assemblies to prevent such access or compromise. This may include shipment in sealed strong containers with tamper evident seals or detection mechanisms. For particularly sensitive parts, trusted couriers, customer pickup, or secure shipping protocols may be employed.

11.3.3 Delivery verification

When a delivery is received by the operator or intended recipient, instructions or processes should be employed to verify that the delivery method was not compromised. For example if a software module, the publishing of the expected hash or digital signature which represents the manufactured image could be used to verify that the software was not altered either intentionally or accidentally during delivery.

11.4 Operation

11.4.1 Overview

During the operation of a module, mechanisms that provide module status, error reporting or diagnostic information may be used to collect information about the functionality of a module that may expose security weaknesses. This type of information can be collectively viewed as module feedback. Feedback can be considered in two forms: feedback that an implementation may provide during an attack, or feedback to the attacker community in regard to design and construction information.

11.4.2 Implementation feedback

An attacker may exercise the modules services in a manner that would reveal not only unique design characteristics but reveal internal sensitive information. These types of attacks are addressed in Clause 9.

11.4.3 Feedback during attack

A module may immediately indicate when an attack has been detected even to the extent of displaying a message “tampering detected”. This immediate feedback may allow the attacker to tell what methods are undetected and what are being detected helping the attached in finding a weakness. A module may be designed that does not report such information immediately and only report such information to an authenticated operator.

12 Physical security evaluation and testing

12.1 Overview

Developers should approach security testing with robustness commensurate with the intended customers use. Customers should procure devices that, at a minimum, are tested and validated to standards by recognized validation authorities with the appropriate security assurance level.

Classification systems have been proposed, accepted and put into use that evaluate or test computing systems according to criteria that measure the difficulty of mounting a successful attack. However many of the methods for evaluation and testing did not lead to comparable results due to the lack of defined evaluation or test methods, scope of the applied methods or the consistency and competence of the evaluators or testers. This had led to the advancement of physical security and evaluation and testing standards; these standards have become accepted as they provide a baseline of repeatable, consistent

