GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

CCS L 80

GM/T 0084-2020

Guideline for the Mitigation of Physical Attacks against Cryptographic Modules

密码模块物理攻击缓解技术指南

Issued on: December 28, 2020 **Implemented on: July 1, 2021**

Issued by: State Cryptography Administration

Table of Contents

Guideline for the Mitigation of Physical Attacks against Cryptographic Modules

1 Scope

This Standard specifies the physical security mechanism of cryptographic modules, physical attack methods, mitigation techniques used to prevent or detect these attacks, as well as mitigation measures at different stages of the life cycle, such as: development, distribution and operation, etc.

This Standard is applicable to the guidance for the implementation of physical attack mitigation techniques in cryptographic modules and the verification of the tested cryptographic modules to achieve the most essential security assurance.

2 Normative References

The content of the following documents constitutes indispensable clauses of this document through normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 25069 Information Security Technology - Glossary

GB/T 37092 Information Security Technology - Security Requirements for Cryptographic Modules

3 Terms and Definitions

What is defined in GB/T 37092, and the following terms and definitions are applicable to this document.

3.1 Data Imprinting Attack

Data imprinting attack refers means to take measures (such as: radiation and high temperature, etc.) to solidify the data in the memory circuit or the equipment containing sensitive information, so that the data cannot be written-in or modified for a certain time.

3.2 Physical Attacks

Physical attacks refer to attacks that cause physical modification or abnormal operation restricts or prevents unauthorized physical access to computing systems by virtue of facilities, such as: guards, cameras, fences and buildings, etc.

The effectiveness of physical security satisfies the following conditions: when an attack is encountered, during the beginning of the attack or the subsequent penetration and destruction, the probability of the attack's success shall be extremely low, and the probability of detecting the attack shall be extremely high.

Physical security mechanism refers to the defensive measure used to protect sensitive data when encountering unauthorized physical access. It includes the utmost difficult to make unauthorized physical access to data (tamper resistance), the possession of a trigger mechanism used to prevent attacks (tamper detection) and the capability of saving traces of an attack attempt and finding previous attack attempts (tamper with traces) in the subsequent detections, etc.

For the cryptographic modules, physical attack refers to an attack that causes physical modification or abnormal operation of the cryptographic modules and performs unauthorized physical access to the cryptographic modules. The mitigation of physical attack refers to the defensive measure used to hinder or mitigate the physical attack.

The cryptographic modules not only have physical security threats when in use, but also may be subject to physical attacks at different stages of the life cycle, such as: development, distribution and operation. Thus, the cryptographic modules shall have the capability of mitigating physical attacks during the development and distribution stages.

6 Physical Security Mechanism

6.1 Overview

The physical security mechanism shall be applicable to different technical implementations, application environments and attack scenarios. Commonly seen physical security mechanisms include physical security mechanisms listed in 6.2 ~ 6.7 and physical security factors that may affect system security.

6.2 Tamper-proofing

Tamper-proofing refers to a physical security mechanism that can resist all known attacks and possible sudden attacks.

6.3 Tamper Resistance

Tamper resistance refers to the capability of providing protective measures to prevent physical security attacks and unauthorized physical access to data. For cryptographic modules that only have tamper resistance, only when tampering occurs does the owner of the cryptographic modules become aware of the occurrence of the tampering.

6.4 Tamper Detection

Tamper detection refers to the cryptographic modules' automatic determination of the behavior that attempts to destroy the physical security. After the cryptographic modules detect the intrusion behavior, they shall immediately and automatically respond.

6.5 Tamper Response

Tamper response refers to the action automatically taken by the cryptographic modules when the behavior that attempts to destroy the physical security of the cryptographic modules is detected. For cryptographic modules that rely on external responses, the operation of alarm may be adopted. For cryptographic modules that cannot rely on external responses, the operation of erasing or destroying secret data may be adopted.

6.6 Tamper with Traces

Tamper with traces can ensure that after the tempering occurs, the evidence left by the tampering will be retained by the cryptographic modules. This mechanism is achieved by chemistry or a combination of chemistry and mechanics. There shall be a long-term effective audit strategy in the cryptographic modules.

6.7 Physical Security Factors

6.7.1 Volume and weight

When realizing the physical security mechanism, the influence of volume and weight shall be considered in combination with the practical application, so as to increase the difficulty of attack.

6.7.2 Mechanism of mixing and layering

Multiple layers and multiple types of physical security mechanism may be adopted to increase the difficulty of attack. Commonly seen hybrid mechanisms include (but are not limited to) the combination of tamper response and tamper resistance, and the deployment of the mechanism of tamper with traces at the periphery of the tamper resistance or tamper response mechanism.

---Combination of tamper response and tamper resistance. If the attacker enhances the techniques and can destroy the cryptographic modules with tamper resistance, the cryptographic modules shall be able to respond and reset the internal sensitive security parameters or data to zero before being destroyed.

---The deployment of the mechanism of tamper with traces at the periphery of the tamper resistance or tamper response mechanism can prevent attack attempts within a certain time. Periodic regular audits may find traces of tampering before the cryptographic modules are completely destroyed and allow other mitigation

7.3 Processing Technique

7.3.1 Overview

Processing technique refers to the removal of the outer packaging, detachable cover or encapsulating material by cutting and drilling the outer packaging, encapsulation or detachable cover of the cryptographic modules to access the circuit under the outer packaging, encapsulation or detachable cover. After the above-mentioned material is removed, probe attack will be possible.

If the cryptographic modules are protected by a physical security mechanism, the attacker shall be able to perform processing operations on the premise of not touching the sensor or leaving any evidence. After the encapsulating material is removed, the attacker shall be able to disable or bypass the sensor and carry out a probe attack.

If the cryptographic modules are protected by the system of tamper with traces, the attacker shall be able to overwrite the evidence after completing the attack.

7.3.2 Manual material removal

Manual material removal refers to the removal of material from encapsulated or airtight containers by using tools like a knife and without triggering the sensor.

7.3.3 Mechanical processing

Mechanical processing refers to a method of material removal that can be completed in a short time using mechanical equipment.

7.3.4 Waterjet processing

Waterjet processing refers to a method of material removal using high-pressure waterjet.

7.3.5 Laser processing

Laser processing refers to a method of material removal using laser. In accordance with the characteristics of the material, the wavelength and intensity of the laser should be adjusted.

7.3.6 Chemical processing

Chemical processing refers to a method of completely removing the coating and encapsulating material through chemical reaction by spraying corrosive solvents.

7.3.7 Sandblasting

Sandblasting refers to a method of accurately removing a small amount of material through high-speed jetting of abrasives, which can achieve micron-level cutting. “Sand” refers to various abrasives ranging from sand to silicon carbide.

7.4 Energy-converged Cutting Technique

Energy-converged cutting technique refers to a material removal technique that accurately penetrates the external packaging at a high speed, causing the circuit to fail before triggering any response. After the external packaging is unwrapped through the energy-converged cutting technique, the attacker shall restore power to the memory before the contents stored in the memory completely disappear.

7.5 Power Attack Technique

7.5.1 Overview

Power attack technique means to destroy the normal working state of the internal circuit of the cryptographic modules through the mode of applying a strong energy field to the cryptographic modules, so as to obtain sensitive information in the cryptographic modules.

7.5.2 Radiation data imprinting attack

Radiation data imprinting attack refers to the use of radioactive materials to radiate the X-ray band (and possibly other bands) to CMOS RAM that stores the key or other secret data, and physically destroy the RAM unit without considering the power failure or overwriting mechanism, so that the contents in the RAM unit are “solidified”. The RAM unit can be read when it is idle.

7.5.3 Temperature data imprinting attack

Temperature data imprinting attack refers to the use of a relatively low temperature (below 0 °C) to imprint data on CMOS RAM, so that the RAM retains its contents within a few seconds to a few hours after power failure. The lower the temperature is, the longer the contents in the RAM will be retained. The operation of overwriting will erase these contents.

7.5.4 High voltage data imprinting attack

High voltage data imprinting attack refers to the injection of a short-time high-voltage pulse signal into CMOS RAM to imprint the contents in the RAM in a mode similar to the radiation data imprinting attack.

7.5.5 Abnormal high and low voltage

Abnormal high and low voltage refers to the induction of abnormal behaviors in the circuit by changing VCC to an abnormally high or low value. The abnormal behaviors include (but are not limited to) processor misinterpretation of instructions, failure of erasing or overwriting circuits, and retention of unnecessary data in the memory, etc.

and forcing the equipment to enter an unpredictable state. Operating the equipment under an unpredictable state may undermine the security of the equipment.

7.6.3 Equipment external encapsulation failure attack

Equipment external encapsulation failure attack refers to the adjustment of the operating temperature that can destroy certain protection mechanisms, for example, tampering with the encapsulating materials or adhesives of the seals.

8 Physical Attack Mitigation Techniques

8.1 Overview

This Chapter specifies the attack mitigation techniques involved in physical security. The attack mitigation techniques are divided into four types: tamper resistance technique, technique of tamper with traces, tamper detection technique and tamper response technique. Each type of mitigation technique contains multiple mitigation methods, and with the continuous improvement of technology, new mitigation methods will be generated. This document only specifies the commonly seen mitigation methods.

The tamper resistance technique can prevent processing and energy-converged cutting attacks, and other attacks that take processing and energy-converged cutting as the pre-step.

The technique of tamper with traces cannot prevent the attack or entry into the protected area, instead, it leaves evidence of the attack or entry operation for further detection.

The tamper detection technique utilizes sensors that detect a certain type of physical signal or physical quantity to automatically detect and determine the behavior of attempting to use the corresponding physical signal or physical quantity to undermine the physical security of the cryptographic modules. For example, the voltage sensor detects the power supply voltage of the circuit of the cryptographic modules.

The tamper response technique refers to the operations automatically taken by the cryptographic modules when a physical attack behavior is detected, making it difficult for the physical attack to achieve the purpose of stealing sensitive security parameters and avoiding further attacks.

The mitigation techniques specified in this Chapter may make it difficult for one or more physical attacks to achieve the intended purpose of attack. Whether each mitigation technique can successfully resist specific physical attacks is closely related to the physical characteristics of the cryptographic modules, the strength of specific physical attacks and the selection of technical parameters and indicators of mitigation, etc. Specific analysis of specific scenarios is necessary. This document does not quantitatively measure the feasibility and effectiveness of the mitigation techniques.

8.2 Tamper Resistance Technique

8.2.1 Overview

The tamper resistance technique is often implemented through two modes. One mode is to resist the attack by choosing materials that are difficult to penetrate or increasing the thickness of the materials, which can prevent processing, probe detection, power or chemical attack. The other mode is to firmly attach the equipment to the tamper-resistant barrier, so that the attempt of either separating the equipment from the tamper-resistant barrier or directly penetrating the barrier will cause damage to the equipment being protected.

8.2.2 Hard shell

Hard shell refers to the use of a shell made of hard materials that can prevent processing, probe detection, power or chemical attack.

8.2.3 Conformal coating

Conformal coating refers to conformal coating of various thicknesses that can be directly attached to electrical components or printed circuit boards. The conformal coating can protect the printed circuit boards or components from moisture, fungus, dust, corrosion, abrasion and other damages triggered by environmental stresses. Hard and opaque conformal coating should be used to prevent processing, probe detection, power or chemical attack, and prevent access to actual implementation details.

8.2.4 Insulating substrate

Insulating substrate refers to the use of materials that cannot be penetrated by infrared lasers to replace silicon materials in the paint.

8.2.5 Special semiconductor topology

Special semiconductor topology refers to the disturbance of the layout of the chip to prevent the key structure of the chip from being exposed.

8.2.6 Opaque

Opaque refers to the use of opaque shells or conformal coatings to prevent visual inspection of the structure of the equipment.

8.3 Technique of Tamper with Traces

8.3.1 Overview

checking the change of resistance value of the stress deformation tester inside the shell.

8.3.8 Disposable photosensitive material

Disposable photosensitive material refers to an instrument used to measure an object that has been irradiated by light waves of different wavelengths. The tester shall be placed in an appropriate position of the cryptographic modules. If the wavelength of the irradiated light changes, the photosensitive material in the tester also undergoes irreversible changes in appearance. The illumination variation of the operating environment shall be detected by recording the changes in the appearance of the photosensitive materials.

8.3.9 Gas analysis

Gas analysis means that when the shell is damaged by an attack, the damage of the shell can be detected by monitoring the change of the composition of gas injected into the shell. Common gas analysis includes one-time gas pressure test and one-time composition change test. One-time gas pressure test detects the damage of the shell (the air pressure drops or is no longer vacuum) by checking the change of the air pressure inside the shell. One-time composition change test detects the damage of the shell by checking the change of the gas composition inside the shell.

8.3.10 Dose sensor

Dose sensor means to detect the radiation data imprinting attack by checking the change of the total radiation dose in the dose sensor.

8.3.11 RFID polling

RFID polling means to detect whether the physical location of the cryptographic modules has changed or been replaced by polling the RFID tags embedded in the equipment or the shell.

8.4 Tamper Detection Technique

8.4.1 Voltage sensor

Voltage sensor means that in order to ensure normal operation of the circuit, the power supply of the circuit shall be detected. Any operation beyond the scope of normal operation shall be considered as an attack and shall be responded to. The voltage monitor shall not be affected by power supply changes.

8.4.2 Probe sensor

Probe sensor refers to the detection of active physical attacks by a set of sensors. The probe sensor shall be sufficiently sensitive and / or small.

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading…): https://www.chinesestandard.net/AboutUs.aspx

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: https://www.linkedin.com/in/waynezhengwenrui/

------ The End ------