Initial Issue Date：2015/3/31

Revised Date：2018/2/2 *1

ECSEC.TRA

Guidance

Introduction

This document is the guidance for the data base (the DB, hereafter) which handles data for threats/vulnerabilities of HW (hardware) security, security objectives and public papers concerned with those technical areas. The development of the guidance was accomplished based on the business plan, which was the cyber security economy infrastructure construction project (vulnerability analysis techniques for hardware) of Ministry of Economy, Trade and Industry, 2014 and was undertaken by Electronic Commerce Security Technology Research Association.

1. Target audience of the guidance

It is intended that the target audience of the guidance and the DB is the groups shown below:

- Users of embedded devices
- Developers of embedded devices
- Developers of parts for embedded devices
- Developers of semiconductor chips
- Persons concerned with security evaluation and certification
- Persons concerned with information security research

2. The definition of information processing functionalities covered by the guidance

The guidance defines the information processing functionalities in information security as follows.

- HW (System LSIs put in embedded devices or parts of embedded devices) and SW (OS + applications) installed in the HW
- They do not rely on any versatile OSs
- Some security functionalities such as cryptographic operational functions depend on the HW (e.g. HW cryptographic libraries are implemented)

3. The scope of attacks

In the document, the attacks concerned with information security are defined as follows.

- The attacks involving HW parts of information processing functionalities defined in the second chapter. That is to say, the attacks limited to SW parts are excluded.

- The attacks are limited to direct accessing for objects. That is, SW attacks via logical interfaces (likely from remote) are excluded.

4. The attack patterns

In the document, the attack patterns concerned with information security are defined as follows.

4.1 Physical Attacks
4.2 Overcoming sensors and filters
4.3 Perturbation Attacks
4.4 Retrieving keys with DFA
4.5 Side-channel Attacks — Non-invasive retrieving of secret data
4.6 Exploitation of Test features
4.7 Attacks on RNG
4.8 Ill-formed Java Card applications
4.9 Software Attacks
4.10 Applet isolation
4.12 Physical Uniclonable Function*1
4.13 Machine Learning*1
4.15 Hardware Trojan*1

The above are quoted from <CC Supporting document/Mandatory Technical Document "Application of Attack Potential to Smartcards" May 2013 Version 2.9 CCDB-2013-05-002 >.

Note that most attack patterns of 4.8 – 4.10 are out of the scope of attacks provided in the third chapter.

In the DB, if a type of attack described in a paper comes under a pattern sorted above, the paper will be categorized with the attack pattern numbers. (An attack pattern number is shown by numerical figures after a decimal point of the section numbers above; e.g. "4.10" → "10")

The DB provides the feature retrieving papers relevant to each attack pattern.

If a paper corresponds to a specific attack pattern, the DB will also provide explanation of the attack pattern and examples of well-known countermeasures for the attack in the detail information column for the respective paper. However, the DB does not necessary provide definite countermeasures for the attacks described in respective papers.

English part of the description in the DB above was quoted from CCDB-2013-05-002, Mandatory Technical Document, Application of Attack Potential to Smartcards, except well-known countermeasures.

Although Japanese part of the description above was quoted from the translated version of CCDB-2013-05-002 by IPA, the underlined part was translated based on discussions by this association. Further, the CC supporting document did not include "well-known

countermeasures". They were described originally by this association.

*1 In FY 2017, three types of attack types were added.This is because new attack types that can not be classified into 1 to 10 are added in this paper addition.

5. Classification of papers

In the DB, every paper is classified with the class number below.

- Attacks for HW, vulnerabilities of HW, countermeasures by HW … class number 1
- References for above items, such as cryptographic algorithms … class number 2
- The rest … class number 3

The DB provides the feature to retrieve the papers based on the classification.

6. Quotation frequency

The DB provides the quotation frequency numbers of respective papers until the present time. Generally, it is well accepted that the papers quoted much tend to include important information for security or be fundamental ones for particular areas. However, it should be noted that the papers such as being stated very before or quoted very much are easy to be abused by attackers.

Also, the DB provides the function to extract the papers quoted more than fifty or hundred times.

7. Implementation environments for information processing functionalities

The information processing functionalities defined in the second chapter will be implemented by embedded devices in various environments. The implementation environments are categorized as shown in Table 1.

Table 1 Implementation environments

Implementation environments	Environment I	Environment II	Environment III	Environment IV
Definition	The target device is circulating in the market and availab	The target device is portable and not protected from	The target device is portable and resistant to external	The target device is fixed physically and protected by

	le without a limit.	carrying-away attacks.	physical attacks.	secure environment.
Examples	• Smartcard • Mobile phone/ smart phone • Memory card (e.g. SIM) • USB memory	• Auto mobile • Financial terminal • Robot • Medical device • Security device	• Some financial terminals • The device equipped with counter measures such as deleting internal information for external attacks.	The device fixed in the strict secure zone which is protected by guards.

The strength of countermeasures for attacks is relied on the implementation environments above. Typically, the countermeasures required to the information processing part are mitigated so that the protection by the environment is sufficient. For example, the attacks “direct accessing for objects” shown in the third chapter are unlikely in the environment IV above. The level of vulnerability analysis required in security assurance also tends to be relevant to the matters above.

8. Information assets

Examples of information assets to be protected by the information processing functionalities defined at the second chapter and the categorization of those assets are shown in Table 2.

Table 2 Categorization of assets

	Assets I	Assets II	Assets III	Assets IV
Definition	Concerning with human life	Affecting serious influence on life of a personal/	Affecting limited influence on life of a personal/	Affecting minor influence on life of a personal/ family

		family	family	
	Threatening national existence	Affecting influence on continuation of activities of a public institution	Damaging large amount of economic value	Damaging limited amount of economic value
	Affecting serious influence on civic life	Threatening subsistence of a corporation	Affecting a continued activity of a corporation	Damaging limited amount of economic activities of a corporation
Examples of systems	• Important infrastructure (energy, financial, communication, etc.) • Governmental information system	• Information system of a public agency • Information system of a corporation • Smart house	• A part of a information system of a corporation • A electronic money system • A small personal information management system	• A point system • A game system

Examples of devices	• Traffic devices (automobile, airplane, etc.) • Medical devices • Some robots • Weapons • Important guard devices	• Smart meter • Some robots • Supplemental guard devices • Information appliances • Control equipments • Station service apparatus	• Smartcard for public services • Credit/debit card • Financial devices such as ATM • Store terminals • Feature phones Smart phones Tablet devices	• Prepaid electronic money cards • Attending/leaving management devices • Some store terminals
Examples of parts	Parts such as M2M modules should follow the highest level of the assets of the device in which they are embedded.			

Strength of the countermeasures to counter an attack is relied on the information assets above. Typically, the strength of the countermeasures that an information processing unit possesses is required much so that the value of the asset becomes high.

The level of vulnerability analysis in security assurance is relevant to the problem above.

9. The relationship between attack patterns and implementation environment

The relationship between the attack patterns shown in the fourth chapter and the implementation environments shown in the seventh chapter is shown in Table 3.

Table 3 The relationship between the attack patterns and the implementation environments

Implementation environments	Environment I	Environment II	Environment III	Environment IV
Definition	The target device is circulating in	The target device is portable and	The target device is portable and	The target device is fixed physic

	the marke t and availa ble witho ut a limit.	not protec ted from carryi ng-aw ay attacks.	resista nt to extern al physic al attacks.	ally and protec ted by secure enviro nment.
1. Physical Attacks	⊙	○	□	□
2. Overcoming sensors and filters	⊙	○	□	□
3. Perturbation Attacks	⊙	○	□	□
4. Retrieving keys with DFA	⊙	○	□	□
5. Side-channel Attacks - Non-invasive retrieving of secret data	⊙	○	□	□
6. Exploitation of Test features	⊙	○	□	□
7. Attacks on RNG	⊙	○	□	□
8. Ill-formed Java Card applications	⊙	○	○	□
9. Software Attacks	⊙	○	○	□
10. Applet isolation	⊙	○	○	□
12. Physical Unclonable Function	⊙	○	○	□
13. Machine Learning	⊙	○	○	□
15.Hardware Trojan	⊙	○	○	□

⊙: strong ○: medium □: low □: none

10. Security assurance

The guidance does not require nor recommend developers nor users specific countermeasures to counter the threats provided by the papers included in the DB. Instead, it is recommended to utilize the scheme for information security evaluation and certification based on ISO/IEC 15408 (Common Criteria). The scheme provides means to assure that an IT product has been designed and implemented to offer appropriate security features, at the time of the evaluation.

Every participating country of CCRA (CCRA is the international arrangement) is operating respective own schemes. The attacks defined in the second chapter are not common evaluation and certification items for all CCRA participants. They are being evaluated and certified by the CC evaluation and certification schemes in Japan and Europe SOGIS (the certificate authorizing countries are France, Germany, Italy, Netherlands, Norway, Spain, Sweden and United Kingdom).

The schemes above are continuously updating the criteria of vulnerability assessment, which is applied to determine whether an IT product is implemented with necessary security features or not at the time of evaluation. Updates are shared among the schemes. As updating is done continuously, the criteria of vulnerability assessment is changing with time. If two certificates were issued on different date, even they provided the same security assurance level, each evaluation might had been done based on the different criteria of vulnerability assessment.

The guidance recommends the security assurance level for hardware CC evaluation as follows. Especially, the seventh chapter “Implementation environments for information processing functionalities” and the eighth chapter “Information assets” should be considered.

For the readers of the guidance, the following procedure is recommended: (i) defines the implementation environment for the target product and the information assets to be protected, (ii) extracts the recommended security assurance levels from Table II and III below and (iii) selects the highest security assurance level among them. The readers should also recognize that the selected level above should be treated as an aim.

Note. Each security assurance level in Table II and III bellow is not indicated with CC security assurance level (EAL: Evaluation Assurance Level) but with components of AVA_VAN, which is a family of vulnerability assessment class. It is used because the CC evaluation part, which relates information of attacks, countermeasures and vulnerabilities stored in the DB, is exactly vulnerability assessment of the target product.

Table I [Examples of embedded devices * Value of information assets]

	Assets I	Assets II	Assets III	Assets IV
Definition	Concerning with human	Affecting serious	Affecting limited	Affecting minor influenc

	Life	influence on life of a personal/ family	influence on life of a personal/ family	e on life of a personal/ family
	Threatening national existence	Affecting influence on continuation of activities of a public institution	Damaging large amount of economic value	Damaging limited amount of economic value
	Affecting serious influence on civic life	Threatening subsistence of a corporation	Affecting a continued activity of a corporation	Damaging limited amount of economic activity of a corporation
Examples of systems	• Important infrastructure (energy, financial, communication, etc.) • Governmental information system	• Information system of a public agency • Information system of a corporation • Smart house	• A part of a information system of a corporation • Electronic money system • Small personal information management system	• Point system • Game system

Examples of devices	- Traffic device (automobile, airplane, etc.) - Medical device - Some robots - Weapons - Important guard device	- Smart meter - Some robots - Supplemental guard device - Information appliance - Control equipment - Station service apparatus	- Smartcard for public services - Credit/debit card - Financial device such as ATM - Store terminal - Feature phone Smart phone Tablet device	- Prepaid electronic money card - Attending/leaving management device - Some store terminals
Examples of parts	Parts such as M2M modules should follow the highest level of the assets of the devices in which they are embedded.			

Table II [Value of information assets * security assurance]

Value of information assets	Asset I	Asset II	Asset III	Asset IV
Security assurance	It is recommended to apply an appropriate evaluation and certification scheme by third parties for information security area based on CC and the like.			
Recommended level of vulnerability assessment	AVA_VAN.5	AVA_VAN.5	AVA_VAN.4	AVA_VAN.3

Table III [Implementation environments * security assurance]

Implementation	Environment I	Environment II	Environment III	Environment IV

environments				
Definition	The target device is circulating in the market and is available without a limit.	The target device is portable and not protected from carrying-away attacks.	The target device is portable and resistant to external physical attacks.	The target device is fixed physically and protected by secure environment.
Examples	• Smartcard • Mobile phone/ smart phone • Memory card (e.g. SIM) • USB memory	• Auto mobile • Financial terminal • Robot • Medical device • Security device	• Some financial terminals • The device equipped with counter measures such as deleting internal information for external attacks.	The device fixed in the strict secure zone which is protected by guards.
Security assurance	It is recommended to apply an appropriate evaluation and certification scheme by third parties for information security area based on CC and the like.		Assurance for environment based on ISMS and the like	
Recommended level of vulnerability assessment	AVA_VAN.5	AVA_VAN.5	AVA_VAN.4	—
Note	Either the high level of vulnerability assessment for the information			

	asset or the implementation environment should be selected.

[How to use the tables above]

(1) Specify the information assets and the implementation environment of the target product.

(2) Select the highest recommended level of vulnerability assessment for the information assets or the implementation environments, specified in Table II and Table III respectively.