A Study on Smart Card Security Evaluation Criteria for Side Channel Attacks

HoonJae Lee[1], ManKi Ahn[2], SeonGan Lim[3], and SangJae Moon[4]

[1] Dongseo University, Busan, 617-716, Korea
hjlee@dongseo.ac.kr
[2] Defense Quality Assurance Agency, Daegu, 706-020, Korea
mkahn@dqaa.go.kr
[3] Korea Information Security Agency, Seoul, 138-160, Korea
seongan@kisa.or.kr
[4] Mobile Network Security Technology Research Center,
Kyungpook National University, Daegu, 702-701, Korea
sjmoon@knu.ac.kr, http://msrc.knu.ac.kr

Abstract. In the course of making electronic services and facilities more widely accessible and usable, more and more IT systems are incorporating smart cards as a component. We analyzes the side channel attacks for the smart card and similar security evaluation criteria for smart card protection profiles based on the common criterion. Futhermore, we proposes the smart card security evaluation criteria for side channel attacks about vulnerability assessment activities in Security Assurance Requirements. It can be useful to evaluate a cryptosystem related with information security technology and in addition, it can be applied to building smart card protection profiles.

Keywords: Common Criteria, Protection Profiles, Vulnerability Assessment Activities, Side Channel Attacks, SPA/DPA, Smart Card.

1 Introduction

A smartcard, based on the idea of embedding an integrated circuit chip within a ubiquitous plastic card, can execute cryptographic operations and provide high reliability and security. Much attention has been paid to the security issues of cryptosystems implemented in tamper-proof devices [1]. Recently, however, this had been a target of the side channel attacks.

This paper[1] analyzes the side channel attacks for smart card devices, and proposes the smart card security evaluation criteria for side channel attacks about vulnerability assessment activities in Security Assurance Requirements. We considers if the side channel attacks are not a covert channel. Accordingly,

[1] This research was supported by Dongseo Frontier Project 2002 and University IT Research Center Project.

we would separate part of side channel analysis from AVA_CCA and AVA_VLA under a discussion on CC public reviewed documents [2–4]. It will be discussed in detail in section 4. Our proposals can be useful to evaluate a cryptosystem related with information security technology and in addition, it can be applied to building smart card protection profiles.

The remainder of this paper is organized as follows: Section 2 overviews Common Criteria and Protection Profiles, while section 3, We experiments on power analysis attacks. Section 4 introduces the propose of smart card security evaluation criteria for side channel attacks. Conclusion is presented in section 5.

2 Preliminaries

2.1 Common Criteria & Protection Profile overview

The Common Criteria (CC)[5] is the set of internationally and nationally recognized technical standards and configurations that allow for security evaluations of Information Technology *IT* products and technology. The CC prescribe a variety of assurance activities, such as design analysis, vulnerability analysis, penetration testing, and examination of development environment.

The evaluation of the IC in the CC Part 3 comprises Security Target, Development, Tests, Guidance, Configuration Management, Life-cycle support, Delivery and operation, and Vulnerability assessment.

Protection Profiles provide a detailed level of security requirements and standards pertinent to a specific technology or security risk area based on the overall CC framework or specific to the evaluated IT product or technology. The increase in the number and complexity of applications in the smart card market is reflected in the increase of the level of data security required.

2.2 Vulnerability assessment (Class AVA)

The assurance class AVA defines requirements directed at the identification of exploitable vulnerabilities. Specifically, the class addresses the existence of exploitable covert channels, the possibility of misuse or incorrect configuration of the TOE.

1. Covert channel analysis (AVA_CCA)
This is directed towards the discovery and analysis of unintended communications channels that can be exploited to violate the intended TSP.

2. Misuse (AVA_MSU)
The objective is to determine whether misleading, unreasonable and conflicting guidance is absent from the guidance, whether secure procedures for all modes of operation have been addressed, and whether use of the guidance will facilitate detection of insecure TOE states.

3. Strength of TOE security functions (AVA_SOF)
The objective is to determine whether Strength of Function (SOF) claims are made in the ST and whether the developer's SOF claims are supported by an analysis that is correct (i.e whether such functions meet or exceed the claim).

4. Vulnerability analysis (AVA_VLA)
Vulnerability analysis consists of the identification of flaws potentially introduced in the different refinement steps of the development. It results in the definition of penetration tests through the collection of the necessary information concerning: the completeness of the TSF and the dependencies between all security functions.

2.3 TOE specific attacks

Side channel analysis is a form of attack against secure tokens by which secret data is pulled out without damaging the device itself. We analyzes a threat and the side channel attacks in relation to such attacks in reference to Common Criteria, SCSUG-SCPP [6], EUROSMARTPP [7–9], FIPS 140-2 [10], FIPS 140-2 DTR [11], NESSIE [12] and CRYPTREC [13]. There included power analysis attacks [14], timing analysis attacks [15], electromagnetic analysis [17], fault attacks [16] and TEMPEST attacks [1]. Among them, the power analysis is more powerful than others. The summarized threats in relation to side channel analysis are shown in Table 1.

Table 1. The threat in relation to side channel attacks .

Threats	Statements
Threats associated with physical attack on the TOE(Target of Evaluation)	
T.P_Probe (Physical Probing of the IC)	An attacker may perform physical probing of the TOE to reveal design information and operation contents
T.P_Alter (Physical Alteration of the IC)	An attacker may perform physical alteration of the TOE in order to reveal operational contents or design information, or to change TSR data or the TOE security functions so that the TOE can be used fraudulently
Threats associated with logical attack on the TOE	
T.Flt_Ins (Insertion of Faults)	An attacker may determine user and TSF information through observation of the results of repetitive insertion of selected data
Threats which monitor information	
T.I_Leak (Information Leakage)	An attacker may exploit TSF data which is leaked from the TOE during normal usage. power analysis is an example of exploitation of information leakage.
T_Link (Linkage of Multiple Observations)	An attacker may observe multiple uses of resources or services and by linking the, these observation, deduce information that may reveal TSF data
Miscellaneous Threats	
T.Env_Str (Environmental Stress)	An attacker may induce errors in the TSF data through exposure of the TOE to environmental stress

3 Experiments of power analysis attacks

The power consumption of a device, such as the smart card, is measured for a single execution of a cryptographic operation, and can be used to identify which operations are performed in what order. In public key cryptosystems, it is possible to distinguish multiplication from square, due to the difference of the differential operation of algorithm. Based on this information, the secret key can be recovered. Attackers are assumed to have various levels of expertise, resources, and motivation. Relevant expertise may be in general semiconductor technology, software engineering, hacking techniques, or in the specific TOE. It is assumed that given sufficient time and expertise, any smart card can be compromised.

3.1 Sample hardware configuration

The hardware configuration in figure 1. demonstrates the typical DPA analysis configuration. In this configuration, a standard PC communicates with Oscilloscope and smart card reader via a standard RS-232 port. the smart card also sets the trigger for the digital oscilloscope connected to the PC. Setting or identifying the trigger allows the digital oscilloscope to take numerous samples in the area of the algorithm that is of most interest. Without the trigger, millions of samples that are irrelevant to the analysis might be collected and could complicate the data acquisition and further examination. With very small measurement samples, DPA computation is performed considerably faster.

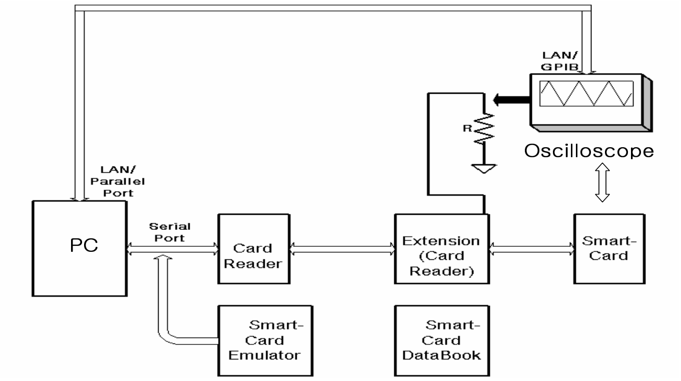
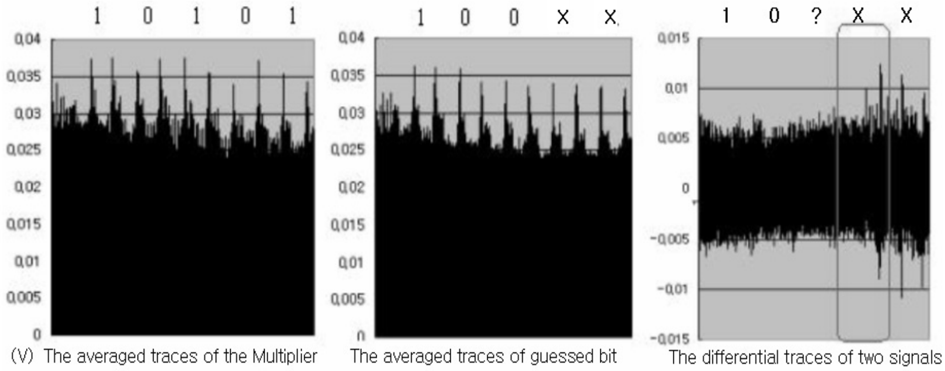


Fig. 1. Simplified DPA configuration.

3.2 The MESD-DPA attacks

Now, we will carry out the MESD attacks [18] using data transition of SPA resistant exponentiation algorithm in the smart card. It is assumed that the target of attack is on the third digit {1} from the correct secret digits {1,0,1,0,...}.

Two hundred traces were analyzed at the target bit position when a device was executed by a multiplier. Since the step of multiplication and square make a difference in the power consumption, when the attacker guessed wrongly, the averaged power peaks occur at the bit period right after the wrongly guessed bit. The experimental results are shown in figure 2. When X means "don't care", the left and the middle of the results are the averaged traces of the correct one {1,0,1,0,...} and the guessed representation {1,0,0,X,...}. The right of results are the difference of those. As the below results, the MESD attack is successful.



(V) The averaged traces of the Multiplier The averaged traces of guessed bit The differential traces of two signals

Fig. 2. The MESD attack of proposed scalar multiplication with averaging over 200 traces .

4 The propose of the smart card security evaluation criteria for Side Channel Attacks

4.1 The propose of side channel analysis family(AVA_SCA)

According to the published PPs[19], it comments T.Covert_channel, T.Fault_generation, T.Interface_attack in the threat, but the assurance class AVA defines only covert channel analysis(AVA_CCA) in Vulnerability Assessment Family. It includes SPA/DPA, timing attack, and electromagnetic attack in vulnerabilities. However, the paper separates only differential fault analysis attack from those other parts. It have a different point of view about the side channel attacks that include not only differential fault analysis attack but also those.

Accordingly, we considers if the side channel attacks are not a covert channel [20]. we will separate the part of side channel analysis from AVA_CCA and AVA_VLA under a discussion on CC public reviewed documents [2–4]. Therefore, this paper introduces assurance family for side channel analysis (An abbreviated AVA_SCA) shown in figure 3.

Assurance family separates side channel timing analysis family(SCA.T), side channel power analysis family(SCA.P), side channel fault analysis family(SCA.F)

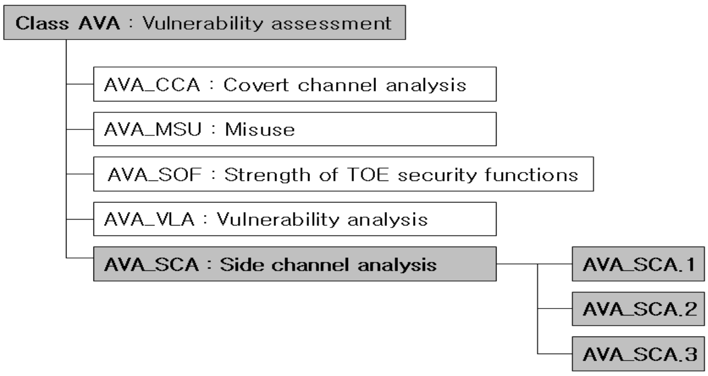

Class AVA : Vulnerability assessment
AVA_CCA : Covert channel analysis
AVA_MSU : Misuse
AVA_SOF : Strength of TOE security functions
AVA_VLA : Vulnerability analysis
AVA_SCA : Side channel analysis
AVA_SCA.1
AVA_SCA.2
AVA_SCA.3

Fig. 3. The proposed side channel analysis family(AVA_SCA).

and side channel E-magnetic analysis family(SCA.E). We analyzes and proposes three components that are grouped on the basis of related assurance as AVA_SCA.1, AVA_SCA.2 and AVA_SCA.3. The family contains three components that are linearly hierarchical (i.e. component 2 requires more than component 1, in terms of specific actions, specific evidence, or rigour of the actions or evidence).

We shortly mentions the assurance requirements for reformed security objectives, the evaluation assurance level and three assurance components in the Table 2, 3, 4.

Table 2. Assurance requirements for reformed security objectives.

Assurance Requirements		Security Objectives
Components	Statement	
ADV_IMP.1	Subset of the implementation of the TSF	O.Phy_Prot
AVA_VLA.3	Moderately resistant	O.Env_Strs, O.Phys_prot
AVA_SCA.2	Systematic side channel analysis	O.Flt_Ins, O.I_Leak

Table 3. The proposed assurance components for side channel analysis.

Assurance Class	Assurance Family	Assurance Components	An Investigation	Comparison of [21]
AVA	**AVA_SCA**	AVA_SCA.1 (Side-Channel Analysis)	An informal search for side channels.	Basic SPA/DPA
		AVA_SCA.2 (Systematic SCA)	A systematic search for side channels.	Advanced SPA/DPA
		AVA_SCA.3 (Exhaustive SCA)	An exhaustive search for side channels.	Exhaustive SPA/DPA

Table 4. The proposed evaluation assurance level in assurance family of class AVA.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ACM: Configuration Management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
:	:				:			
:	:				:			
AVA: Vulnerability Assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4
	AVA_SCA		**1**	**1**	**2**	**2**	**2**	**2**

4.2 The development of assurance component for Side Channel Attacks

Objectives

The AVA_SCA is carried out to determine the existence and potential capacity of unintended signalling channels (i.e. illicit information flows) that may be attacked during the operation of TOE. The assurance requirements address the threat that unintended and attackable signalling paths exist that may be exercised to violate the SFP.

Component levelling

The components are levelled on increasing rigour of side channel analysis.

Application notes

Channel capacity estimations are based upon informal engineering measurements, as well as actual test measurements. Examples of assumptions upon which the side channel analysis is based may include processor speed, system or network configuration, memory size, and cache size. The selective validation of the side channel analysis through testing allows the evaluator the opportunity to verify any aspect of the side channel analysis (e.g. SPA, DPA, SEMD-DPA, MESD-DPA, ZEMD-DPA, IPA, HO-DPA, TA, FA, DFA, TEMPEST). This does not impose a requirement to demonstrate the entire set of side channel analysis results. If there are no information flow control SFPs in the ST, this family of assurance requirements is no longer applicable, as this family applies only to information flow control SFPs.

1. AVA_SCA.1 Side Channel Analysis

Objectives

The objective is to identify side channels that are identifiable, through an informal search for side channels.

Developer action elements:

AVA_SCA.1.1D The developer shall conduct a search for side channels for each information flow control policy.

AVA_SCA.1.2D The developer shall provide side channel analysis documentation.

Content and presentation of evidence elements:

AVA_SCA.1.1C The analysis documentation shall identify side channels and estimate their capacity.

AVA_SCA.1.2C The analysis documentation shall describe the procedures used for determining the existence of side channels, and the information needed to carry out the side channel analysis.

AVA_SCA.1.3C The analysis documentation shall describe all assumptions made during the side channel analysis.

AVA_SCA.1.4C The analysis documentation shall describe the method used for estimating channel capacity, based on worst case scenarios.

AVA_SCA.1.5C The analysis documentation shall describe the worst case exploitation scenario for each identified side channel.

Evaluator action elements:

AVA_SCA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SCA.1.2E The evaluator shall confirm that the results of the side channel analysis show that the TOE meets its functional requirements.

AVA_SCA.1.3E The evaluator shall selectively validate the side channel analysis through testing.

2. AVA_SCA.2 Systematic Side Channel Analysis

Objectives

The objective is to identify side channels that are identifiable, through a systematic search for side channels.

Application notes

Performing a side channel analysis in a systematic way requires that the developer identify side channels in a structured and repeatable way, as opposed to identifying side channels in an ad-hoc fashion.

Developer action elements:

AVA_SCA.2.1D - AVA_SCA.2.2D There are the same contents that those in AVA_SCA.1

Content and presentation of evidence elements:

AVA_SCA.2.1C - AVA_SCA.2.5C There are the same contents that those in AVA_SCA.1

AVA_SCA.2.6C The analysis documentation shall provide evidence that the method used to identify side channels is systematic.

Evaluator action elements:

AVA_SCA.2.1E - AVA_SCA.2.3E There are the same contents that those in

AVA_SCA.1

3. AVA_SCA.3 Exhaustive Side Channel Analysis

Objectives
The objective is to identify side channels that are identifiable, through an exhaustive search for side channels.

Application notes
Performing a side channel analysis in an exhaustive way requires that additional evidence be provided that the plan that was followed for identifying side channels is sufficient to ensure that all possible ways for side channel exploration have been exercised.

Developer action elements:
AVA_SCA.3.1D - AVA_SCA.3.2D There are the same contents that those in AVA_SCA.2

Content and presentation of evidence elements:
AVA_SCA.3.1C - AVA_SCA.3.5C There are the same contents that those in AVA_SCA.2
AVA_SCA.3.6C The analysis documentation shall provide evidence that the method used to identify side channels is exhaustive.

Evaluator action elements:
AVA_SCA.3.1E - AVA_SCA.3.3E There are the same contents that those in AVA_SCA.2

5 Conclusion

We analyzed the side channel attacks for the smart card until comparatively lately and made an experiment in power analysis attacks. And then, We separated the part of side channel analysis from AVA_CCA and AVA_VLA in CC and proposed the smart card security evaluation criteria for side channel attacks about vulnerability assessment activities in Security Assurance Requirements. It was composed of side channel analysis family(AVA_SCA) and Assurance components(AVA_SCA.1, AVA_SCA.2, AVA_SCA.3). Our proposals could be useful to evaluate a cryptosystem related with information security technology.

References

1. R. Anderson and M. Kuhn, "Tamper resistance- a cautionary note," *In Proceedings of the 2nd USENIX Workshop on Electronic Commerce,* pp. 1-11, 1996.
2. CCIMB-2002-04-001-ASE(Draft v0.6) "Security Target Evaluation Common Criteria and Methodology for Public Review," available on http://www.commoncriteria.org/review_docs/
3. CCIMB-2002-07-001-AVA(Draft v0.68) "Vulnerability Analysis and Penetration Testing," available on http://www.commoncriteria.org/ review_docs/
4. CCIMB-2002-11-003-AttackPotential(Draftv0.5) "Characterisation of Attack Potential ," available on http://www.commoncriteria.org/review_docs/

5. http://www.commoncriteria.org/
6. Common Criteria for Information Technology Security Evaluation ; Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP), Version 3.0, September, 2001.
7. EUROSMART-PP/0010, Protection Profile Smart Card IC with Multi-Application Secure Platform (ver. 2.0), Nov., 2000.
8. EUROSMART-PP/9911, Protection Profile Smart Card Integrated Circuit with Embedded Software (ver. 2.0).
9. EUROSMART BSI-PP-0002, Smartcard IC Platform Protection Profile (Version 1.0), July, 2001.
10. FIPS 140-2, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
11. FIPS 140-2 DTR, http://csrc.nist.gov/cryptval/140-1/fips1402DTR.pdf.
12. NESSIE, http://www.cosic.esat.kuleuven.ac.be/nessie/
13. CRYPTREC, http://www.ipa.go.jp/security/
14. P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," *In Proceedings of Advances in Cryptology-CRYPTO '99, ,* LNCS 1666, pp. 388-397, Springer-Verlag, 1999.
15. P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, " *In Proceedings of Advances in Cryptology-CRYPTO'96,* LNCS 1109, pp. 104-113, Springer-Verlag , 1996.
16. E. Biham and A. Shamir, "Differential Fault Analysis of Secret Key Cryptosystems," *In Proceedings of Advances in Cryptology-CRYPTO'97,* LNCS 1294, pp. 513-525, Springer-Verlag, 1997.
17. J.R. Rao and P. Rohatgi., "The EM Side-Channel(s),"*In Pre-Proceedings of Workshop on Cryptographic hardware and Embedded Systems-CHES'02,* LNCS 2523, pp. 29-45, Springer-Verlag, 2002.
18. T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Power Analysis Attacks on Moular Exponentiation in Smart cards, " *In Proceedings of Workshop on Cryptographic Hardware and Embedded Systems-CHES'99,* LNCS 1717, pp. 144-157, Springer-Verlag , 1999.
19. Electronic Commerce Security Technology Research Association, "Multi-Application Secure System LSI Chip Protection Profile ," JICSAP ver 2.0 Protection Profile part 1, available on http://www.ssi.gou.fr/fr/confiance/documents/PP0301.pdf, June 6, 2003.
20. Douglas E. McGovern, "Developing Protection Profiles Getting Started ," available on http://www.acsac.org/2000/presentations/mcgovern.pdf, 16th ACSAC December 14, 2000.
21. Joint Interpretation Library, "Integrated Circuit Hardware Evaluation Methodology - Application of Attack Potential to Smartcards," at Version 1.0, March, 2002.