스마트카드 부채널공격관련 안전성 평가기준 제안

이 훈 재[†] · 이 상 곤[†] · 최 희 봉[††] · 김 춘 수[†††]

요 약

본 논문에서는 스마트카드 소자에 대한 부채널공격(side-channel attack)기법을 분석하며, 또한 부채널관련 스마트카드 안전성 평가기준을 제안한다. 부채널공격관련 스마트카드 안전성 평가기준을 설정하기 위하여 유사 암호 알고리듬, 암호 모듈, 그리고 국제공통 평가기준(CC)에 따른 스마트카드 보호 프로파일을 분석한다. 그리고 스마트카드 제품 평가시에 적용될 수 있는 보호 프로파일 수준의 부채널공격관련 안전성 평가기준을 제안한다. 제안된 평가기준은 정보보호 기술과 연관된 암호 시스템을 평가하는데 유용하며, 또한 스마트카드 보호 프로파일 개발에 적용될 수 있다.

A Study on Smartcard Security Evaluation Criteria for Side-Channel Attacks

HoonJae Lee[†] · SangGon Lee[†] · HeeBong Choi[††] · ChunSoo Kim[†††]

ABSTRACT

This paper analyzes the side channel attacks for smartcard devices, and proposes the smartcard security evaluation criteria for side-channel attacks. To setup the smartcard security evaluation criteria for side-channel attacks, we analyze similar security evaluation criteria for cryptographic algorithms, cryptographic modules, and smartcard protection profiles based on the common criterion. Futhermore, we propose the smartcard security evaluation criteria for side-channel attacks. It can be useful to evaluate a cryptosystem related with information security technology and in addition, it can be applied to building smartcard protection profile.

키워드 : 스마트카드(Smartcard), DPA, 국제공통평가기준(CC), 부채널공격(Side-channel Attack)

1. 서 론

국내에서는 최근 다양한 정보보호 시스템의 평가를 원활히 하고 수출 활성화를 촉진하기 위한 기반으로 2002년 8월 5일 정보통신부 고시 제 2002-4호 "정보보호 시스템 공통평가기준"과 정보통신부 고시 제 2002-41호 "정보보호 시스템 평가·인증지침"이 고시되었다[1]. 이 지침은 국제공통평가기준 CC(common criteria)[2]를 따른다.

한편, 부채널(side-channel)에 의한 스마트 카드 공격 기술을 일반적으로 부채널공격(side-channel attack)[3]이라고 부르며, <표 1>과 같이 시차정보에 의한 시차공격(TA, timing attack), 결함 오작동 정보에 의한 결함 주입 공격(FA, fault-insertion attack), 전자파 누출 정보에 의한 전자파 누출 공격(EA, electromagnetic emition attack), 그리고 전력선 누출 정보에 의한 전력분석 공격(PA, power analysis attack)으로 대별된다. 전력분석 공격[3]은 <표 2>와 같이 단순 전력분석(SPA, simple power analysis) 공격과 차분 전력분석(DPA, differential power analysis) 공격, 그리고 추론 전력분석(IPA, inferential power analysis) 공격으로 대별된다. 전력분석 공격은 카드 내부에 내장된 암호 알고리듬과 암호용 비밀 키가 작동되는 순간에 IC 칩의 순간적인 전압(전력) 변화를 관측하여 각종 정보의 이진 코드를 읽어낸 후 통계적인 방법으로 중요 정보 분석은 물론 위·변조까지 가능한 암호해독 기술이다. DPA 기술은 전압변화를 관측할 수 있는 몇 가지 장치를 구비하면 비밀 키의 추정이 가능하기 때문에 전용의 해독기계 또는 슈퍼 컴퓨터를 동원한 전수공격(brute-force attack) 보다 훨씬 효과적인 것으로 분석되고 있다.

본 논문에서는 신분카드, 교통카드 및 전자화폐 등 앞으로 여러 분야에서 사용될 스마트카드에서의 부채널공격관련 안전성 평가기준에 대해 연구한다. 스마트카드 부채널공격 중에서 위협적인 전력분석 공격을 적용한 실험연구 결과를 활용하여, 국제공통 평가기준(CC)의 부채널관련 안전성 평

† 정 회 원 : 동서대학교 인터넷공학부 교수
†† 종신회원 : 한국전자통신연구원 부설 국가보안기술연구소 선임연구원
††† 정 회 원 : 한국전자통신연구원 부설 국가보안기술연구소 팀장
논문접수 : 2003년 5월 6일, 심사완료 : 2003년 7월 24일

〈표 1〉 부채널공격 비교

항 목	Timing attack(TA)	Fault-insertion attack(FA)	Power analysis attack(PA)	비 고
공격 개념	스마트카드에 내장된 비밀키 값에 따른 마이크로코드상에서의 동작시간상의 차이를 비교 분석하는 공격기법	스마트카드에 내장된 비밀키 값에 따른 마이크로코드상에서의 외형적인 값(동작시간, 전력 정보 등)과 비교 값과의 차이를 외부에서 오류주입을 통하여 분석하는 공격기법	스마트카드에 내장된 비밀키 값에 기반한 마이크로코드상에서의 전력 측정값이 여러 종류의 평문(암호문) 입력변화에 따른 전력소모의 차이로 나타남을 이용하는 통계적 데이터 분석 공격기법	PA 공격 방법이 가장 강력하다고 알려짐.
전제 조건	① 암호시스템 제공 ② 마이크로코드 제공	① 암호시스템 제공 ② 마이크로코드 제공 ③ 알려진 키에 대한 기준 값 (reference) 제공	① 암호시스템 제공 ② 마이크로코드 제공 ③ 상당수의 평문 ④ 암호문쌍 제공	
분 석 파라메터	임의의 키에 따른 명령어 수행시간 차이	임의의 키에 따른 시간 또는 중간 데이터 값의 차이	임의의 키에 따른 통계적인 소모전력의 차이	
최초 제안	Paul Kocher (Cryptography Research Co., USA), CRYPTO'96	Biham & Sharmir, CRYPTO'97	Paul Kocher, Jaffe & Jun, CRYPTO'99	
유사 방법	TA	DFA(Differential Fault Attack)	1) SPA/DPA(HO-DPA)/IPA : DES-like 2) SEMD/MESD/ZEMD : RSA-like	

〈표 2〉 전력분석 공격 방법 비교 요약

항 목	SPA	DPA(HO-DPA)	IPA	비 고
공격 개념	스마트카드에서 연산되는 암호 프로세서의 전력소비를 직접 관찰하여 카드 내부에 저장되어 있는 비밀키를 직접 공격하는 방법	스마트 카드가 암호학적 연산을 실행 시에 소비되는 전력을 표본화하여 그 데이터를 수집한 다음, 표본화된 데이터를 잡음신호 감소와 차분 신호의 명확성을 위해 디지털 신호 해석과 통계적인 방법으로 분석하는 공격 기법	공격자가 필요로 하는 정도의 소비전력 신호를 가질 수 없고 평문과 암호문의 쌍을 가질 수 없다면, 암호 시스템이 암호 알고리듬을 실행할 때 몇 번째 키가 어디에서 반응하는지 그 시점을 확인한 후 키 정보를 추출하는 공격기법	DPA 공격 방법이 가장 강력하다고 알려짐.
전제 조건	① 암호 시스템 제공 ② 마이크로코드 제공	① 암호 시스템 제공 ② 마이크로코드 제공 ③ 상당수의 평문-암호문쌍 제공	① 암호 시스템 제공 ② 마이크로코드 제공 ③ 제한적인 평문-암호문쌍 제공	
분 석 파라메터	단순한 소모전력	임의의 키에 따른 통계적인 소모전력의 차이	일부의 키에 따른 반응시점 정보	
최초 제안	Paul Kocher, Jaffe & Jun, '98 homepage ; /CRYPTO'99	Paul Kocher, Jaffe & Jun, CRYPTO'99	P. Fahn and P. Pearson, CHES'99	
공격 대상	• DES like	• DES/AES • RSA/D-H • ECC	• DES-like	

가기준을 제안한다. 또한 국제공통 평가기준과 관련된 유사 평가 문서들로부터 부채널분석과 관련된 평가기준 항목을 분석한다. 즉, 암호 알고리듬 측면에서의 평가기준[4-7], 암호 모듈 측면에서의 평가기준[8, 9], 그리고 암호 시스템인 스마트카드 측면[10-13]에서의 부채널공격관련 보호 프로파일(Protection Profile)을 분석한다. 마지막으로 스마트카드 제품 평가시에 적용될 수 있는 보호 프로파일 수준의 부채널공격관련 안전성 평가기준을 제안한다.

2. 부채널관련 안전성 평가기준 분석

2.1 암호 알고리듬 평가

2.1.1 NESSIE

NESSIE에서 시행되고 있는 암호 알고리듬 평가항목 중에는 안전성, 효율성, 기타사항이 있으며, 안전성 평가를 위한 세부적인 요구사항은 다음과 같다[4].

① 가장 일반적인 공격인 전수조사, birthday attack 등이 최상의 공격방법이어야 한다.
② 시차공격, 전력분석 공격 등과 같은 분석도 고려되어야 한다.
③ 제출자에 의해 제시된 안전성 분석에 대한 객관적인 검정을 통한 평가가 이루어져야 한다.
④ 난수 통계 테스트를 만족하여야 한다.

위에서 보는 바와 같이 전력분석 공격, 시차공격은 안전성 평가 항목에 들어 있을 정도로 중요한 평가요소가 되고 있다.

2.1.2 AES와 CRYPTREC

현재 개발이 완료된 미국의 AES에서는 implementation attack(시차공격, 전력분석 공격 등)[5, 6] 공격 사례가 포함되어 있다.

일본의 CRYPTREC 과제[7]에서도 안전성 평가를 위하여 공개 평가 과정을 거치게 되며, 이 과정에서 implementa-

tion 공격에 대한 암호 알고리듬 평가를 거친다.

결과적으로, 암호 알고리듬 개발시 DPA 공격에 대한 안전성 평가과정이 반드시 필요하다고 할 수 있다.

2.2 암호 모듈 평가

FIPS 140-2[8, 9] 안전성 요구조건에는 ① 암호 모듈 규격(cryptographic module spcification), ② 암호 모듈 포트 및 인터페이스, ③ 역할(roles), ④ 서비스(services), ⑤ 인증, ⑥ 유한상태모델(finite state modtsel), ⑦ 물리적 암호, ⑧ 동작환경(operational environment), ⑨ 암호학적 키 관리, ⑩ EMI/ EMC, ⑪ 자기진단(self-tests), ⑫ 설계보증(design assurance), 그리고 ⑬ 다른 공격의 완화(mitigation of other attacks) 등의 13개 부분으로 구성되어 있다.

그 중에서 다른 공격의 완화 부분에서는 전력분석, 시차공격, 오류 주입, TEMPEST에 대한 방어가 암호 모듈에 설계되어 있으며, 모듈의 보안정책(security policy)에 적용된 보안 메커니즘을 명시하도록 되어 있다.

FIPS 140-2[8, 9] 표준문서의 "11. Mitigation of other attacks" 내용 개요는 다음과 같다. 암호 모듈은 전력분석, 시차 분석, 오류 주입 분석처럼 표준에서 유효하지 않는 다른 공격에 민감할 수 있고, 또한 TEMPEST 공격과 같이 표준화 되어있지 않은 경우도 있다. 이들 공격의 암호 모듈 민감성은 모듈 방식, 구현 방식, 구현 환경에 따라 다르다. 그러한 공격은 특히 적대적 환경에서 구현된 암호 모듈에 대해서 관련성이 높다. 여기서 공격자는 모듈을 조작하도록 허가받을 수도 있다. 그러한 공격 방식들은 일반적으로 모듈의 물리적인 외부 환경으로부터 얻어진 정보의 분석에 의존한다. 모든 경우에 공격은 암호 모듈 내부에 있는 CSP 정보와 암호키에 관한 정보를 알아내고자 하는 것이다. 암호 모듈 평가시 부채널공격에 대하여 검토되어야 할 사항은 다음과 같다.

2.2.1 암호 모듈의 전력분석

전력소모분석을 기반으로 한 공격은 일반적으로 SPA와 DPA로 나뉘어진다. SPA는 전기적인 전력 소모 형태의 직접적인 분석과 암호 처리 과정 동안 암호 모듈에 의해 실행되는 각각의 명령어의 수행으로부터 유도된 시차를 포함한다. 패턴은 암호 모듈의 전기적인 전력 소모에서의 변화를 측정함으로써 얻어진다. DPA는 같은 목적을 가지지만 좀 더 개선된 통계적인 방법을 이용하여 암호 모듈의 전기적인 전력 소모의 변화를 분석하는 다른 기술이다. 외부 전력을 이용하는 암호 모듈에서 큰 위험이 t있을 수 있다. 전력분석 공격의 전체적인 위험을 줄이는 방법에는 전력 소모를 고르게 하는 커패시터를 사용하는 것, 내부 전력을 사용하는 것, 암호 처리 과정 동안 전력 소모의 비율을 고르게 하거나 알고리듬에서 각각의 연산을 조작하는 것이 있다.

2.2.2 암호 모듈의 시차분석

시차 분석 공격은 암호 알고리듬이나 처리와 관련된 특정한 수학적 연산을 수행하기 위해서 암호 모듈에 의해 요구된 시간을 정확히 측정함으로써 위협적일 수 있게 된다. 수집된 시차 정보는 모듈로 들어가는 입력과 기초가 되는 알고리듬 처리에 의해 사용된 암호 키의 관계를 결정하기 위해 분석된다. 이러한 관계의 분석은 암호 키나 CSP를 누출하는데 시차 측정을 이용하기 위하여 사용될 수 있다. 시차 분석 공격은 공격자가 암호 모듈의 설계에 대한 지식이 있다고 가정한다. 처리 과정 동안 시차 변동을 줄이기 위해 알고리듬이나 처리 과정의 각 연산을 조작하는 것은 이 공격의 위험을 줄이는 한 방법이다.

2.2.3 암호 모듈의 오류 주입 분석

오류 주입 공격은 암호 모듈 내부에 처리상의 오류를 야기하기 위해 마이크로파, 극단의 온도, 전압 조작과 같은 외부의 힘을 활용한다. 제한된 물리적 보안의 암호 모듈은 큰 위험이 있을 수 있다. 물리적 보안 특성의 적당한 선택은 이 공격의 위협을 줄이기 위해 사용될 수 있다.

2.2.4 암호 모듈의 TEMPEST 분석

TEMPEST 공격은 처리 과정 동안 관련된 장치와 암호 모듈로부터 방출되는 전자파 신호의 수집과 멀리 있거나 외부의 탐지를 포함한다. 이러한 공격은 키보드를 누르는 정보, 비디오 스크린에 나타나는 메시지, 암호키와 같은 중대한 보안 정보의 형태를 얻기 위해 사용될 수 있다. 네트워크 케이블링을 포함한 모든 성분의 특별한 차폐는 이러한 공격의 위험을 줄이기 위해 사용되는 메커니즘이다. 차폐는 전자파 신호의 방출을 줄이고 어떤 경우에는 막기도 한다.

암호 모듈이 하나 이상의 특수한 공격을 완화하기 위해 설계된다면 모듈의 보안 정책은 공격을 완화하기 위한 모듈에 의해 사용되는 보안 메커니즘을 조건으로 지정할 것이다.

2.3 스마트카드 보호 프로파일

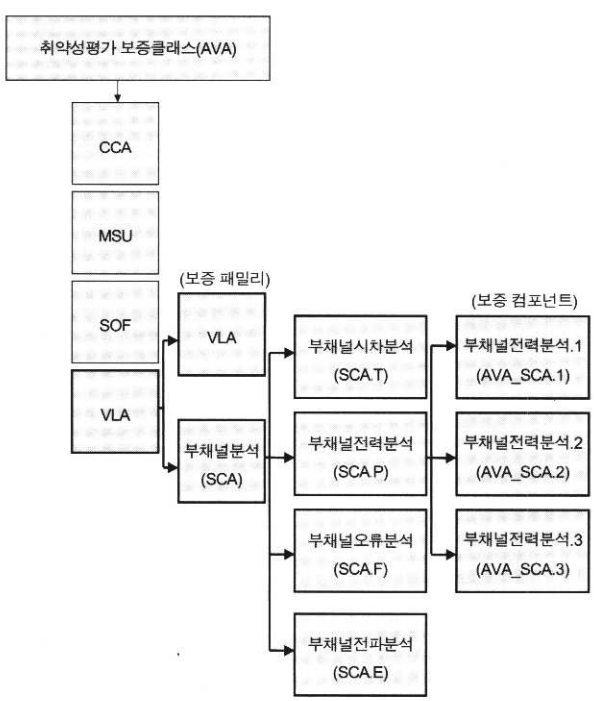
미국 NIAP(NIST & NSA) 후원 아래 American Express, Europay International, JOB Co Ltd., MasterCard International, Mondex International, Visa International 등 스마트카드 보안 사용자 그룹(SCSUG, smartcard security user group)에서 개발된 스마트카드 보호 프로파일 SCSUG-SCPP[10], 유럽 스마트카드 연구 그룹에서 개발한 EURO-SMART-PP[11-13], 그리고 국제공통기준 CC[2]를 참조하여 부 채널 분석 관련 위협요소를 분석한 결과[14]는 <표 3>과 같이 요약된다.

〈표 3〉 SCSUG-PP에서의 부채널공격 위협요소

명 칭	의 미	설 명
• TOE(Target of Evaluation)에 대한 물리적 공격 관련 위협		
T.P_Probe	IC의 물리적 검사 (Physical Probing of the IC)	공격자가 설계정보와 동작 내용을 밝혀내기 위해 TOE에 대한 물리적 검사를 수행할 수 있다. IC failure analysis, IC reverse engineering 등의 기술을 이용
T.P_Alter	IC에 대한 물리적 변경 (Physical Alteration of the IC)	공격자가 운용내용과 설계정보를 밝혀내거나, TSF(TOE Secrity Function) 데이터나 TOE 보안 기능을 변경하여 결국 TOE가 부정하게 사용될 수 있도록 TOE에 대한 물리적인 변경을 수행
• TOE에 대한 논리적 공격 관련 위협		
T.Flt_Ins	오류주입 (Insertion of Faults)	공격자가 선택된 데이터의 반복주입 결과를 관찰함으로서 사용자 정보 및 TSF 정보를 결정할 수 있다.
• 정보 감시 위협		
T.I_Leak	정보누출 (Information Leakage)	공격자가 TOE의 정상적인 사용으로부터 누출된 TSF 데이터를 이용할 수 있다. 전력분석(power analysis)는 정보누출의 한 예가 될 수 있다.
T_Link	다수관찰의 결합 (Linkage of Multiple Observations)	공격자가 자원 또는 서비스의 다수의 사용을 관찰하고 이러한 관찰을 결합하여 TSF 데이터를 드러내는 정보를 유추한다.
• 기타 위협		
T.Env_Str	환경적 스트레스 (Environmental Stress)	공격자가 TOE를 환경적인 스트레스 상에 노출시킴으로써 TSF 데이터에서 에러를 야기한다. 기온, 전압, 클럭 주파수 등의 정상적인 파라미터 극한값 또는 외부 에너지 장과 같은 비정상적인 조건이 될 수 있다.

3. 부채널관련 안전성 평가기준 제안

본 절에서는 현재 v2.1에서 v3.0으로 버전 수정이 진행중인 CC 공개 검증문서[15-17]의 취약성분석 보증 패밀리(AVA_VLA)의 분리와 연관하여 (그림 1)과 같이 부채널분석에 대한 보증 패밀리(AVA_SCA)를 분리할 것을 제안한다. 또한 부채널분석 보증 패밀리(SCA : Side-Channel Analysis Family)는 부채널시차분석 보증 패밀리(SCA.T : Side-Channel Timing Analysis Attack Family)와 부채널전력분석 보증 패밀리(SCA.P : Side-Channel Power Analysis Attack Family), 부채널오류분석 보증 패밀리(SCA.F : Side-Channel Fault Analysis Attack Family), 그리고 부채널전파분석 보증 패밀리(SCA.E : Side-Channel E-Magnetic Analysis Attack Family)로 기능 분리할 수 있다. 부채널분석 보증 패밀리(AVA_ SCA)는 상기 네 가지 기능을 통합하여 다시 1등급(AVA_SCA.1), 2등급(AVA_SCA.2), 3등급(AVA_SCA.3) 컴포넌트로 분류 · 제안한다.



(그림 1) 제안된 부채널분석 보증 패밀리(AVA_SCA)

3.1 부채널분석 보증 패밀리(AVA_SCA) 제안

비밀채널(covert channel) 보증 패밀리(AVA_CCA)와 취약성분석 보증 패밀리(AVA_VLA)를 참고하여 <표 4>, <표 5> 및 <표 6>과 같이 부채널분석 보증 패밀리(AVA_SCA)를 추가할 것을 제안한다. <표 6>의 부채널분석 보증 컴포넌트는 기본 부채널공격에 해당하는 부채널분석 보증 컴포넌트, 고급 부채널공격에 해당하는 체계적인 부채널분석 보증 컴포넌트, 그리고 철저한 부채널공격에 해당하는 철저한 부채널분석 보증 컴포넌트 등 3개 등급으로 구분하여 제안하였다.

〈표 4〉 수정된 보안목적관련 보증 요구사항

보 증 요 구 사 항		보안목적
컴 포 넌 트	컴포넌트 이름	
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*	체계적인 부채널공격 분석 (Systematic side-channel analysis)	O.Flt_Ins, O.I_Leak

※ Side-Channel Analysis(추가 사항).

〈표 5〉 수정된 평가보증등급 요약

보증 클래스	보증 패밀리	평가보증등급에 따른 보증 컴포넌트						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
형상관리	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
배포 및 운영	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
개발	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
설명서	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
생명주기 지원	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
시험	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
취약성 평가	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*

※ Side-Channel Analysis(추가 사항).

3.2 부채널분석 보증 컴포넌트 개발

3.2.1 목 적

부채널분석은 TOE에 대하여 공격이 가능한 의도하지 않은 신호채널(예 : 허용되지 않은 정보흐름)의 존재와 잠재적인 용량을 결정하기 위하여 수행된다. 부채널분석(AVA_SCA, Side-Channel Analysis) 패밀리의 보증등급 요구사항은 의도하지 않았으나 SFP를 위반하는데 악용할 수 있는 신호경로가 존재할 위협을 다룬다.

3.2.2 컴포넌트 계층관계 및 설명

이 패밀리의 컴포넌트들은 부채널분석의 엄밀성에 기반하여 계층화되어 있다.

3.2.3 응용시 주의사항

채널 용량 추정은 실제 시험 측정뿐만 아니라 비정형화된 공학적 측정에 기반한다. 부채널분석이 기반으로 하는 가정사항의 예는 클럭 속도, 프로세서의 속도, 시스템 또는 네트워크 구성, 메모리 용량, 캐쉬 용량 등을 포함한다. 시험을 통한 부채널분석의 선택적 검증은 평가자에게 부채널분석(예 : SPA, DPA, SEMD-DPA, MESD-DPA, ZEMD-DPA, IPA, HO-DPA, TA, FA, DFA, TEMPEST 등)측면을 검증할 수 있는 기회를 제공한다. 이는 부채널분석 결과 전체를 입증해야 함을 요구하지는 않는다. 이 패밀리는 정보 흐름통제 SFP에만 적용되는 것이므로, 보안 목표명세서에 정보 흐름통제 SFP가 없다면 더 이상 적용할 수 없다.

3.3 AVA_SCA.1 부채널분석(Side-Channel Analysis)

3.3.1 목 적

이 컴포넌트의 목적은 부채널에 대한 비정형화된 조사를 통하여 식별 가능한 부채널을 식별하는 것이다.

3.3.2 개발자 요구사항

- AVA_SCA.1.1D 개발자는 각 정보 흐름통제 정책에 대하여 부채널을 조사해야 한다.
- AVA_SCA.1.2D 개발자는 부채널분석 문서를 제공해야 한다.

3.3.3 증거 요구사항

- AVA_SCA.1.1C 부채널분석 문서는 부채널을 식별하고 그 용량을 추정해야 한다.
- AVA_SCA.1.2C 부채널분석 문서는 부채널의 존재를

〈표 6〉 제안된 부채널분석 보증 컴포넌트

보증 클래스	보증 패밀리	보증 컴포넌트	목 적	응용시 주의사항	비 고 예) DPA[17]
취약성평가	AVA_SCA	AVA_SCA.1 (Side-Channel Analysis)	부채널에 대한 비정형화된 조사를 통하여 식별가능한 부채널을 식별함.	소스 코드 비공개 상태에서의 분석임.	Basic SCA Ex) Basic SPA/DPA
		AVA_SCA.2 (Systematic SCA)	부채널에 대한 체계적인 조사를 통하여 식별 가능한 부채널을 식별함.	부채널을 체계적으로 분석하는 것은 개발자가 부채널을 임시적인 방식으로 식별하는 것이 아니라 구조적이고 반복 가능한 방법으로 식별할 것을 요구함	Advan-ced SCA Ex) Advan-ced SPA/DPA
		AVA_SCA.3 (Exhaustive SCA)	부채널에 대한 철저한 조사를 통하여 식별 가능한 부채널을 식별함.	철저한 방식의 부채널분석은 부채널식별에 사용된 계획이 부채널조사를 위해 가능한 모든 방법이 이용되었음을 보증하기에 충분하다는 추가적인 증거를 제공하도록 요구함	Exhaus-tive SCA Ex) Exhaus-tive SPA/DPA

결정하는데 사용된 절차와 부채널분석을 수행하는데 필요한 정보를 서술해야 한다.

- AVA_SCA.1.3C 부채널분석 문서는 부채널분석 중에 사용된 모든 가정사항을 서술해야 한다.
- AVA_SCA.1.4C 부채널분석 문서는 최악의 경우의 시나리오에 기반하여 채널 용량을 추정하는데 사용된 방법을 서술해야 한다.
- AVA_SCA.1.5C 부채널분석 문서는 식별된 각 부채널에 대하여 최악의 경우를 악용한 시나리오를 서술해야 한다.

3.3.4 평가자 요구사항

- AVA_SCA.1.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
- AVA_SCA.1.2E 평가자는 부채널분석 결과가 TOE가 TOE 기능 요구사항을 만족함을 보이는지 확인해야 한다.
- AVA_SCA.1.3E 평가자는 시험을 통하여 부채널분석을 선택적으로 검증해야 한다.

3.4 AVA_SCA.2 체계적인 부채널분석(Systematic Side-Channel Analysis)

3.4.1 목 적

이 컴포넌트의 목적은 부채널에 대한 체계적인 조사를 통하여 식별 가능한 부채널을 식별하는 것이다.

3.4.2 응용시 주의사항

부채널을 체계적으로 분석하는 것은 개발자가 부채널을 임시적인 방식으로 식별하는 것이 아니라 구조적이고 반복 가능한 방법으로 식별할 것을 요구한다.

3.4.3 개발자 요구사항

- AVA_SCA.2.1D 개발자는 각 정보 흐름통제 정책에 대하여 부채널을 조사해야 한다.
- AVA_SCA.2.2D 개발자는 부채널분석 문서를 제공해야 한다.

3.4.4 증거 요구사항

- AVA_SCA.2.1C 부채널분석 문서는 부채널을 식별하고 그 용량을 추정해야 한다.
- AVA_SCA.2.2C 부채널분석 문서는 부채널의 존재를 결정하는데 사용된 절차와 부채널분석을 수행하는데 필요한 정보를 서술해야 한다.
- AVA_SCA.2.3C 부채널분석 문서는 부채널 분석 중에 사용된 모든 가정사항을 서술해야 한다.
- AVA_SCA.2.4C 부채널분석 문서는 최악의 경우의 시나리오에 기반 하여 채널 용량을 추정하는데 사용된 방법을 서술해야 한다.
- AVA_SCA.2.5C 부채널분석 문서는 식별된 각 부채널에 대하여 최악의 경우를 악용한 시나리오를 서술해야 한다.
- AVA_SCA.2.6C 부채널분석 문서는 부채널 식별에 사용된 방법이 체계적이라는 증거를 제공해야 한다.

3.4.5 평가자 요구사항

- AVA_SCA.2.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
- AVA_SCA.2.2E 평가자는 부채널분석 결과가 TOE가 TOE 기능요구 사항을 만족함을 보이는지 확인해야 한다.
- AVA_SCA.2.3E 평가자는 시험을 통하여 부채널분석을 선택적으로 검증해야 한다.

3.5 AVA_SCA.3 철저한 부채널분석 (Exhaustive Side-Channel Analysis)

3.5.1 목 적

이 컴포넌트의 목적은 부채널에 대한 철저한 조사를 통하여 식별 가능한 부채널을 식별하는 것이다.

3.5.2 응용시 주의사항

철저한 방식의 부채널분석은 부채널 식별에 사용된 계획이 부채널 조사를 위해 가능한 모든 방법이 이용되었음을 보증하기에 충분하다는 추가적인 증거를 제공하도록 요구한다.

3.5.3 개발자 요구사항

- AVA_SCA.3.1D 개발자는 각 정보 흐름통제 정책에 대하여 부채널을 조사해야 한다.
- AVA_SCA.3.2D 개발자는 부채널분석 문서를 제공해야 한다.

3.5.4 증거 요구사항

- AVA_SCA.3.1C 부채널분석 문서는 부채널을 식별하고 그 용량을 추정해야 한다.
- AVA_SCA.3.2C 부채널분석 문서는 부채널의 존재를 결정하는데 사용된 절차와 부채널분석을 수행하는데 필요한 정보를 서술해야 한다.
- AVA_SCA.3.3C 부채널분석 문서는 부채널 중에 사용된 모든 가정사항을 서술해야 한다.
- AVA_SCA.3.4C 부채널분석 문서는 최악의 경우의 시나리오에 기반하여 채널 용량을 추정하는데 사용된 방법을 서술해야 한다.
- AVA_SCA.3.5C 부채널분석 문서는 식별된 각 부채널에 대하여 최악의 경우를 악용한 시나리오를 서술해야

한다.

- AVA_SCA.3.6C 부채널분석 문서는 부채널 식별에 사용된 방법이 철저하다는 증거를 제공해야 한다.

3.5.5 평가자 요구사항

- AVA_SCA.3.1E 평가자는 제공된 정보가 모든 증거 요구사항을 만족하는지 확인해야 한다.
- AVA_SCA.3.2E 평가자는 부채널분석 결과가 TOE가 TOE 기능요구 사항을 만족함을 보이는지 확인해야 한다.
- AVA_SCA.3.3E 평가자는 시험을 통하여 부채널분석을 선택적으로 검증해야 한다.

4. 결 론

본 논문에서는 암호 알고리듬, 암호 모듈, 정보보호 제품 평가에 적용되고 있는 부채널 관련 기준을 분석하였으며, 국제공통 평가기준에서 독립적인 평가항목으로 평가되어야 함을 보였다. 이를 위하여 신분카드, 교통카드, 전자화폐 등 앞으로 여러 분야에서 사용될 스마트카드에서의 부채널분석 공격에 대한 안전성 평가기준을 제안하였다. 제안된 보증 컴포넌트는 취약성 평가 보증 클래스의 AVA_VLA에서 독립된 AVA_SCA(Side-Channel Analysis) 보증 패밀리를 분리하였으며, 기존의 AVA_CCA(Covert Channel Analysis)의 평가기준을 참조하여 보증 컴포넌트를 AVA_SCA.1, AVA_SCA.2, AVA_SCA.3 등 3등급으로 구분하였다. 본 논문에서 제안된 내용은 개정이 추진중인 CC 버전 3.0에 반영될 필요가 있다고 판단된다.

참 고 문 헌

[1] http://www.kisa.or.kr/sysevaluation.

[2] http://www.commoncriteria.org/.

[3] P. Kocher, J. Jaffe and B. Jun, "*Differential Power Analysis*," in Proceedings of Advances in Cryptology-CRYPTO '99, pp.388-397, Springer-Verlag, 1999.

[4] NESSIE, http://www.cosic.esat.kulcuven.ac.be/nessie/.

[5] J. Daeman and V. Rijmen, "The Design of Rijndael," Springer-Verlag, 2002.

[6] S. Chari, C. Jutla, J. R. Rao and P. Rohtgi, "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards," 2nd AES conference available on http://csrc.nist.gov/encryption/aes/round1/conf2/aes2conf.htm.

[7] CRYPTREC, http://www.ipa.go.jp/security/.

[8] National Institute of Standards and Technology, "Security Requirements for Cryptographic Modules," Federal Information Processing Standards Publication 140-2, May, 2001.

[9] FIPS 140-2 DTR, http://csrc.nist.gov/cryptval/140-1/fips1402DTR.pdf.

[10] Common Criteria for Information Technology Security Evaluation ; Smart Card Security User Group Smart Card Protection Profile (SCSUG-SCPP), Version 3.0, Sep., 2001.

[11] EUROSMART-PP/0010, Protection Profile Smart Card IC with Multi-Application Secure Platform (ver. 2.0), Nov., 2000.

[12] EUROSMART-PP/9911, Protection Profile Smart Card Integrated Circuit with Embedded Software (ver. 2.0).

[13] EUROSMART BSI-PP-0002, Smartcard IC Platform Protection Profile (Version 1.0), July, 2001.

[14] 이훈재, 이상곤 외, "스마트카드 비밀채널 평가/분석기술 연구", 한국전자통신연구원 부설 국가보안기술연구소, 최종보고서, 2002.

[15] CCIMB-2002-04-001-ASE (Draft v0.6), "Security Target Evaluation Common Criteria and Methodology for Public Review," at http://www.commoncriteria.org/review_docs/.

[16] CCIMB-2002-07-001-AVA (Draft v0.68), "Vulnerability Analysis and Penetration Testing," at http://www.commoncriteria.org/review_docs/.

[17] CCIMB-2002-11-003-AttackPotential (Draftv0.5), "Characterisation of Attack Potential," at http://www.commoncriteria.org/review_docs/.

이 훈 재

e-mail : hjlee@dongseo.ac.kr

1985년 경북대학교 전자공학과(학사)

1987년 경북대학교 전자공학과(석사)

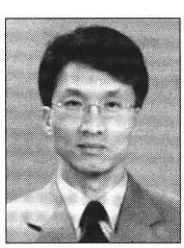
1998년 경북대학교 전자공학과(박사)

1987년~1998년 국방과학연구소 선임연구원

1998년~2002년 경운대학교 컴퓨터전자정보공학부 조교수

2002년~현재 동서대학교 인터넷공학부 정보네트워크공학전공 조교수

관심분야 : 정보보안, 네트워크보안, 정보통신네트워크



이 상 곤

e-mail : nok60@dongseo.ac.kr

1986년 경북대학교 전자공학과(학사)

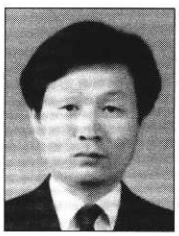
1988년 경북대학교 대학원 전자공학과(통신공학, 공학석사)

1993년 경북대학교 대학원 전자공학과(정보통신공학, 공학박사)

1991년~1997년 창신대학 정보통신과 조교수

1997년~현재 동서대학교 인터넷공학부 정보네트워크공학전공 조교수

관심분야 : 암호이론, 네트워크보안, 시스템 보안, 부호기술, Java 기술



최 희 봉

e-mail : hbchoi@etri.re.kr

1984년 부산대학교 전기공학과(학사)

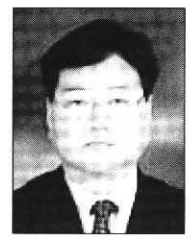
1987년 부산대학교 전기공학과(석사)

2002년 성균관대학교 전전컴공학부(박사)

1987년~2000년 국방과학연구소 선임연구원

2000년~현재 한국전자통신연구원 부설 국가보안기술연구소 선임연구원

관심분야 : 정보보호, 보안시스템 설계 및 평가



김 춘 수

e-mail : jbr@etri.re.kr

1987년 숭실대학교 전기공학과(학사)

1989년 숭실대학교 전기공학과(석사)

1998년 숭실대학교 전기공학과(박사)

1990년~1999년 한국전자통신연구원 팀장

2000년~현재 한국전자통신연구원 부설 국가보안기술연구소 팀장

관심분야 : 보안시스템 설계 및 평가