특집 10

정보보호용 암호 칩에 대한 해킹 및 대응책

목 차

백이루 · 하재철
(호서대학교)

1. 서 론

최근 각종 해킹 사건과 사고들이 많이 일어나고, 개인 정보 노출로 인한 피해 사례들이 많아지고 있다. 이러한 위협들 속에서 민감한 정보들을 보호하기 위해 가장 많이 사용하는 것이 암호화 기법이다. 이렇듯 비밀 정보들을 안전하게 보호하기 위해 많은 암호 알고리듬들이 연구되었고, 알고리듬의 암호학적 안전도를 높이기 위해 많은 노력이 있었다. 그러나 대부분 암호 알고리듬의 안전도가 수학적 난제에 의존하고 있다는 점 때문에 이론적인 분석을 통해 안전성을 검증하는 경우가 많았다. 반면, 이러한 검증을 실시함에 있어 암호 알고리듬을 실제로 수행하는 암호용 칩이나 하드웨어 장치들에 대해서는 이미 안전하다고 가정하였다.

한편, 1997년 Kocher 등은 암호 알고리듬을 수행하는 칩의 전력 소비를 측정하여 칩에 내장된 비밀 정보를 추출할 수 있는 전력분석 공격을 제안하였다[1,2]. 또한 전력 소비뿐만 아니라 알고리듬의 수행 시간을 측정하거나 전자기장을 측정하는 공격도 시도되었다. 이와 같이 암호 알고리듬을 수행하는 칩에서 발생하는 부가적인 정보를 이용하여 비밀 정보를 추출하는 수동적 공격을 부채널 공격(Side Channel Attack)이라 부른다. 같은 해 Boneh 등은 중국인의 나머지 정리 이론(Chinese Remainder Theorem, CRT)을 기반으로 하는 RSA 암호 알고리듬이 오류주입 공격(Fault Injection Attack)에 취약함을 증명하였다[3]. 오류주입 공격에서는 먼저 암호 알고리듬을 수행하는 칩에 어떤 물리적인 수단을 이용하여 오작동을 일으키게 함으로써 정상적인 결과 값이 아닌 잘못된 값이 출력되도록 한다. 그리고 출력된 오류 결과 값을 분석하여 암호 연산에 사용된 비밀키를 해킹하게 된다.

위에서 설명한 공격들은 암호 알고리듬이 갖는 이론적인 안전성과 상관없이 알고리듬이 구현되는 물리적인 환경에 민감하게 작용한다. 즉, 스마트카드나 IC 카드, 마이크로프로세서들과 같은 정보보호용 암호 칩을 대상으로 공격을 시도한다. 이에 따라 암호학적 안전도의 연구 범위도 알고리듬의 이론적인 분석에서 이를 수행하는 하드웨어적 환경에 대한 보호까지 확대되었다. 여러 물리적 해킹 공격들 중에서 특히 오류

주입을 이용한 해킹 공격은 AES(Advanced Encryption Algorithm), RSA, RSA+CRT (RSA with CRT), DSA(Digital Signature Algorithm) 등과 같이 이미 사용 중인 표준 암호 알고리듬뿐만 아니라 대부분의 암호 알고리듬에 적용이 가능하다. 또한, 향후에는 더 세밀하고 정밀한 오류 주입 공격이 예상되므로 매우 위협적인 공격 기법으로 인식되고 있다. 이에 따라 국내·외에서 다양한 방법의 오류주입 공격 사례들이 선보이고 있으며 암호용 칩 제조사들은 이미 이에 대한 대응책들을 강구하고 있다. 우리의 실생활 속에서 정보보호용 암호 칩이 내장된 소형 기기들이나 스마트카드 등이 여러 분야에 걸쳐 다양하게 활용되고 있고, 그 수요 또한 높아지고 있기 때문에 오류주입 해킹 공격과 그에 대한 대응책을 연구하는 것은 상당히 중요하다고 할 수 있다.

본고에서는 정보보호용 암호 칩에 대한 해킹 기법 중 오류주입 공격 기법에 대해 알아보고 오류주입 공격의 종류와 최근 동향을 분석한다. 특히, 오류주입 공격에 매우 취약한 특성을 보이고 있는 RSA+CRT 알고리듬에서의 실질적인 공격 사례를 중심으로 설명할 것이다. 또한, 이러한 물리적 해킹 공격에 대응할 수 있는 방법에 대해서 살펴보고자 한다.

2. 오류주입 해킹 공격 개요

오류주입을 이용한 해킹 공격에서의 오류는 다양한 형태로 나타날 수 있다. 먼저 오류는 영구적 오류와 일시적 오류로 분류할 수 있는데, 여기서 영구적 오류는 칩의 특정 메모리 셀을 파괴하거나 데이터 버스 선을 끊는 것으로 인해 영구적으로 오류를 발생시키는 것이고, 일시적 오류는 칩이 어떤 작업을 수행하고 있을 때, 특정 메모리 셀에 어떤 물리적인 공격을 통해 상태를 일시적으로 변화시켜 저장 값을 바꾸는 것이다.

또한, 오류 범위에 따라 오류를 비트 또는 바이트 단위로 주입하거나 특정 메모리 값을 0 또는 1로 고정시키는 오류 등도 있으며, 오류를 주입하여 특정 명령어 코드를 생략하는 경우도 있다. 오류 주입 공격의 위치도 RAM, CPU, EEPROM, EPROM, 데이터 혹은 버스 라인 등 매우 다양하게 시도될 수 있다. 공격자는 위와 같은 다양한 오류 모델 중에서 목표 알고리듬에 대한 공격이 용이한 모델을 선택하여 공격을 수행하게 된다.

오류주입 공격은 크게 비침투형(non-invasive) 공격, 준침투형(semi-invasive) 공격, 침투형(invasive) 공격으로 분류할 수 있다. 비침투형 공격은 칩에 대해서 어떠한 사전 처리 없이도 공격을 수행할 수 있는데 반해, 준침투형 공격과 침투형 공격은 공격을 위해 대상 칩의 패키징(packaging)을 벗겨내는 디캡핑(decapping)이란 사전 처리가 필요로 하게 된다. 준침투형과 침투형 공격은 칩 디캐핑 후 공격 시점에서 직접적으로 표면에 접촉하는지, 그렇지 않은지로 구별하게 된다. 아래 〈표 1〉은 오류주입 공격의 형태에 따라 공격들을 분류한 것이다.

〈표 1〉 오류주입 공격의 형태에 따른 공격 기법들의 분류

공격 형태 / 해킹 기법	비침투형 공격	준침투형 공격	침투형 공격
오류주입 공격	■온도 ■전압 글리치 ■클럭 글리치	■빛(레이저) ■외부 전기장/와전류 ■X-ray	■이온 ■능동 프로브

2.1 비침투형 공격

2.1.1 온도

전자 장비들은 정의된 특정 범위의 온도 내에서 정확한 동작을 수행하게 된다. 오류는 이러한 동작 온도의 특정 범위를 벗어나는 경우에서 생겨나게 된다. 따라서 극단의 온도를 설정한 환경

에서 동작되는 장치는 오류가 주입될 수 있는 가능성을 갖게 된다. 예를 들어, 온도를 극도로 낮춘 환경에서 칩을 동작시킨다고 가정할 때, RAM의 셀에서는 임의의 변형이 일어나거나 비휘발성 메모리의 읽기-쓰기 동작에서 비동기가 발생할 수도 있다[4].

2.1.2 전압 글리치(glitch)

스마트카드와 같은 장비는 스스로 전원을 공급하지 않기 때문에 리더기로부터 전원을 공급받아야 한다. ISO 규격에서 정의된 스마트카드의 정격 전압은 5V로 정의되어 있지만 실제로는 약 ±10%의 여유를 두고 있다. 전압 글리치 공격은 장치의 정격 전압을 벗어나는 외부의 전원이 공급될 때, 메모리상의 오류나 프로그램의 동작에 있어서 오류를 나타내는 등의 스마트카드의 불안정적인 동작을 유도한다[5].

2.1.3 클럭 글리치

클럭 글리치 공격은 전압 글리치 공격과 마찬가지로 스마트카드와 같은 장비는 스스로 클럭 신호를 만들 수 없기 때문에 공격자는 이런 칩 특성을 이용하여 외부에서 비정상적으로 높거나 혹은 낮은 클럭 주파수를 주입함으로써 오류 동작을 유도할 수 있다[6].

2.2 준침투형 공격

2.2.1 빛(레이저)

빛 또는 레이저를 이용한 오류주입 공격은 칩에 강한 광원을 주입하여 메모리의 비트 값을 바꾸는 공격이다[7]. 특히, 레이저 시스템은 다양한 파장과 방사 강도를 조절하여 장치의 특정 영역을 대상으로 하여 조준할 수도 있으며 반응 속도가 정교하므로 암호용 칩에 대해서 공간적, 시간적으로 정밀 공격이 가능하다.

2.2.2 외부 전기장/와전류

외부 전기장 변화를 이용한 오류주입 공격은 전기장의 변화에 따라 트랜지스터나 메모리 셀 등에 영향을 미쳐 오류를 유도하는 것이고, 와전류를 이용한 공격은 도체 내부를 지나는 자기력선 속의 변화로 인해서 생기는 와전류의 주입을 통해 메모리 셀에 영향을 주어 오류를 유도하는 것이다[8].

2.2.3 X-ray

X-ray 방사를 이용한 오류주입 공격은 CMOS RAM에 영향을 주어 오류를 유도하는 것이다. 상용화된 X-ray는 공항에서 가방을 스캔하는 용도로 사용되는 것으로 오류를 주입할 수 있을 만큼의 충분한 에너지를 공급할 수 없기 때문에 오류 주입 공격을 위해서는 고에너지의 X-ray를 사용한다[9].

2.3 침투형 공격

침투형 공격은 오류주입을 위해서 칩의 패키징을 벗겨내는 디캡핑 과정에 추가로 표면의 보호막층(passivation)을 벗겨내야 한다. 침투형 공격은 마이크로프로빙을 통해 직접적으로 회로를 관측하여 조작하거나 내부 금속 층까지도 이온 빔을 방사하는 오류 주입 공격을 포함한다[4].

2.3.1 이온

표면이 벗겨진 칩에 대해서 국부적으로 충분히 집중된 이온 빔을 방사하여 회로상의 신호에 영향을 주거나 버스 라인 또는 회로의 요소를 파괴하는 등의 오류 주입 공격이 가능하다.

2.3.2 능동 프로브

능동 프로브를 사용하여 신호 또는 정보를 시스템에 주입 가능한 특성을 이용하는 공격으로 암호 칩의 내부 회로에 직접 능동 프로브를 접촉하여 오류를 주입하거나 비밀키를 추출하는 공격이다.

3. 암호용 칩 공격 사례

최근의 오류주입 공격에 대한 실험적 분석들을 살펴보면 스파크를 이용한 전압 글리치 공격과 레이저를 이용한 오류주입 공격에 대한 실험들이 많이 이루어지고 있다. 레이저를 이용한 오류주입 공격은 전자 현미경으로 디캡핑된 칩의 내부를 관찰하여 정밀한 위치에 오류주입이 가능하다. 이 절에서는 오류주입 공격에 대한 몇 가지 실험적 분석 사례를 통해 오류주입 공격의 동향을 알아본다. 비밀 키를 공격하는 실험은 주로 중국인의 나머지 정리에 기반한 RSA+CRT 알고리듬을 대상으로 많이 이루어졌으므로 이를 중심으로 연구 사례를 소개하고자 한다.

3.1 전자기 오류주입 공격

오스트리아의 IAIK(Institute for Applied Information Processing and Communication)에서는 RSA+CRT 서명 알고리듬에서 전자기 오류를 주입하여 비밀 키를 추출하는 실제적인 공격을 수행하였다[10]. IAIK에서는 고주파수의 스파크를 칩에 주입하여 유동 전류에 매우 빠른 변화를 인가함으로써 강력한 전자기장 폭발을 일으켜 오류를 주입하였다.

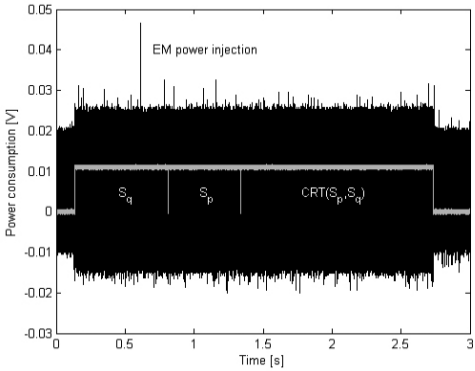
실험에 사용된 RSA+CRT 서명 알고리듬은 아래의 (그림 1)과 같다. 여기서 p와 q는 사용자의 비밀 정수에 해당하며 합성수 $N=pq$이다. 또한, $q_I = q^{-1} \bmod p$이고 $p_I = p^{-1} \bmod q$이며 d는 비밀키이고 공개키는 $e = d^{-1} \bmod (p-1)(q-1)$이다. 서명하고자 하는 메시지는 m이며 최종 서명은 $S = m^d \bmod N$이 된다. 공격자의 최종 목표는 비밀 키 p나 q를 찾아내는 것인데 공격 방법은 S_p나 S_q연산시 오류를 넣고 그 결과 서명을 얻으면 된다. 예를 들어 S_p에 오류가 주입된 후 S_p'이 되고 이를 사용한 출력 서명이 S'이라면 $q = GCD(S'^e - m,\ N)$ 를 이용하여 비밀 키를 추출하게 된다.

Input: p, q, d, p_I, q_I, N, m, Output: $S = m^d \bmod N$
1. $S_p = m^{d_p} \bmod p$, where $d_p = d \bmod (p-1)$
2. $S_q = m^{d_q} \bmod q$, where $d_q = d \bmod (q-1)$
3. $S = (S_p \bullet (q \bullet (q_I)) + (S_q \bullet (p \bullet (p_I)) \bmod N$
4. return S

(그림 1) Gauss 방법을 이용한 RSA+CRT 서명 알고리듬

(그림 1)에서 오류가 주입되는 위치는 단계 1이나 단계 2이며 (그림 2)와 같이 RSA+CRT 알고리듬을 장착한 마이크로 컨트롤러를 공격하였다. 이 마이크로 컨트롤러 내부에는 비밀키가 내장되어 있으며 이 서명 연산을 수행하는 동안 고주파수의 전자기파를 주입하여 오류를 발생시켰다. (그림 3)은 이 마이크로 컨트롤러에서 RSA+CRT 서명 알고리듬이 수행되는 동안의 소비 전력을 측정한 것이다. 여기서 검은 영역은 소비 전력을 나타내고, 회색부분은 측정을 위한 트리거 신호이다. (그림 3)에서 볼 수 있듯이 서명 값 S_p, S_q와 전체 CRT 연산이 뚜렷하게 구분됨을 확인할 수 있으며 파형의 관측을 통해서 연산이 시작하고 대략 600㎳ 지점에 전자기 스파크가 주입되었음을 확인할 수 있다. 따라서 서명 연산 동안 주입된 오류를 통해서 얻은 잘못된 서명 값을 이용하여 비밀 소수 q값을 추출할 수 있다.

(그림 2) 마이크로 컨트롤러의 표면에 작용하는 스파크



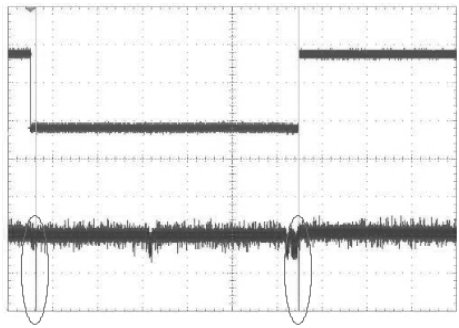
(그림 3) 전자기 오류가 주입되는 동안의 소비 전력 파형

3.2 전압 글리치를 통한 오류주입 공격

2007년 Kim 등은 RSA+CRT 알고리듬에 대해 전압 글리치를 이용한 오류주입 공격을 실험하였다[11]. 이 공격에서는 이미 오류 주입 공격을 방어하도록 설계된 알고리듬을 재공격한 사례이다. 이 실험에서는 오류 검사를 이용한 대응책이 적용된 RSA+CRT 알고리듬에 대해서 두 번의 오류주입을 통해 2차 오류 공격이 성공할 수 있음을 증명하였다. 즉, RSA+CRT 서명 생성 과정 중 S_p나 S_q에 첫 번째 오류를 주입하고, 오류를 검사하는 단계에서 두 번째 오류를 주입하여 오류 검사 과정을 수행하지 않게 함으로써 오류가 주입된 서명 값을 출력하게 하였다. 이렇게 획득한 오류 서명 값을 이용하여 비밀 정보를 추출할 수가 있다. 이 공격 실험에서는 RSA+CRT 알고리듬을 수행되는 Atmega168 칩을 대상으로 하였으며 (그림 4)와 같이 고전력 펄스 발생기를 이용하여 전압 글리치 오류를 주입하는 방법을 사용하였다.

(그림 5)는 RSA+CRT 알고리듬이 동작할 때 소비 전력을 나타낸 것으로 1차 오류는 S_p를 계산하는 과정에 주입되었고 2차 오류는 오류 주입 여부를 검사하는 명령어를 건너뛰기 위해 사용되었다. (그림 5)에서 볼 수 있듯이 두 번의 오류가 정확히 주입되었고 비밀 키를 추출할 수 있음을 확인할 수 있다.

(그림 4) 오류주입 공격 실험 환경



(그림 5) 오류주입 시 소비 전력 신호

RSA+CRT에서 비밀 키를 찾아내는 공격은 S_p나 S_q에서 오류를 넣기만 하고 그 결과 값을 얻을 수 있으면 바로 성공할 수 있을 만큼 취약하다. 그 만큼 오류의 시간적 범위도 충분하며 비트 오류, 바이트 오류, 연산 오류, 명령어 오류 등의 오류 종류에 제한을 받지 않는다. 반면, AES와 같은 대칭키 암호 시스템의 경우에는 최소 바이트 단위 정도의 오류 주입 기술이 있어야 충분히 비밀 키를 찾아낼 수 있다[12, 13]. 즉, RSA+CRT에 대한 공격보다는 어렵지만 취약한 암호 칩에 AES를 탑재하여 사용할 경우에는 해킹 가능성이 높다고 할 수 있다.

4. 오류주입 공격의 대응책

앞에서 설명했듯이 오류주입 공격은 AES, RSA, RSA+CRT, DSA 등 이미 사용 중인 대부

분의 암호 알고리듬에 적용이 가능하고, 오류주입 기술이 계속 발전하고 있어 이에 대한 대응책을 마련하는 것은 매우 중요한 일이다. 오류주입 공격에 대응하기 위해서는 암호 알고리듬이 구현된 환경이 오류주입 공격을 방어할 수 있도록 설계되어야 하고, 암호 알고리듬 또한 오류가 주입되었을 경우, 이를 탐지할 수 있도록 하는 것이 중요하다. 따라서 오류주입 공격의 대응책은 두 가지 관점에서 생각해볼 수 있다. 첫 번째는 하드웨어 관점에서 대응책을 마련하는 것이고, 두 번째는 소프트웨어 관점에서 대응책을 마련하는 것이다.

4.1 하드웨어 관점에서의 대응책

하드웨어 관점에서 오류주입 공격을 방어하기 위해서는 칩을 설계할 때, 오류주입 공격을 방어하기 위한 보호 기능을 탑재하여 설계하는 것이다. 예를 들어, 지금 현재 스마트카드에 탑재된 칩의 경우 온도 센서와 빛 또는 레이저 등이 주입되었을 때, 이를 감지할 수 있는 보안 센서들을 내장하고 있어 오류주입 공격을 방어하고 있다. 또한 전압 글리치나 클럭 글리치와 같이 정격 전압을 벗어나는 외부 신호 입력 공격을 시도했을 때는 칩의 동작을 초기화(reset)하는 대응책도 사용된다. 그러나 무엇보다도 오류 주입 공격은 잘못된 오류 값을 출력한다는 전제로 시도되므로 오류가 들어오면 결과 값을 출력하지 않도록 하는 것이 중요하다. 최근에 출시되는 스마트카드는 보안성이 중요시되므로 이러한 물리적인 공격에 대한 보호 기능들로 인해 오류주입 공격에 안전한 것으로 알려져 있다. 그러나 범용 마이크로 프로세서에 암호 알고리듬을 탑재하고 비밀 키를 이용한 연산을 하는 경우에는 공격에 매우 취약한 특성을 보이고 있다. 이와 같이 하드웨어 관점에서 보면 오류 주입 공격이 물리적 공격인 만큼 하드웨어 자체에 대한 안전성을 강화하는 것이 기본적인 대응책이라 할 수 있다. 그러나 하드웨어적인 대응 회로를 추가하는 것이 구현 측면에서 얼마나 효과적인지도 고려해봐야 한다.

4.2 소프트웨어 관점에서의 대응책

소프트웨어 관점에서 오류주입 공격을 방어하기 위해서는 암호 알고리듬을 소프트웨어로 구현할 때, 오류가 주입되었는지 여부를 확인할 수 있도록 오류 탐지 기법을 개발하여 적용하거나 공격자가 잘못된 정보로부터 비밀 값을 추출할 수 없도록 비밀 값과 상관없는 랜덤한 값을 출력할 수 있도록 해야 한다. 특히, RSA+CRT 알고리듬은 오류주입 공격에 매우 취약한 것으로 알려져 이에 대한 많은 대응책들이 연구되고 있다[14-17]. 효율적이고 안전한 RSA+CRT 구현을 위해 지금까지 제시된 소프트웨어적인 대응책을 정리하면 다음과 같다.

4.2.1 중복 연산 기법

같은 연산을 두 번 실행하여 그 결과 값을 비교하는 방법이 있다. 그러나 소요 시간이 2배로 소요된다는 점과 영구적인 오류로 인해 같은 오류 결과 값을 출력하는 경우 이 역시 공격에 취약하다는 단점이 있다. 이를 코드로 표현하면 다음과 같은 나타낼 수 있는데 여기서 서명 연산은 $S = Sig(m) = m^d \bmod N$을 의미한다.

$$\mathrm{if}\,(Sig(m) \equiv Sig(m))\,then\,Return(S)\;else\,Return(Error)$$

4.2.2 결과 값 복원 후 확인 기법

어떤 메시지에 대한 연산 결과를 다시 복원하여 원래 메시지와 비교하는 방법이다. 예를 들어 비밀키로 연산된 RSA+CRT 서명문을 다시 공개키로 복원하여 최초 입력과 동일한지 검증한 후 맞으면 최종 서명문을 출력한다. 그러나 공개키 길이가 비밀키 길이와 동일한 경우에는 연산 소요 시간이 두 배로 늘어나는 단점이 있다. 여

기서 서명 검증식 $Ver(S)$은 $S^e \bmod N$을 의미한다.

$$\text{if}(Ver(Sig(m)) \equiv m) \, then \, Return(S) \\ else \, Return(Error)$$

4.2.3 오류 검사 기법

서명 연산 과정에서 발생하는 연산의 중간 값을 이용하여 계산상 오류가 주입되었는지 검사하는 기법이다[14-16]. 그러나 이 오류 검사 기법은 비교를 위한 중간값을 계산하는데 추가 연산이 필요하며 최종적인 결과를 비교하는 구문을 건너뛸 수 2차 오류 주입 공격에 취약한 특성을 가질 수 있다.

4.2.4 오류 확산 기법

서명 연산 과정에서 오류가 주입되었을 경우 인위적으로 랜덤한 결과 값을 출력하도록 하는 대응 기법이다[17]. 따라서 공격자에게는 오류 주입에 따른 최종 결과 값을 출력해 주지만 자신의 비밀키와 전혀 관련이 없는 값이므로 해킹 공격을 방어할 수 있다. 이 방법은 RSA+CRT에서 S_p나 S_q 중 하나에만 오류가 발생하면 공격되는 성질을 이용하여 S_p에 오류가 주입되더라도 오류 확산 기법에 의해 S_q도 오류값을 가지도록 한 것이 특징이다.

따라서 소프트웨어 관점에서 오류주입 공격의 대응책은 오류가 주입되었을 때, 먼저 이를 탐지할 수 있는 기법이 필요하며 공격자가 비밀 정보를 추출할 수 없도록 정보를 숨길 수 있는 대응 기법 등을 고려하여 구현해야 할 것이다. 이때 대응 기법들은 다양화되고 정밀화된 공격에도 안전성을 보증할 수 있는 검증된 기법들을 사용해야 한다. 그러나 소프트웨어적인 대응책은 하드웨어적인 대응책에 비해 소요 시간은 많이 들지만 구현의 효율성 측면에서는 유리하다.

5. 결 론

본고에서는 정보보호용 암호 칩에 대한 해킹 기법 중 오류주입 공격에 대해서 설명하고 오류주입 공격에 대한 실험적인 분석 사례를 통해 동향을 분석해 보았다. 오류주입 공격은 암호 칩에 오류를 주입하는 형태에 따라 비침투 공격, 준침투 공격, 침투 공격으로 나누어지는데 공격자의 능력이나 칩 특성에 따라 다양한 시도가 있을 수 있다. 특히, 오류주입 공격은 암호 알고리듬의 이론적인 안전성과 상관없이 알고리듬이 구현된 환경의 취약점을 이용하므로 상당히 위협적이며 관련한 해킹 기술이 발전하고 있어 지속적인 연구가 필요하다. 즉, 앞으로 더 정밀한 계측 장비나 레이저 장비 등을 이용하여 칩에 대한 해킹 공격이 이루어질 가능성이 있기 때문에 현재 상용되고 있는 스마트카드나 암호용 칩에 대한 취약점을 보완하도록 해야 한다. 따라서 비밀키가 내장된 암호용 칩을 사용할 경우에는 오류주입 공격에 대비하여 하드웨어뿐만 아니라 소프트웨어 관점에서도 대응책을 마련해야 한다. 또한 오류주입 공격이 물리적 공격인 만큼 기본적으로 암호 칩에 대한 하드웨어의 안전성을 확보해야 하며, 오류가 주입되더라도 비밀 정보를 노출시키지 않도록 알고리듬적인 강도를 개선하는 기술이 요구된다.

참고문헌

[1] C. Kocher, "Timing attacks on Implementations of Diffie-Hellman, RSA, DSS, and other system", CRYPTO-96, LNCS, Vol. 1109, No. 1996, pp. 104 - 113, Springer-Verlag, 1996.

[2] C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", CRYPTO-99, LNCS Vol. 1666, No. 1999, pp. 388-397,

Springer-Verlag, 1999.

[3] D. Boneh, R. A. DeMillo and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," EUROCRYPT-1997, LNCS Vol. 1233, pp. 37-51, 1997.

[4] S. H. Weingart, "Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses," CHES-2000, LNCS, Vol. 1965, pp. 302-317, 2000.

[5] O. Kommerling, K. Gandolfi and F. Oliver, "Design principles for tamper-resistant smartcard processors," In Proceedings of the USENIX Workshop on Smartcard Technology, USENIX Association, pp. 9-20, 1999.

[6] J. BlÖmer, J. P. Seifert, "Fault based cryptanalysis of the Advanced Encryption Standard (AES)," In Financial Cryptography(FC-2003), LNCS vol. 2742, pp. 162-181, 2003.

[7] S. P. Skorobogatov, R. J. Anderson, "Optical Fault Induction Attacks," CHES-2002, LNCS, Vol. 2523, pp. 31-48, 2003.

[8] J. J.Quisquater, D. Samyde, "Eddy current for magnetic analysis with active sensor," In the proceedings of E-Smart 2002, Sept. 2002.

[9] S. Govindavajhala, A. Appel, "Using memory errors to attack a virtual machine," In Proceedings of the IEEE Symposium on Security and Privacy, pp. 154-164, 2003.

[10] J. Schmidt, M. Hutter, "Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results," In Proceedings of the Austrochip-07, Citeseer, 2007.

[11] C. H. Kim, J. J. Quisquater, "Fault Attacks for CRT Based RSA: New Attacks, New Results, and New Countermeasures," WISTP-2007, LNCS Vol. 4462, pp. 215-228, 2007.

[12] G. Piret, J. J. Quisquater, "A Differential Fault Attack Technique against SPN Structures, with Application to the AES and KHAZAD," CHES-2003, LNCS vol.2779, pp.77-88, 2003.

[13] C. H. Kim, J. J. Quisquater, "New Differential Fault Analysis on AES Key Schedule: Two Faults Are Enough," CARDIS-2008, LNCS vol. 5189, pp.48-60, 2008.

[14] S. M. Yen, S. J. Kim, S. G. Lim, S. J. Moon, "RSA speedup with residue number system Immune against hardware fault cryptanlysis," ICISC-2001, LNCS, Vol. 2288, pp. 397-413, Springer-Verlag, 2001.

[15] C. Giraud, "Fault resistant RSA im plementation," Fault Diagnosis and Tolerance in Cryptography, FDTC-2005, pp. 142-151, 2005.

[16] A. Boscher, R. Naciri, and E. Prouff, "RSA+CRT Algorithm Protected Against Fault Attacks," Workshop in Information Security Theory and practices, WISTP-2007, LNCS, Vol.4462, pp. 237-252, 2007.

[17] J. C. Ha, C. H. Jun, J. H. Park, S. J. Moon, "A New RSA+CRT Scheme Resistant to Power Analysis and Fault Attacks," ICCIT-2008, Vol. 2, pp. 351-365, IEEE-CS, 2008.

저자약력

백 이 루

2008년 8월 호서대학교 정보보호학과(학사)
2008년 9월~현재 호서대학교 정보보호학과 석사과정
관심분야 : 네트워크 보안, 프로토콜, 스마트 카드 보안
이 메 일 : blr83@nate.com

하 재 철

1989년 2월 경북대학교 전자공학과(학사)
1993년 8월 경북대학교 전자공학과(석사)
1998년 2월 경북대학교 전자공학과(박사)
1998년 3월~2006년 1월 나사렛대학교 전자계산소장, 학술정보관장, 입시학생처장
1998년 3월~2007년 2월 나사렛대학교 정보통신학과 부교수
2006년 7월~2006년 12월 QUT in Australia 연구 교수
2007년 3월~현재 호서대학교 정보보호학과 부교수
2002년 3월~현재 한국정보보호학회 이사, 논문지 편집위원
2009년 1월~현재 한국산학기술학회 이사
관심분야 : 암호학, 정보보호, 네트워크 보안, 스마트카드 보안
이 메 일 : jcha@hoseo.edu