보안 칩에서 중요 키의 공격(부채널 공격 중심) 기술 동향


최 두 호
한국전자통신연구원


최 용 제
한국전자통신연구원

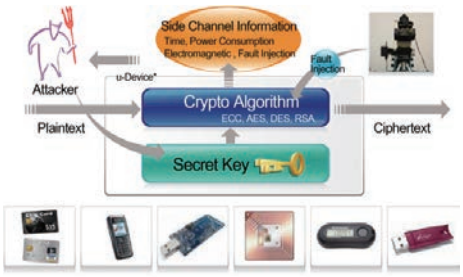
Ⅰ. 서 론

디바이스에 대한 물리적 취약점 공격은 디바이스의 물리적인 특성으로 기인하는 취약점을 이용한 디바이스내의 비밀 정보(패스워드나 암호키)를 해킹하는 공격이다. 물리적 취약점 공격은 비교적 많은 시간과 비용 및 전문적인 지식이 필요한 공격이기는 하나, 금융 디바이스나 보안 칩과 같은 높은 보안성이 요구되는 제품에서는 이러한 물리적 취약점들에 대한 고려와 대응이 필요하다. 실제 이러한 부채널 공격이라는 불리우는 물리적 취약점 공격을 통해, Chrysler, 대우, Fiat, GM, Honda, Toyota, Volvo, Volkswagen, Jaguar 등의 자동차 스마트키에 사용되는 KeeLoq(Microchip Tech. 社) 해킹[1]되거나, NXP社 Mifare Classic 부채널 분석을 통한 해킹을 통해 런던의 교통카드인 Oyster card를 및 출입통제 카드가 복제되었다[2].

디바이스의 다양한 물리적 취약점 공격 중 대표적인 공격은 부채널분석 공격이다.

Black Hat 2010에서 Infineon社 TMP칩에 대한 메모리의 마이크로프로빙에 의한 크랙킹 사례[3]가 발표되었으며, RSA 2012에서 인체부착 인슐린펌프 무선 조정 장치 해킹을 통해, 인슐린 펌프의 컨트롤 장악하는 치명적인 공격 가능성이 발표[4]되는 등 물리적 취약점 공격을 통한 디바이스 해킹 위협이 날로 늘어나고 있다.

다양한 물리적 취약점 공격 중 대표적인 공격이 부채널 공격(Side Channel Attack)이며, 부채널 공격은 디바이스내의 보안모듈이 구동되면서 발생하는 다양한 부채널 정보(Side Channel Information)로부터 보안모듈의 암호키를 크랙킹하는 공격이다. 부채널 공격은 1996년 P. Kocher의 시차분석공격(TA, timing attack)에 대한 연구를 발표하



〈그림 1〉 부채널 공격 개념

면서 시작되었으며[5], 공격에서 사용하는 대표적인 부채널 정보로는 보안모듈 구동 시간, 전력소모량, 전자파 신호, 오류에 대한 출력값 등이 있다.

본 고에서는 보안 칩 중요 키 공격 기술인 부채널 공격 기술 동향에 대하여 알아본다. 이를 위하여 2장에서는 부채널 공격 유형 및 특징에 대하여 살펴보고, 3장에서는 최근 부채널 공격 경향을 알 수 있는 사례에 대하여 기술하고, 마지막으로 4장에서 결론을 맺는다.

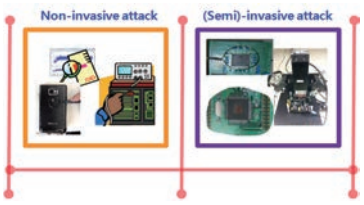
Ⅱ. 부채널 공격

1. 부채널 공격 정의

부채널 공격은 디바이스내의 보안모듈이 구동되면서 발생하는 다양한 누수정보(전력 소모, 전자기파, 오류 주입 결과 등)를 획득 및 가공, 분석하여 보안모듈의 암호키를 크랙킹하는 공격이다. 부채널 공격은 디바이스의 훼손 여부에 따라, 비침투형 공격(non-invasive attack)과 (준)침투형 공격((semi)-invasive attack) 두가지 유형으로 구분할 수 있다.

부채널분석 공격은 디바이스내에서 보안모듈이 구동되면서 발생하는 다양한 부가적인 누수정보를 이용하여 암호키를 크랙킹하는 공격이다.

대표적인 비침투형 공격 유형의 부채널 공격은 전력분석(Power Analysis), 비침투형 전자파분석



〈그림 2〉 부채널 공격 유형

〈표 1〉 공격자 능력에 따른 공격 모델 구분

공격 모델	설명
Black-box Attack	공격자는 연산이 일어나는 도중 연산 장치 내부의 정보를 관찰할 수 없고 알고리즘의 입력문과 출력문만 관찰할 수 있음. 본 모델에서의 대표적인 공격방법은 선택평문공격(CPA)와 선택암호문공격(CCA)가 있음. CPA는 공격자가 평문을 선택하면 그에 해당하는 암호문이 주어지고 CCA는 그와 반대로 공격자가 선택한 암호문에 대한 평문이 주어짐
Gray-box Attack	공격자가 block-box 모델에서 획득할 수 있는 정보에 부채널 정보까지 추가적으로 접근할 수 있는 모델임. Gray-box 모델에서 추가적으로 접근할 수 있는 부채널 정보는 연산 시간, 전력 소비량, 자기장 등이 있음. 따라서 Black-box 모델에서 안전한 알고리즘이 Gray-box 모델에서 안전함을 보장할 수 없음
White-box Attack	세가지 공격모델 중 공격자에게 가장 많은 능력을 부여하는 모델로서 gray-box 모델에서 획득할 수 있는 정보 이외에 소프트웨어의 실행시 연산이 이루어지는 장비 내부의 모든 계산과정을 관찰하는 것과 메모리에 대한 접근과 변경이 허용

(Electromagnetic Analysis) 공격이 있으며, (준)침투형 공격 유형의 부채널 공격의 대표적인 공격은 레이저 오류주입(Fault Injection) 공격이 있다. 디바이스에 오류를 주입하는 방법은 전압을 갑자기 떨어뜨리거나, 올리는 전압가변 방식, 디바이스의 동작주파수에 변화를 주는 클럭가변 방식, 레이저 오류주입 방식, 강한 EM 방사를 통해 오류를 주입하는 방식 등이 있다. 이 중, 전압이나 클럭가변 방식의 오류주입은 비침투형 공격 유형에 해당할 수 있다. 암호에 대한 공격자의 능력에 따른 공격 모델을 구분하면, 〈표 1〉과 같이 Black-box Attack, Gray-box Attack, White-box Attack 모델로 나눌 있으며, 부채널 공격은 Gray-box Attack 모델에 해당한다.

2. 전력/전자파 분석 공격

부채널 공격 중 가장 대표적인 공격인 전력분석 공격은 1999년 P. Kocher에 의해 DES가 공격된 이후[6], 지난 10여 년간 현대 암호시스템을 위협하는 가장 강력한 공격 수단으로 연구되어 왔다.

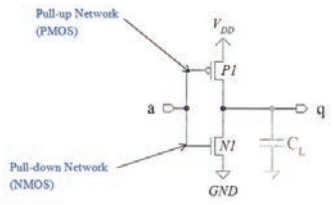
가) 전력/전자파 분석 공격

전력/전자파 분석 공격은 DES 암호 뿐 아니라, AES, ARIA, SEED, RSA, ECC 등 거의 모든 암호 알고리즘에

적용되고 있다. 따라서, 부채널 공격 대응 방법이 강구되지 않은 보안 디바이스의 대부분이 전력/전자파 분석 공격에 취약할 수 있으며, 저가의 오실로스코프 정도의 공격 환경으로도 실현할 수 있기 때문에 향후 공격 대상은 스마트폰 등과 같은 스마트 디바이스로 확대될 것을 예측되고 있다. 전력/전자파 분석 공격에는 대표적으로 단순 전력/전자파 분석 공격(SPA, SEMA)와 차분 전력/전자파 분석 공격(DPA, DEMA)가 있다. 전자파 분석 공격은 2001년 Quisquater 등이 처음 제안한 공격 방법으로써 디바이스의 전자파 방사를 측정하여 암호키를 해킹하는 공격이다[7]. 디바이스에서 누출되는 EM 방사는 다음과 같이 크게 두 가지로 분류할 수 있다.

- 직접방사(Direct Emanations): 회로 내부에서의 의도적인 전류 흐름에 기인하며, 신호 선로의 불연속 구간(예를 들어, 평판 회로에서 신호 전송 선로가 급격히 굽혀진 상태 등)에서 전류 흐름의 불연속을 야기하여 넓은 대역의 주파수에 걸쳐 회로 외부로 EM 신호가 방출됨. 낮은 주파수 대역에서는 노이즈 및 간섭이 강하므로 오히려 높은 주파수 신호는 공격자에게 상당히 유용하게 이용될 수 있음. 복잡한 회로에서는 다른 신호와의 간섭으로 인하여 이러한 지접적인 EM 누출을 방지하는 것은 상당히 어려움. 누출된 EM 신호를 획득하기 위해서는 신호원에 아주 근접하여 소형의 필드 프로브를 사용해야 하며 원하는 신호를 추출하기 위한 특수 필터를 사용할 필요도 있음
- 비의도적 방사(Unintentional Emanations): 복잡하고 소형회된 CMOS 디바이스는 서로 근접해 있는 회로 요소 간에 전기적 또는 전자기적 커플링을 야기함. 이러한 EM 방사는 디바이스 내부에서 발생 또는 제공되는 캐리어 신호들의 변조 형태로 나타남. 전형적인 캐리어 신호는 조화 함수 형태의 클럭 신호를 담고 있으며, 내 · 외부적으로 통신에 이용됨. 커플링의 형태에 따라서 AM, FM 또는 그 밖의 복잡한 형태의 변조로 분류됨. 만약 이러한 변조된 캐리어 신호가 추출되면, 캐리어 주파수에 동조된 수신기와 적절한 복조 과정을 거쳐 정보신호가 복구될 수 있음

부채널분석 중 대표적인 전력/전자파 공격은 연산장치의 비트가 스위치되면서 발생하는 동적전력소모량이 비트변화(해밍디스턴스)와 연관이 있음에 기인한다.



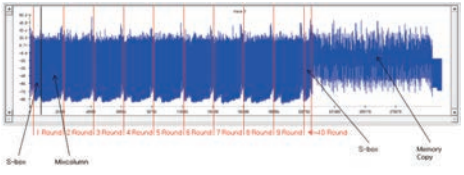
〈그림 3〉 CMOS 인버터 회로

나) 전력/전자파 분석 공격 원리

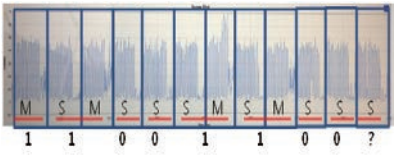
CMOS 공정에 의해 만들어진 연산 장치의 전력 소모는 정적 소모량과 동적 소모량의 합으로 생각할 수 있으며, 이 중 전력 소모의 지배적인 부분은 동적 전력 소모량이다. 이러한 전력 소모의 대부분인 동적 전력 소모는 "1 → 0", "0 → 1"로 변환되면서 발생하며, 연산 장치의 연산 시 발생하는 전력 소모는 연산의 출력값의 변환된 "1" 값들의 합(해밍무게)에 비례하게 된다. 이에 따라, 공격자는 암호의 부분키를 예측하고 이로부터 계산되는 암호의 중간 연산값을 해밍무게 값을 이용하여 예측한 부분키가 사용되었을 때의 전력 소모 모델을 예측한다. 부채널 공격은 실제 소모된 전력량을 측정한 후 통계적 처리를 통하여 공격자의 전력 소모 모델이 실제 전력 소모량과 유사한지를 비교하여 실제 사용된 부분키를 예측한다.

전력/전자파 분석 공격은 수집 파형 및 분석 기법에 따라 단순 전력/전자파 분석과 차분 전력/전자파 분석 등으

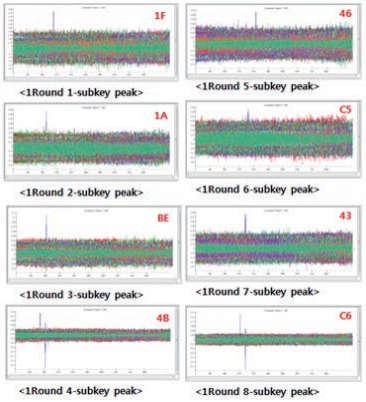
〈그림 4〉 단순 전력/전자파 분석 공격 대상 내부함수 형태



〈그림 5〉 AES 암호 연산시 발생하는 전력 소모 패턴 구분



〈그림 6〉 RSA 전력 소모 패턴 구분에 의한 비밀키 누출



〈그림 7〉 SEED 암호에 대한 차분 전력 분석 공격 결과

로 구분할 수 있다. 단순 전력/전자파 분석은 통계적 수단을 이용하지 않고, 암호모듈의 전력 소모량을 관찰한 후, 패턴을 특징을 이용하여 암호모듈의 중간 함수들을 구분하여 비밀 정보를 추정하는 공격 방법이다. 〈그림 4〉와 같이 내부함수들이 연산될 경우, 소모되는 전력량이 다르기 때문에, 전력 소모량은 내부함수 종류에 따라 서로 다른 패턴을 띄게 될 것이고 이를 관찰할 수 있게 된다. 실제 AES 비밀키 암호와 같은 경우 〈그림 5〉와 같이 라운드 연산 구분이 가능하며(키를 바로 확인할 수는 없음), RSA와 같은 공개키 암호와 같은 경우 〈그림 6〉과 같이 하나의 전력 패턴으로 비밀키 추출이 가능할 수도 있다.

차분 전력/전자파 분석은 암호모듈의 모든 가능한 부분키에 대한 암호연산 중간값의 전력 소모 모델을 제시하고, 제시된 전력 소모모델과 실제 측정된 전력 소모량을 통계적인 기법으로 비교하여 가장 높은 유사도가 있는 전력 소모모델의 부분키를 실제 암호모듈의 부분키로 예측하는 공격이다. 이러한 통계적인 기법에 의한 가장 높은 유사도가 나온 부분키에 대해서는 〈그림 7〉에서와 같은 다른 비교 파형과 확연히 구분되는 피크 형태의 비교 파형을 통해 부분키 공격이 가능하다.

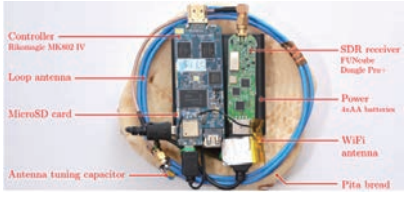
최근 부채널 공격은 비침투/원거리 (전자파,소리 등)에서 PC나 노트북 등 일반 컴퓨터급을 대상으로 해킹형 공격으로 진화하고 있다.

Ⅲ. 부채널 공격 최근 사례

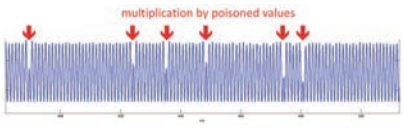
본 장에서는 최근 부채널 공격이 전자파 , 소리 등과 같은 비침투형 공격 중심으로, 공격대상도 스마트카드 등 자원 제약적 디바이스에서 노트북, PC 등 계산 자원이 풍부한 디바이스로 옮겨가고 있을 시사하는 두 가지 연구결과 사례를 살펴보고, 마지막으로 실제 학계에서 논문상으로 제안하는 물리적 공격 가능성들이 얼마나 빠르게 실제 범죄 등에 악용될 수 있는지를 보여주는 사례에 대해 살펴보고자 한다.

1. PC에 대한 전자파 부채널 공격

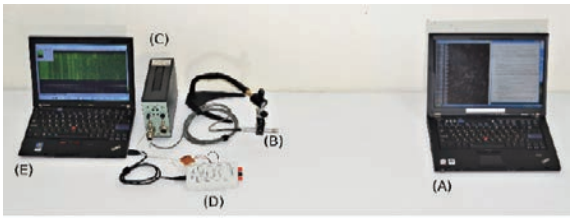
이스라엘 Tel Aviv 대학에서는 피타 브레드(Pita Bread)모양의 장치(〈그림 8〉)를 이용하여 컴퓨터에 저장된 암호화 키를 훔쳐낼 수 있는 빠르고 저렴한 방법을 고안했다고 밝혔다[8]. 발표된 논문에서는 피타 브레드 장치를 컴퓨터로부터 전자파 부채널 신호를 수집하여 암호키를 분석한다. PITA(Portable Instrument for Trace Acquisition) 장치는 루프 안테나로 덮지 않은 구리와 암호화 키 정보를 유출할 수 있는 1.7MHz 범위의 주파수를 엿들을 수 있도록 설계된 커패시터로 구성돼 있으며, 대략 50cm 떨어져 전자기적 신



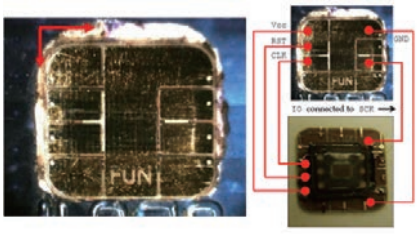
〈그림 8〉 피타 브레드 파형 수집 장치[8]



〈그림 9〉 RSA 연산 구분을 통한 키 추출[8]



〈그림 10〉 소리를 통한 공격 시스템 구성[9]



〈그림 11〉 범죄에 사용된 변형된 도난카드[10]

호를 모은다. 논문에서는 RSA와 엘가말(Elgamal) 키 암호화 알고리즘을 사용하는 오픈소스 암호화 프로그램인 GnuPG 1.x를 구동하는 노트북에서 신호를 수집하여 키를 추출하였으며, 내장 마이크로 SD카드에 수집된 신호를 토대로 오프라인 분석으로 수 초 만에 암호화 키를 추출하였다. 또한 로드 마스터(Road Master)라고 불리는 상업용 라디오 리시버를 사용하여 동일한 키 추출이 가능함을 보였다. 라디오 리시버 신호는 HTC 에보(EVO) 4G 스마트폰의 마이크 입력에 연결하여 저장한다.

2. 소리를 통한 부채널 공격 사례

이스라엘 Tel Aviv 대학과 Weizmann 대학에서는 소리를 이용하여서도 PC에 대한 부채널 공격이 가능함을 보였다[9]. 논문에서는 〈그림 10〉과 같이 마이크로 전달되는 신호를 이용하여 부채널 분석을 수행한다.

RSA 알고리즘이 구동중인 (A)공격 대상 PC의 프로세서 소리를 (B)수집용 마이크로 수집하며, (D)주파수 필터를 통해 분석에 필요한 소리만 필터링한다. 필터링 된 소리를 (E)공격용 PC에서 분석을 수행하여 RSA 비밀키 분석한다. 이는 부채널 분석 원리와 동일하게 RSA 비밀키의 '0'과 '1'의 차이에 의한 프로세서 사용 증가로 전력소모량 증가하며, CPU의 전력소모량 증가로 CPU가 동작하는 소리의 특성이 변화한다. CPU 소리의 변화를 파형으로 저장하여 평문과의 비교하여 곱셈, 덧셈 등 RSA의 비밀키와 관련된 연산을 식별하며, 식별된 연산 정보를 이용하여 비밀키 획득하게 된다. 논문에서는 스마트폰에서도 분석 툴 설치 및 분석이 가능하다고 주장하였다.

디바이스에 대한 실험실레벨의 물리적 공격 분석이 실제 사이버 범죄 등에 활용되는 기간이 빨라지고 있으며, 이러한 취약성 공격 대응을 고려하는 하는 것은 필수사항이 되고 있다.

3. 학계 연구결과가 범죄에 악용된 사례

2016년 C에 발표된 2011년 5월 프랑스에서 발생한 신용카드 도난 사건 및 도난 신용카드를 사용한 범죄사건이 있어났으며, 이 도난카드에 대한 범죄 포렌식 분석을 한 결과가 Cryptographic Engineering 저널에 2016년 4월 발표되었다[10]. 본 범죄에서 유출한 도난 신용카드를 이용하여 대량의 상품을 구입하였는데, 본 포렌식 분석의 주안점은 도난 IC카드에서 PIN 코드 입력부분을 어떻게 우회하였는지를 밝히는 것이었다.

〈그림 11〉와 같이 실제 도난카드의 칩 위에 또 다른 IC카드 덮붙여서 실제 중간자 공격을 통한 PIN 코드 위회를 수행하도록 한 것이다. 더욱 놀라운 사실은 본 중간자를 통한 PIN 코드 우회 공격은 본 범죄 발생 이전해인 2010년 IEEE Symposium on Security and Privacy 학회에서 본 공격이 가능함을 겨우 실험실에서 FPGA를 이용하여 입증[11]한 공격이라는 것이다. 이러한 학계의 연구결과가 발표된지 불과 1년 후에, 이 기법을 사용하여 실제 범죄에 이용하였다는 사실은 시사해주는 바가 크다고 할 수 있다.

Ⅳ. 결 론

디바이스에 대한 부채널 공격은 디바이스가 암호모듈을 구동하는 동안 발생하는 다양한 부가정보를 활용하여 암호키를 크랙킹하는 공격이다. 1990년대 후반에 이러한 부채널 공격이 발견된 이후, 스마트카드 업계를 중심으로 그 심각성을 반영하여 제품 개발 시, 부채널 공격에 대한 검증과 대응을 하고 있다. 그럼에도 불구하고, 다양

한 부채널 취약점을 통한 부채널 공격에 대한 사례가 발생하고 있는 실정이다. 특히, 사물인터넷 서비스 환경이 확대됨에 따라, 부채널 등 물리적 공격에 대한 우려도 커지고 있다고 할 수 있다. 본고에서는 부채널 공격 개념과 종류, 공격 동향 등을 설명하고, 두가지 최근 부채널 공격 동향을 살펴보았다. 본 두 가지 공격 사례가 시사하는 바는, (1) 부채널 공격의 대상이 IC카드 등 단순한 디바이스에서 점점 일상적인 시스템(PC나 노트북 등)으로 확대되고 있으며, (2) 사용한 부채널 정보가 전자파, 소리 등 (원거리)무선으로 수집이 가능한 정보를 활용함으로써, 공격 대상을 파괴하지 않는 비침투 공격으로 전개되고 있다는 사실이다. 이를 통해, 점점 부채널 공격은 전문가적인 보안검증 수준에서 실제 해커의 공격 수준으로 발전하고 있다는 것을 알 수 있다. 또한, 학계 실험실 수준의 공격 입증 결과가 얼마나 빨리 실제 범죄에 악용될 수 있는지를 보여주는 극단적인 사례를 살펴보았다.

보안칩은 점점 디바이스를 구성하는 필수 불가결한 요소로써 다루어지고 있으면, 이런한 보안칩 또는 보안 하드웨어에 대한 부채널 공격 등과 같은 물리적 공격은 이제 보안성 검증 또는 실험실 상에서의 위협 가능성만을 의미하는 것이 아닌 실제 해킹 등 범죄에 악용될 수 있는 치명적인 공격이 될 수 있음을 인지하고, 보안칩 설계 및 개발 시, 이에 대한 다양한 검토 및 대응이 필수적으로 고려되어야 한다.

참고문헌

[1] KeeLoq, by Wikipedia, http://en.wikipedia.org/wiki/KeeLoq

[2] Why being open about security makes us all safer in the long run, Bruce Schneier, The Guardian, Aug. 2008, http://www.guardian.co.uk/technology/2008/aug/07/hacking.security

[3] "Unhackable" Infineon Chip Physically Cracked, Fox Business, Feb. 2010, http://www.foxbusiness.com/personal-finance/2010/02/11/unhackable-infineon-chip-physically-cracked/

[4] Hacker Shows Off Lethal Attack By Controlling Wireless Medical Device, Bloomberg, Feb. 2012, http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/

[5] Timing Attack on Implementation of Diffie-Hellman, RSA, DSS and other Systems, P. Kocher

[6] Differential Power Analysis, P. Kocher, J. Jaffe, B. Jun, Crypto'99, LNCS 1666, 1999

[7] ElectroMagnetic Analysis(EMA): Measures and Countermeasures for Smart Cards, J. Quisquater, D. Samyde, E-smart 2001, LNCS 2140, 2001

[8] Daniel Genkin, Itamar Pipman, Eran Tromer, Get your hands off my laptop: physical side-channel key-extraction attacks on PCs, proc. Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2014, LNCS 8731, 242-260, Springer, 2014

[9] Daniel Genkin, Adi Shamir, Eran Tromer, RSA key extraction via low-bandwidth acoustic cryptanalysis, proc. CRYPTO 2014, part I, LNCS 8616, 444-461, 2014

[10] Houda Ferradi, Remi Geraud, David Naccache, Assia Tria, When organized crime applies academic results: a forensic analysis of an in-card listening device, Journal of Cryptographic Engineering, Volume 6, Issue 1, pp 49-59, April 2016

[11] Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond, Chip and PIN is Broken, proc. 2010 IEEE Symposium on Security and Privacy, pp. 433-446, May 2010

최 두 호

• 1994년 2월 성균관대학교 수학과 졸업
• 1996년 2월 KAIST 수학과 석사
• 2002년 2월 KAIST 수학과 박사
• 2002년 1월~현재 한국전자통신연구원 실장/책임연구원
• 2009년 3월~현재 한국과학기술연합대학원대학교(UST) 교수

〈관심분야〉
암호엔지니어링(부채널분석, 암호 구현, 키관리)

최 용 제

• 1996년 8월 전남대학교 전자공학과 졸업
• 1999년 2월 전남대학교 전자공학과 석사
• 1999년 2월~8월 전남대학교 전자통신연구소 인턴연구원
• 1999년 8월~현재 한국전자통신연구원 책임연구원

〈관심분야〉
보안 프로세서 하드웨어 설계, 부채널 분석 시스템