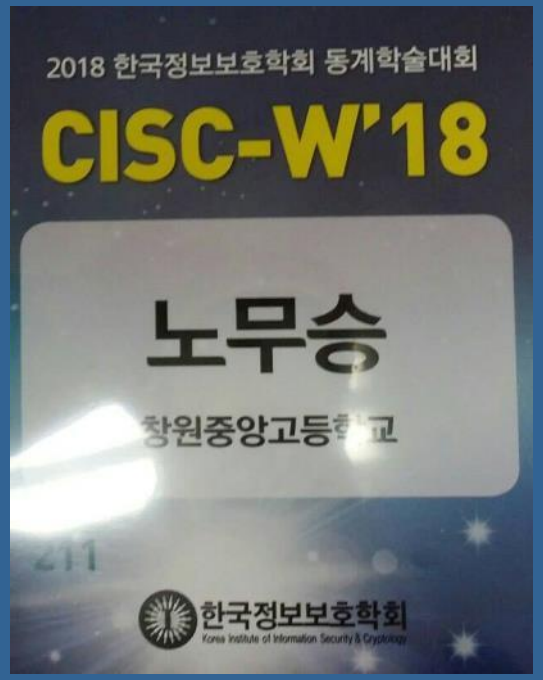
RFID 카드 해킹

중부대 SCP 정보보안 동아리

92113566 1학년 부원 노무승

2018 한국정보보호학회 논문



2019 제19회 POC 동계 해킹캠프

2019 Codegate Junior 세션

+ 추가 연구

Federal Law provides severe civil and criminal penalties for the unauthorized reproduction, distribution, or exhibition of copyrighted motion pictures (Title 17, United States Code, Sections 501 and 508). The Federal Bureau of Investigation investigates allegations of criminal copyright infringement (Title 17, United States Code, Section 506).

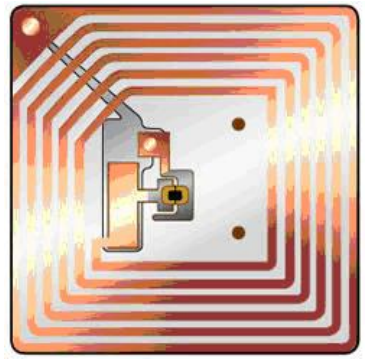
본 발표에서 다루는 내용을
불법적인 목적으로 사용하다 적발 시
모든 책임은 본인에게 있습니다.

목차

1. 이론적 배경

1-1. RFID카드?

출처. S-RFID



RFID카드:

저장된 데이터를 무선주파수를 이용하여 비접촉으로 읽는 카드

1-1. RFID 카드?

1-2. RFID 해킹 도구 (1)

※ Proxmark3 Easy

RFID 태그를 해킹하여
데이터 변조, 복제 등 가능함.

Proxmark3 Easy 2018 512M Kit
기준 13만원 (2018 때 가격임)

지원 모델: 125Khz, 134kHz, **13.56Mhz**

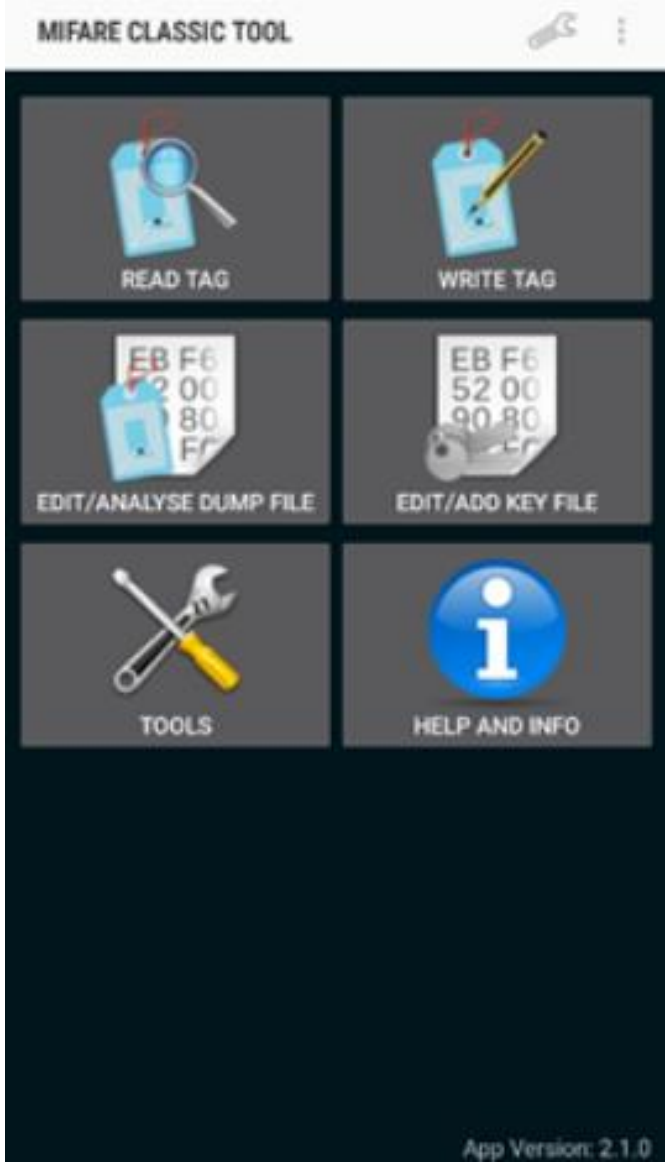
Tags	Recognize	Read& Write	Advanced Operation					
			Offline Decryption	Online Sniffing	Default Key Crack	Data Dump	Simulation	Copy
MIFARE CLASSIC	✓	✓	✓	✓	✓	✗	✓	✓
MAFARE CLASSIC (CHINESE Magic Card/UID)	✓	✓	✗	✓	✓	✓	✗	✓
MAFARE Ultralight	✓	✓	✗	✗	✗	✓	✗	✗
HID	✓	✓	✗	✗	✗	✗	✓	✓
HID iClass	✓	✓	✓	✓	✗	✓	✓	✓
ISO14443a	✓	✓	✗	✓	✗	✓	✓	✓
ISO14443b	✓	✓	✗	✓	✗	✗	✓	✓
ISO15693	✓	✓	✗	✓	✗	✓	✓	✓
SRI512	✓	✓	✗	✗	✗	✗	✓	✗
SRIX4K	✓	✓	✗	✗	✗	✗	✓	✗
Legic	✓	✓	✗	✗	✗	✓	✓	✗
epa	✓	✓	✗	✗	✗	✗	✗	✗
em410X	✓	✓	✗	✗	✗	✗	✓	✓
Em4x50	✓	✓	✗	✗	✗	✓	✓	✓
Ti	✓	✓	✗	✗	✗	✗	✗	✗
Hitag/Hitag2	✓	✓	✗	✓	✗	✗	✓	✗
indala	✓	✓	✗	✗	✗	✗	✗	✓
T55xx	✓	✓	✗	✗	✗	✗	✗	✓
FlexPass	✓	✓	✗	✗	✗	✗	✗	✗
VeriChip	✓	✓	✗	✗	✗	✗	✗	✗
PCF7931	✓	✓	✗	✗	✗	✗	✗	✗
Kantech ioProx	✓	✓	✗	✗	✗	✗	✗	✗

1-3. RFID 해킹 도구 (2)

※ MCT(Mifare Classic Tool)

Mifare Classic 카드를 R/W 할 수 있는 어플.

대신 Key 해킹은 불가능하며,
사전 기반 브루트포싱을 통해 Key를 알아낼 수 있음.



1-3. RFID 해킹 도구 (3)

※ 아두이노 + RC522모듈

Mifare Classic 카드를 R/W 하고
Code 레벨에서 제어 할 수 있음.

마찬가지로 Key 해킹은 불가능하며,
사전 기반 브루트포싱을 통해 Key를 알아낼 수 있음.

1-4. Mifare Classic 카드란?

취약하다!

보안 특징

1. UID는 기본적으로 읽기만 가능

2. 태그와 리더 사이에 Key로 인증

3. Crypto1 암호화 알고리즘 사용

네덜란드 NXP반도체의 RF 기술이며, 이용하는 주파수는 13.56MHz 이다.
수 년 동안 3억~5억 장이 발행되었으며, 현재 2억장 이상이 사용되고 있다.

1-5. 대표적인 Mifare Classic 공격 방식

1. Default Key Attack
   기본적으로 많이 사용하는 Key를 이용하여 공격 가능.

2. Nested Attack
   LFSR의 난수 생성 알고리즘의 동작 원리를 응용한 공격 기법이다.
   하나의 키를 알아내면, 다른 키를 모두 알아 낼 수 있음.

3. Brute Force Attack
   기본적으로 하나의 키는 6byte에 불과함으로
   무차별 대입 공격이 먹히게 됨.

...

1-6. Mifare Classic UID Changeable Card

UID를 포함한 다른 데이터 영역에 모두 쓰기 가능한 카드

1-7. Mifare Classic 1k 구조

BLOCK	Byte Number within a Block																Description
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
63	Key A						Access Bits				Key B						Sector Trailer
62																	Data
61																	Data
60																	Data
59	Key A						Access Bits				Key B						Sector Trailer
58																	Data
57																	Data
56																	Data
⋮																	
7	Key A						Access Bits				Key B						Sector Trailer
6																	Data
5																	Data
4																	Data
3	Key A						Access Bits				Key B						Sector Trailer
2																	Data
1																	Data
0																	Manufacture Blcok*

0~63 블록, 총 64개의 블록.

1개의 블록 당 16byte로,
총 1024byte임.

1-7. Mifare Classic 1k 구조

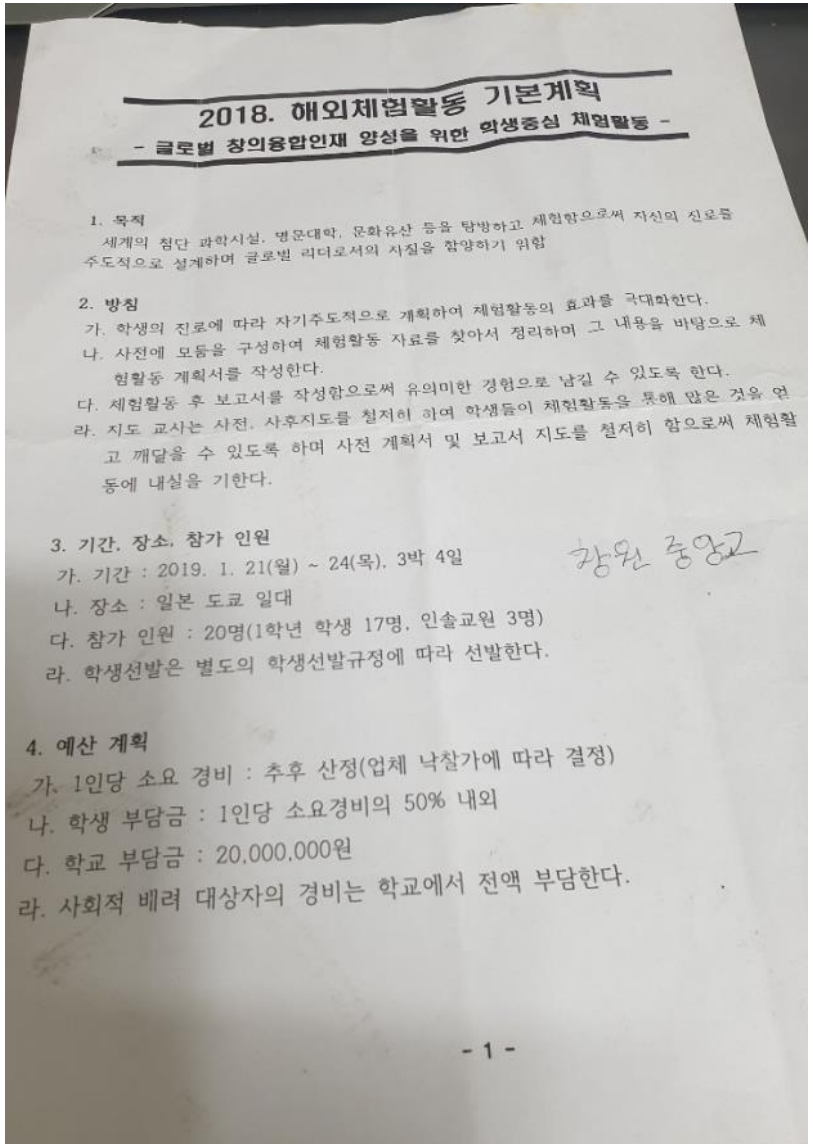
BLOCK	Byte Number within a Block																Description
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
63	Key A						Access Bits				Key B						Sector Trailer
62																	Data
61																	Data
60																	Data
59	Key A						Access Bits				Key B						Sector Trailer
58																	Data
57																	Data
56																	Data
⋮																	
7	Key A						Access Bits				Key B						Sector Trailer
6																	Data
5																	Data
4																	Data
3	Key A						Access Bits				Key B						Sector Trailer
2																	Data
1																	Data
0																	Manufacture Blcok*

4개의 블록 당 1개의 섹터로,
섹터의 마지막 블록은 해당 섹터의
키 정보를 담고 있음.

따라서 총 16개의
Key A와 Key B가 존재함.

2. 카드 복제 실습

2-1. 호텔 도어락 카드 복제 시연



2018. 해외체험활동 기본계획

- 글로벌 창의융합인재 양성을 위한 학생중심 체험활동 -

1. 목적

세계의 첨단 과학시설, 명문대학, 문화유산 등을 탐방하고 체험함으로써 자신의 진로를 주도적으로 설계하며 글로벌 리더로서의 자질을 함양하기 위함

2. 방침

가. 학생의 진로에 따라 자기주도적으로 계획하여 체험활동의 효과를 극대화한다.

나. 사전에 모둠을 구성하여 체험활동 자료를 찾아서 정리하며 그 내용을 바탕으로 체험활동 계획서를 작성한다.

다. 체험활동 후 보고서를 작성함으로써 유의미한 경험으로 남길 수 있도록 한다.

라. 지도 교사는 사전, 사후지도를 철저히 하여 학생들이 체험활동을 통해 많은 것을 얻고 깨달을 수 있도록 하며 사전 계획서 및 보고서 지도를 철저히 함으로써 체험활동에 내실을 기한다.

3. 기간, 장소, 참가 인원

가. 기간 : 2019. 1. 21(월) ~ 24(목), 3박 4일

나. 장소 : 일본 도쿄 일대

다. 참가 인원 : 20명(1학년 학생 17명, 인솔교원 3명)

라. 학생선발은 별도의 학생선발규정에 따라 선발한다.

창원중앙고

4. 예산 계획

가. 1인당 소요 경비 : 추후 산정(업체 낙찰가에 따라 결정)

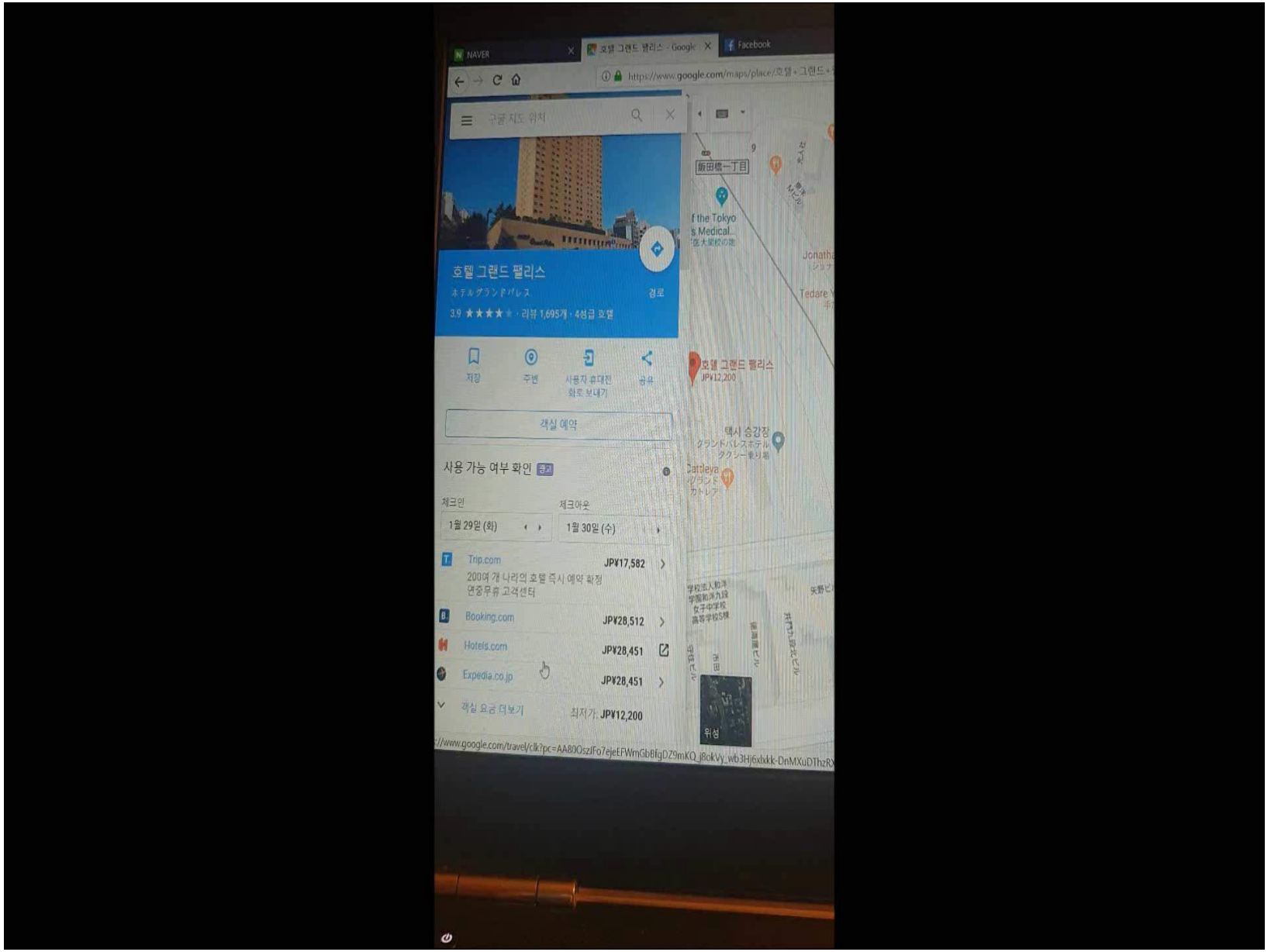
나. 학생 부담금 : 1인당 소요경비의 50% 내외

다. 학교 부담금 : 20,000,000원

라. 사회적 배려 대상자의 경비는 학교에서 전액 부담한다.

- 1 -

2-1. 호텔 도어락 카드 복제 시연

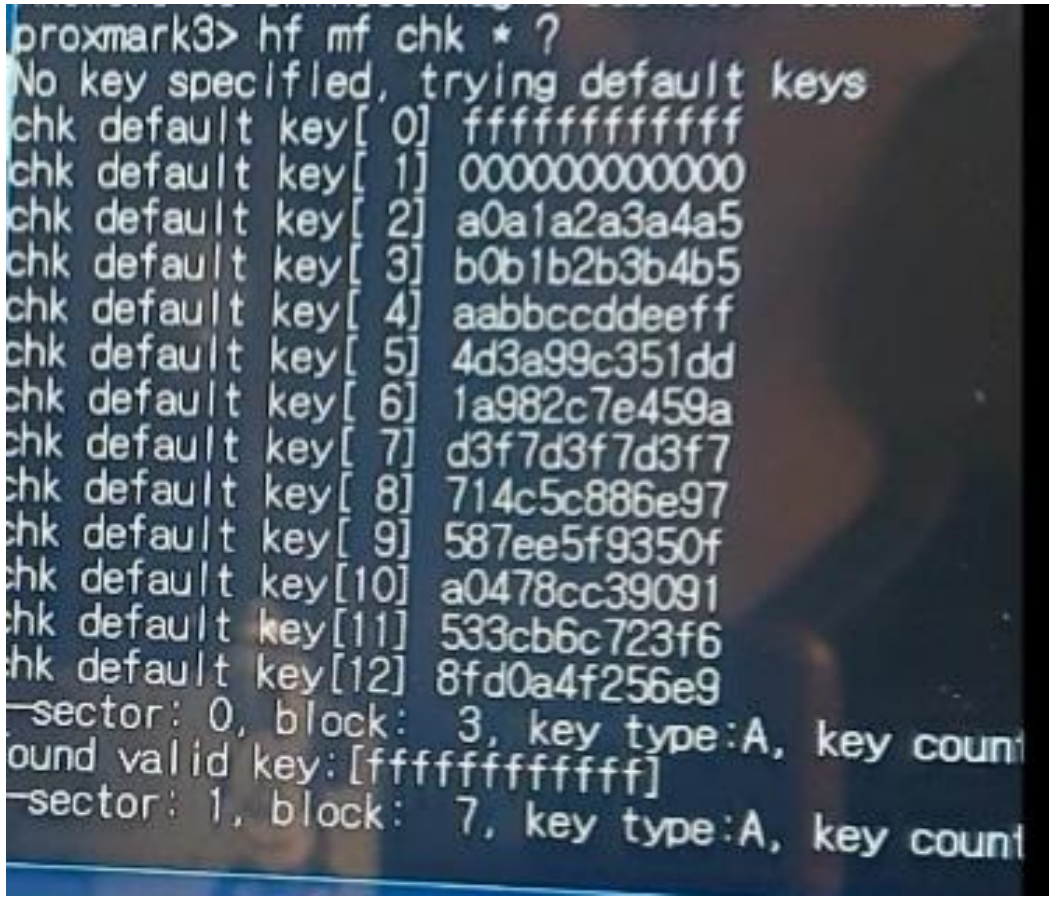


2-2. 실제 아파트 도어락 카드 복제 시연

2-3. RFID 복제 과정 (1)

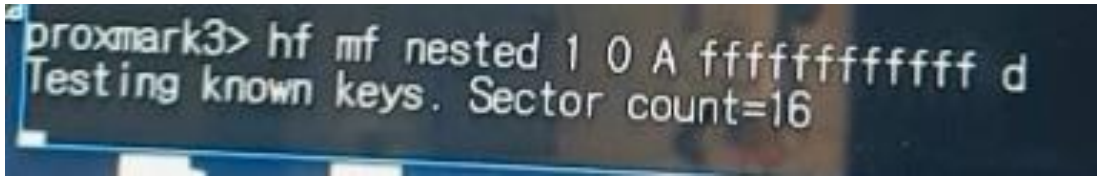
어떤 카드 종류인지 확인하여
취약한 카드인지 살펴보는 것이 우선.

2-3. RFID 복제 과정 (2)

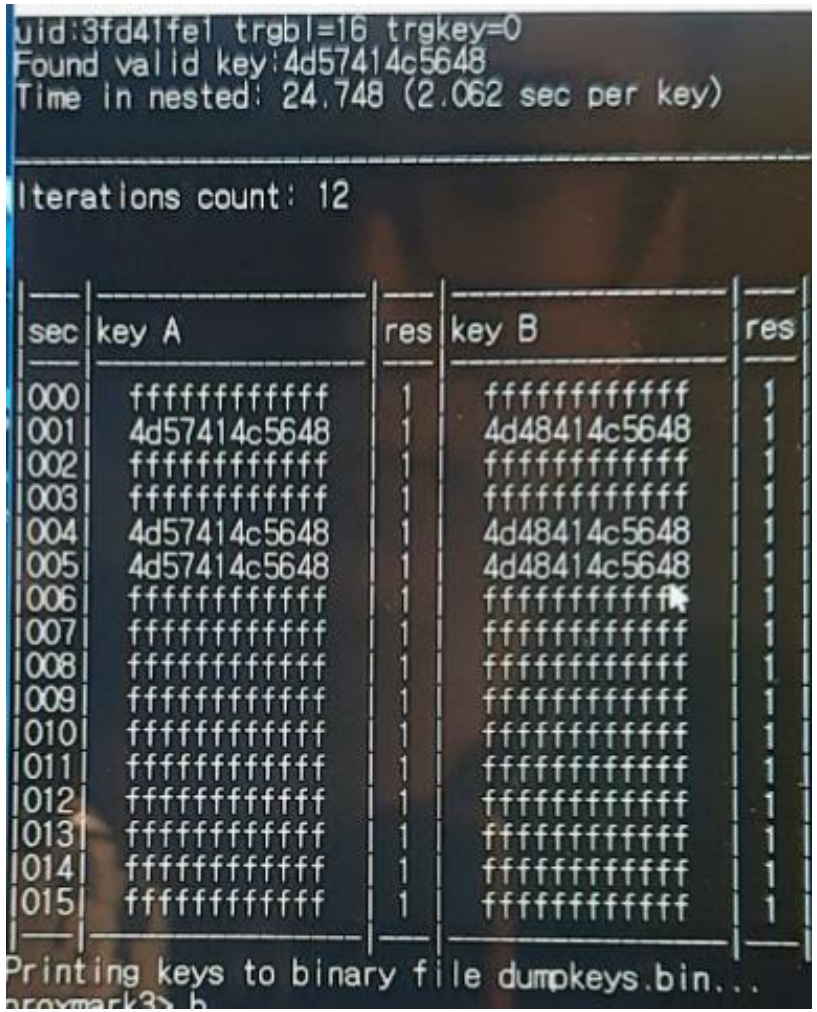


Default Key Attack으로 Key 1개 이상을 알아냄.

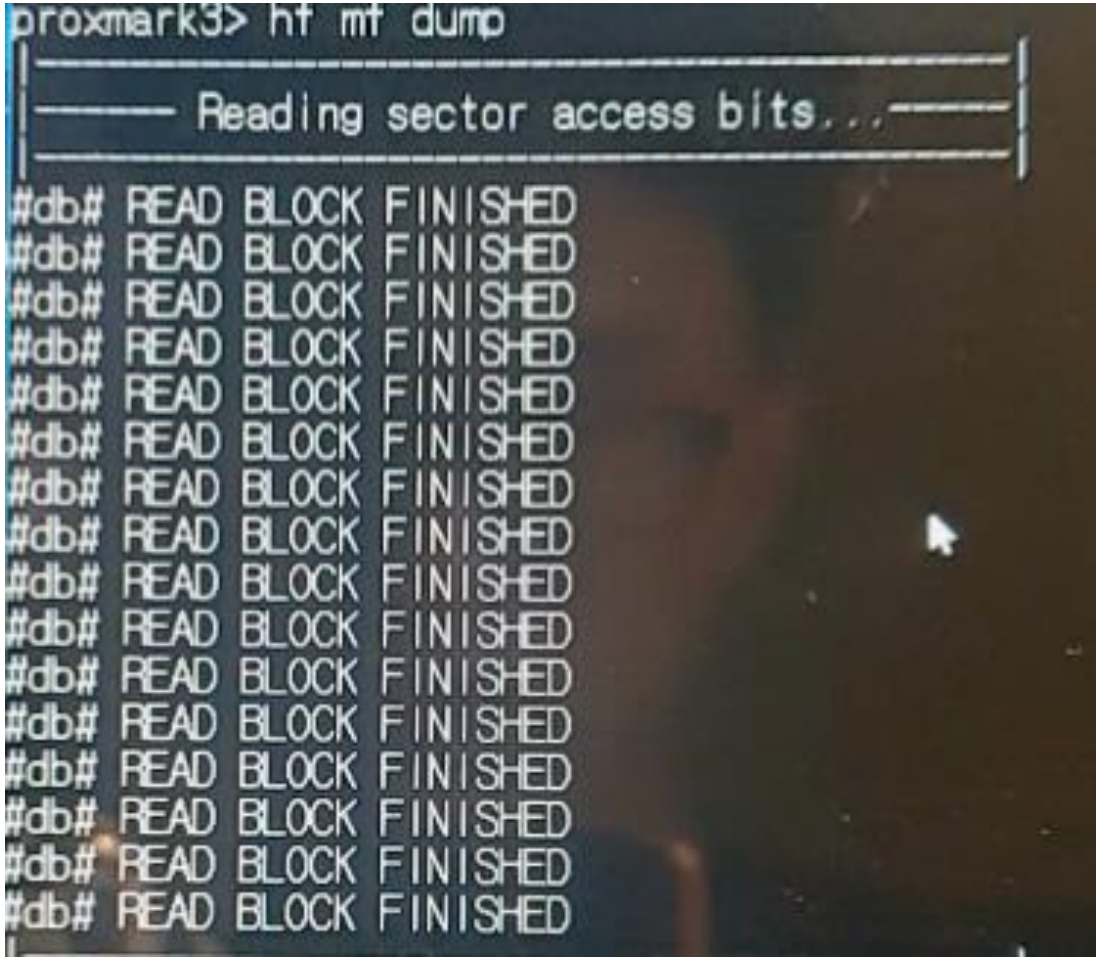
2-3. RFID 복제 과정 (1)



Nested Attack을 가해
모든 블록의 Key를 구함.



2-3. RFID 복제 과정 (1)



알아낸 Key List를 이용하여 각 블록의 데이터를 읽어옴.

4. 대비 방안

4-1. 대비방안

Q & A

감사합니다