Evaluation of the feasible attacks against RFID tags for access control systems

Hristo Dimitrov & Kim van Erkelens
University of Amsterdam

February 4, 2014

Contents

1. Introduction
2. Background
3. Methods
4. Findings
5. Conclusion

RFID and access control systems

- Proximity Integrated Circuit Card (PICC)

Research questions

Main question

What should one focus on when performing a security testing of an implementation of an RFID access control system?

Subquestions

1. Which are the known attacks against the tags for various implementations of RFID access control systems?
2. How feasible are those attacks and what kind of threat do they introduce?
3. What is the applicability of these attacks for different types of systems?

Related work

Previous Research

- Known attacks against RFID systems: *Classification of RFID attacks*
- Practical attacks against RFID systems
- *A Framework for Assessing RFID System Security and Privacy Risks*

Our contribution

- Test and give an overview of the known attacks
- Advice about a practical approach for assessments

Experimental setup

System	Description	Supported tag types
A	External Company 1	MIFARE Classic
B	External Company 2	HID
C	Demo Kit 1	MIFARE Classic and DESFire
D	Demo Kit 2	EM410x

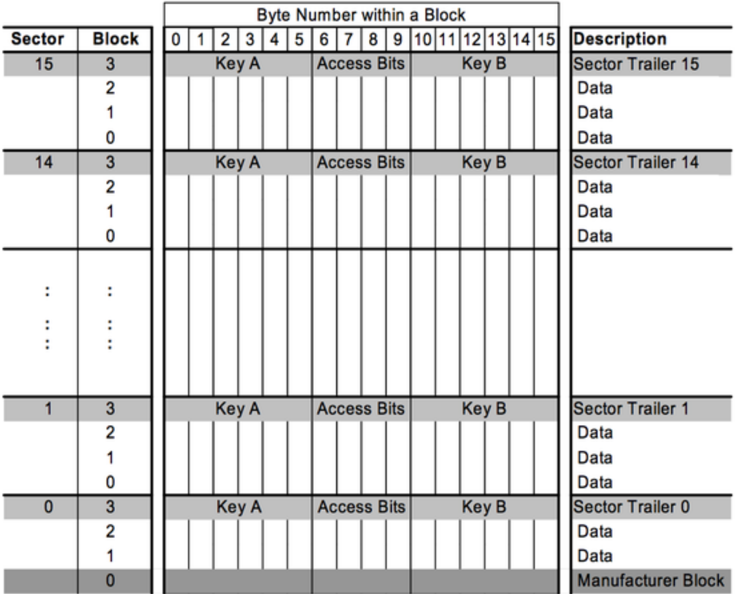
Low Frequency (120 - 150 kHz)

- HID (ProxCard II)
- EM410x

High Frequency (13.56 MHz)

- MIFARE Classic
- MIFARE DESFire
- MIFARE UltraLight

Sector layout of MIFARE Classic 1K



		Byte Number within a Block																
Sector	**Block**	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	**Description**
15	3	Key A						Access Bits				Key B						Sector Trailer 15
	2																	Data
	1																	Data
	0																	Data
14	3	Key A						Access Bits				Key B						Sector Trailer 14
	2																	Data
	1																	Data
	0																	Data
: : :	: : :																	
1	3	Key A						Access Bits				Key B						Sector Trailer 1
	2																	Data
	1																	Data
	0																	Data
0	3	Key A						Access Bits				Key B						Sector Trailer 0
	2																	Data
	1																	Data
	0																	Manufacturer Block

Tools

Hardware

- Proxmark 3
- NFC readers

Software

- Proxmark client (revision 840)
- libnfc 1.7.0
- Kali Linux

Approach

Measured specifications

- Time
- Knowledge and Skills
- Resources
- Success Rate
- Gain
- Additional requirements

Findings

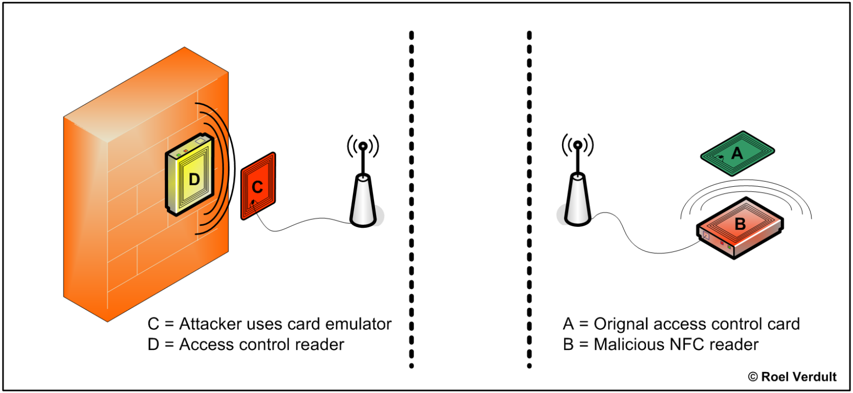
Attacks:
Key Retrieval

- Default Keys
- DarkSide Attack
- Snooping and MFKey
- Nested Attack

Faking a valid tag

- Tag Emulation
- Tag Cloning
- Relay attack

Relay attack


D
C
A
B
C = Attacker uses card emulator
D = Access control reader
A = Orignal access control card
B = Malicious NFC reader
© Roel Verdult

Feasibility: Slow, Intermediate to Perform

Default Keys

- Against MIFARE Classic tags
- Performed using the Proxmark Tool

Tag	Status
6	SUCCESSFUL
7	SUCCESSFUL
8	SUCCESSFUL
10	SUCCESSFUL
11	SUCCESSFUL
12	SUCCESSFUL
13	SUCCESSFUL
14	SUCCESSFUL
17	SUCCESSFUL
18	SUCCESSFUL
19	SUCCESSFUL
20	SUCCESSFUL
21	SUCCESSFUL
22	SUCCESSFUL
29	SUCCESSFUL

Table: Results from the Default Keys attack for all MIFARE Classic tags.

Feasibility: Fast, Easy to Perform, High Success Rate

DarkSide Attack

- Against MIFARE Classic tags
- Performed using the Proxmark Tool

Tag	Status
6	NOT SUCCESSFUL (Hanging)
7	NOT SUCCESSFUL (Hanging)
8	SUCCESSFUL
10	NOT SUCCESSFUL (Hanging)
11	NOT SUCCESSFUL (Hanging)
12	SUCCESSFUL
13	SUCCESSFUL
14	NOT SUCCESSFUL (Hanging)
17	SUCCESSFUL
18	SUCCESSFUL
19	SUCCESSFUL
20	SUCCESSFUL
21	SUCCESSFUL
22	SUCCESSFUL
29	SUCCESSFUL

Table: Results from the DarkSide attack for all MIFARE Classic tags.

Feasibility: Fast, Easy to Perform, Rather High Success Rate

Snooping and MFKey

- Against MIFARE Classic tags
- Performed using the Proxmark Tool

Tag	System	Status
14	C	SUCCESSFUL
22	A	NOT SUCCESSFUL (Could not capture the entire authentication handshake)

Table: Results from the Snooping and MFKey attack for MIFARE Classic tags.

Feasibility: Rather Fast / Intermediate, Rather Easy to Perform

Nested Attack

- Against MIFARE Classic tags
- Performed using the Proxmark Tool and the NFC reader

Tag	Proxmark3	NFC ACR122 Reader	Status
6	Successful	Successful	SUCCESSFUL
7	Successful	Successful	SUCCESSFUL
8	Successful	Error: I/O error	SUCCESSFUL
10	Error: Sending bytes to proxmark failed	Error: I/O error	NOT SUCCESSFUL
11	Error: Sending bytes to proxmark failed	Successful	SUCCESSFUL
12	Successful	Error: I/O error	SUCCESSFUL
13	Successful	Error: I/O error	SUCCESSFUL
14	Error: Sending bytes to proxmark failed	Error: I/O error	NOT SUCCESSFUL
17	Successful	Not Tested	SUCCESSFUL
18	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
19	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
20	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
21	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL
22	Successful	Not Tested	SUCCESSFUL
29	4K tag - finds the keys and hangs	Not Tested	SUCCESSFUL

Table: Results from the Nested attack for all MIFARE Classic tags.

Feasibility: Fast, Rather Easy to Perform, Rather High Success Rate

Tag Emulation

Performed using the Proxmark Tool
MIFARE Classic tag:

- Directly after nested attack
- With help of dump file
- Successful on demo kit
- Not successful on External Company 2 (System A)

HID Low Frequency tag:

- Only UID needs to be known
- Successful on External Company 3 (System 3)

EM410x tag:

- Reading successful, but emulating not (System D)

Feasibility: Fast, Easy to Perform, Intermediate Success Rate

Tag Cloning

Performed using the Proxmark Tool

MIFARE Classic tag:

- Cards with writable UID
- Successful on real systems A and C

MIFARE UltraLight tag:

- No special writable UID, Lock Bits and OTP bits was used
- Not Successful

HID Low Frequency tag:

- Writable HID cards
- Successful on real system B

Feasibility: Fast, Easy to Perform, High Success Rate

Tested attacks feasibility overview

	Time	**Knowledge & Skills**	**Resources**	**Success Rate**	**Requirements**
Default keys	little	easy	Proxmark3 / NFC reader	high	Access to valid tag
DarkSide	little	easy	Proxmark3	rather high	Access to valid tag
Snooping	average	intermediate	Proxmark3	-	Access to a valid authentication handshake
Nested attack	little	intermediate/easy	Proxmark3 /NFC reader	rather high low	Access to valid tag
Emulate tag	little	easy	Proxmark3	intermediate	Dump of a valid tag
Clone tag	little	easy	Proxmark3 / NFC reader A writable tag	high	Dump of a valid tag
Relay attack*	a lot	intermediate	2x NFC reader	-	Simultaneous access to valid tag and reader
	* Attack can be performed without knowing the keys for tags that use encryption				

Conclusion

RFID access control system assessment guidelines:

- Identify the type of the used tags.
  - MIFARE Classic - Ensure that: no default keys used, encryption properly used
  - MIFARE DESFire - Rather secure
  - MIFARE UltraLight - Not suitable for access control systems
  - HID or EM410x LF tags - Not secure
  - Others - Not researched
- Ensure that no sensitive information is written on the tags
- Ensure security awareness of the employees
- Ensure that secure enclosures are used for the tags when they are not in use
- Ensure surveillance around the readers

Questions?