

A practical guide to RFID badge copying

[5 Replies](#)

During red teaming assignments we are sporadically asked to attempt to gain access to certain physical “flags”. These flags could be the inside of a server room, or the workstation of a member of the management team.

Aside from these red teaming assignments, in most organisations, access badges are often the single factor of security that stands between us and the inside of a building, a server room or an office. There are many different RFID card reading systems on the market. Unfortunately, the security they provide is often lacking. With this blog post we want to demonstrate how easy it is to bypass the card reader security mechanism when it is insufficiently secured.

Specialised hardware is required to clone existing RFID cards, this hardware can easily be obtained and is relatively inexpensive. For this case study, we use the Proxmark3, which is a device developed by Jonathan Westhues that allows sniffing, reading and cloning of RFID (Radio Frequency Identification) tags.

NVISO Labs is the research arm of [NVISO](#), focused on innovation & cutting-edge infosec research. This is where our lab rats share the results!

Tweets by [@NVISO_Labs](#)

 NVISO Labs Retweeted



Johannes Weber 🎸
[@webernetz](#)

Nice research by [@daanraman](#) "Going beyond Wireshark: experiments in visualising network traffic". Hoping there will be a tool for this soon.

blog.nviso.be/2018/02/15/goi...



DISCLAIMER: This blog post, and by extent any other blog post written by NVISO LABS, are intended for educational purposes only. It is not intended and should not be used for the illegitimate cloning of RFID badges without prior permission.



Cloning and abusing the card



May 3, 2018

NVISO Labs Retweeted

SANS CyberDefense
@SANSDefense

Discover the latest updates to **#SEC599** :
Defeating Advanced Adversaries - Purple
Team Tactics & Kill Chain Defenses. Join
@ErikVaBu and **@Steph3nSims** for the
webcast: sans.org/u/CPv **#PurpleTeam**
#KillChain



May 3, 2018

NVISO Labs
@NVISO_Labs

Lab rats represent! Meep Meep 🐹
@HackBelgium **#hackbelgium**



Below we'll provide a step by step example on how to clone an HID global RFID card. Note that the Proxmark3 is able to copy many different types of cards.

We have two types of antennas that we can connect to our Proxmark3: a low frequency one and a high frequency one. The low frequency card, operating at 125kHz and 134kHz, can communicate with e.g. HID Prox II, HITAG, and EM4100 tags. The high frequency card, operating at 13.56Mhz, can communicate with e.g. Mifare Classic/Ultralight and iClass tags.



After starting up the proxmark3 interface, we can run the "*hw tune*" command to see if any card is detected. Currently the LF antenna is connected to the Proxmark3 and at this point there is no card in the presence of our LF antenna.



Apr 26, 2018

NVISO Labs Retweeted



Didier Stevens
@DidierStevens

My SDR workshop at #HITB2018AMS :-)



Apr 12, 2018

NVISO Labs Retweeted



Erik Van Buggenhout
@ErikVaBu

We just published a new Cuckoo auto install script (original version by Buguroo Security) used in @SANSInstitute #SEC599!

Check it out at

```
client — proxmark3 • sudo — 204x53
~/Desktop/proxmark3/client — proxmark3 • sudo

proxmark3> help
help      This help. Use '<command> help' for details of a particular command.
data      { Plot window / data buffer manipulation... }
hf        { High Frequency commands... }
hw        { Hardware commands... }
lf        { Low Frequency commands... }
reveng    Crc calculations from the software reveng1-30
script    { Scripting commands }
quit      Exit program
exit      Exit program
proxmark3> hw tune

Measuring antenna characteristics, please wait...#db# Measuring antenna characteristics, please wait...
.....#db# Measuring complete, sending report back to host

# LF antenna: 12.35 V @ 125.00 kHz
# LF antenna: 25.51 V @ 134.00 kHz
# LF optimal: 25.30 V @ 131.07 kHz
# HF antenna: 0.55 V @ 13.56 MHz
# Your HF antenna is unusable.
Displaying LF tuning graph. Divisor 89 is 134khz, 95 is 125khz.
```

When repeating the “*hw tune*” command, this time with the card within reach of our antenna, we see a clear difference in voltage in comparison with the previous screenshot. This indicates we are dealing with a low frequency card.

```
client — proxmark3 • sudo — 204x53
~/Desktop/proxmark3/client — proxmark3 • sudo

proxmark3> hw tune

Measuring antenna characteristics, please wait...#db# Measuring antenna characteristics, please wait...
.....#db# Measuring complete, sending report back to host

# LF antenna: 10.88 V @ 125.00 kHz
# LF antenna: 19.07 V @ 134.00 kHz
# LF optimal: 20.95 V @ 134.83 kHz
# HF antenna: 0.58 V @ 13.56 MHz
# Your HF antenna is unusable.
Displaying LF tuning graph. Divisor 89 is 134khz, 95 is 125khz.

proxmark3> █
```

Our next step is finding the type of card we have. Using the “*lf search*” command we can scan the card. Before executing this command, make sure the card is already on the antenna. If not, the search command will return errors.

blog.nviso.be/2018/04/12/pai...



Apr 12, 2018

[Embed](#)

[View on Twitter](#)

RECENT POSTS: NVISO LABS - BLOG

[Painless Cuckoo Sandbox Installation](#)

[Filtering out top 1 million domains from corporate network traffic](#)

[Creating custom YARA rules](#)

[How CSCBE's "Modbusted" challenge came to be](#)

[Intercepting Belgian eID \(PKCS#11\) traffic with Burp Suite on OS X / Kali / Windows](#)

[Going beyond Wireshark: experiments in visualising network traffic](#)

CATEGORIES

[android](#) (1)

[application whitelisting](#) (1)

[Buffer overflow](#) (1)

[burpsuite](#) (2)

[CSCBE](#) (4)

```
client — proxmark3 • sudo — 204x53
~/Desktop/proxmark3/client — proxmark3 • sudo

proxmark3> lf search
#db# buffer samples: 93 59 1a 00 50 bc ff c6 ...
Reading 30000 bytes from device memory

Data fetched
NOTE: some demods output possible binary
      if it finds something that looks like a tag
False Positives ARE possible

Checking for known tags:

HID Prox TAG ID: 07848[REDACTED] ( [REDACTED] ) - Format Len: 37bit - FC: [REDACTED] - Card: [REDACTED]

Valid HID Prox ID Found!
proxmark3> █
```

The proxmark3 confirms we are working with a HID global RFID card and we discover its ID: 07848XXXX (redacted). Now we need to use the according command to clone the card.

Using the Proxmark3 help function for the HID cards, we see we can use the clone function.

```
proxmark3> lf hid help
help          This help
fskdemod      ['1'] Realtime HID FSK demodulator (option '1' for one tag only)
sim           <ID> -- HID tag simulator
clone         <ID> ['1'] -- Clone HID to T55x7 (tag must be in antenna)(option '1' for 84bit ID)
proxmark3>
```

The T55x7 you see in the output above, is a type of card that is extremely versatile and supports multiple encoding formats of the majority of 125 Khz RFID tag transponders. We can thus use this type of card to emulate our HID card.

```
proxmark3> lf hid clone 07848[REDACTED]
Cloning tag with ID 07848[REDACTED]
#db# DONE!
proxmark3>
```

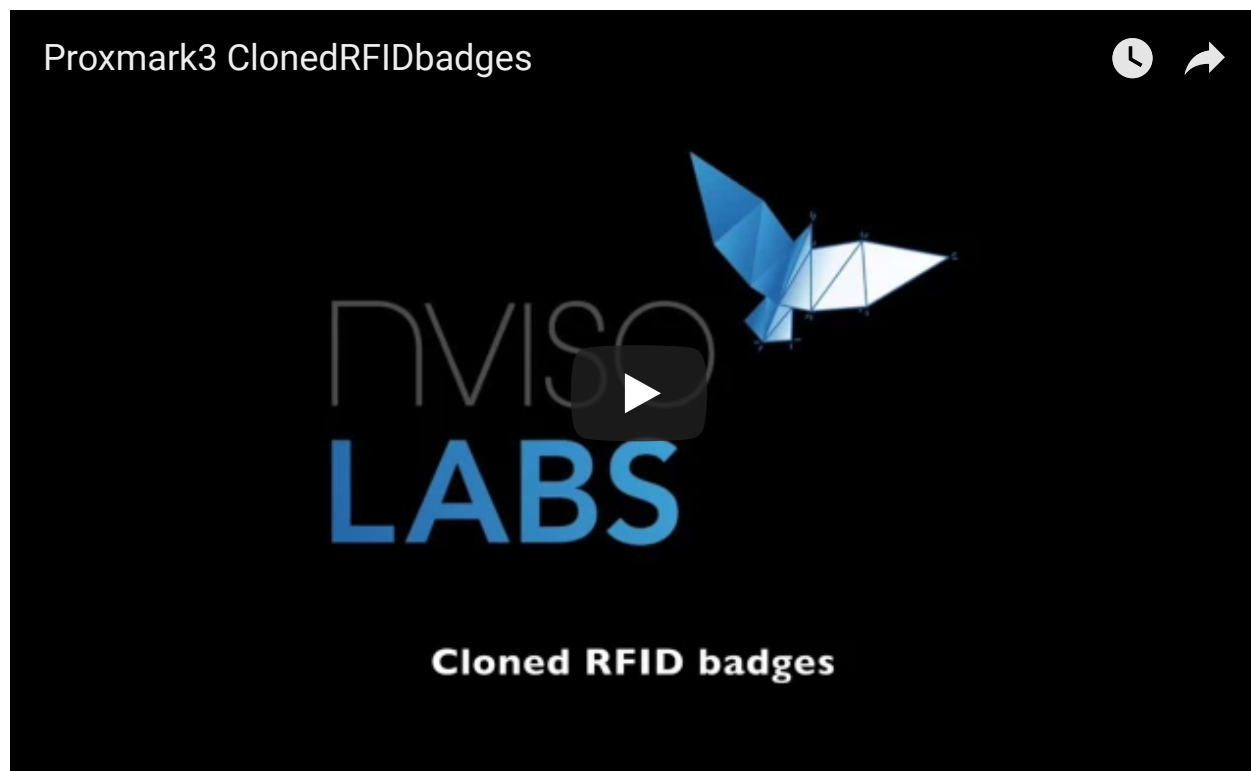
After executing the command above, including the HID Prox TAG ID identified in the previous steps, we have successfully cloned our card.

- [CVE-2015-0235](#) (1)
- [CVE-2017-7494](#) (1)
- [CVE-2017-9805](#) (1)
- [cyber threat mitigation](#) (2)
- [cyber threats](#) (11)
- [data visualisation](#) (2)
- [IDS](#) (3)
- [IoT](#) (1)
- [maldoc](#) (13)
- [malware](#) (20)
- [Mobile](#) (2)
- [nviso](#) (11)
- [Passwords](#) (1)
- [patch management](#) (2)
- [PDF](#) (1)
- [Ransomware](#) (2)
- [remote code execution](#) (5)
- [SEC599](#) (2)
- [software](#) (3)
- [Tools](#) (6)
- [Uncategorized](#) (26)
- [videos](#) (3)
- [Web application](#) (1)

ARCHIVES

[April 2018](#) (3)

That's all it takes! Check the video below for proof.



On a final note, when your office building is protected by such an insecure card reading system, often the only solution to fix this vulnerability is to replace the card reading infrastructure and all access badges. Needless to say this will have a significant impact on your organisation.

The following recommendations can be made to improve the security:

[March 2018](#) (2)
[February 2018](#) (1)
[January 2018](#) (3)
[December 2017](#) (2)
[November 2017](#) (1)
[October 2017](#) (3)
[September 2017](#) (2)
[August 2017](#) (4)
[June 2017](#) (4)
[May 2017](#) (6)
[April 2017](#) (4)
[March 2017](#) (6)
[February 2017](#) (3)
[January 2017](#) (3)
[December 2016](#) (4)
[November 2016](#) (2)
[November 2015](#) (1)
[July 2015](#) (1)
[May 2015](#) (1)
[April 2015](#) (3)
[March 2015](#) (1)
[January 2015](#) (1)
[August 2014](#) (2)
[July 2014](#) (1)
[March 2014](#) (1)
[January 2014](#) (1)
[November 2013](#) (2)
[October 2013](#) (1)

- Use of encryption to ensure that the ID is not sent in clear text. Think of challenge response authentication;
- Use of contactless smart cards which have encryption, mutual authentication and message replay protection incorporated.

[June 2013](#) (1)

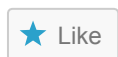
[April 2013](#) (1)

[March 2013](#) (3)

[February 2013](#) (1)

Additionally, it is known that attackers try to covertly copy your RFID cards, for example during a trip on the metro. You can try using an RFID protected sleeve/wallet, but research has shown that not all of them are effective at preventing covert copying. Be sure to test yours out and share your findings!

Share this:



One blogger likes this.

This entry was posted in [Uncategorized](#) on [January 11, 2017](#) by [sasjareynaert](#).

[← Decompiling py2exe Executables](#)

[Detecting py2exe Executables: YARA Rule →](#)

5 thoughts on “A practical guide to RFID badge copying”

Wagner Bertolini Junior

January 14, 2017 at 9:42 pm

That's why we use Mifare's with data encrypted inside. Then, you need a key to (authenticate and) read data. But you are right, at almost all physical access security systems this basic logic (unique id) its used to give access to someone.

★ Like

[Reply](#) ↓

Amal

February 21, 2017 at 11:30 pm

If you're talking about Mifare S50 1k or S70 4k "classic" tags, they use Crypto1 which has been broken, and can easily be cloned using the Proxmark (or other tools). It took me a matter of minutes to unlock all access keys and clone an entire Mifare 4k tag.

★ Like

[Reply](#) ↓

Wagner Bertolini Junior

March 1, 2017 at 10:23 am

@Amal, i didn't know about it! Is there a guide or something to learn how to exploit it?

Besides cloning is it possible to extract its encryption key?

Thanks!

★ Like

Pingback: [IT Security Weekend Catch Up – January 13, 2017 – BadCyber](#)

Pingback: [A practical guide to RFID badge copying – #OpIcarus](#)

Leave a Reply

Enter your comment here...



5