



Btw. not only cards use the RFID technology. Car keys, hotel doors, phones and a lot of stuff are being used with RFID.

How to protect yourself

So, what can we do in order to get some protection from being a RFID Hijacking victim? Use RFID tags based on a smart identification mechanism which is located before the broadcast information such as CryptoRF tags.

Use RFID tags which are realizing the RSA principle, and thus actually prevent from different sources to get to the non-encrypted information.

Use token based RFID tags

Use RFID tag which based on encryption keys of 128-bit and more (BUSlink, for example)

Some relevant links

<http://www.rfidjournal.com/articles/view?1415>

<http://www.videogold.de/iw/chaos-communication-camp-2007-24c3-mifare-security/>

<http://www.altera.com/products/devkits/altera/kit-cyc2-2C20N.html>

<http://tv.boingboing.net/2008/03/19/how-to-hack-an-rfide.html>

<http://rfidiot.org/>

shouts to Th3PonyWizard, peace.

Spoiler ([Click to View](#))

p.s: sorry for grammar mistakes.

**Bewbs** - October 25, 2013, 4:17 am

Wow this is actually a nice and fking interested tutorial!

Thanks :)

**Keeper** - October 25, 2013, 6:39 am

I'd lie if I say that I'm gonna read it since I'm not into hardware but anyway nice to see something new.

**-?Divine-** - October 25, 2013, 6:39 am

Looking good mate. Very nicely written.

**ida** - October 25, 2013, 6:45 am

This looks interesting, and I will definitely read more about this.

**nicksaban1** - October 25, 2013, 6:46 am

Nice tutorial, but RFID has been around for years. It's not mainstream because it is not useful at home. RFID has a range of up to 200 meters on the 3 GHz band, but doesn't go through walls. The Soviet Union used it to track its own agents to see if they were double crossers.

This post might have helped a little when I did a term paper on RFID.

Another useful tidbit is that the Govn't is injecting these in citizens to track them (without their knowing by having surgeons and dentists inject them) /

edit- saw "new" sry

**axmetmcl** - October 25, 2013, 7:16 am

thanks for this nice tutorial, i am sure i will try it in a short time :)

**mmuzammil** - October 25, 2013, 7:18 am

I remember a few years ago, this attack also happend.

It was in London Picadilly circus, there were some Paki's parked in a car with all these things, and they were getting everybody's details of there bankpas.

They made 2,3 million and after that they got caught by the FBI.

**SIM-1808688** - October 25, 2013, 7:55 am

I must admit this is a very interesting tut, looking forward to see more :-)

**Mad76e** - October 25, 2013, 10:35 am

Now things getting interesting.. Good work!

**WealthyHustler** - October 25, 2013, 10:38 am

This is actually getting really scaring knowing that this is starting to get popular :O

**Zixem** - October 26, 2013, 12:21 pm

thanks everyone

(Oct 25, 2013 06:46 AM)Nick Saban Wrote: [\[CITE\]](#) Nice tutorial, but RFID has been around for years. It's not mainstream because it is not useful at home. RFID has a range of up to 200 meters on the 3 GHz band, but doesn't go through walls. The Soviet Union used it to track its own agents to see if they were double crossers.

This post might have helped a little when I did a term paper on RFID.

Another useful tidbit is that the Govn't is injecting these in citizens to track them (without their knowing by having surgeons and dentists inject them) /

edit- saw "new" sryno worries :3

glad you liked it

(Oct 25, 2013 10:38 AM)PetWussy Wrote: [\[CITE\]](#) This is actually getting really scaring knowing that this is starting to get popular :Oindeed .\_.

**Shanks** - October 26, 2013, 12:38 pm

I really.. don't understand this kind of things but looks like a very well written guide and will probably help a lot of users.

Good work!

**.Cobra.** - October 26, 2013, 12:58 pm

thanks for this nice tutorial, i am sure i will try it

**Ergo** - October 26, 2013, 1:04 pm

Finally, something that isn't a "RAT Setup" or another pointless "SQLi Tutorial".

Nice tutorial.

**Vets** - October 26, 2013, 2:28 pm

Thanks for this awesome tutorial dude ! :)

**bighekur** - October 26, 2013, 2:39 pm

Quite nice, I think I saw something about defcon where they were able to snap data from 50m away, which actually is quite scary.

However most places can just add a 2-step verification in order to stop the person.

**høpud Th? d?sTrøya** - October 26, 2013, 7:15 pm

Very good guide, written extremely well.

**Rees** - October 28, 2013, 7:59 am

Thanks for this Zixem, very high quality tutorial.

**greensurre** - October 28, 2013, 8:21 am

What can this hacking actually do ?

**cheatson** - October 28, 2013, 8:45 am

Nice introduction to the subject, a subject I know next to nothing about besides what you just wrote, thnx! :)

**Nob** - October 28, 2013, 9:38 am

Something else to protect yourself you should add : You can put your cards into a wallet making faraday cage.

**arabiansquid** - October 28, 2013, 12:38 pm

I know this is off topic but that wolf graphic, is so nice. But the tutorial is good also I'm not really into hardware but this is a good read.

**Terick** - October 28, 2013, 2:19 pm

Omg, exactly what i was searchin for. You've got PM! ;)

**Tru?Bit** - October 28, 2013, 4:29 pm

Wow, this is a nice and really helpful tutorial. Very HQ. Thank you for the tutorial. Bookmarked.

**Reciprocal** - October 28, 2013, 6:44 pm

This is interesting read the whole thread but it isn't really of any use to me. Anyways nice post.

**Shaggy** - October 30, 2013, 10:44 am

Will try my best for this, I am not much of a engineer guy/.

**Euphorical** - October 30, 2013, 11:12 am

Hmm... I dont get the overall point of the attack...

Edit: After posting this i sounded like a post-whore fag

Just to clarify, If you can justify the bands/networks/ and what you can actually use this for, it would be great.

**Tru?Bit** - October 30, 2013, 12:21 pm

(Oct 30, 2013 11:12 AM)Euphorical Wrote: [\[CITE\]](#) Hmm... I dont get the overall point of the attack...

Edit: After posting this i sounded like a post-whore fag

Just to clarify, If you can justify the bands/networks/ and what you can actually use this for, it would be great.

You can gain access to places that are restricted by copying someones access card or whatsoever. I am not sure if you can copy for example an Oyster card or something. That would be amazing btw. (Oyster card is the official travelling card from the UK.)

**-?Divine-** - October 30, 2013, 12:25 pm

(Oct 28, 2013 12:38 PM)arabiansquid Wrote: [\[CITE\]](#) I know this is off topic but that wolf graphic, is so nice. But the tutorial is good also I'm not really into hardware but this is a good read.

Quite interesting, as all I've heard so far are complaints about it.

**L33D5cr3w** - October 30, 2013, 2:33 pm

Thanks that was very interesting

35 CHAR

**Zixem** - *October 31, 2013, 11:20 am*

thanks for the positive feedback folks~

(Oct 28, 2013 08:45 AM)cheatson Wrote: [\[CITE\]](#) Nice introduction to the subject, a subject I know next to nothing about besides what you just wrote, thnx! :)nice to see you posting here bro <3 glad you learned something

**Cedric.** - *October 31, 2013, 4:04 pm*

nice tutorial bro, i will try to use this in the near future. I think it will work at my school, the lockers all open with a different card. So is worth trying  
:)

**Apple J4ck.** - *November 2, 2013, 1:32 am*

Extremely HQ tutorial right here.

Spoiler [\(Click to View\)](#)

**hikashin** - *March 12, 2016, 3:21 am*

noted for this good work :D

**arun hacker** - *May 1, 2016, 10:07 am*

Really nice and informative post mate? THanks 4 sharing!

**jonathanxx1** - *May 1, 2016, 11:02 am*

Is there anyone who purchased a RFID Reader on ebay or amazon and have a link?  
I ask because want to buy something from a good vendor. And not too expensive.