

GRANDADMIRALTHRAWNS TECHNOLOGY WEBLOG AT XIN.AT. INCOMPATIBILITY IS WEAKNESS!



Jun
30
2015

The dangers of NFC-capable banking cards, and how to detect and disable the feature

Hardware, Security

[Add comments](#)



NFC – or “near-field communication” technology is a now-booming system for sending and receiving small chunks of data over very short distances. You may have heard about modern cellphones supporting the system to read information from small tags – in essence chips you stick onto something to provide local, small pieces of information. This can serve augmented reality purposes for instance, in a sense at least, providing metadata about objects anywhere in the world.

It’s nowadays also being used for payment though, both in conjunction with smartphones and their active NFC chips as well as debit/credit banking cards and their integrated, passive NFC circuitry.

Index:

1. [NFC basics](#)
2. [NFC-capable banking cards](#)
3. [Using a modern Android phone to fetch data from a banking card](#)
4. [The theft issue](#)
5. [Modern cards may be more close-lipped](#)
6. [Killing NFC for good](#)

1.) NFC basics

So there are connections between active chips (say: phone to phone) as well as active-passive ones, in which case the



XIN.at IRC chat server web access

If you would like to get in contact with me, you can easily join me via web chat here. This is an encrypting web gateway to `irc+ssl://www.xin.at:6697` or plain `irc://www.xin.at:6666`.

[\[Link to web chat!\]](#)



Decentralized YaCy web search:

[Search](#)

Pages

[about:XIN.at](#)

[The XViewer Project](#)

[XP x64 post-mortem updates](#)

active side (a phone, an electronic cashier) will talk to the passive one. In the latter case, the active chip will generate an electromagnetic field which reaches a copper coil embedded in the passive device or tag, creating enough inductive voltage to power that passive NFC chip.

According to information that can be found on the web and in some specifications, the range should be about 20cm with data transfer rates of 106kbit/s, 212kbit/s or 424kbit/s, and in some non-standard cases 848kbit/s. That'd be 13.25kiB/s, 26.5kiB/s, 53kiB/s or 106kiB/s respectively. The time to build up a connection is around one tenth of a second. There are NFC range extenders [[like this one](#)] for active chips however, which can boost the range up to almost 1 meter! And that's where the alarms start ringing in my head.

Now, why is any of that dangerous to begin with? Because it's being used for payments and because there may be a significant information leaking issue with some of those banking cards.

2.) NFC-capable banking cards

First of all, I'd like to thank two of my colleagues, which shall remain anonymous, for providing a.) a fully affected debit card and b.) a NFC-capable Android smartphone.

Let's take a look at our affected card (*click to enlarge images, as usual*):



A PayPass-based NFC-capable debit card, see that PayPass logo?

Now this is not my own card, so I didn't have unlimited access to it. Since my own cards – both debit and credit – were not NFC-capable yet, I simply ordered a new one from my bank. There are other people on the web who used CT/X-Ray like [[here](#)] or [[here](#)] to visualize the internals of such cards, but I wanted a cheap solution that every layman can copy easily.

Categories

- Hardware
 - Audio
 - Graphics Cards
 - Processors
 - Storage
- Media
 - Anime & Manga
 - Movies
 - Music
- Philosophy
- Politics
- Software
 - Benchmarking
 - Gaming
 - Linux
 - Media Encoding
 - Powerful Tools
 - Programming
 - Scripting
 - Security
 - Server
 - Unix
 - Windows
- t3h intarweb
- Travelling
- Uncategorized

Recent Posts

- Building the 54.5TiB "Taranis" RAID-6 array and the hardware around it, part 4: It's done!
- Building the 54.5TiB

As a matter of fact, any bright light (even a cellphones LED flash, when used as a torch) is sufficient, see here:



The NFC coil on my new card, visualized by normal light, in this case a Sigma EVO X halogen lamp used for riding mountain bikes at night. This is a stitched image assembled from 11 individual photographs. And yes, I left my given name in the clear there. 😊

For more clarity, see the next image:



Here I emphasized the coil a bit, so you would know what to look for

“Taranis” RAID-6 array and the hardware around it, part 3½: Disasters and also some benchmarks

And here we go again: My G.SHDSL doesn't like Wednesdays

Font anti-aliasing round 2

The Kirino Kousaka 1/2.5

Scale Superfigure, or how things just got out of control at some point...

Recent Comments

George on Encoding

stereoscopic 3D video with x264 and AviSynth

thrown on Spare parts for this IBM PC Server 704

fifio on Spare parts for this IBM PC Server 704

tk Tucker on Intel X58 chipset and 48GB RAM: Impossible? No!

thrown on Intel X58 chipset and 48GB RAM: Impossible? No!

Links

Mausmaki – technology and politics – a friends view

The Umlux Project

The x264 benchmark results list

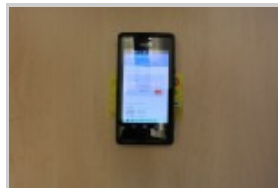
VoodooAlert

Now this coil has two functions: First – as mentioned above – it provides inductive voltage and with it up to 15mA of power to run the NFC chip and potentially some flash memory. Second, it also is the NFC chips' antenna to properly receive the signal on NFCs 13.56MHz radio frequency spectrum. So, how about we talk to that chip a little ourselves, now shall we?

3.) Using a modern Android phone to fetch data from a Banking card

A Frenchman named [[Julien Millau](#)] luckily has developed an Android app called "Banking card reader NFC (EMV)", which you can find on [[Google Play](#)] for free, including the source code as it's licensed under the [[Apache License, v2.0](#)]. There are other apps too, tailored towards cards with local features (I'll get to those later), but this is a good, generic one.

So what you'll need is an NFC-capable Android smartphone, that app, and some banking card with NFC enabled. If you've got a chatty one on top of things, you can do this:



Basic card information



Raw transaction log



Decoded transaction log

The basic card info might not look like much, as it's supposed to show only the cards serial number. Some cards – like this one here – however give you the bank account number instead! Nice one. So this is our information leak #1.

As you can see on the other two images, the card also features some flash memory, holding a very interesting transaction log. By sending hexadecimal commands of the form `00 B2 NN 5C 00` to the card, where `NN` equals the log entry number, we can get a nice transaction log including amounts paid. So `00 B2 01 5C 00` would get log entry #1, `00 B2 08 5C 00` gets #8, `00 B2 0E 5C 00` gets #14 and so on. After decoding, you get the date and amount of money spent for each transaction, and that includes both NFC transactions and normal full-contact transactions, where you put your card into a real chip reader and enter your pin.

So no matter how you pay, it will be logged on such cards. And that log can be read. Given that NFC is completely pinless, we can just fetch such data without any authentication or encryption holding us back! That's leak #2. Again, keep in mind that there are those range boosters for active NFC chips! If I put a powered NFC patch kit on my Android phone, in a worst-case scenario I could just walk by you and potentially fetch your transaction logs and bank account number!


Now that did raise a few eyebrows, which is why some banks have reacted to the issue, like my own bank too. But first, to another problem:


4.) The theft issue

Archives

December 2015
 November 2015
 October 2015
 September 2015
 August 2015
 July 2015
 June 2015
 May 2015
 April 2015
 March 2015
 February 2015
 January 2015
 December 2014
 November 2014
 October 2014
 September 2014
 July 2014
 June 2014
 May 2014
 April 2014
 March 2014
 January 2014
 December 2013
 November 2013
 October 2013
 September 2013
 August 2013
 July 2013
 June 2013
 May 2013
 April 2013
 March 2013
 February 2013

Besides leaking information, there is another problem: As said, NFC access is pinless. It's used for 25€ micropayments mostly, limiting the damage somewhat. Typically, you'll get 3-5 payments before you have to plug the card back into an ATM or electronic cashier and re-authenticate it using the pin, after which you'll get another 3-5 contactless payments activated. So with 5 usable payments, you can lose 125€, should your card be stolen. But it doesn't end there.

In my own country, Austria, we also have an offline cash replacement technology called [Quick] . With that, you can basically charge your banking card and carry the charge around like real cash. It's being used for machines where online connections are economically unfeasible, like cigarette vending machines or pay and display machines, where you buy tickets for car parking. The maximum charge for Quick amounts to 400€ total.

Thing is, should you ever choose to charge the full amount, this triggers an activation of Quick-over-NFC! This is actually intentional, so that's what you have to do to get to that feature, contactless offline payments. The real problem is, that with Quick-over-NFC, all limits are gone, which is confirmed [here] . So a thief could just waste the entire charge of the card at his hearts' content, upping the potential worst case loss to a full 525€! Holy hell, that does actually hurt already! Even if you call your bank and get the card locked due to theft, that money is still gone due to the offline nature of Quick. Just like real cash. So better hold on to your card, if you've already got that feature activated and money charged onto it!

But let's get back to the data leak issue again:

5.) **Modern cards may be more close-lipped**

Banks aren't entirely ignorant to the problem and related criticisms received, so some of them actually did try to improve the situation. When trying to read my brand-new card from Bank Austria for instance, what we get is this:



A newer cards' basic card information



No logs here, move along please...

First of all, this newer card doesn't give away my bank account number, but really just the serial number. That takes care of leak #1 to at least some degree. Secondly, the card doesn't seem to have a transaction log anymore. At least it doesn't hand one out using known commands. It can of course still be used for NFC payments using [PayWave] or, as it is in my case, [PayPass] and Quick, if activated. But yes, this is more secure, at least when considering the info leak.

But what if I just want to lock it down for good, once and for all?

We can never be sure that there *really* is no transaction log after all. Maybe we just don't know the necessary commands.

January 2013
December 2012
November 2012
October 2012
September 2012
August 2012
July 2012
June 2012
May 2012
April 2012
March 2012
February 2012
January 2012

Plus, there still is the micropayment issue.

Now, some banks give you the option to deactivate the feature at your local branch bank, sometimes for free. Volksbank here does this for instance. Not sure how this works and whether it's really final though. Others may give you the option to send you a NFC-free card, as my bank does. That is if you do know about it and proactively order one for 14€... By default they'd just send you a fully NFC-capable one before the old one expires.

Some banks do neither of the two. Which is why you may want to handle things yourself.

6. Killing NFC for good

Remember that poor mans' X-Ray from above? All we need to do is to cut the copper coil to fully disable *all* NFC functionality. I used a microdrill for this, which may be slightly dangerous for the chip due to fast static charge buildup, but it worked fine in my case. You can also use a manual drill or even melt your way through with a soldering iron. Just make sure to not pick a spot that sits within the cards magnetic strip! In any case, we mark the spot first:



A red X above the NFC "wave" logo marks the spot. Notice that this card shows both the PayPass and that NFC wave logo.

A few seconds later, my cards' NFC feature has effectively been dealt with. Tests with both Android phones and actual electronic cashiers have shown that yes, it's truly gone. All the other full-contact functions like cash withdrawal and payments have also been tested and still work absolutely fine!



Universal Solution™: If it bugs you, just drill holes in it 'till it's dead!

So that's it, no more contactless payments, no more reading information out of the card wirelessly, no more Quick-over-NFC (which only concerns Austrian people anyway, but yeah). Just make sure that the edge of the hole is properly deflashed, so your card won't get stuck in any ATMs or whatever.

So, all of the good things are still there, and all of what I consider to be the bad things are now gone! Finally, I can put my tin foil hat off again.

Ah yes, tin foil! Before I forget it, another colleague of mine also tried to shield his card using tin foil instead. And indeed, that seems to be sufficient too, in case you don't wanna physically modify your card. You can even buy readily-made shielded card sleeves to protect you from unauthorized NFC accesses, like [[this one here](#)].

I do prefer the final solution instead, but it's up to you, the option to do it temporarily instead is there also.

So, stay safe! 😊



The dangers of NFC-capable banking cards, and how to detect and disable the feature by [The GAT at XIN.at](#) is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License](#).

Posted by thrawn at 10:29

Tagged with: Android, banking card, banking card reader, contactless, credit, debit, information leak, micropayment, NFC, payment, PayPass, PayWave, pinless, Quick, tap to

pay

4 Responses to "The dangers of NFC-capable banking cards, and how to detect and disable the feature"

1. **Sjaak Trekhaak** says:

July 3, 2015 at 03:39



It's great you're sorting this stuff out!

With some sort of copper plug you might be able to restore the coil again. Which is what we want: a hardware switch to only enable this sort of stuff when we want and/or need it, not always.




[Reply](#)**thrawn** says:


July 3, 2015 at 07:27



Morning Sjaak,

I think this might not work. For the purpose of an antenna yes, but to get voltage to the chip you need a proper coil with individual traces (for the induction). If you cross-connect the traces it becomes a single trace basically, which I think *might* not get the voltage up high enough.

What you might want is one of the shielded sleeves, that's basically an "on/off" switch. I linked to one in the USA, but you can get them in the EU too, like [\[this one\]](#), [\[this one\]](#) or [\[that one\]](#).

There was actually a case in Germany, where VISA credit cards became exploitable, and you could really withdraw larger amounts of money from them! German scientists/engineers proved that in an experiment (likely using an NFC booster pack), drawing money from an affected VISA by just walking by it with a properly equipped smartphone. The article about it can be found [\[here\]](#).

So I believe we'd be quite right to be extremely careful with this technology... Oh yeah, sorry that was all German links, but heh...

[Reply](#)**Sjaak Trekhaak** says:

July 5, 2015 at 00:39



Oh, I just thought it was a coil with a single winding.

[Reply](#)

thrawn says:
July 5, 2015 at 09:59



Well, I can't say for 100% sure with my card, but judging from the X-Rays and CTs I've seen on the web, most cards seem to have 4-5 windings. So I'm guessing most cards would have around that many.

With my simple method of visualizing the coil you simply couldn't see any individual traces. But I wanted something "cheap", because not everybody has access to an X-Ray machine or something as massive and exclusive as a CT.

[Reply](#)

Leave a Reply

Name (required)

E-mail (required)

URI

Your Comment



By clicking "Submit Comment" you agree to have your comments' content released under the [CC BY-NC-SA 4.0 international license](#) (Contents need to be attributed to you when copied, may be altered and/or re-shared under the same license, but may not be used for commercial purposes). You will of course retain your © on any of your own content in line with the license terms. Your email address will never be published.

You may use these [HTML](#) tags and attributes: ` <abbr title=""> <acronym title=""> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <s> <strike> <pre lang="" line="" escaped="" cssfile="">`

Submit Comment

Building the 54.5TiB "Taraniş" RAID-6 array and the hardware around it, part 3: A dead machine and how to run Corsair Link on XP x64