



HACKAD

[HOME](#) [BLOG](#) [HACKADAY.IO](#) [TINDIE](#) [HACKADAY PRIZE](#) [SUBM](#)

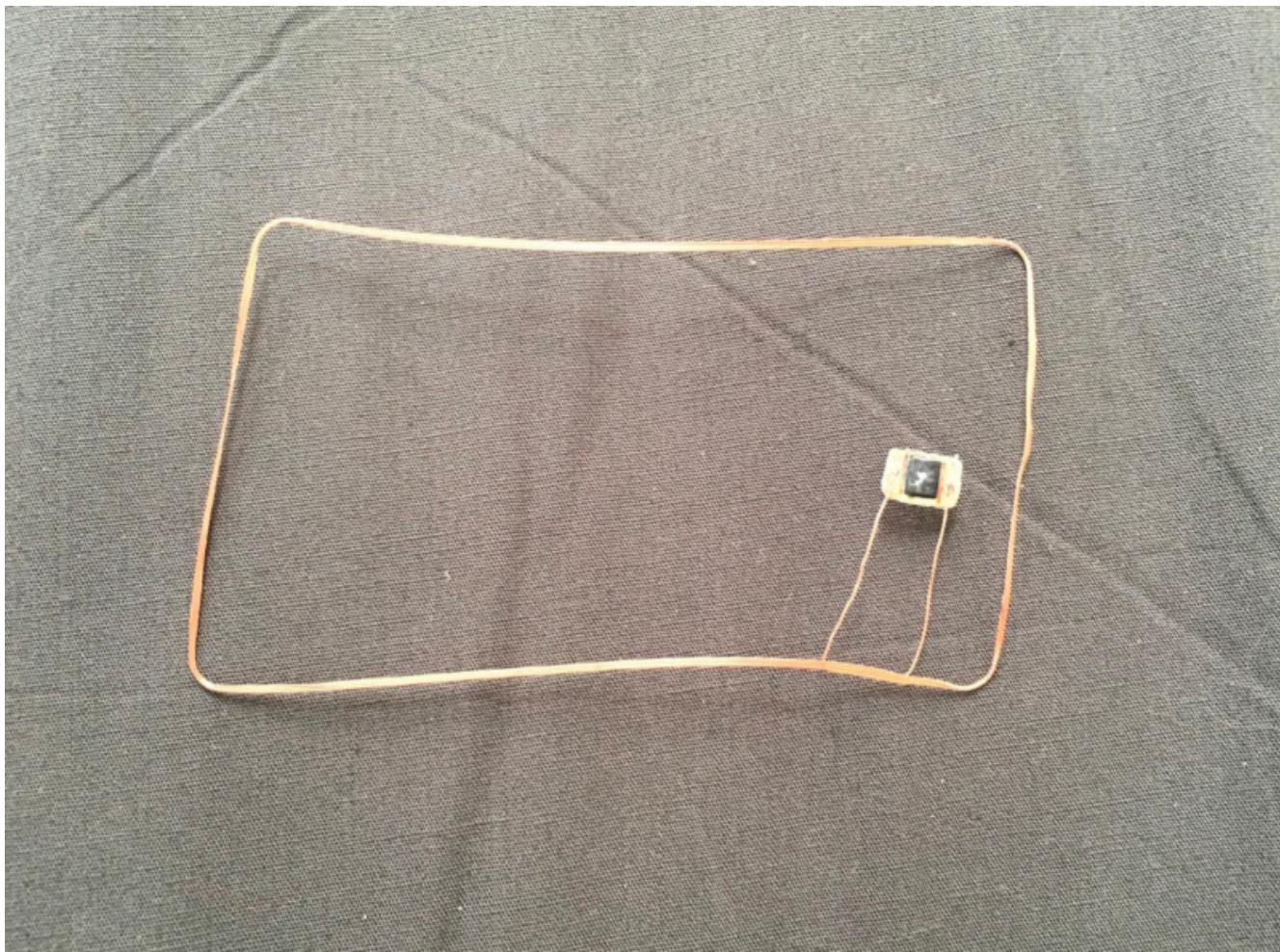
MAKING A WEARABLE NFC BUS PASS

by: **John Baichtal**

34 Comments



June 20, 2017



[Stephen Cognetta] is trying to get the total number of things he owns down below 115, and he's always looking for ways to streamline his life.

Toward this goal he dissolved his SF Transit Clipper Card in acetone to **get at the NFC tag** embedded inside. The tag consists of a tiny chip attached to an antenna the size of the card itself. It took about three days (video below the break) for the layers



to separate and [Stephen] was able to extricate the tag.

He ended up trying a few different ways of storing the delicate chip and antenna, including a lump of Sugru as well as a waterproof aspirin band, pictured to the right.

One supposes the transit pass idea might save you a little time, but what would really simplify your life would be having a single wearable tag that unlocked a bunch of things. Also it should be noted that, un-coolly, damaging a card violates SF Transit's terms of service...

HaD has covered NFC wearables before, including the [phone-unlocking NFC ring](#) as well as the [NFC ring box](#). This [NFC-controlled infinity mirror](#) makes great use of the technology.

An error occurred.

Try watching this video on www.youtube.com, or enable JavaScript if it is disabled in your browser.

Posted in [Lifehacks](#)

Tagged [NFC](#), [transit](#), [wearable](#)

← RESTORING A RETRO
747 CONTROL DISPLAY
UNIT

PRACTICAL IOT
CRYPTOGRAPHY ON THE
ESPRESSIF ESP8266 →

34 THOUGHTS ON “MAKING A WEARABLE NFC BUS PASS”

Something says:

June 20, 2017 at 4:13 am

i always wonder, doesnt this approach also disolve the enamel of the wire?
anyone?

Reply

Report comment

peterlarson233 says:

June 20, 2017 at 5:41 am

It will soften it a bit, but won't really dissolve it (assuming it's polyimide).
At work I believe we use xylene to dissolve polyimide, but usually you
just burn it off in a lye pot or something if you actually want to remove it.

Reply

Report comment

0xFFFF says:

June 20, 2017 at 3:57 pm

It does not dissolve the enamel. I have done this many times before. In some rare cases it will soften as @peterlarson233 pointed out.

Reply

Report comment

Saabman says:

June 20, 2017 at 4:14 am

Speaking of NFC devices I've been trying to find info on reading car key transponders but not really coming up with any useable information. What information I have found is some what contradictory and lacking any technical detail.

I could see the SF transit people getting a little upset by the modification of the card but it would be good for them to allow altering the form to suit personal use.

Reply

Report comment

tomás zero says:

June 20, 2017 at 4:32 am

Yeah. There should be a law stating "You shall not make unnecessary rules".

For it to carry some weight there should be some payment to the "victims" of unnecessary ruling (proving a rule "necessary" resp. "unnecessary" will be somewhat involved too, but the burden should be more on those imposing the rules than on those challenging them).

The devil is in the details, of course. But you get the idea.

Reply

Report comment

timgray1 says:

June 20, 2017 at 5:35 am

The problem is they chose a crappy form factor the card. If they chose a capsule based NFC tag as an option then people would have been able to put it in their watch band or whatever, heck the keyfob is even better. I did that back in the days when Mobil gas had a NFC pay system, I took the capsule out of their keyfob and put it in my watch band.

[Reply](#)

[Report comment](#)

tepfarkas says:

June 20, 2017 at 9:26 am

@timgray1 – I was just thinking of those! They actually did have a few watches (Casio, I believe) made with the NFC capsule built in to the watchband. I actually owned one, since I did work for ExxonMobil for the initial SpeedPass rollout. The “leather” watchband deteriorated quickly and the NFC capsule popped out, but was still a neat thing (hipster mode on) way back before it NFC/RFID was “cool”. :-)

[Reply](#)

[Report comment](#)

Jermaine Falken says:

June 20, 2017 at 6:39 pm

Chicago's CTA has NFC transit cards too, but you add money to the card, so e-pickpocketing becomes a concern. In fact, Chase dished out NFC debit cards, and when both cards were in a wallet then used, BOTH cards got bilked out of the fare! I have one of these CTA "Ventra" cards and I taped 2 pieces of sheet metal to it like a butterfly knife. I also have, kept separate, an NFC debit card that I also protect with a sheet metal and tape pouch.

Chicago had a forerunner NFC card 10 years ago when I

discovered the problem. A lady boarded a bus, used her card, put it back in her purse, and when her purse rubbed against the reader, BEEP BEEP! she got zapped for another fare. That night, I went to a Home Depot, and protected the card a decade before the rise of the e-pickpocketer.

[Reply](#)

[Report comment](#)

Dan says:

June 20, 2017 at 5:43 am

> I've been trying to find info on reading car key transponders but not really coming up with any usable information.

There is lots of similar standards and system. You should first work out what your own vehicle is using and attempt to read and clone it. Generally automakers use various third parties systems. Typically there is a remote control central locking on 433Mhz EU or 315Mhz USA. Then when you insert the key in the ignition barrel it uses an RFID non powered transponder that has a single ID with a number of bits. This is normally 125Khz EU & 134Khz USA. If the vehicle likes the unique ID it allows the vehicle to start when the key is turned. Often locksmiths can read the ID and put the same ID into a blank chip in another key thus cloning the ID, without needing to connect into the car and add a new ID to the system. Sometimes if you own two valid keys for a vehicle it will allow an unknown third key to be added. If you search for a particular make and model you may find spare keys, transponder, remote central locking guides and instructional videos on youtube. I managed to add an extra key to my vehicle. Another quick cheat is to remove a valid transponder from a working key, and glue it beside the reader in the ignition barrel. Then any key turning the ignition will see a valid chip and the car will start. You lose the security benefits, but you can get copied mechanical keys for a few dollars.

[Reply](#)

[Report comment](#)

Peter says:

June 20, 2017 at 5:57 am

If the chips could be easily cloned then why wouldn't they do that to replace a lost or stolen key? Specifically for Honda and Nissan autos, when you replace a key you have to have all other keys present and the car is reprogrammed to recognize the keys. If you don't bring one of the keys with you then it stops functioning.

[Reply](#)

[Report comment](#)

Dan says:

June 20, 2017 at 2:57 pm

It's probably because most attempts at cloning or 'borrowing' another tag at a distance etc would show a doctored card or an RFID device connected to an arduino etc
So mandating the pass is the standard size/shape is probably going after the low hanging fruit of fraud?

[Reply](#)

[Report comment](#)

Harvie.CZ says:

June 20, 2017 at 4:15 am

Looks like the acetone is evaporating away... You probably need better lid...

[Reply](#)

[Report comment](#)

Peter says:

June 20, 2017 at 6:00 am

I have this problem with acetone when I make ABS slurry and I can't seem to find a vessel, baring the container it comes in, that will seal tightly enough to keep it from evaporating.

[Reply](#)

[Report comment](#)

Jonathan Wilson says:

June 20, 2017 at 4:29 am

For the transit networks I have used here in Australia, not only would there likely be rules against damaging the card in this way but if the ticket inspectors decided to do a ticket check, you would probably be hit with a huge fine (since they likely wont believe that your funky wristband is actually a valid Go Card or whatever)

[Reply](#)

[Report comment](#)

Paul says:

June 20, 2017 at 5:37 am

Makes me wonder if you could just duplicate it somehow? Brisbane's Go cards are a pain in the butt... took me forever to remember to touch off.

[Reply](#)

[Report comment](#)

Peter says:

June 20, 2017 at 6:04 am

Our transit system is like that too, I don't understand why they won't just let you use your phone. We have a network of car chargers called ChargePoint that works off of RFID tags or you can just install the App on your phone and use it straight away. It's brilliant because I can leave the tag in the car glove box for anyone who borrows the car but then I don't have to go fishing it out if I

need to top up the car. It all comes out of the same account.

[Reply](#)

[Report comment](#)

mxb says:

June 20, 2017 at 5:45 pm

Somewhere in Sydney they are trialing the credit cards PayPass system to let you do a ‘pre-withdrawal-credit-check-thingy’ when you tap on and finalize payment when you tap off.

This would allow you to use your phone or watch’s payment process.

Stupid idea. They should be selling personalized tags/wristbands/keyfobs/stickers etc.

Haven’t given any thought to how ticket inspectors will check this but I’d assume this system would require a central database (shudder) of card numbers and payment details that they verify your card with.

[Reply](#)

[Report comment](#)

blah says:

June 20, 2017 at 11:33 pm

They’d just route the transactions to your bank the same as any other Visa or Mastercard transaction.

So the ‘Centralised database’ of card numbers is your bank.

[Report comment](#)

Electra says:

June 20, 2017 at 6:24 am

Do NOT duplicate them. They are dodgy Mifare Classics, but copying them is breaking crypto laws and you can get in /serious/trouble.

Dissolving the card(50/50 acetone and xylene works great) and using the chip in another formfactor(I recommend also leaving the 'Go' part of the card so it looks right:) is just vandalising the card. \$300 fine.. Instead of jail time.

I did that to one of my spare cards and made a keyfob(Using a cheap keyring NFC tag) and most of the time the ticket inspectors don't care so long as you tap on and it's a valid card.

Once or twice I've gotten a 'we'll only let you off this once' or a 'you really should get a new card'. "Just cut it up and glued it in." works for half the inspectors. Others you need to explain what you did and why.

[Reply](#)

[Report comment](#)

dwywit says:

June 21, 2017 at 2:31 am

My nephew in london told me a story – someone was seen using a magic wand to touch on and off on the london underground. Turns out this person had removed the chip from the travel card/oyster card, and glued it to the tip of a Harry Potter souvenir wand. No mention of robes or funny pointed hats.

[Reply](#)

[Report comment](#)

CampGareth says:

June 20, 2017 at 6:00 am

I'm not sure whether it's a shame NFC cards are kinda hard to emulate or not. I've got a key card for the office that I'm always forgetting and at the same time I've stopped carrying my bank cards since my phone can fill the role, so I've been trying to figure out how to get my phone to act as a key card for the door. Unfortunately it can't even get a successful read on the card as it doesn't support... whatever's at the heart of it.

I'm sure there are security reasons why this is hard but convenience darnit!

[Reply](#)

[Report comment](#)

Peter says:

June 20, 2017 at 6:07 am

There are a number of different NFC standards and RFID is just a subset of them. Your phone only works with RFID.

It's a shame there's no way for your phone to emulate an RFID tag but from a usability perspective, you'd need to open an App and choose which RFID tag to emulate before you touch it.

[Reply](#)

[Report comment](#)

Dan says:

June 20, 2017 at 6:39 am

There is little to no security on most RFID systems and any with even basic security are generally 20 year old crypto which is broken now.

Ideally find out the make and model of the system in use and research this. Also using a good radio scanner check if it is 13.56Mhz or 125Khz, by putting it close to the reader on the door. That narrows down the

systems in use. Generally unrooted phones dont allow raw access to the 13.56Mhz hardware, if the phone has this. Typically you need a system compatible with the standard in use, and then you can often read and clone the card. In some systems the card will not respond unless it sees the correct system ID, which is broadcast from every door.

[Reply](#)

[Report comment](#)

CampGareth says:

June 20, 2017 at 7:16 am

I should be more precise, my Android phone notices there's a card nearby, attempts to read but fails to do so. I was using NFC Tag Cloner which reports "Low level read of this tag type is not supported yet". I should really go ask the in-building makerspace people what's going on, they recently ran a small competition and got entrants by having people scan their cards at an arduino or similar with an add-on board, they probably know more about what's going on.

[Reply](#)

[Report comment](#)

mkomarinski says:

June 20, 2017 at 6:40 am

I have 5 NFC badges with me at any one time. Fortunately one doubles as a building pass and MBTA pass.

[Reply](#)

[Report comment](#)

Alphatek says:

June 20, 2017 at 6:13 am

115? The man's a crazy fool. There's no way to get below 127.

Reply

Report comment

Dan says:

June 20, 2017 at 3:00 pm

He'd have 112 if he hadn't had to own acetone, sugary, and a spare wristband.

If you want to 'simplify', I own 2 things: a house and a car. Small stuff inside them counts as part of the larger item.

Reply

Report comment

Paul says:

June 20, 2017 at 7:50 pm

You are a true hacker. :)

Reply

Report comment

Electra says:

June 20, 2017 at 6:26 am

50/50 acetone and xylene works great and does it in about 2-3 hours. :)

Doesn't damage the chip at all. Some cards use printed/foil tracks so they just fall apart.

Get a NFC tag/strap/etc of the form factor you like and transplant the chip.

Reply

Report comment

Elliot says:

June 20, 2017 at 7:44 am

Shameless plug: <http://tinylabs.io/keysy>. Won't work for mass transit and other 13.56MHz cards but works for virtually any 125kHz card (typically used for building access control, public garages, etc)

Reply

Report comment

dave says:

June 20, 2017 at 8:07 am

Wait, what is a 'waterproof aspirin band' I don't live in the US.

Reply

Report comment

dave says:

June 20, 2017 at 8:18 am

OK, duckduckged it(eff google), an aspirin band is a red silicone wrist band(Lance Armstrong style) with water resistant chambers for two Bayer 325mg emergency aspirin pills for use when chest pan is felt. Cool idea itself!

Reply

Report comment

chandwki says:

June 20, 2017 at 9:49 am

Anyone know how you can go about cloning these?

Reply

Report comment

0xFFFF says:

June 20, 2017 at 4:37 pm

The card is most likely Mifare DESFire EV1. Assuming you are familiar with all of the necessary commands you only need to know the application ID, Algorithm, file ID, write and read key.

[Reply](#)

[Report comment](#)

Leave a Reply

Email (required)

(Address never made public)

Name (required)

Website

Save my name, email, and website in this browser for the next time I comment.

Notify me of new comments via email.

[Post Comment](#)

Notify me of new posts via email.

Please be kind and respectful to help make the comments section excellent. ([Comment Policy](#))

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)



[HOME](#)

[BLOG](#)

[HACKADAY.IO](#)

[TINDIE](#)

[HACKADAY PRIZE](#)

[VIDEO](#)

[SUBMIT A TIP](#)

[ABOUT](#)

[CONTACT US](#)

NEVER MISS A HA



SUBSCRIBE TO NE

Enter Email Address

Copyright © 2023 | Hackaday, Hack A Day, and the Skull and Wrenches Logo are Trademarks of Hacka

Digital Services Act

Powered by WordPress VIP