



HOME

TECHNOLOGY

SECURITY NEWS ▾

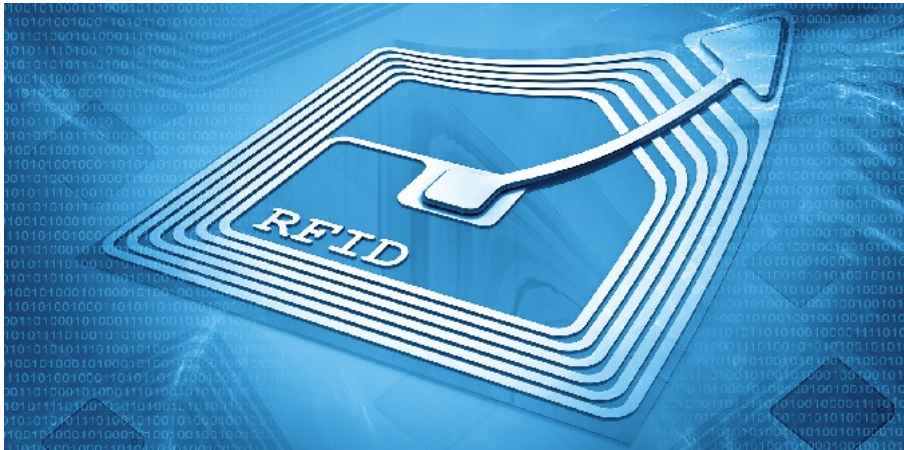
INTERNET ▾

LAWS AND LEGALITIES

GADGETS ▾

SCIENCE

YOU ARE AT: Home » Hacking news » Hacking RFID Payment Cards Now Possible with an Android App



## Hacking RFID Payment Cards Now Possible with an Android App

0

BY DELWYN PINTO ON NOVEMBER 24, 2014

HACKING NEWS, SECURITY NEWS, VULNERABILITY



Mifare 1K Price  
US\$ 0.10+

ISO/IEC14443-A, Non-NXP  
High Quality and High  
Volume

● ○



### Hacking RFID Payment Cards Now Possible with Android App

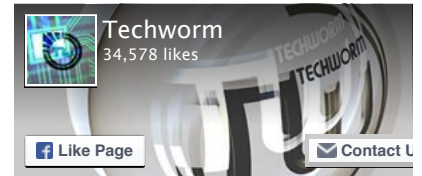
Use of RFID based smart cards has grown popular with the introduction of NFC in our smart phones. With Apple also embracing it, the technology is set to make a revolutionary boom. And as with every popular technology, the hacks and attacks have now begun to surface against RFID cards. Researchers at [TrendMicro Labs](#) have discovered that hacking RFID based payment cards is possible through a Android

App.

### Android App as the medium

Trend researchers have discovered a high-risk Android app detected as [ANDROIDOS\\_STIP.A](#) in Chile. This app is used to recharge smart cards that use RFID and is being spread via blogs, forums and other sites. Paying via RFID cards is becoming more popular nowadays as more mobile devices add NFC support. Banks, merchants or public services issue RFID cards to their customers with prepaid credits. The Apple Pay service has only added to the momentum of NFC based payments.

How was the tool's author able to rewrite the card's information despite not having the correct



Techworm  
34,578 likes  
6 hrs



US officials fear that Russia



SUBSCRIBE NOW

Your e-mail address

Subscribe

READERS CHOICE



The Pirate Bay holds strong as Popcorn Time shuts down, YIFY knocked offline and...



Top 10 Tips And Tricks for WhatsApp users:



PirateSnoop Browser to Unblock Blocked Torrent Websites

authentication keys? This is because these cards are based on an older version of the MIFARE.



MIFARE refers to a family of chips widely used in contactless smart cards and proximity cards.) series of cards (MIFARE Classic), which is known to have multiple security problems. An attacker is able to clone or modify a MIFARE Classic card in under 10 seconds, and the equipment (such as the Proxmark3), together with any needed support, is sold online. Trend Micro researchers have given the instance of recent hacking of BIP.

INFO

NDEF

IC manufacturer

NXP Semiconductors

IC type

MIFARE Classic (MF1S50)

Memory content

Sector 0 (0x00)

[00]

0C B3 F3 9C D0 88 04 00

|.....|

r--

47 41 45 56 65 10 06 08

|GAEVe...

[01]

00 00 00 00 00 00 00 00

|.....|

rwi

00 00 00 00 00 00 00 00

|.....|

[02]

00 00 00 00 00 00 00 00

|.....|

rwi

00 00 00 00 00 00 00 00

|.....|

[03]

FF:FF:FF:FF:FF:FF

Factory default key

wxx

FF:07:80 69

(r)

FF:FF:FF:FF:FF:FF

Factory default key

Sector 1 (0x01)

[04]

00 00 00 00 00 00 00 00

|.....|

rwi

00 00 00 00 00 00 00 00

|.....|

[05]

00 00 00 00 00 00 00 00

|.....|

rwi

00 00 00 00 00 00 00 00

|.....|

[06]

00 00 00 00 00 00 00 00

|.....|

rwi

00 00 00 00 00 00 00 00

|.....|

[07]

FF:FF:FF:FF:FF:FF

Factory default key

wxx

FF:07:80 69

(r)

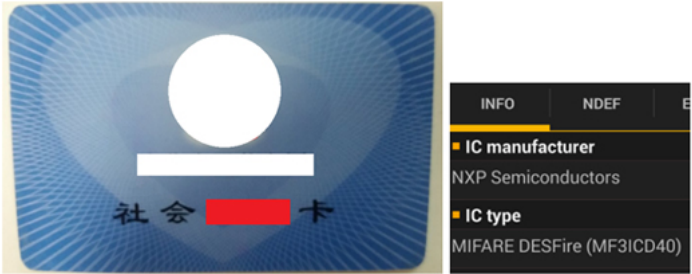
FF:FF:FF:FF:FF:FF

Factory default key

Manufacturer and memory content of a MIFARE Classic card

Working

Trend researchers, after inspecting the app have found that the app could read and write onto the smart cards through any phone equipped with NFC. This particular app can rewrite data on the card for example, increasing the balance left on it to 10,000 Chilean pesos (approximately 15 US dollars). This is however restricted to only these specific cards because of the format restrictions. Using tools available in abundance, the attacker managed to crack the authentication of the cards. Once that was done, the card was cloned and the data on it rewritten through the android app.



The Top Ten Hacker Tools of 2015

SnoopSnitch App uses radio signals to find nearby tracking devices

Trending Today Sponsored by Revcont



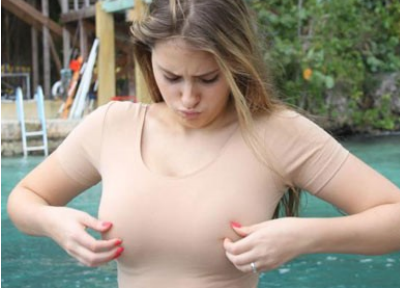
Taiwan Millionaires Hope Their Secret Will Never Be Revealed



Taiwan Man Exposes A Secret To Earn \$3,200/Week From Home



Taipei Mom Shares Secret That Makes her \$87/Hour!



My Dad's Trick To Seducing 19 Year Olds



Taipei, Taiwan : Shocking Trick! Regrows Hair Naturally

Other successful attacks

Attacks on other kinds of MIFARE cards (specifically, MIFARE DESFire and MIFARE Ultralight) are known to exist. The researchers stated that there were at least three vulnerable cards, a social security card with banking service, a payment card for transportation and shopping, and a dining card. The social security card has approximately seven million users. The card in question in the dining card uses MIFARE Classic card, which is known to be easy to manipulate. The other two use MIFARE DESFire, which in turn are vulnerable to side-channel attacks. The cryptosystems in these cards can leak information, leading to the full keys leaking out in around 7 hours. Once the keys have been leaked the card can be manipulated to any extent according to the attackers wishes.

These cards have been discontinued a long time ago, because of the risks mentioned. But looks like some organizations have preferred using the older cards thus putting their customers at risk.

Resource : [TrendMicro Labs](#)

5.9k

199

28

0

0

23

ABOUT AUTHOR

DELWYN PINTO

A person proud to have an alternate view

Trending Today

Sponsored by Revcontent

Taiwan M Hope The Never Be

Odd Trick To Kill Belly Fat In A Week

My Dad's Trick To Seducing 19 Year Olds

Say 'Goodbye' To Eye Bags - Simple 2 Step

http://www.techworm.net/2014/11/hacking-rfid-payment-cards-now-possible-android-app.html

3/5



From The Web

Top 10 Movie Sexually Attractive of All Time!  
Share The Buzz

Lifehack #247: Get A Good (Snore-Free) Night's Sleep With This Trick  
Stop Snoring Today

Better to marvel at rugby giants than confront them - FT.com  
Financial Times

The Most Exciting MMORPG You've Ever Played. Don't miss this!  
Sparta Online Game

Build Amazing Simple Website In Only 10 Minutes !  
Wix.com

That's How You Find Super Cheap Flights!  
Save70

RELATED POSTS



OCTOBER 27, 2015 0

The arrest and bail saga of 15 year old alleged TalkTalk hacker



OCTOBER 27, 2015 0

WhatsApp collects users phone numbers and call duration



OCTOBER 26, 2015 0

Is LulzSec back? TalkTalk hacker claims he is from Lulzsec

0 Comments

Sort by Top



Add a comment...

Facebook Comments Plugin

LEAVE A REPLY

Your Name

Your Email

Your Website

Your Comment

POST COMMENT

ABOUT US

***Techworm*** is a Security News Platform that centers around Infosec, Hacking, Xero-days, Malware, Vulnerabilities,Cyber Crime, DDoS, Surveillance and Privacy Issues and to keep you Informed and Secure.

PAGES

About Us




Contact Us

Home Page

Privacy Policy

Security Researcher Acknowledgments

Submission Guidelines



Copyright © 2014  
Techworm  
All rights reserved

The Authors' opinions may not necessarily reflect the official position of TechWorm

Techworm