Implantable RFID

Is Cyborgification Right For You?

BSides RDU

2024-09-13

Shouts and Greets to Co-Presenters Here in Spirit

Max Power

Babak Javadi

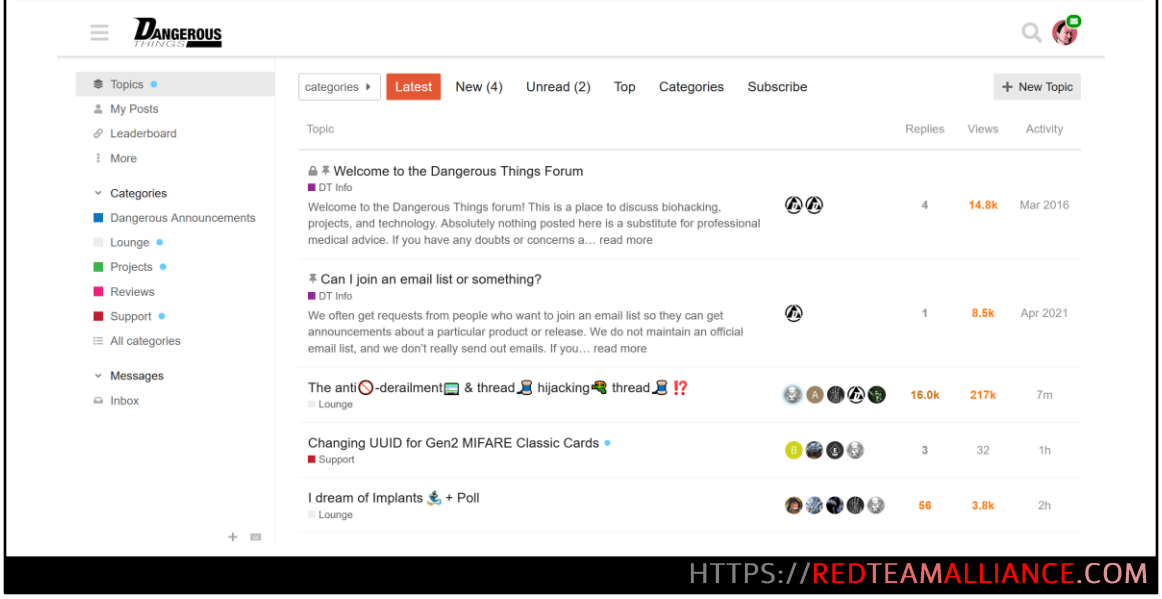
APOLOGIES TO BSIDESORL

Many Thanks to Pioneers in This Field

Amal Graafstra
Dangerous Things

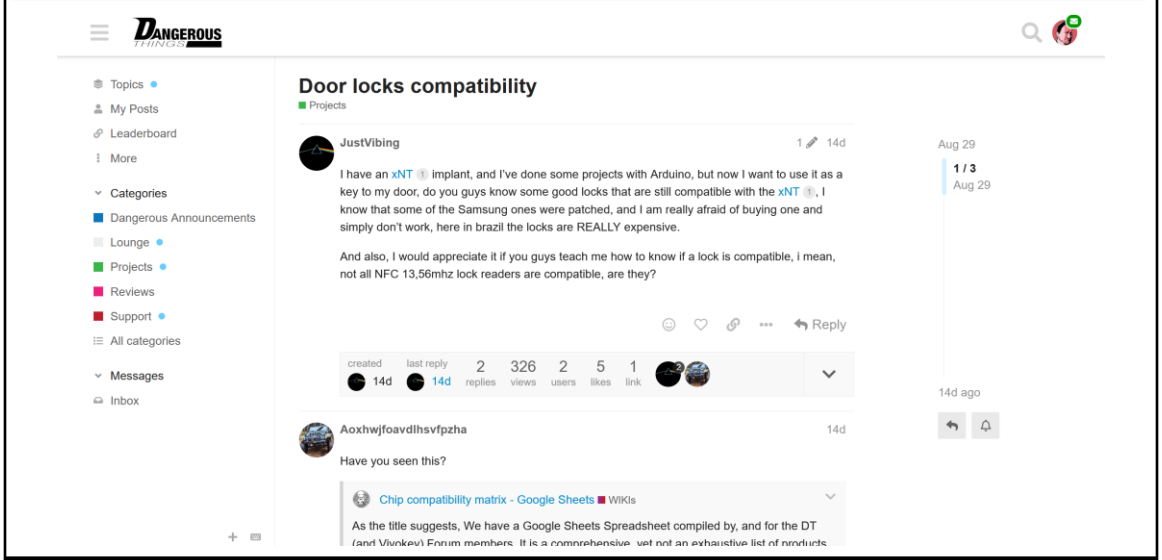
Christian Herrmann
"Iceman"

IF YOU WANT TO LEARN MORE – FORUM.DANGEROUSTHINGS.COM



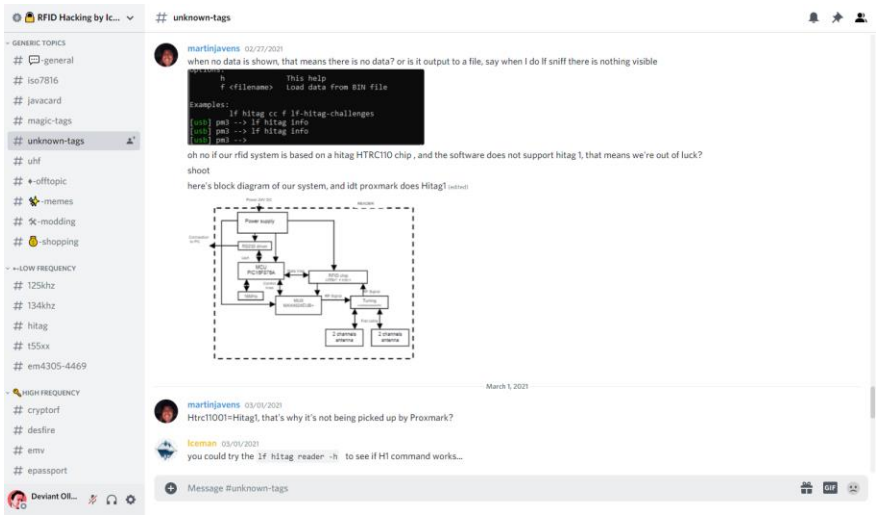
HTTPS://REDTEAMALLIANCE.COM

IF YOU WANT TO LEARN MORE – FORUM.DANGEROUSTHINGS.COM



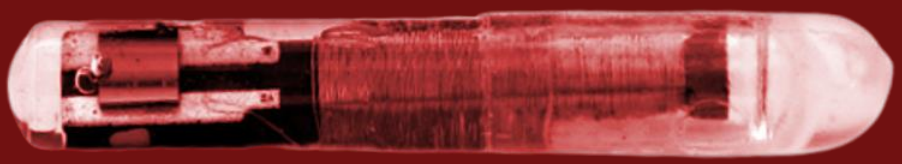
HTTPS://REDTEAMALLIANCE.COM

IF YOU WANT TO LEARN MORE – DISCORD.GG/ICEMAN



HTTPS://REDTEAMALLIANCE.COM

Electronic Credentials



WHO USES ELECTRONIC CREDENTIALS?

HTTPS://REDTEAMALLIANCE.COM

Many RFID Credentials are Simply Like Folders

Many RFID Credentials are Simply Like Folders

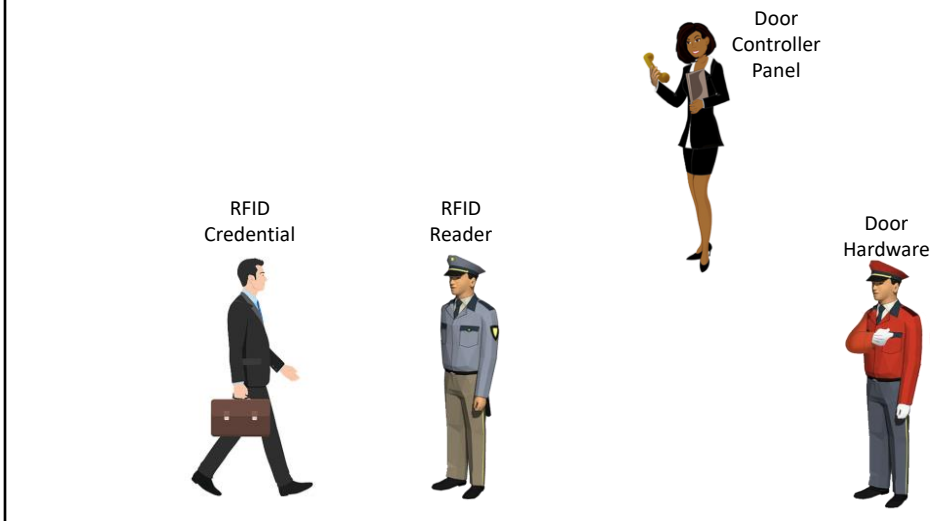
HTTPS://REDTEAMALLIANCE.COM

Many RFID Credentials are Simply Like Folders

An RFID Credential Analogy

HTTPS://REDTEAMALLIANCE.COM

Access Control System Analogy



ACCESS CONTROL SYSTEM ANALOGY

Door Controller Panel

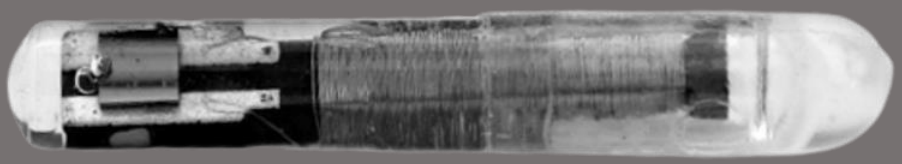
RFID Credential

RFID Reader

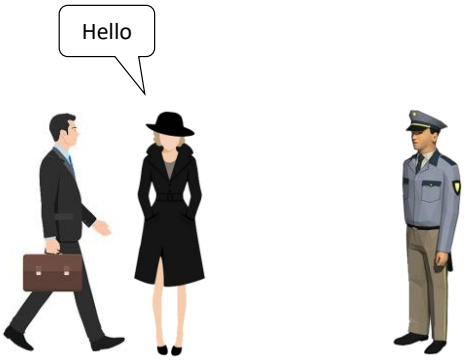
Door Hardware

HTTPS://REDTEAMALLIANCE.COM

Credential Cloning Attacks

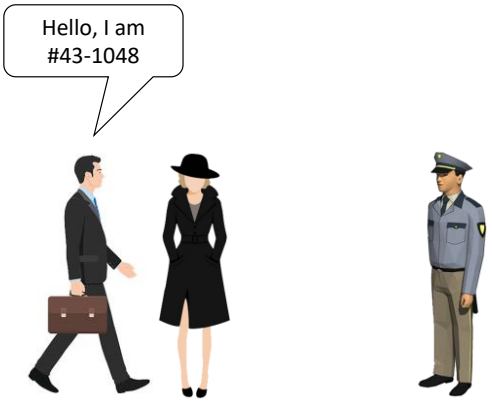


CREDENTIAL CLONING ATTACKS



HTTPS://REDTEAMALLIANCE.COM

CREDENTIAL CLONING ATTACKS



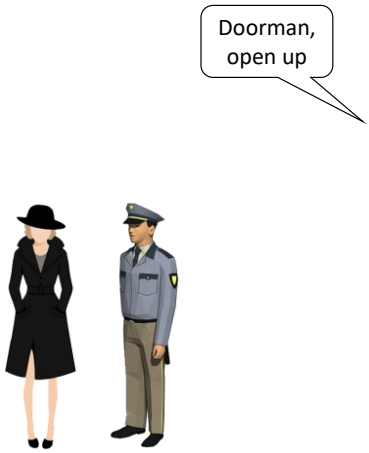
CREDENTIAL CLONING ATTACKS

CREDENTIAL CLONING ATTACKS

CREDENTIAL CLONING ATTACKS

CREDENTIAL CLONING ATTACKS

CREDENTIAL CLONING ATTACKS



HTTPS://REDTEAMALLIANCE.COM

CREDENTIAL CLONING IS NOT HARD

HTTPS://REDTEAMALLIANCE.COM

This is a “service” being provided with ease by kiosks at hardware stores now. We’ll explain why it’s so simple and what technology makes it so cheap.

Credential Cloning is not Hard

Credential Cloning is not Hard

HTTPS://REDTEAMALLIANCE.COM

Credential Cloning is not Hard

HTTPS://REDTEAMALLIANCE.COM

Remember Our Credential Analogy

HTTPS://REDTEAMALLIANCE.COM

Remember Our Credential Analogy

HTTPS://REDTEAMALLIANCE.COM

Remember Our Credential Analogy

HTTPS://REDTEAMALLIANCE.COM

You Don't Have to Understand The Data Format

HTTPS://REDTEAMALLIANCE.COM

You Just Have to be Able to Read What's in the Credential

RFID Credential and Reader

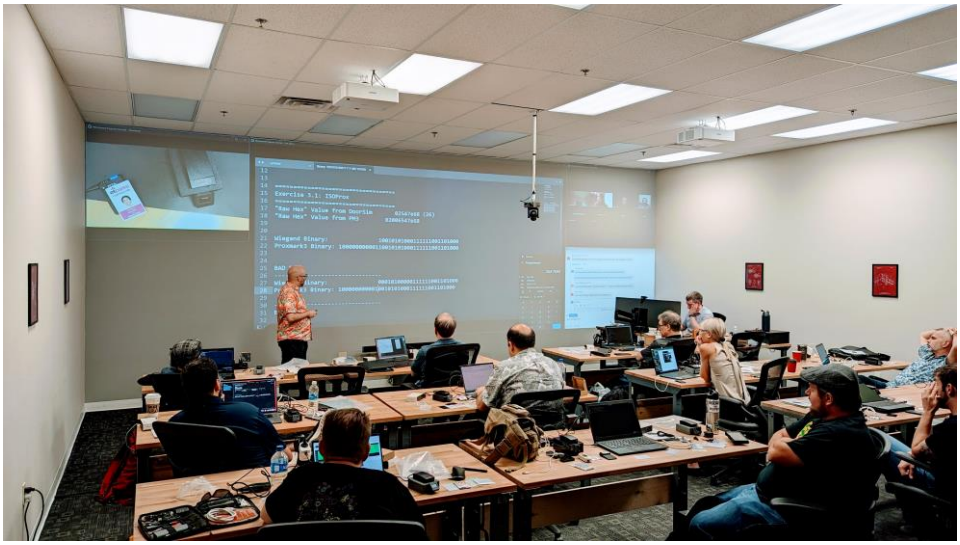
HTTPS://REDTEAMALLIANCE.COM

RFID Credential and Reader

Hacking Electronic Credentials

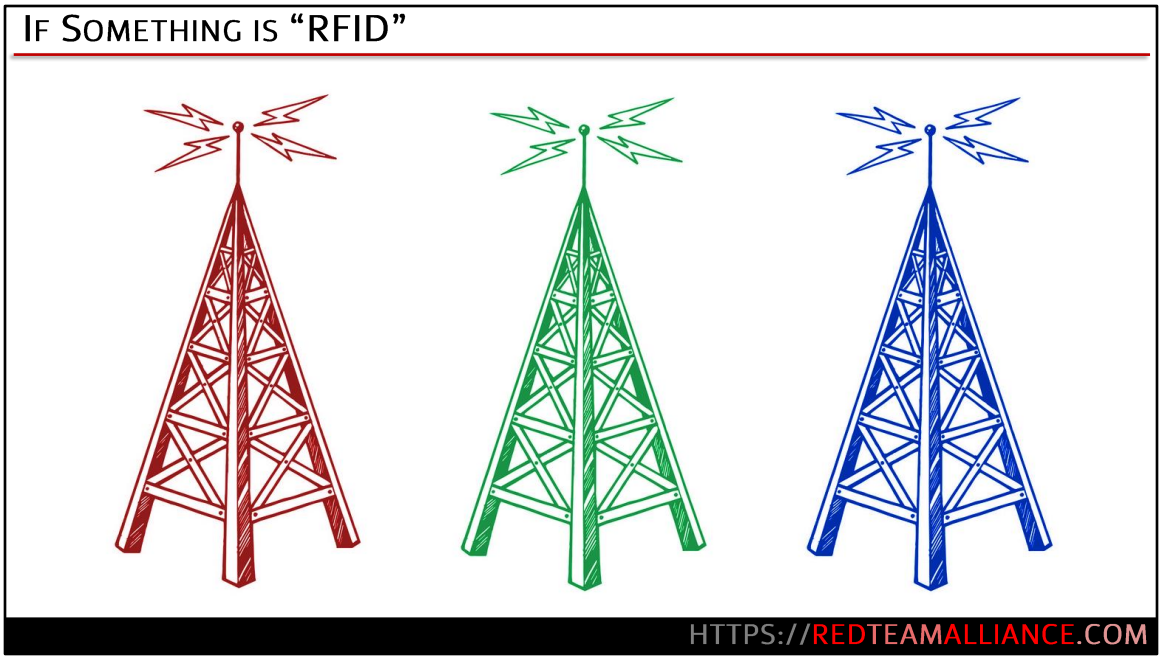
HTTPS://REDTEAMALLIANCE.COM

Hacking Electronic Credentials



HTTPS://REDTEAMALLIANCE.COM

If Something is "RFID"



You need three things for a system to be "RFID"

If Something is "RFID"

Credential

Reader

If Something is "RFID"

Antenna

Credential

Reader

HTTPS://REDTEAMALLIANCE.COM

If Something is "RFID"

Antenna

Credential

Antenna

Reader

INDUCTIVE COUPLING

HTTPS://REDTEAMALLIANCE.COM

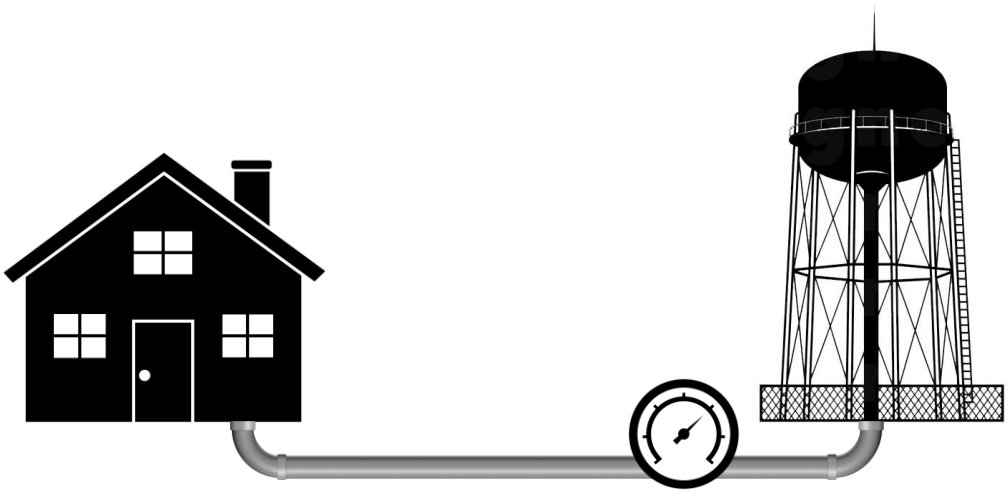
read distances aren't possible over many feet
The fob or card has no power of its own
(this is why “tracking” is not possible)

Communication by Power Draw

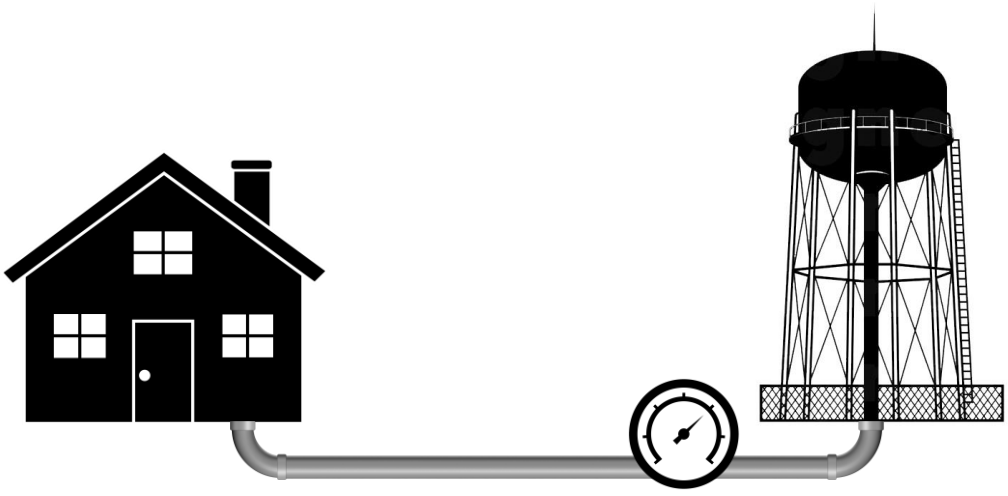
Communication by Power Draw

Communication by Power Draw

Communication by Power Draw



Communication by Power Draw



Communication by Power Draw

Communication by Power Draw

Communication by Power Draw

HTTPS://REDTEAMALLIANCE.COM

Communication by Power Draw

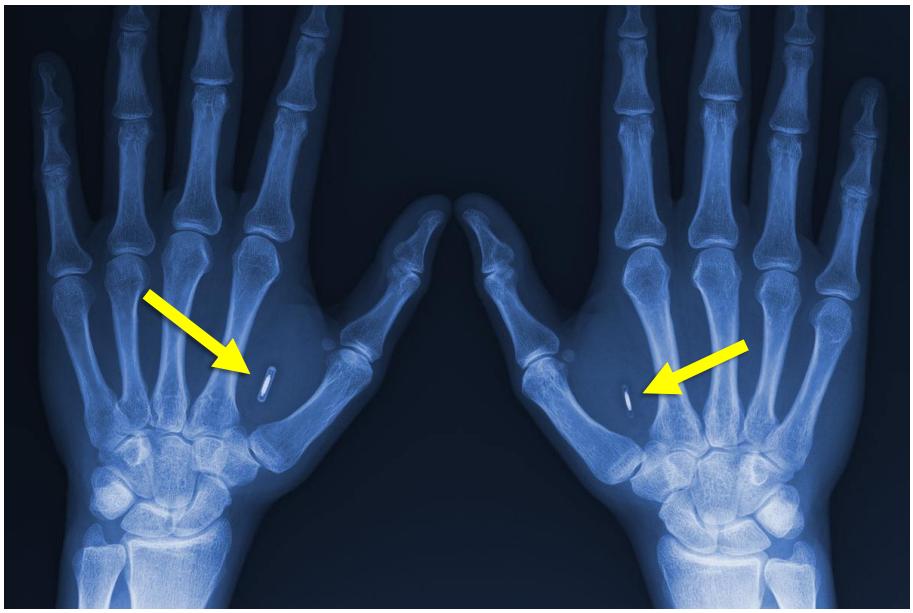
HTTPS://REDTEAMALLIANCE.COM

RFID Credentials

RFID Credentials

RFID Credentials

Embedded RFID Credentials



HTTPS://REDTEAMALLIANCE.COM

Dev and his wife Tarah have some unique hands

Injected in between the 1st and 2nd metacarpal of both hands

Embedded RFID Credentials

HTTPS://REDTEAMALLIANCE.COM

Not a joke… you can come feel them later or watch the video online of me getting mine. ;-)

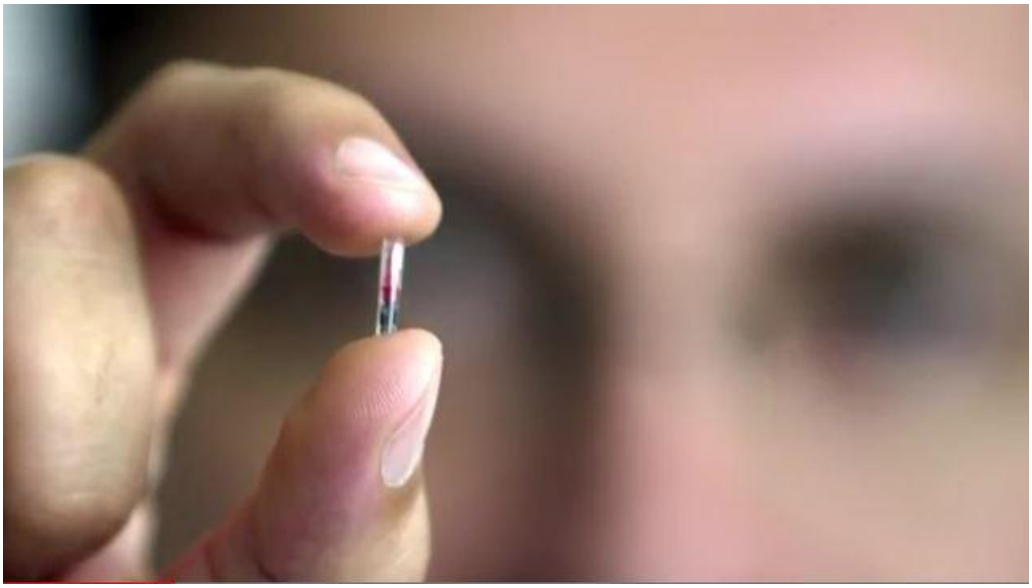
Embedded RFID Credentials

HTTPS://REDTEAMALLIANCE.COM

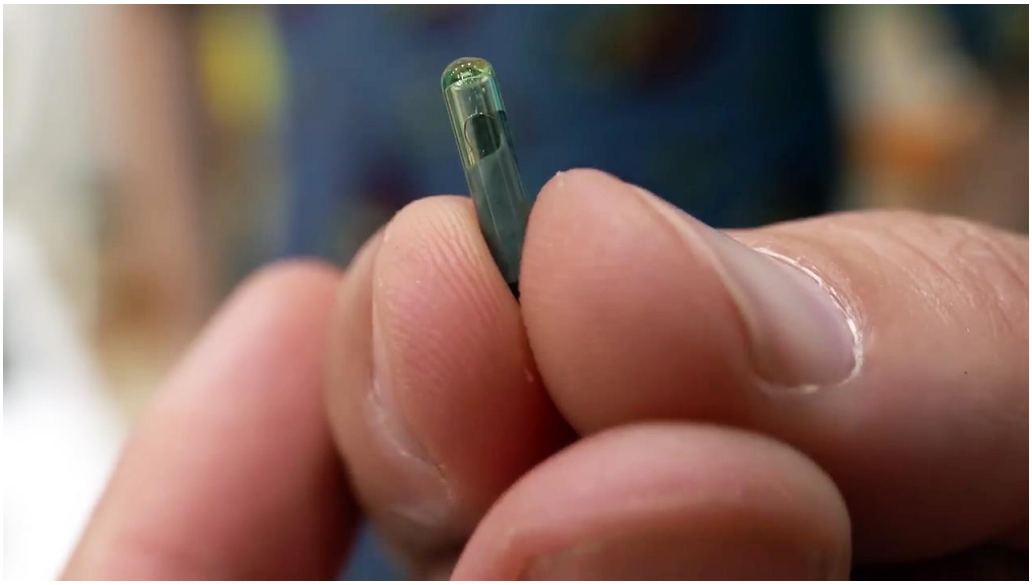
RFID chips in each hand… one low freq and one high freq

Tarah had her badge cloned to her hand and can now open all doors at the facility with a literal flick of the wrist. Freaked out the PhysSec guys when she demonstrated it. ;-)

Biohacking: Glass RFID Implants

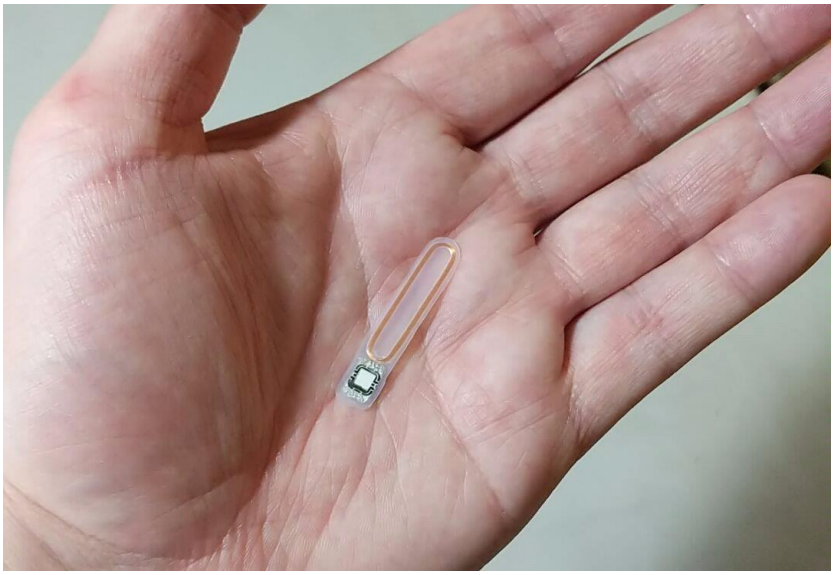


Biohacking: Glass RFID Implants

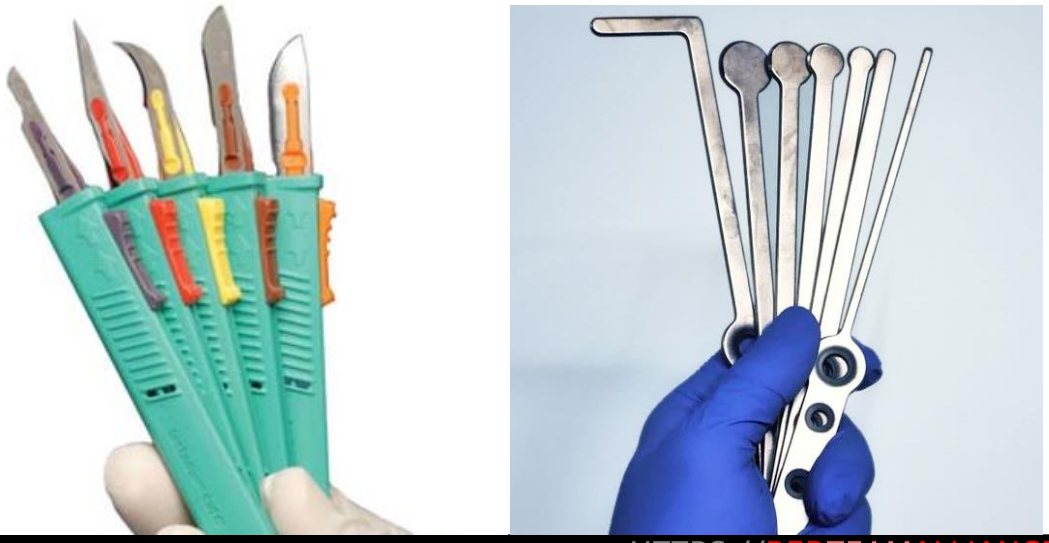


Biohacking: Glass RFID Implants

Biohacking: Flex RFID Implants



Biohacking: Flex RFID Implants



Installing the older style “flex” implants was more of a procedure… Scalpels, dermal elevators, etc

BIOHACKING: MINIFLEX RFID IMPLANTS

HTTPS://REDTEAMALLIANCE.COM

I nicknamed these the “mini” flex but they are really just about the full line of flex implants now.

BIOHACKING: MINIFLEX RFID IMPLANTS

HTTPS://REDTEAMALLIANCE.COM

Little bowtie antenna (length can vary)

56 pico farad
30-20 pico farad (Chinese weird chips)
17 pico farad (longer antenna but width remains the same)
20 pico fara
^ they have antennas for all of these ranges

BIOHACKING: MINIFLEX RFID IMPLANTS

HTTPS://REDTEAMALLIANCE.COM

Little bowtie antenna (length can vary)

56 pico farad
30-20 pico farad (Chinese weird chips)
17 pico farad (longer antenna but width remains the same)
20 pico fara
^ they have antennas for all of these ranges

BIOHACKING: MINIFLEX RFID IMPLANTS

HTTPS://REDTEAMALLIANCE.COM

4 gauge (~5mm) piercing needle/syringe can be used to install. No knives needed.

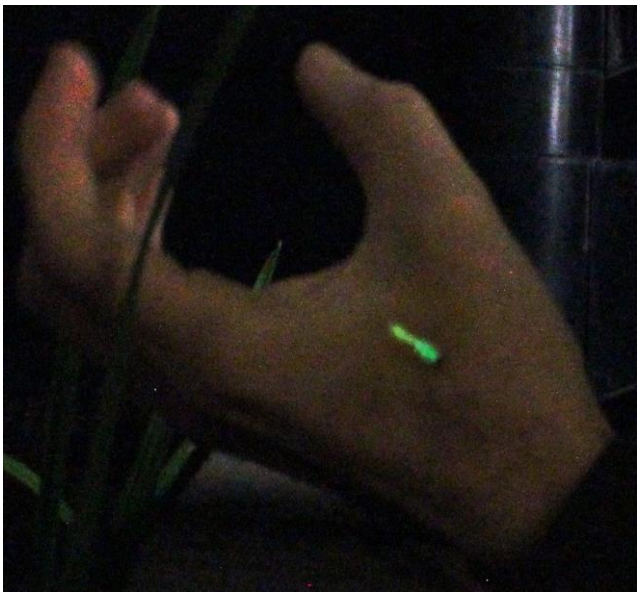
BIOHACKING: MAGNETS

Biohacking: Magnets

Biohacking: Magnets

BIOHACKING: MAGNETS

BIOHACKING: TRITIUM "FIREFLY TATTOOS"

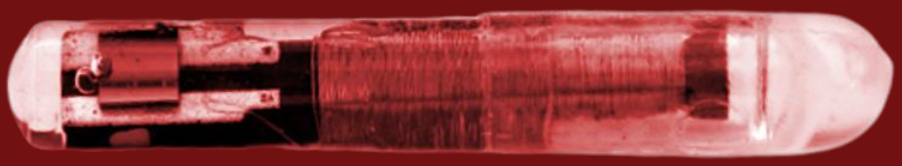


HTTPS://REDTEAMALLIANCE.COM

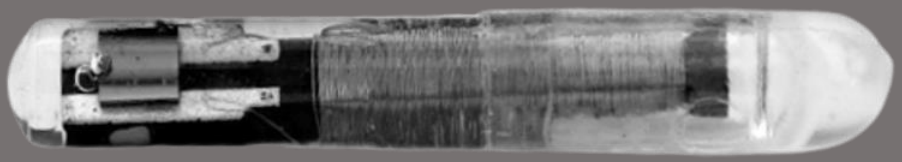
Tritium inserts
(from cyberize.me and biohack.me … not as safe)

Biohacking: Subdermal LEDs

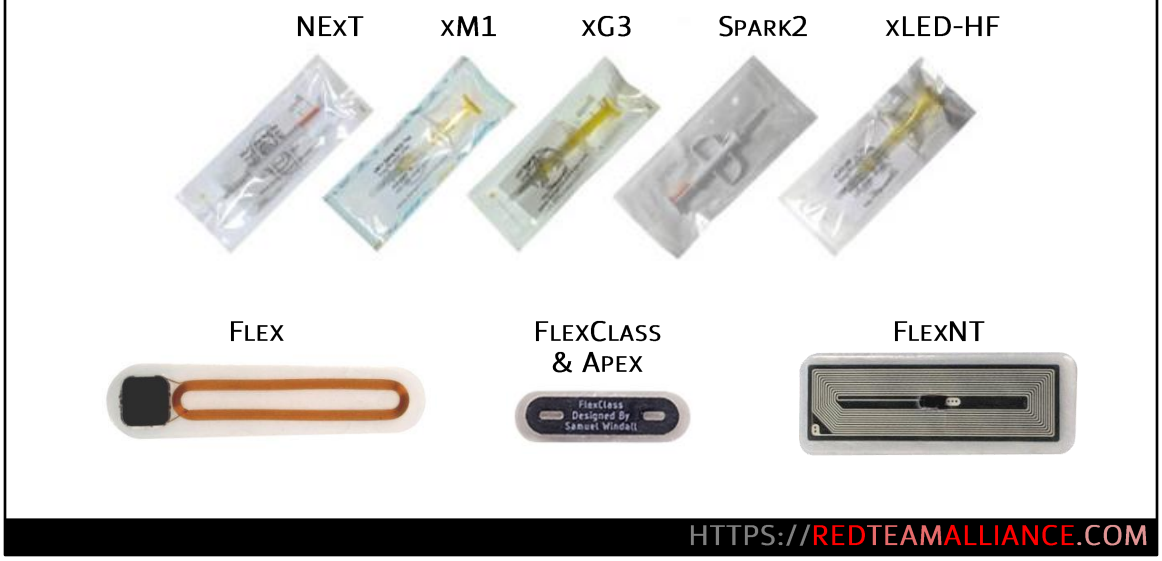
Questions and Concerns From Hackers



Different Chips, Different Products



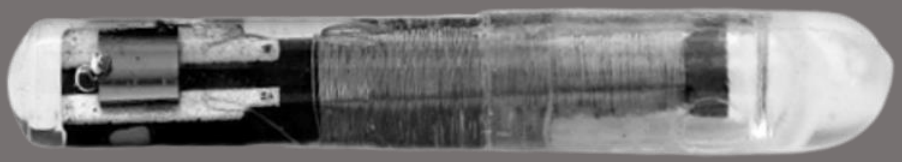
Making Sense of Different Chips and Products



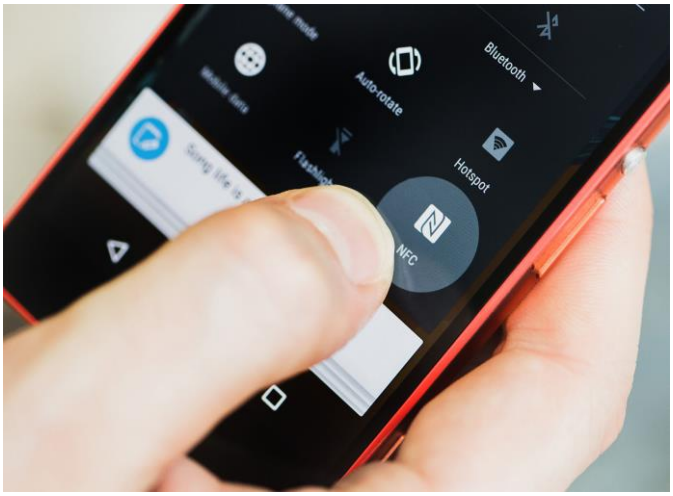
FlexNT is an antenna designed by ClearCo using this inlay Used to be used in rings, etc. But performance is better when flat.

DangerousThings bought them in bulk from NFCRing and did the encapsulation. Very robust but large. Can go in a middle finger, etc. (Blade and dermal elevator)

Two Often-Confused Terms

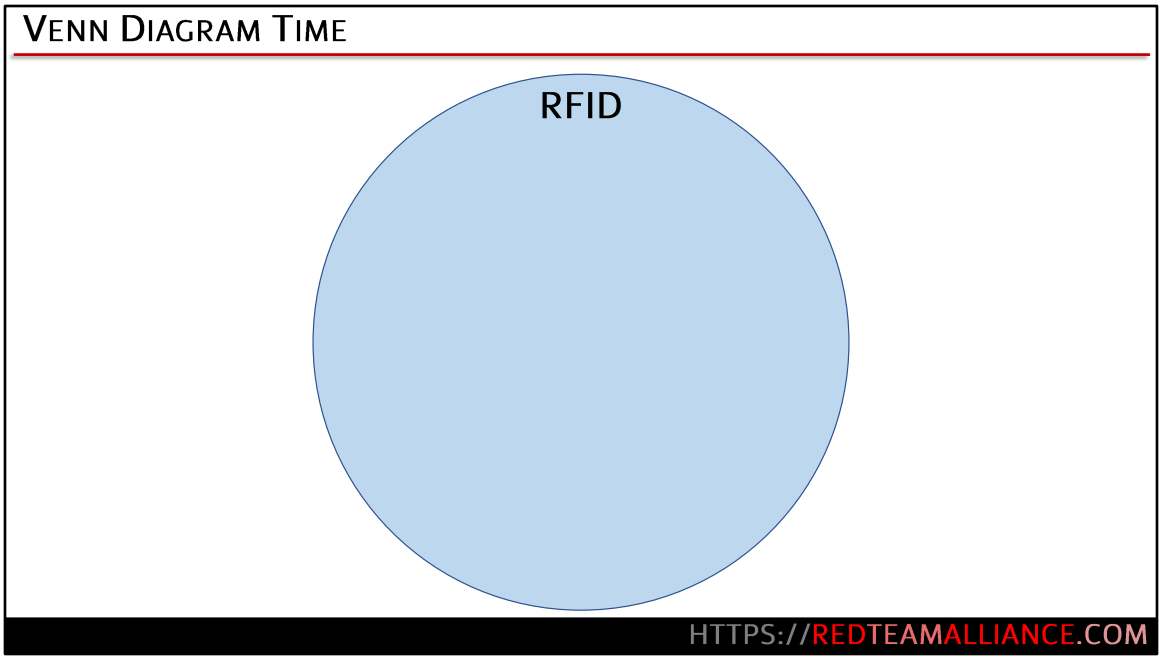


"RFID... That's Like the Same Thing as NFC, Right?"



HTTPS://REDTEAMALLIANCE.COM

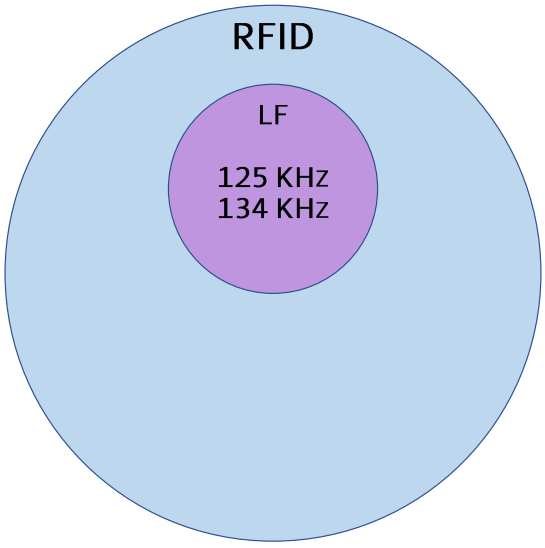
VENN DIAGRAM TIME



Remember, to be RFID all a system needs is…

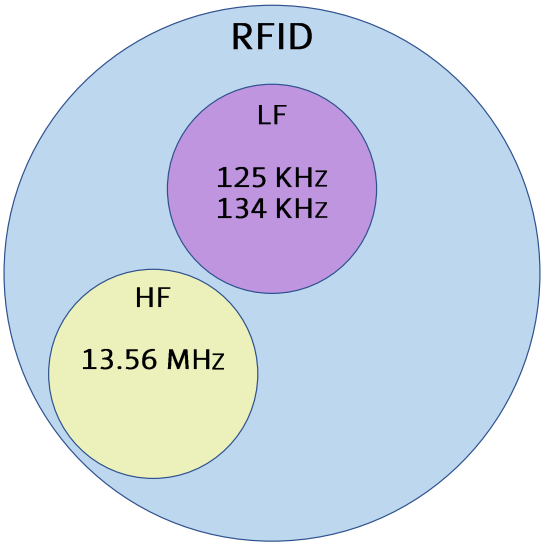
1. Device
2. Reader
3. Antennas and Inductive Coupling To Communicate

Venn Diagram Time

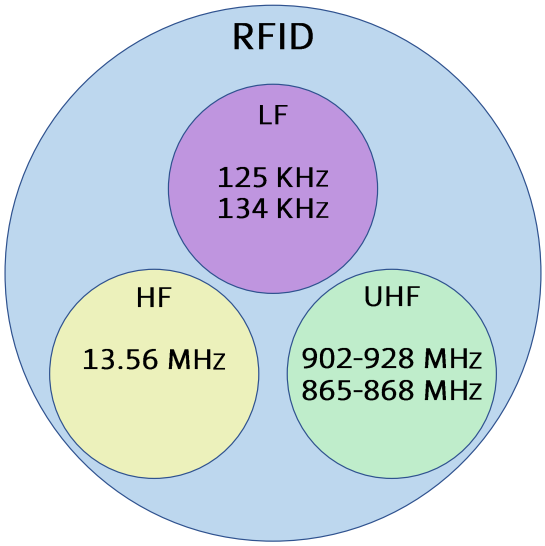


HTTPS://REDTEAMALLIANCE.COM

Venn Diagram Time

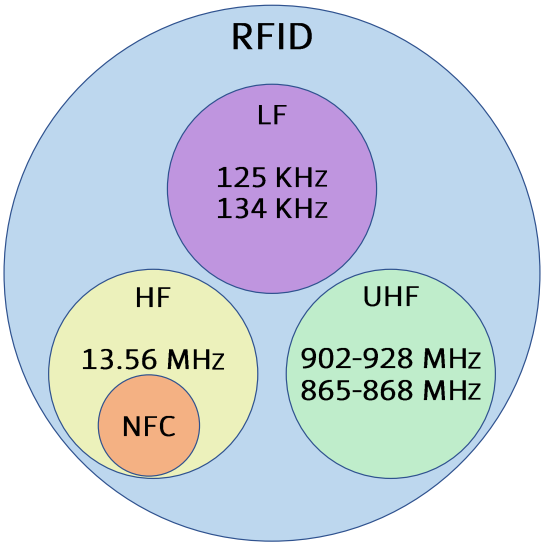


Venn Diagram Time



HTTPS://REDTEAMALLIANCE.COM

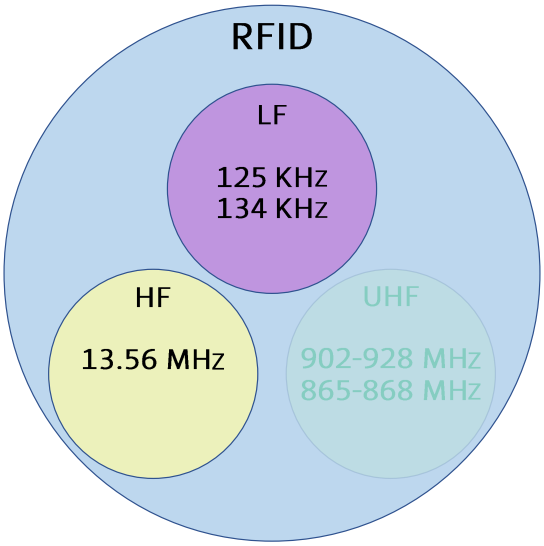
Venn Diagram Time



HTTPS://REDTEAMALLIANCE.COM

NFC…
ISO 14443
FeliCa
ISO 18092

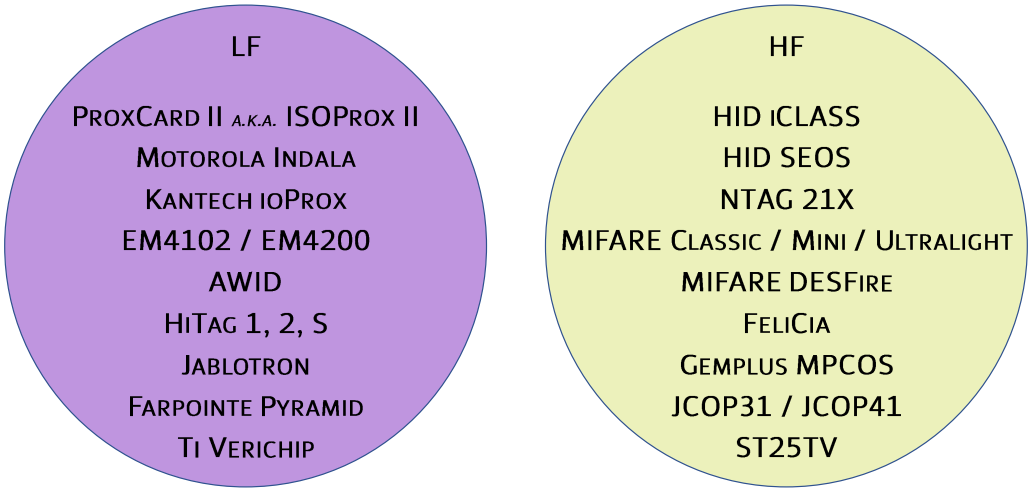
WE'RE NOT DISCUSSING UHF AT ALL TODAY



HTTPS://REDTEAMALLIANCE.COM

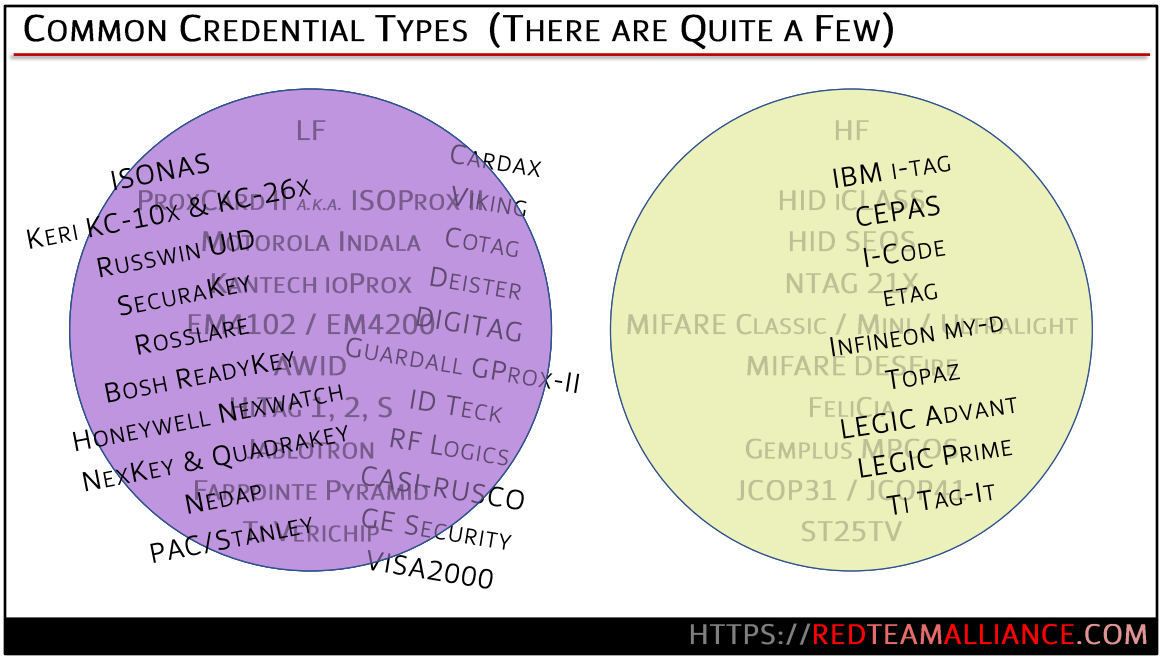
(we're going to ignore UHF for now because almost no one is using that for implants and there's basically zero reason you'd want to)

Common Credential Types



HTTPS://REDTEAMALLIANCE.COM

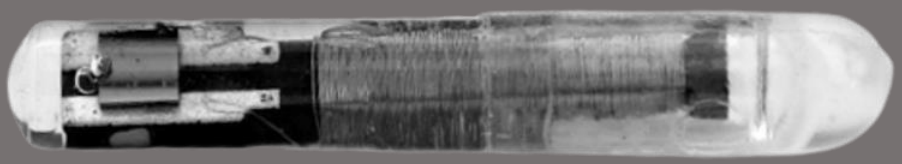
Explain what is meant by “credential type” here… it’s both the RFID coupling technology *AND THE FEATURE SET ON THE CHIP*



Explain what is meant by “credential type” here… it’s both the RFID coupling technology *AND THE FEATURE SET ON THE CHIP*

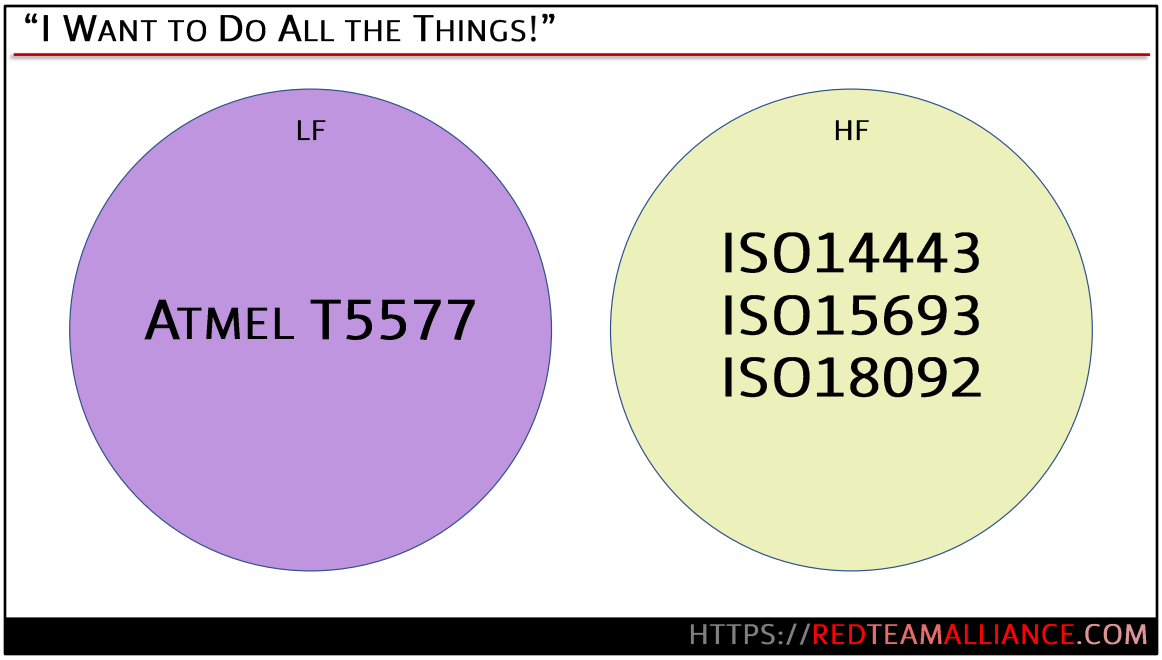
That's a Lot of Credential Types!

How Do I Choose the Right One?



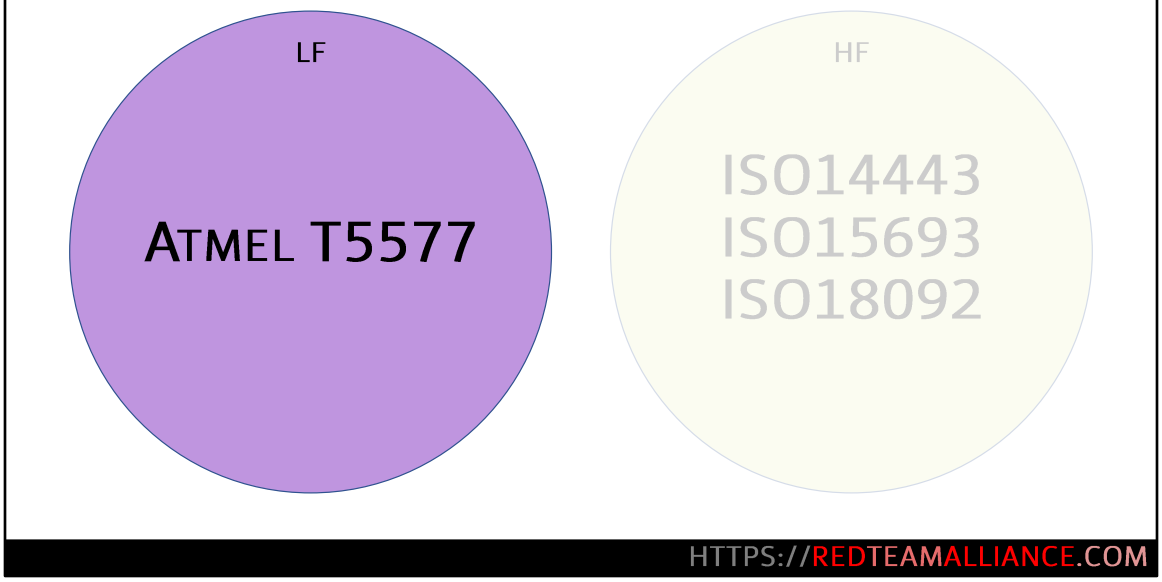
"I WANT TO DO ALL THE THINGS!"

Fortunately, it's not necessary go out and get a dozen implants all over your body, hah. But more power to you if you want to. =)



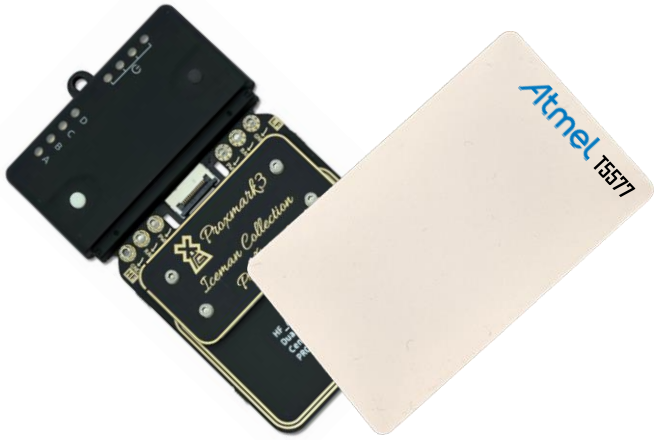
We can simplify the landscape considerably. Let's re-make those two Venn Diagram circles.

Let's Talk Low Frequency First...

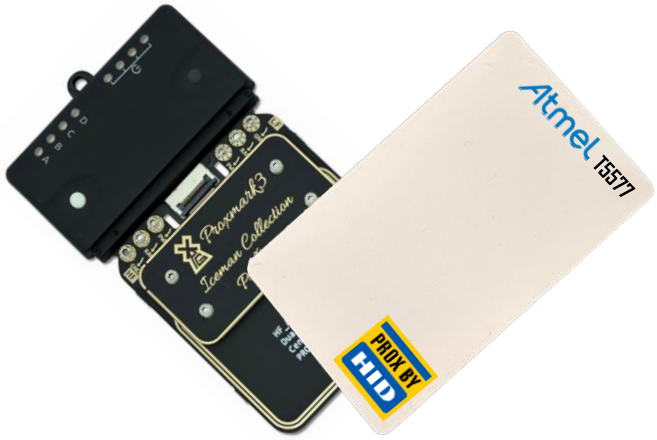


We've collapsed the Low Frequency side of things to a single name

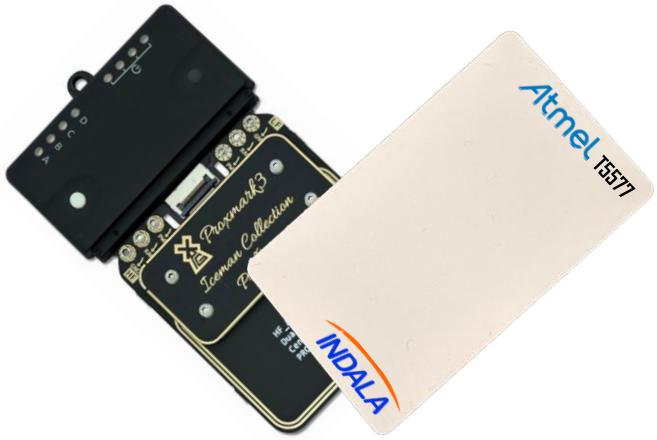
ATMEL T55XX (AND EM4X50)



ATMEL T55XX (AND EM4X50)

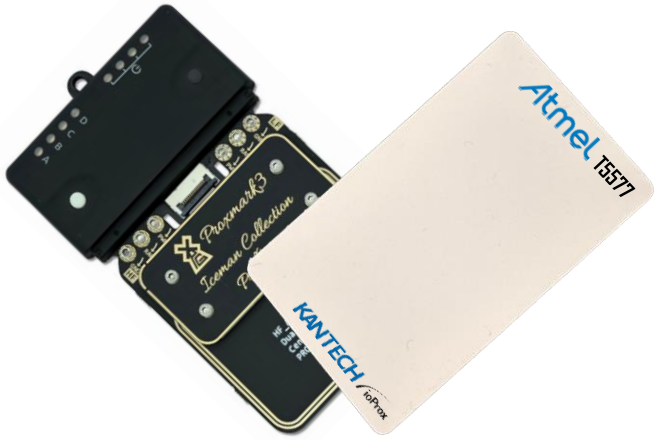


ATMEL T55XX (AND EM4X50)



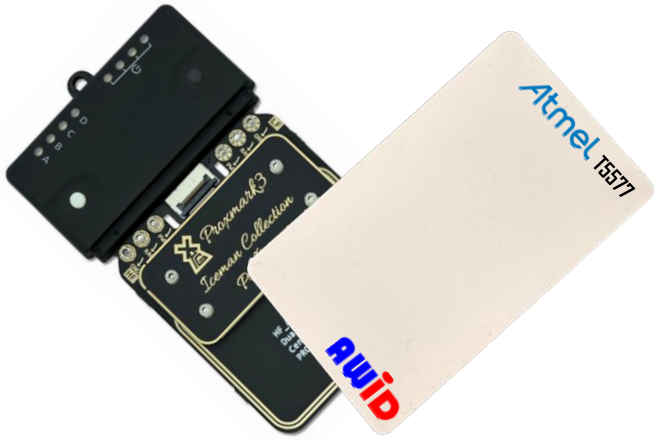
HTTPS://REDTEAMALLIANCE.COM

ATMEL T55XX (AND EM4X50)



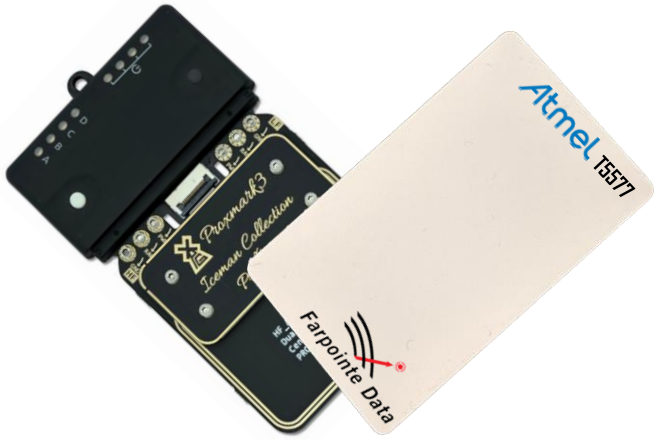
ATMEL T55XX (AND EM4X50)

ATMEL T55XX (AND EM4x50)



ATMEL T55XX (AND EM4X50)

ATMEL T55XX (AND EM4X50)



HTTPS://REDTEAMALLIANCE.COM

ATMEL T55XX (AND EM4x50)

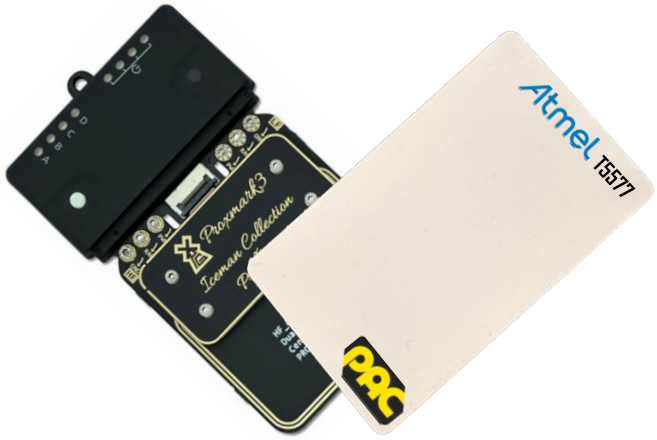
ATMEL T55XX (AND EM4X50)

ATMEL T55XX (AND EM4X50)

ATMEL T55XX (AND EM4X50)

ATMEL T55XX (AND EM4X50)

ATMEL T55XX (AND EM4X50)



ATMEL T55XX (AND EM4X50)

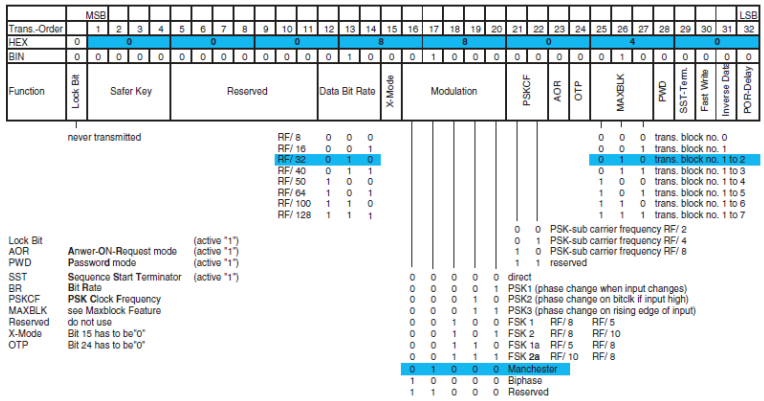
ATMEL T55XX (AND EM4x50)

ATMEL T55XX (AND EM4X50)

HTTPS://REDTEAMALLIANCE.COM

LOW FREQUENCY: ATMEL T5577 / T5567 / T5557 (T55XX)

Figure 0-2. ATA5577/ATA5567/T5557 Block 0 Initial Configuration Setting



HTTPS://REDTEAMALLIANCE.COM

T5555 is the same as “Q5” a.k.a. Temic
Temic had their T5551, T5552, T5553, T5554, T5555 and T5557 family.

The others are all T55x7, and the entire family is generally called “T55xx” (as are the proxmark commands, many of which have switches in case someone is using an old Q5 chip)

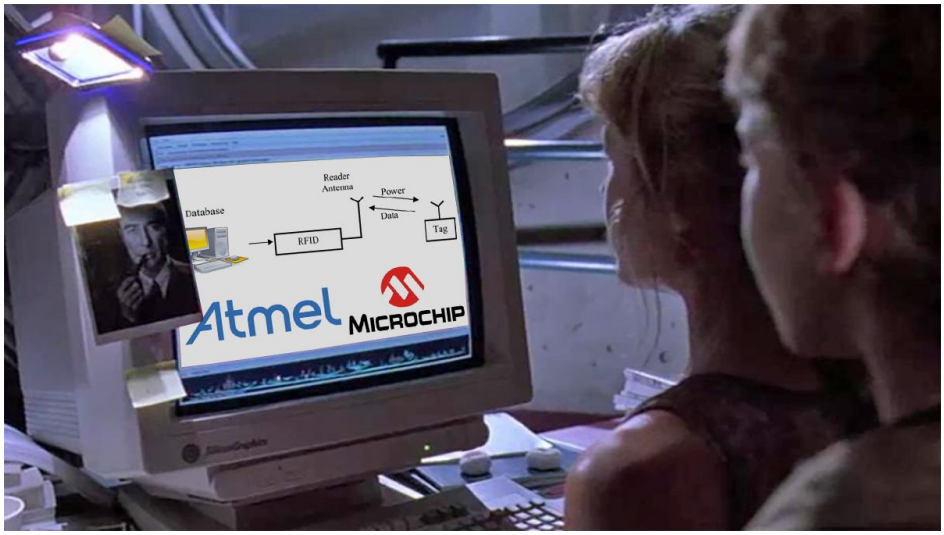
Atmel T5577, Temic Q5, and EM4x05 / EM4x50 tags can all be used to mimic LF credentials

T55xx is stable and EM4x05/4x50 is experimental today. HID uses EM for their ISOproxII

Link to 0xFFFF ’s T55xx block calculator
http://cardinfo.barkweb.com.au/index.php?location=19&sub=29

"Wow... Did They Make These for Hackers?"

"Wow... Did They Make These for Hackers?"



HTTPS://REDTEAMALLIANCE.COM

NO... SOME CREDENTIAL TYPES ARE JUST VERY OLD

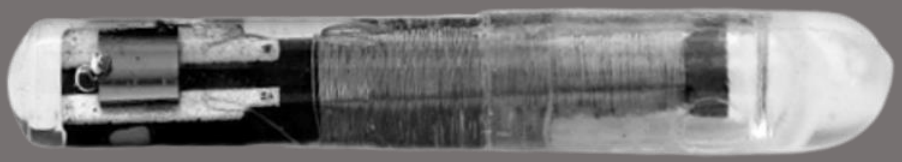
HTTPS://REDTEAMALLIANCE.COM

(HID acquired Indala from Motorola in 2003)

No... Some Credential Types Are Just Very Old

(HID acquired Indala from Motorola in 2003)

What Can I Do With It?



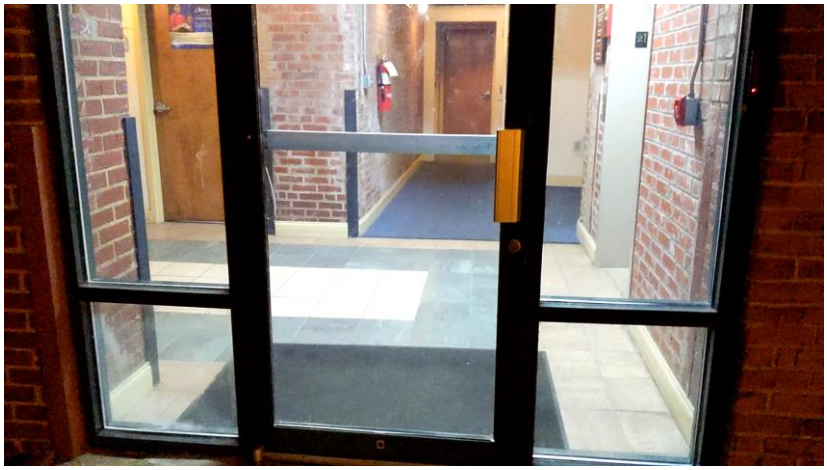
"I Put That Chip In Its Place… Now Whatcha Goin' *Do* With It"

HTTPS://REDTEAMALLIANCE.COM

Now the BIG question

Low Frequency: xEM – Atmel T5577

xEM – Atmel T5577



HTTPS://REDTEAMALLIANCE.COM

$49
Accessing your office or gym or vehicle gate

Low Frequency: xEM – Atmel T5577

xEM – Atmel T5577

HTTPS://REDTEAMALLIANCE.COM

$49
Accessing your office or gym or vehicle gate

(some readers will be fussier than others… it depends a lot on coil size with the antennas and also orientation, position, etc. You may have to play a little bit)

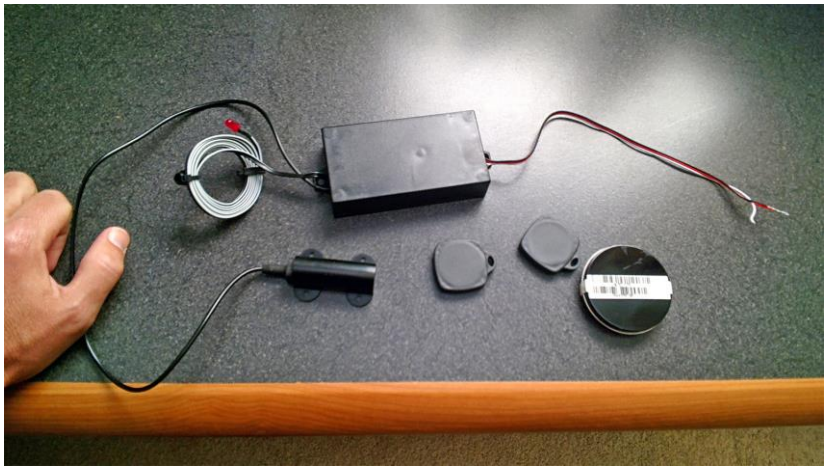
Low Frequency: xEM – Atmel T5577

xEM – Atmel T5577

HTTPS://REDTEAMALLIANCE.COM

Sometimes offices have objected
Potential solution: ask about getting an **additional** credential, as opposed to **duplicating** one

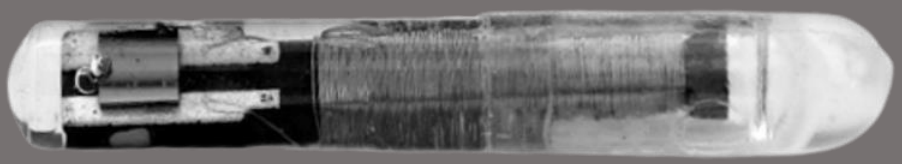
LOW FREQUENCY: XEM – ATMEL T5577



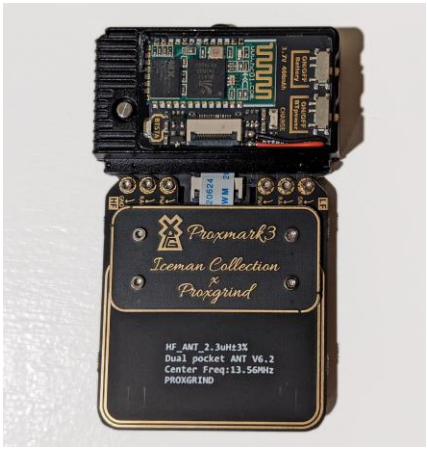
HTTPS://REDTEAMALLIANCE.COM

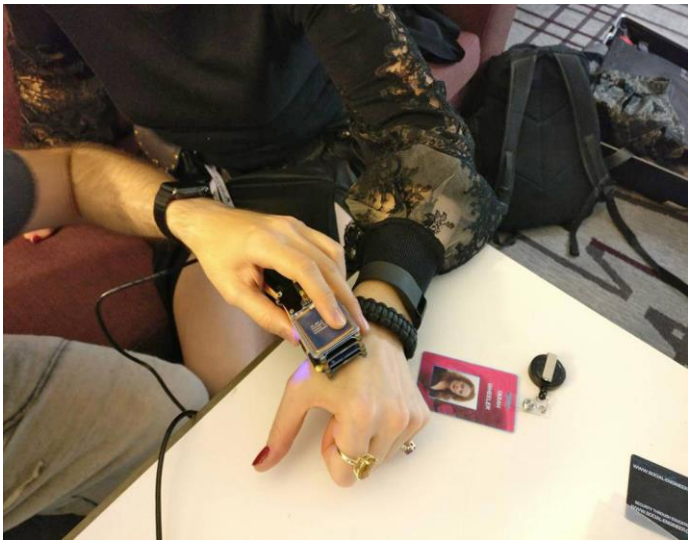
$49
"xEM access controller"
low freq reader (EM mode only)
coil antenna is on a coax... so you can place it somewhere
white wire outputs 12 volts

How Do I Configure It?



PROGRAMMING: PROXMARK3





HTTPS://REDTEAMALLIANCE.COM

Hands-down, the best tool with the greatest functionality

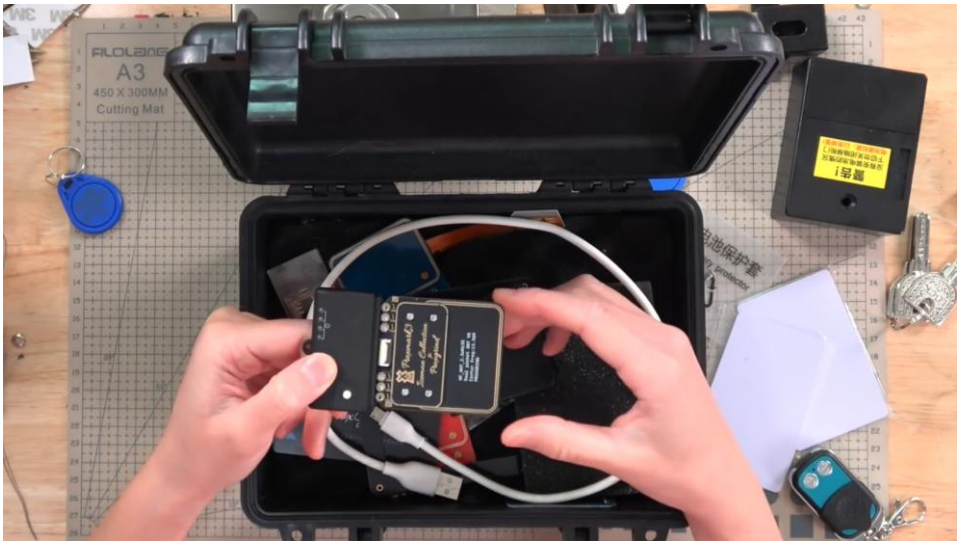
Stock antenna can be iffy, sadly

PROGRAMMING: PROXMARK3

HTTPS://REDTEAMALLIANCE.COM

My friend Naomi did a video about RFID cloning and she showed the proxmark3, as well

PROGRAMMING: PROXMARK3



HTTPS://REDTEAMALLIANCE.COM

My friend Naomi did a video about RFID cloning and she showed the proxmark3, as well

PROGRAMMING: CHEAPER CLONER TOOLS

HTTPS://REDTEAMALLIANCE.COM

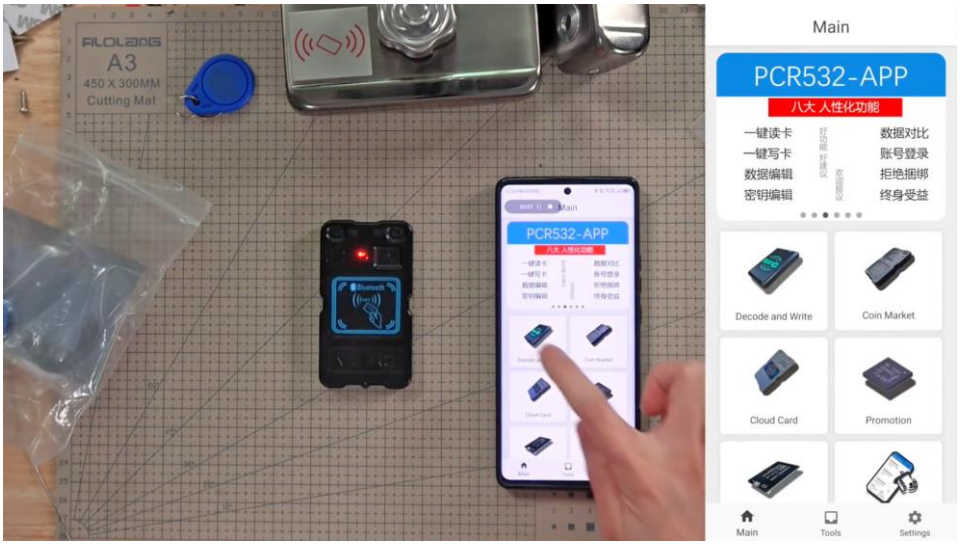
She showed some of the other tools on the market for working with RFID tags, as well

PROGRAMMING: CHEAPER CLONER TOOLS

HTTPS://REDTEAMALLIANCE.COM

NFC Tool

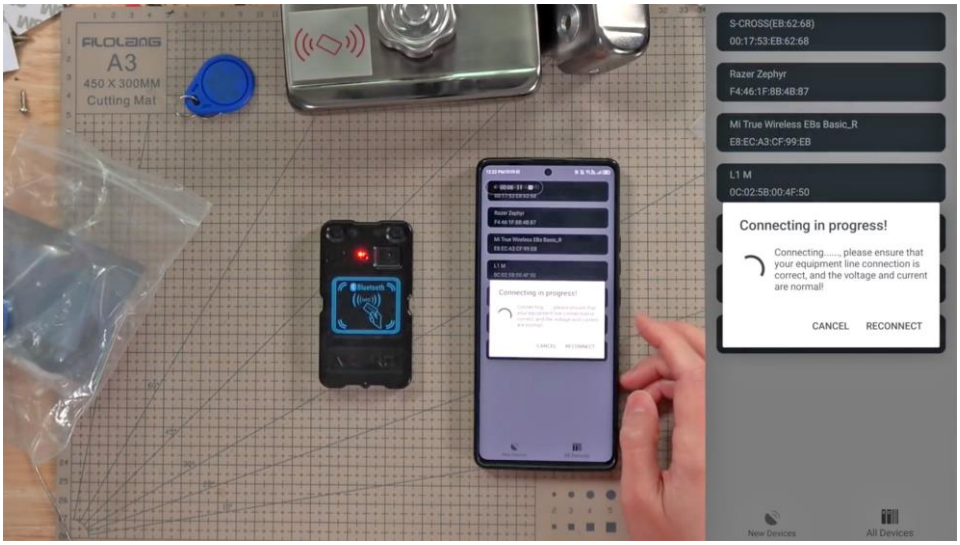
PROGRAMMING: CHEAPER CLONER TOOLS



HTTPS://REDTEAMALLIANCE.COM

Using the NFC Tool… kind of janky, but she can make it work on unencrypted tags

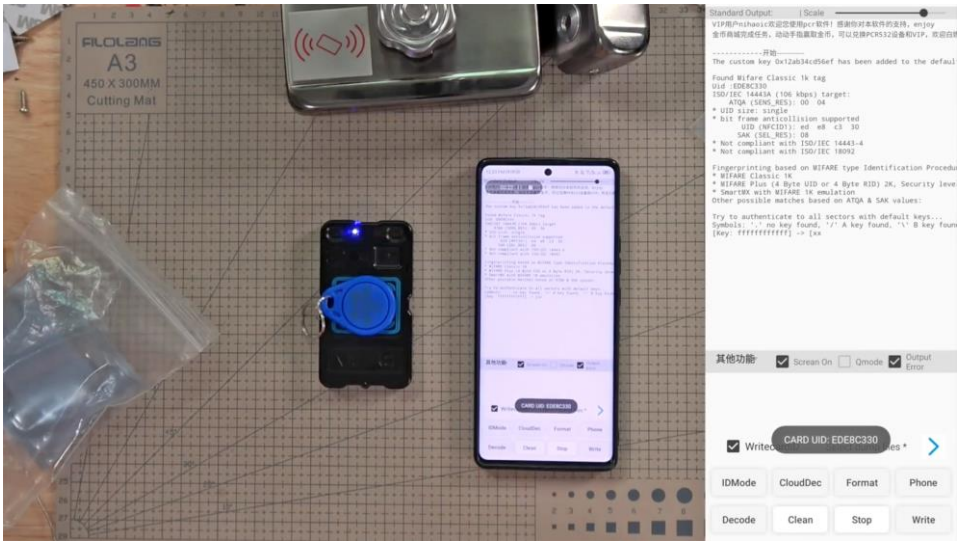
PROGRAMMING: CHEAPER CLONER TOOLS



HTTPS://REDTEAMALLIANCE.COM

Using the NFC Tool… kind of janky, but she can make it work on unencrypted tags

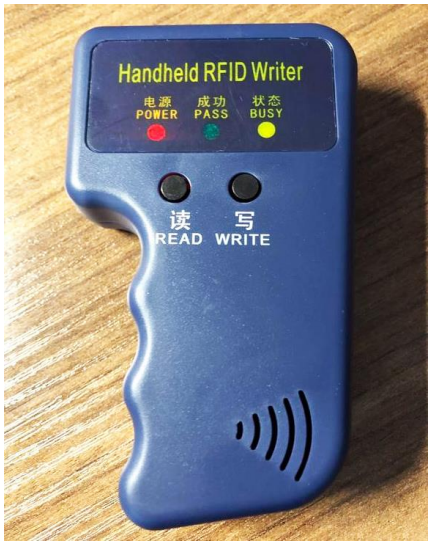
PROGRAMMING: CHEAPER CLONER TOOLS



HTTPS://REDTEAMALLIANCE.COM

Using the NFC Tool… kind of janky, but she can make it work on unencrypted tags

PROGRAMMING: HANDHELD CHEAP CLONERS



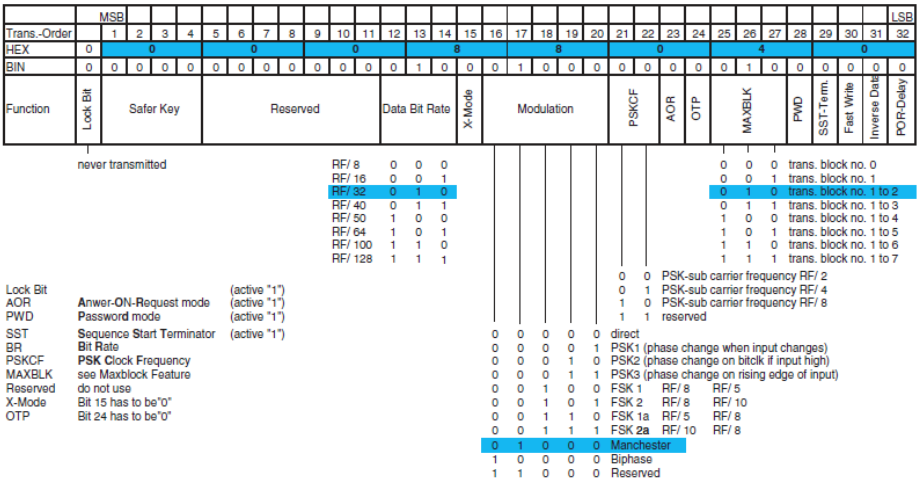
HTTPS://REDTEAMALLIANCE.COM

Programming: Handheld Cheap Cloners

HTTPS://REDTEAMALLIANCE.COM

PROGRAMMING: HANDHELD CHEAP CLONERS

Figure 0-2. ATA5577/ATA5567/T5557 Block 0 Initial Configuration Setting

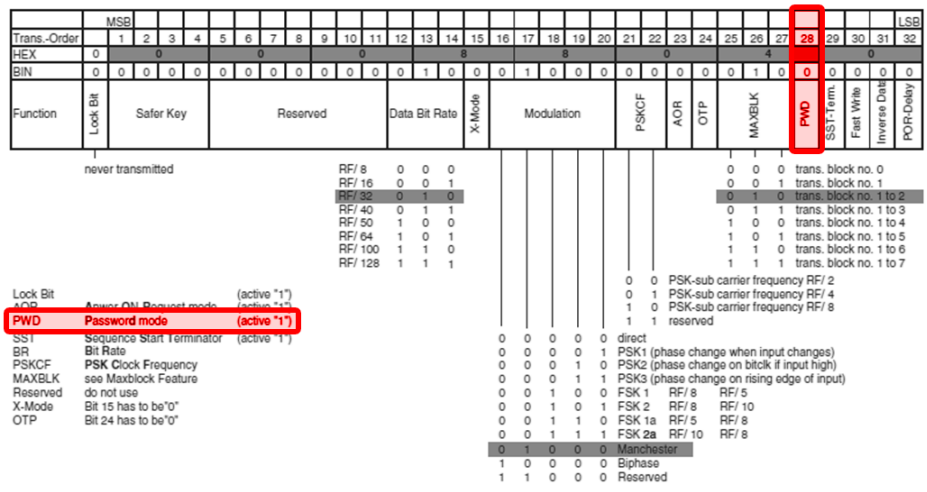


HTTPS://REDTEAMALLIANCE.COM

Have a closer look at that configuration diagram for the T55xx family of chips

PROGRAMMING: HANDHELD CHEAP CLONERS

Figure 0-2. ATA5577/ATA5567/T5557 Block 0 Initial Configuration Setting



HTTPS://REDTEAMALLIANCE.COM

Yeah… they support password protection.

And many cheap cloners, for whatever reason, like to set this bit and set their own password

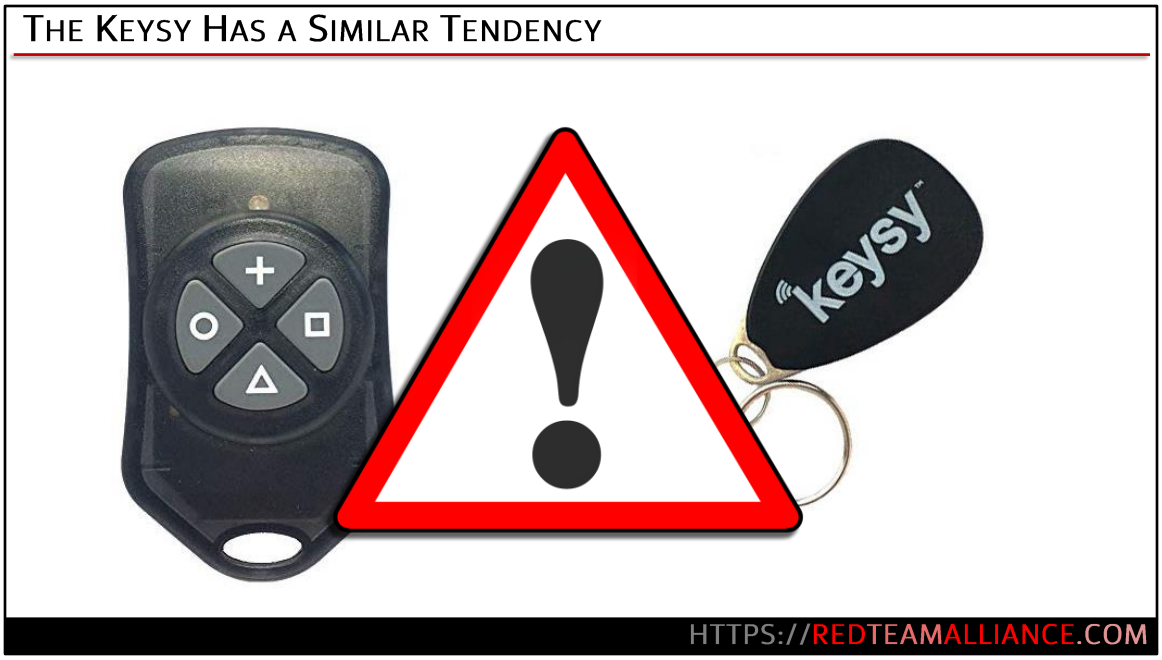
PROGRAMMING: HANDHELD CHEAP CLONERS

We've had that happen to some folk. It's happened to me, as well. Quite the "oh shit" moment. =)

I had to defuckulate mine, and we also had to do the same for some folk at a DEF CON event in NYC

It's a shame, though, because they have good antennas. Not PERFECT antennas, however

The Keysy Has a Similar Tendency



Other products like the Keysy cloner also like to password protect chips

Another Problem with Programming

HTTPS://REDTEAMALLIANCE.COM

Tearing Protection

Another Problem with Programming

		MSB																									
Trans.-Order		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
HEX	0	0				0				0				8				8				0				4	
BIN	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	1
Function	Lock Bit	Safer Key				Reserved				Data Bit Rate				X-Mode		Modulation						PSKCF		AOR		OTP		MANRUK	

Tearing Protection

PROGRAMMING: ANTENNA HACK

HTTPS://REDTEAMALLIANCE.COM

People mod their antennas

PROGRAMMING: ANTENNA HACK

HTTPS://REDTEAMALLIANCE.COM

Best advice is generally to try to have the implant “cross” the antenna coil at a perpendicular

(you want the “coils” to be in the same geometry with one another)

PROGRAMMING: PROXMARK3 WITH TOM HARKNESS LF ANTENNA

HTTPS://REDTEAMALLIANCE.COM

https://cyborg.ksecsolutions.com/product/proxlf-antenna-for-the-proxmark3-rdv4/

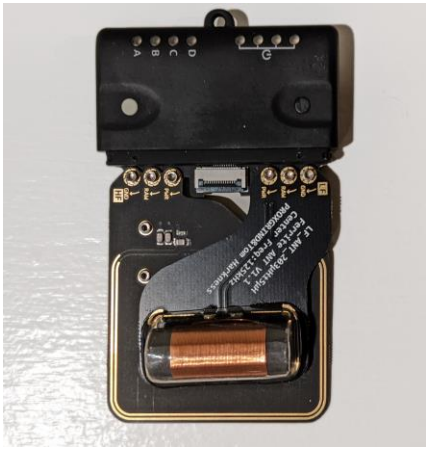
$45 roughly

PROGRAMMING: PROXMARK3 WITH TOM HARKNESS LF ANTENNA

HTTPS://REDTEAMALLIANCE.COM

Best advice is generally to try to have the implant “parallel” alongside of the antenna coil

PROGRAMMING: PROXMARK3 WITH TOM HARKNESS LF ANTENNA



HTTPS://REDTEAMALLIANCE.COM

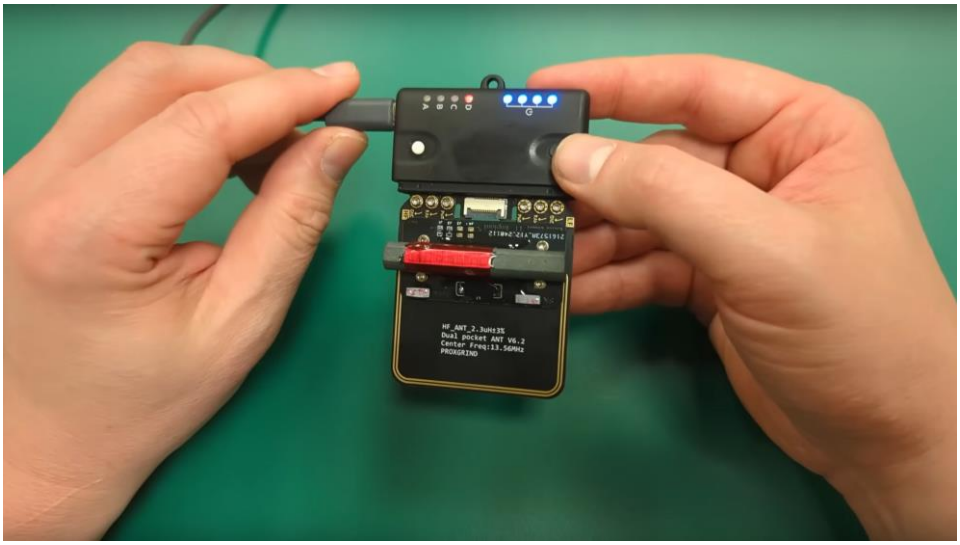
Best advice is generally to try to have the implant “parallel” alongside of the antenna coil

PROGRAMMING: PROXMARK3 WITH TOM HARKNESS LF ANTENNA

HTTPS://REDTEAMALLIANCE.COM

I have some with me today to give away

PROGRAMMING: PROXMARK3 WITH WARREN KUMARI LF ANTENNA



HTTPS://REDTEAMALLIANCE.COM

https://datatracker.ietf.org/person/warren@kumari.net

https://github.com/wkumari

PROGRAMMING: BOOSTING SIGNAL WITH HAMSPICED'S TANK CIRCUITS

HTTPS://REDTEAMALLIANCE.COM

Hamspiced's GitHub...
https://github.com/hamspiced

Hamspiced's on the Dangerous Things forums...
https://forum.dangerousthings.com/u/hamspiced/summary

Hamspiced's Tindie shop...
https://tindie.com/stores/hamspiced/

PROGRAMMING: BOOSTING SIGNAL WITH HAMSPICED'S TANK CIRCUITS

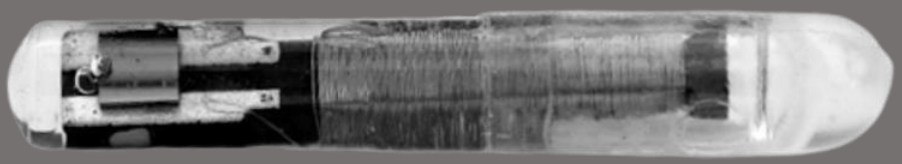
HTTPS://REDTEAMALLIANCE.COM

Hamspiced's GitHub...
https://github.com/hamspiced

Hamspiced's on the Dangerous Things forums...
https://forum.dangerousthings.com/u/hamspiced/summary

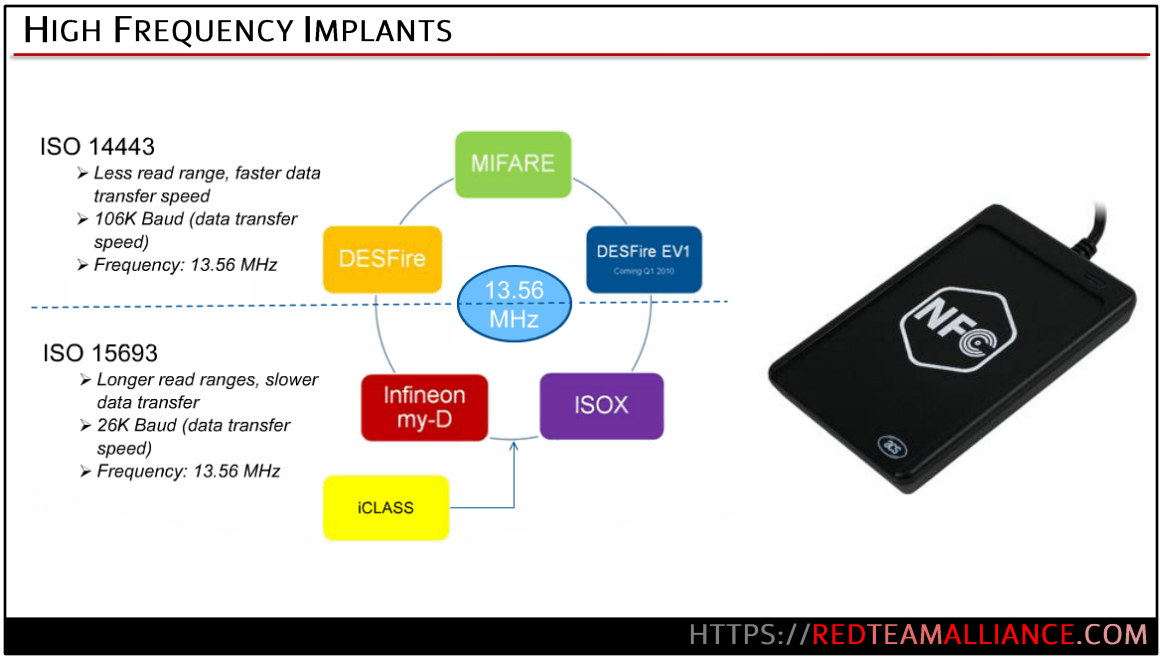
Hamspiced's Tindie shop...
https://tindie.com/stores/hamspiced/

Neat! Is High Frequency Equally Simple?



On the High Frequency Side...

HIGH FREQUENCY IMPLANTS



NFC Forum
non-profit
March 18, 2004
NXP, Sony, and Nokia

Five distinct tag types that provide different communication speeds and capabilities covering flexibility, memory, security, data retention and write endurance (Type 5 has grown obscure, and is the only example of ISO15693)

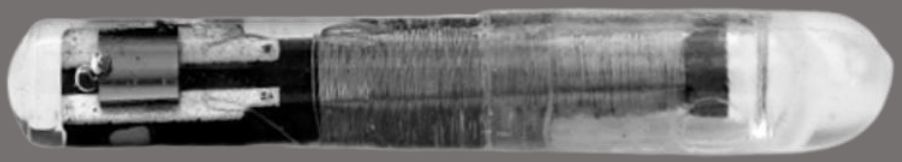
HIGH FREQUENCY IMPLANTS

	NFC Forum Platform				
	Type 1 NFC-A	Type 2 NFC-A	Type 3 NFC-F	Type 4 NFC-A / NFC-B	Type 5 NFC-V
Compatible Products	Broadcom Topaz	MIFARE Ultralight MIFARE Ultralight C NTAG 21s (F) NTAG 12C	Sony FeliCia	DESFire SmartMX-JCOP ST Microelectronics	ICODE SLI (x) Ti Tag-It HF-I EM423x ST Microelectronics
Memory Size	454 Bytes	48 / 128 / 144 / 504 888 / 1904 Bytes	1 / 4 / 9 KBytes	2 / 4/ / 8 KBytes up to 144 KBytes 106 KBytes	32 / 112 / 128 / 160 256 Bytes
Price	Low	Low	High	Med to High	Low to Medium
Data Access	Read/Write	Read/Write or Read-only	Read/Write or Read-only	Read/Write or Read-only	Read/Write
Specification	ISO 14443-3 A	ISO 14443-3 A	JIS 6319-4	ISO 14443-4 A/B	ISO 15693

HTTPS://REDTEAMALLIANCE.COM

This is also something of an eye chart. Essentially there are a variety of chips that have differing features and protocols. But if they follow NFC spec and certain ISO standards, loads of devices (most notably: smartphones) can talk to them

What Can I Do With Them?



HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216

HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

storing vCard details, BTC addresses, some private strings, or novelty things like links to share
think of the "Jason Borne" kind of implant with a swiss bank account number, etc

HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216

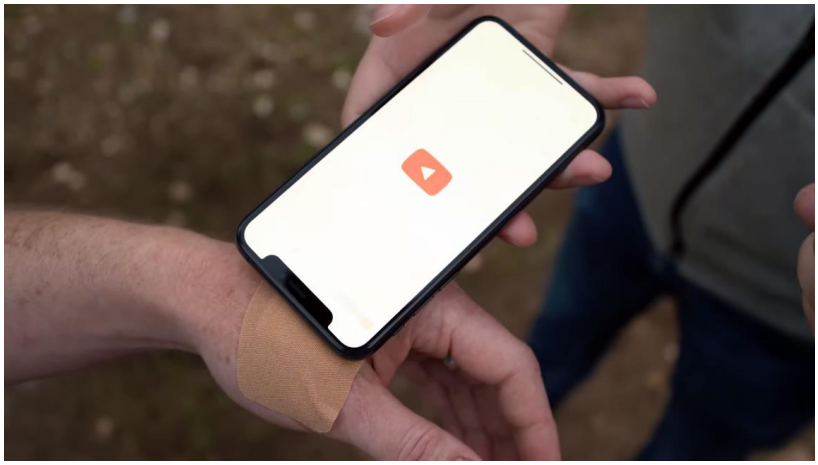
HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

storing vCard details, BTC addresses, some private strings, or novelty things like links to share
think of the "Jason Borne" kind of implant with a swiss bank account number, etc

HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216



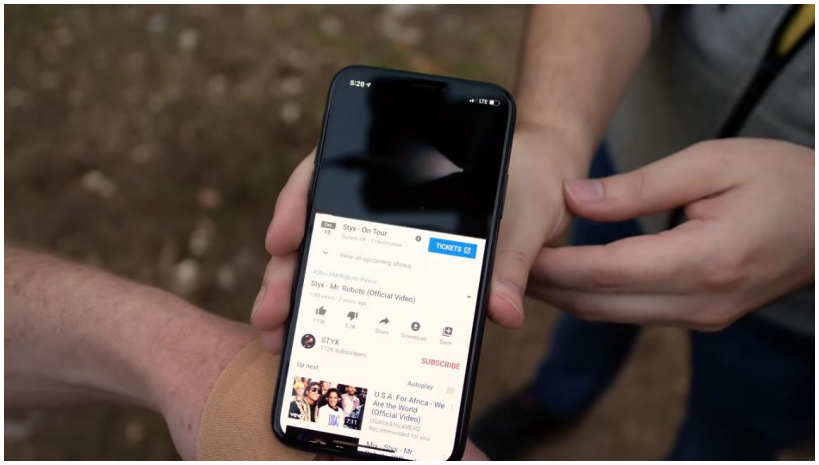
HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

storing vCard details, BTC addresses, some private strings, or novelty things like links to share
think of the "Jason Borne" kind of implant with a swiss bank account number, etc

HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216



HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

storing vCard details, BTC addresses, some private strings, or novelty things like links to share
think of the "Jason Borne" kind of implant with a swiss bank account number, etc

HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216

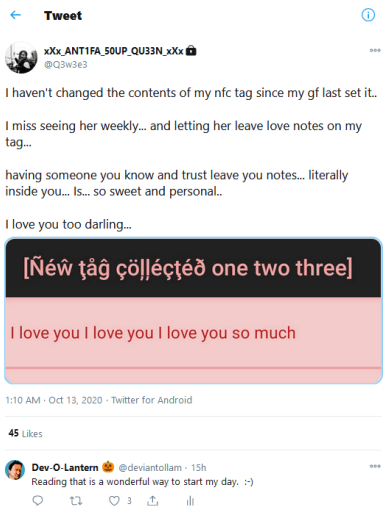
HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

storing vCard details, BTC addresses, some private strings, or novelty things like links to share
think of the "Jason Borne" kind of implant with a swiss bank account number, etc

HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216

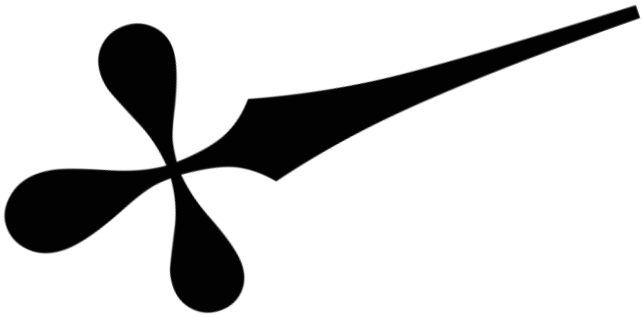


HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

HIGH FREQUENCY IMPLANTS: XNT – NTAG216

xNT – NTAG216



HTTPS://REDTEAMALLIANCE.COM

$70
Type 2 NFC (non-user-changeable CSN/UID)

NTAG FAMILY

Roll over image to zoom in

NTAG216 888 Bytes Memory NFC Stickers NFC Tags Fully Programmable,25mm Round,TimesKey NFC Tag Compatible with All NFC Enabled Smartphones and Devices,55 Pieces

Visit the Timeskey NFC Store

★★★★★ 7 ratings

Was: ~~$29.99~~
Price: $24.99 prime
You Save: $5.00 (17%)

- 55 Pieces Adhesive Brand New NTAG216 NFC Stickers, 9.84 inches (25mm Diameter)
- PET + Paper Material For Fexibility and Durability
- NFC Tags NXP NTAG216 NFC Chipset With 888 Bytes of Memory, Readable, Writable, Adhesive anywhere you want.[Note: Not supported to use on metal surface]
- NFC 216 Tags Compatible With ALL NFC cell phones and other NFC devices.PLEASE PAY ATTENTION !!! : Some of the iPhone Model can not support reading the nfc tags, so it can not recognizes the nfc tags, it is not tags problem,please understand it clearly before your buying.
- High Quality NFC 216 Tag With 100% Satisfaction Guaranteed Services,Just Contact us through TimesKey Seller Page.

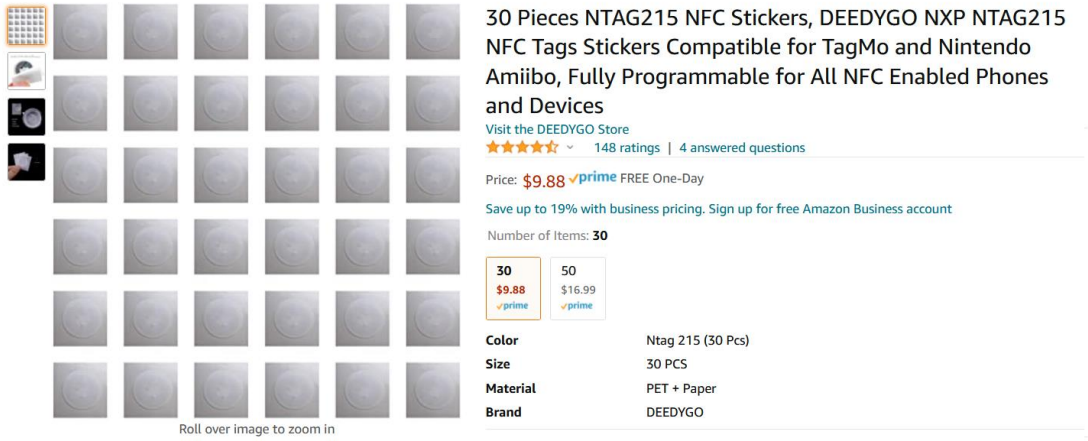
Compare with similar items

Report incorrect product information.

HTTPS://REDTEAMALLIANCE.COM

NTAG 216 (and family)

NTAG FAMILY



HTTPS://REDTEAMALLIANCE.COM

NTAG 216 (and family)

Someone may notice that this is NTAG **215**

what's the difference among that family of chips?

NTAG Family

	Ntag213	Ntag215	Ntag216
User Memory	144 Bytes	504 Bytes	888 Bytes
Max URL	136 Chars	488 Chars	872 Chars
Total memory (bytes)	180	540	924
UID (bytes)	7	7	7

HTTPS://REDTEAMALLIANCE.COM

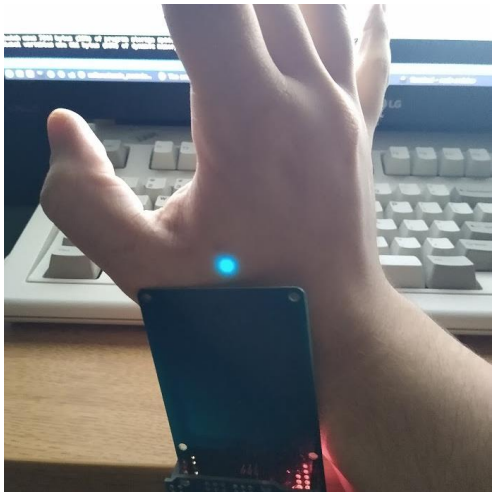
Only difference is storage capacity

Data transfer rate, Capacitance, endurance cycles, and standards/protocols/features are all the same

All released in 2013 at the same time by NXP. Only difference is storage and cost.

HIGH FREQUENCY IMPLANTS: XSIID – NTAG216 + LED

xSIID – NTAG216 + LED



HTTPS://REDTEAMALLIANCE.COM

$120
Type 2 NFC (non-user-changeable CSN/UID)

And an LED in the package
User chooses R, G, B, or White

Based on NTAG I2C. Being redesigned. It's going to be the NextV2 as a dual package including a T5577.

HIGH FREQUENCY IMPLANTS: XDF2 – DESFIRE EV2

xDF2 – DESFire EV2

HTTPS://REDTEAMALLIANCE.COM

$139
Type 4 NFC (non-user-changeable CSN/UID… but you can *randomize* it)
8 kB "application" space (currently out of stock… hard to source the bare die. xDF3 is coming soon in very limited quantity)

stored value and other things tied to a larger framework that events are setting up
ships with factory default master keys... EV2 "attempts to solve the master key problem"
can enable "private UID" randomized per session... have to authenticate with chip to see real UID
can set up a secure channel between chip and reader to move data in a secure tunnel

HIGH FREQUENCY IMPLANTS: XDF2 – DESFIRE EV2

xDF2 – DESFire EV2

HTTPS://REDTEAMALLIANCE.COM

DESFire EV2 is what Disney corp opted to use when they implemented their Magic Band system

HIGH FREQUENCY IMPLANTS: xSLX

xSLX

HTTPS://REDTEAMALLIANCE.COM

$59
A rare Type 5 NFC

13.56MHz ISO15693 & NFC Type 5
(ICODE SLIX2 … helpful for some devices that require Type 5. padlock, pistol case)

So Who or What is VivoKey?

HTTPS://REDTEAMALLIANCE.COM

started with a smartcard chip, Apex, and focus on payment features and the like but put on indefinite hold

then it became an identity platform, which is now the Spark2.

(the Spark1 was around but then Google broke their NFC stack and phones couldn't work with the Spark1 for a few years)

HIGH FREQUENCY IMPLANTS: VIVOKEY SPARK 2

VIVOKEY SPARK 2

HTTPS://REDTEAMALLIANCE.COM

$109
Type 4 NFC (non-user-changeable CSN/UID) FIPS 197 compliant

Like other NFC tags… it can pass a URL to a service, etc
VivoKey service platform - OpenIDConnect (like "login with Facebook")
Wordpress
Discords/Forum
vault service (like 1Password/Tresorit/etc)
if you root your phone - possible to do lock/unlock but that feature isn't going to be the norm in future on stock OSs

HIGH FREQUENCY IMPLANTS: VIVOKEY SPARK 2

VIVOKEY SPARK 2

HTTPS://REDTEAMALLIANCE.COM

Spark2 is a symmetric crypto challenge response validation system. There's an API, you can interact with the chip, etc.

SparkActions is a redirector service. Every Spark has a hard-set URL that's unique and interacts with their servers through the API.

SAML identity provider integration... so, sign into GoogleWorkspace, Octa, 1Login, etc.

Spark is NTAG424, very small, 2mm x 12mm injectable. Cryptographic proof of identity. "Unlock my laptop" or "Unlock my phone" may be projects in the works, but they would require the API being online

"CAN I USE THIS TO UNLOCK MY PHONE?!?"

HTTPS://REDTEAMALLIANCE.COM

Common question: "Can I use this to unlock my phone?"

People love the idea of a phone that will only unlock if it's in your own hand (I love this idea, too)

Sadly we're not quite there. Closest we can come is integration with wearables, etc.

"NFC SmartLock" on Google was removed a while ago. Wasn't all that smart, just read the UID, and might have interfered with GooglePay so that's likely why they removed it.

HIGH FREQUENCY IMPLANTS: VIVOKEY APEX

VIVOKEY APEX

HTTPS://REDTEAMALLIANCE.COM

Replacing the Spark

Partnered with Fidesmo

Collaboration with VISA, Mastercard, etc.

HIGH FREQUENCY IMPLANTS: XM1 – "MAGIC" MIFARE CLASSIC

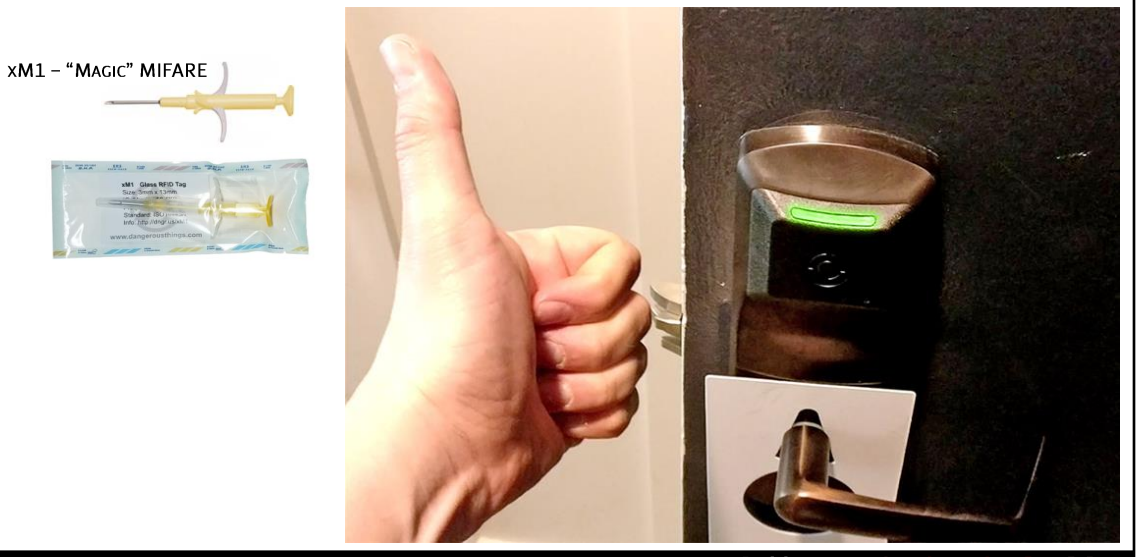
XM1 – "MAGIC" MIFARE

HTTPS://REDTEAMALLIANCE.COM

$120
MIFARE Classic is **not *truly*** NFC

This can emulate MIFARE Classic S50 credential and has backdoor commands "UID Changeable" chip. (Beware on the market of "change one time" vs "change infinite number of times")

HIGH FREQUENCY IMPLANTS: XM1 – "MAGIC" MIFARE CLASSIC



$120
MIFARE Classic is **not *truly*** NFC

This can emulate MIFARE Classic S50 credential and has backdoor commands "UID Changeable" chip. (Beware on the market of "change one time" vs "change infinite number of times")

HIGH FREQUENCY IMPLANTS: XM1 – "MAGIC" MIFARE CLASSIC

HTTPS://REDTEAMALLIANCE.COM

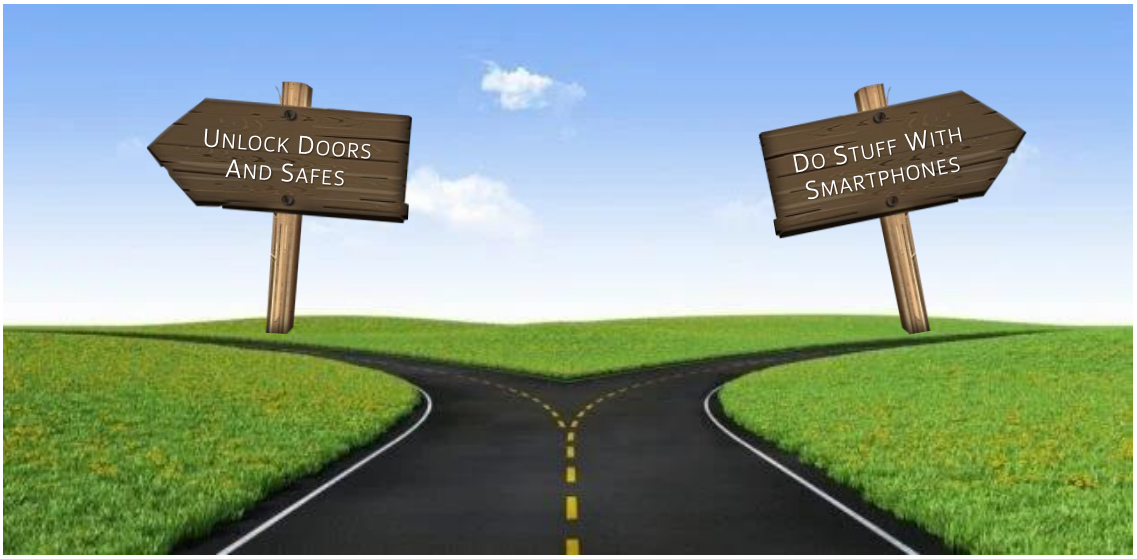
Never lose your hotel key again, no matter how hard you party

High Frequency Implants: xM1 – "Magic" MIFARE Classic

HTTPS://REDTEAMALLIANCE.COM

Never lose your hotel key again, no matter how hard you party

"So... I Have to Make a Choice?"



DUAL FREQUENCY IMPLANT: NEXT

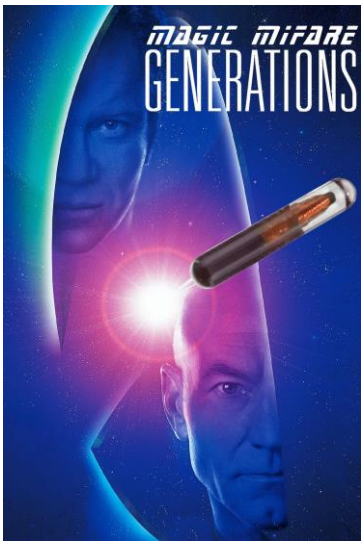
NExT – NFC NTAG & T5577

HTTPS://REDTEAMALLIANCE.COM

$90
hf NFC NTAG and lf T5577

DUAL FREQUENCY IMPLANT: XMAGIC

xMAGIC – MAGIC MIFARE & T5577



HTTPS://REDTEAMALLIANCE.COM

$149

Magic MIFARE + T5577 *(they're basically trying to shove a T5577 into everything they do now)*

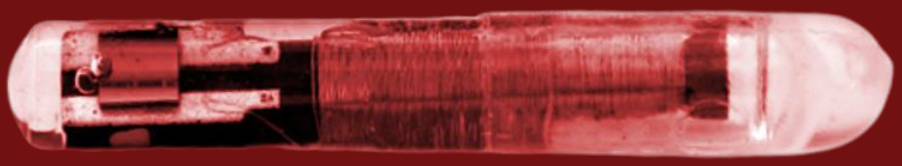
Magic MIFARE now available in gen1a or gen2

FlexUG4 - gen4 Magic MIFARE (can do 4byte, 7byte, Ultralight, MIFARE NTAG)

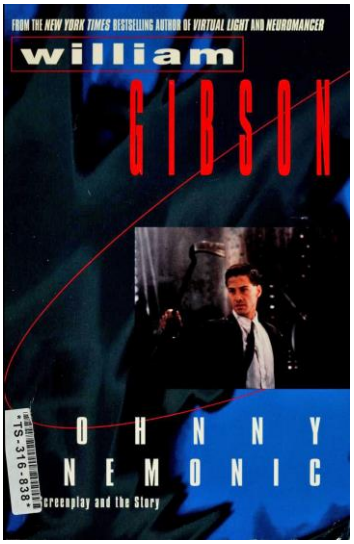
ZUID - supports gen1a backdoor features and also turn on gen2 and open up sector zero. can recover bad sectors, etc. can't avoid gen1 detection if a reader is smart enough to do that.

DualPackage available... xMAGIC (trying to shove a T5577 into basically everything now)

Really Bold Biohackers Are Always Pushing the Envelope



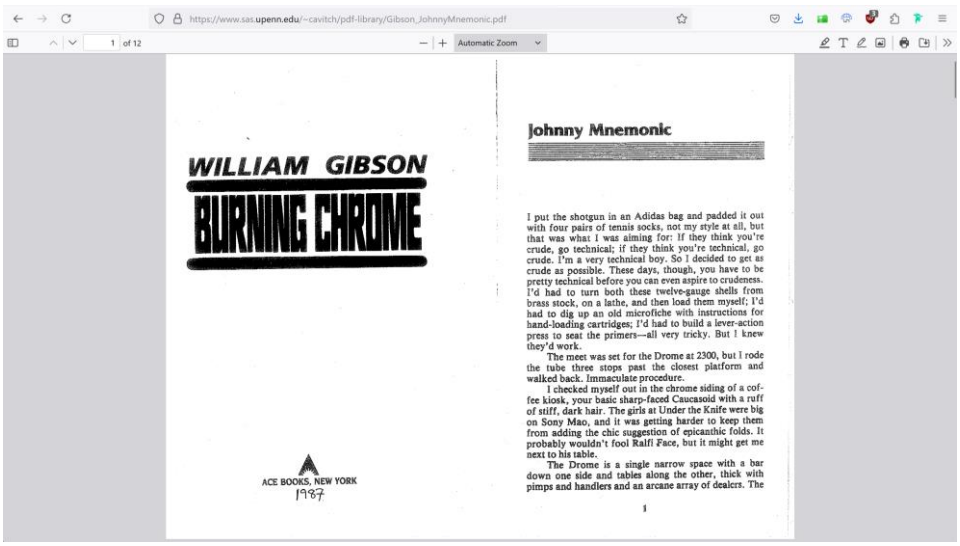
JOHNNY MNEMONIC



HTTPS://REDTEAMALLIANCE.COM

https://www.sas.upenn.edu/~cavitch/pdf-library/Gibson_JohnnyMnemonic.pdf

HTTPS://WWW.SAS.UPENN.EDU/~CAVITCH/PDF-LIBRARY/GIBSON_JOHNNYMNEMONIC.PDF



WILLIAM GIBSON

BURNING CHROME

ACE BOOKS, NEW YORK
1987

Johnny Mnemonic

I put the shotgun in an Adidas bag and padded it out with four pairs of tennis socks, not my style at all, but that was what I was aiming for: If they think you're crude, go technical; if they think you're technical, go crude. I'm a very technical boy. So I decided to get as crude as possible. These days, though, you have to be pretty technical before you can even aspire to crudeness. I'd had to turn both these twelve-gauge shells from brass stock, on a lathe, and then load them myself; I'd had to dig up an old microfiche with instructions for hand-loading cartridges; I'd had to build a lever-action press to seat the primers—all very tricky. But I knew they'd work.

The meet was set for the Drome at 2300, but I rode the tube three stops past the closest platform and walked back. Immaculate procedure.

I checked myself out in the chrome siding of a coffee kiosk, your basic sharp-faced Caucasoid with a ruff of stiff, dark hair. The girls at Under the Knife were big on Sony Mao, and it was getting harder to keep them from adding the chic suggestion of epicanthic folds. It probably wouldn't fool Ralfi Face, but it might get me next to his table.

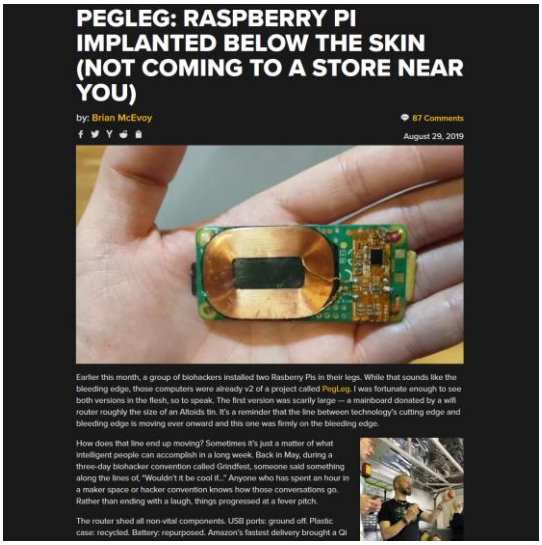
The Drome is a single narrow space with a bar down one side and tables along the other, thick with pimps and handlers and an arcane array of dealers. The

1

HTTPS://REDTEAMALLIANCE.COM

https://www.sas.upenn.edu/~cavitch/pdf-library/Gibson_JohnnyMnemonic.pdf

PEGLEG PROJECT



PEGLEG: RASPBERRY PI IMPLANTED BELOW THE SKIN (NOT COMING TO A STORE NEAR YOU)

by: Brian McEvoy

87 Comments

August 29, 2019

Earlier this month, a group of biohackers installed two Rasberry Pis in their legs. While that sounds like the bleeding edge, those computers were already v2 of a project called PegLeg. I was fortunate enough to see both versions in the flesh, so to speak. The first version was scarily large — a mainboard donated by a wifi router roughly the size of an Altoids tin. It's a reminder that the line between technology's cutting edge and bleeding edge is moving ever onward and this one was firmly on the bleeding edge.

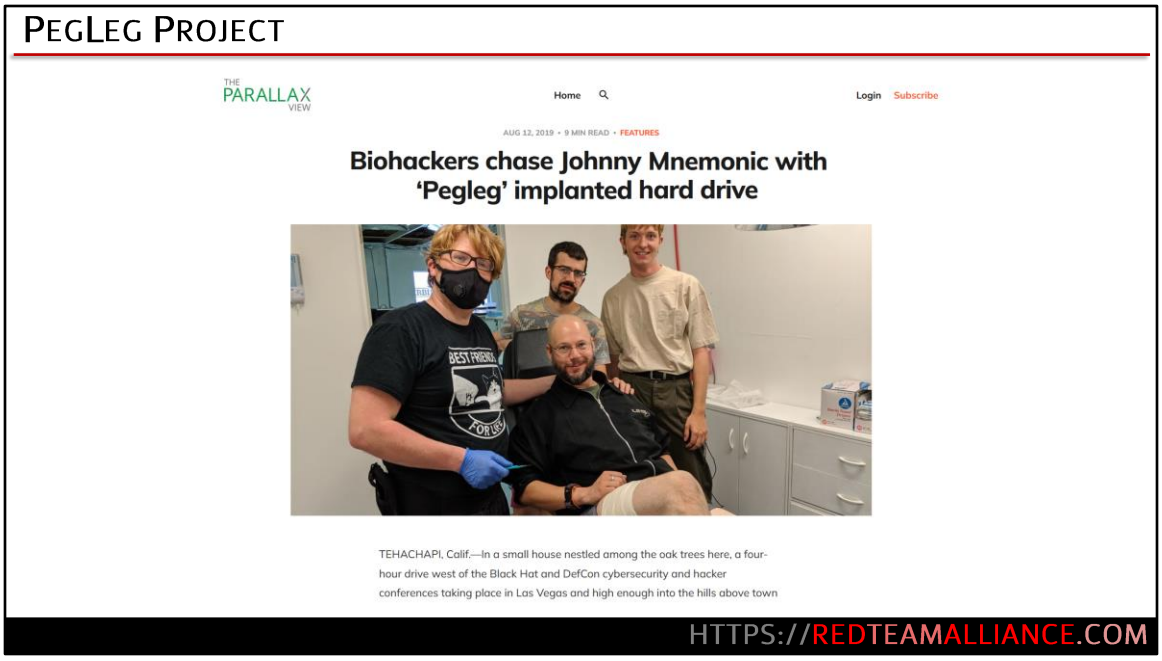
How does that line end up moving? Sometimes it's just a matter of what intelligent people can accomplish in a long week. Back in May, during a three-day biohacker convention called Grindfest, someone said something along the lines of, "Wouldn't it be cool if..." Anyone who has spent an hour in a maker space or hacker convention knows how those conversations go. Rather than ending with a laugh, things progressed at a fever pitch.

The router shed all non-vital components. USB ports: ground off. Plastic case: recycled. Battery: repurposed. Amazon's fastest delivery brought a Qi

HTTPS://REDTEAMALLIANCE.COM

https://hackaday.com/2019/08/29/pegleg-raspberry-pi-implanted-below-the-skin-not-coming-to-a-store-near-you/

PEGLEG PROJECT

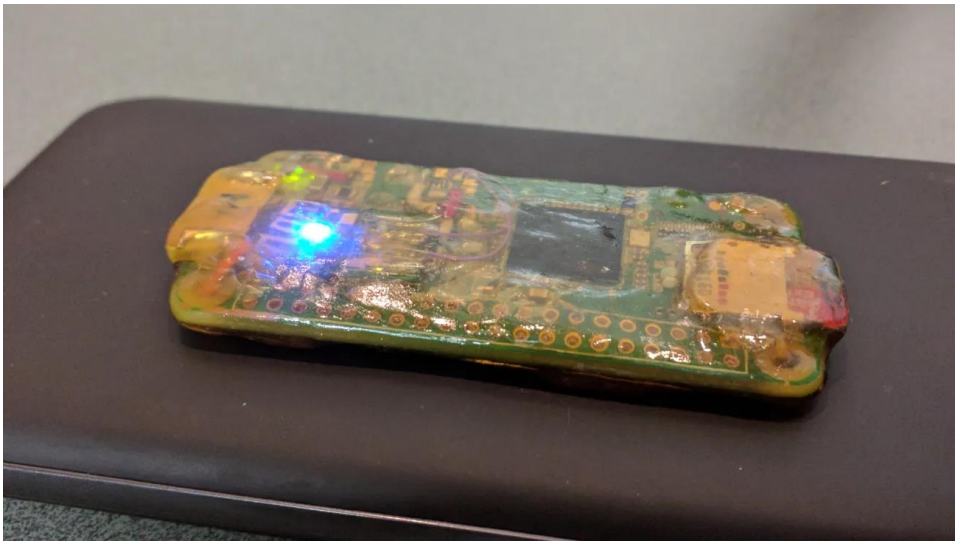


https://www.the-parallax.com/defcon-biohackers-johnny-mnemonic-pegleg/

PEGLEG PROJECT

HTTPS://REDTEAMALLIANCE.COM

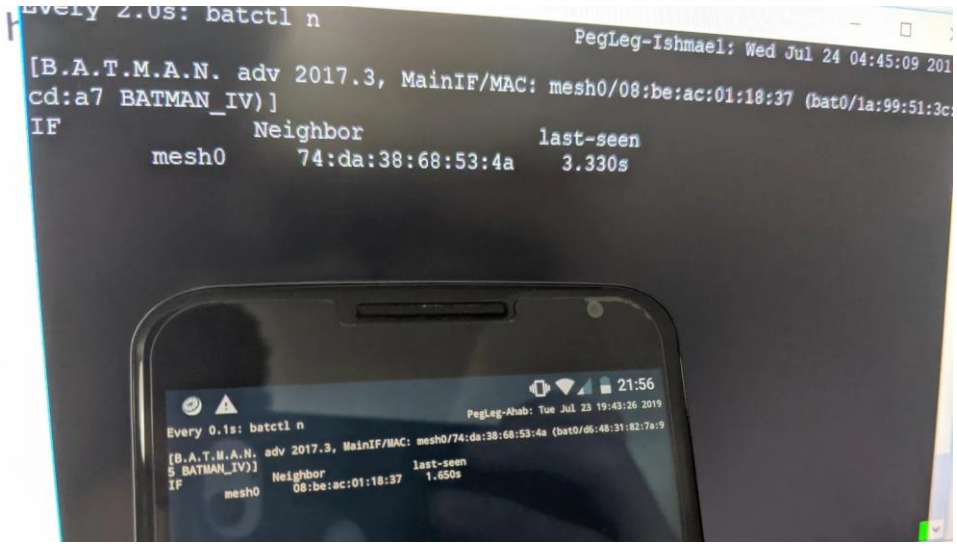
PEGLEG PROJECT



PEGLEG PROJECT

HTTPS://REDTEAMALLIANCE.COM

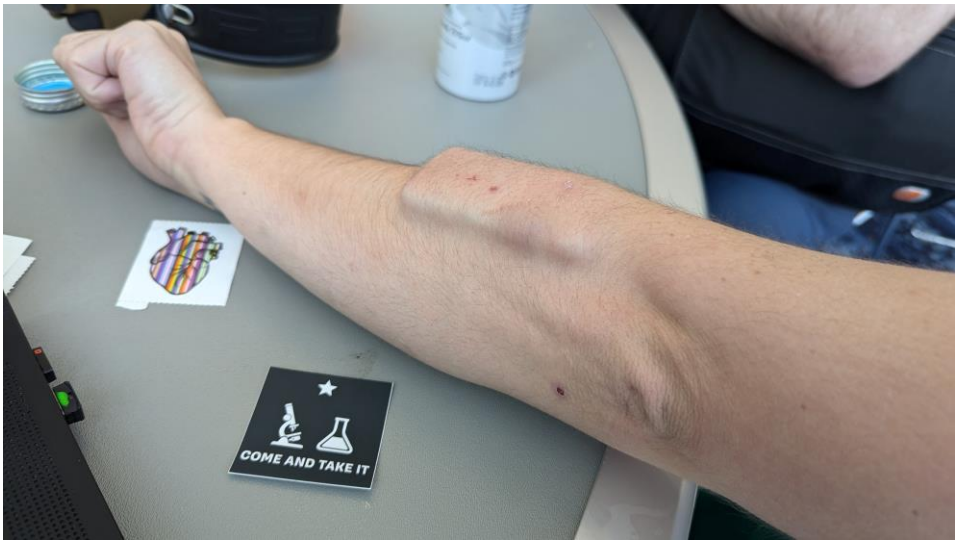
PEGLEG PROJECT



HTTPS://REDTEAMALLIANCE.COM

You Can Carry a Phone or External Hard Drive...

...How About one that Can't Be Stolen or Surrendered?



...How About one that Can't Be Stolen or Surrendered?

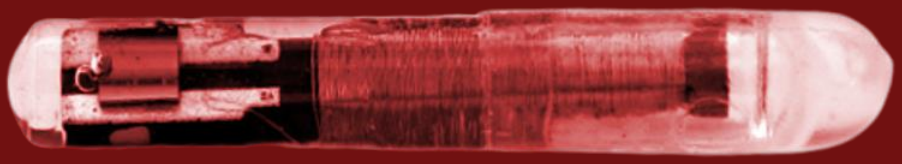
BioHackers & Grinders FTW

HTTPS://REDTEAMALLIANCE.COM

PegLeg v1
RasPi with Qi charger and 64GB of memory

PegLeg v2
Pi0W (Raspberry Pi Zero W) with a Qi receiver, capacitor, WiFi dongle, and half of a terabyte for storage. Three of them were made for implantation during DEFCON 27

This is a Lot, I Know



I'm throwing a lot at you, but it's because I want you to understand your options and have all the best info you can before doing something that's kind of significant

"I Don't Know If I'm Ready For This Yet"

Still Hesitant? You Can Take Baby Steps

HTTPS://REDTEAMALLIANCE.COM

NFC rings

Wristbands
https://www.aliexpress.us/item/2251832767411687.html

DIY Watch Credential

HTTPS://REDTEAMALLIANCE.COM

Jakub from Czech Republic

"I have extracted the chip itself from a key fob I got on Ebay for like 2 €. The coil antenna is underneath the PCB, wrapped around the display, and trust me it was very difficult to make the 12ish turns exactly the right width to fit inside the casing, I had to do it like a hundred times because it always was a millimeter too wide or too narrow. Soldering the terminals was also a lot of fun but not as difficult as the previous part. Hope this information makes your presentation even more interesting than it already is."

DIY RFID Ring

HTTPS://REDTEAMALLIANCE.COM

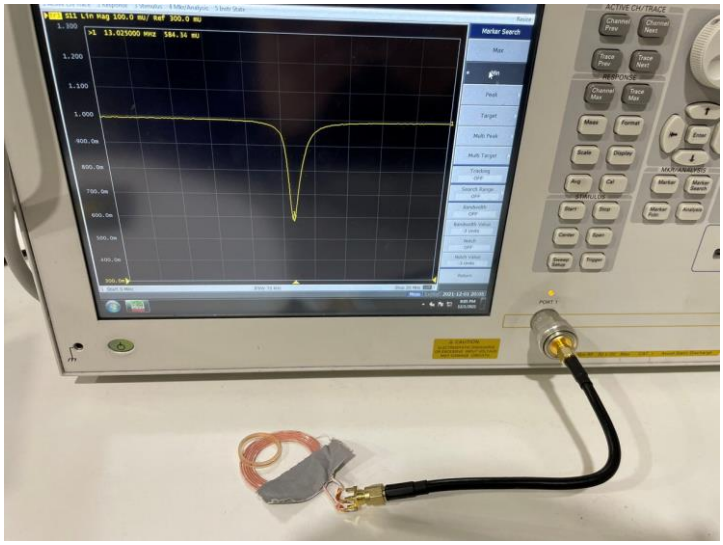
Someone dissolved their RFID badge in acetone to get the antenna coil and the chip, and they 3D printed a small wearable “ring” into which they incorporated that silicone and copper

DIY RFID Ring

HTTPS://REDTEAMALLIANCE.COM

Someone dissolved their RFID badge in acetone to get the antenna coil and the chip, and they 3D printed a small wearable “ring” into which they incorporated that silicone and copper

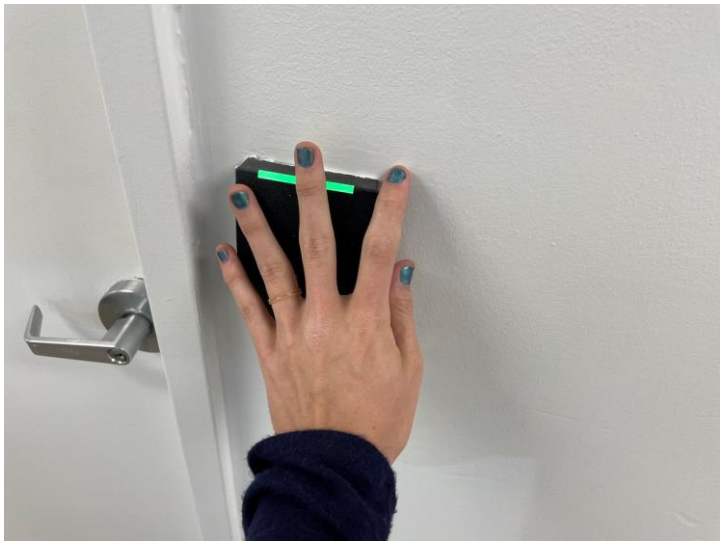
DIY RFID RING



HTTPS://REDTEAMALLIANCE.COM

Someone dissolved their RFID badge in acetone to get the antenna coil and the chip, and they 3D printed a small wearable “ring” into which they incorporated that silicone and copper

DIY RFID Ring



HTTPS://REDTEAMALLIANCE.COM

Someone dissolved their RFID badge in acetone to get the antenna coil and the chip, and they 3D printed a small wearable “ring” into which they incorporated that silicone and copper

DIY RFID NAILS

HTTPS://REDTEAMALLIANCE.COM

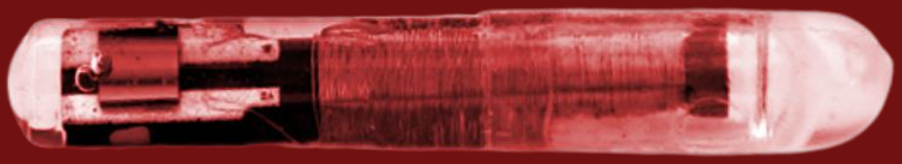
DIY RFID NAILS

DIY RFID NAILS

HTTPS://REDTEAMALLIANCE.COM

DIY RFID NAILS

More Questions and Capabilities



Mobile Payments? Transportation?

Mobile Payments? Transportation?

Mobile Payments? Transportation?

HTTPS://REDTEAMALLIANCE.COM

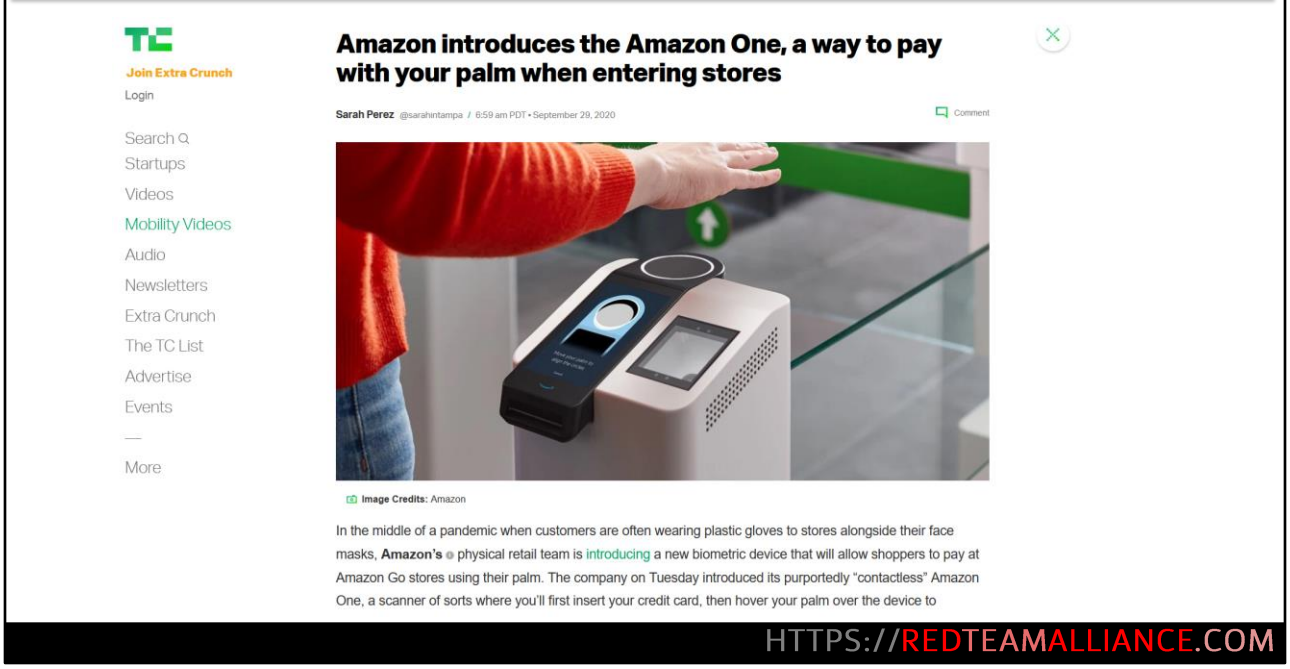
The next generation of implant are already in the works and there are significant inroads happening with integration across other systems
Based on SmartMX … one of NXP's latest chips (it's what HID uses in their SEOS product line of credentials, BTW)

NXP SmartMX3 P71 (JCOP4)

https://www.vivokey.com/apex

As of right now… some transit systems are checking to see if cards respond to "Magic" backdoor commands, and if they do, the system will disable that credential. (Hence the ladders and walls game with new generations of "Magic" card)

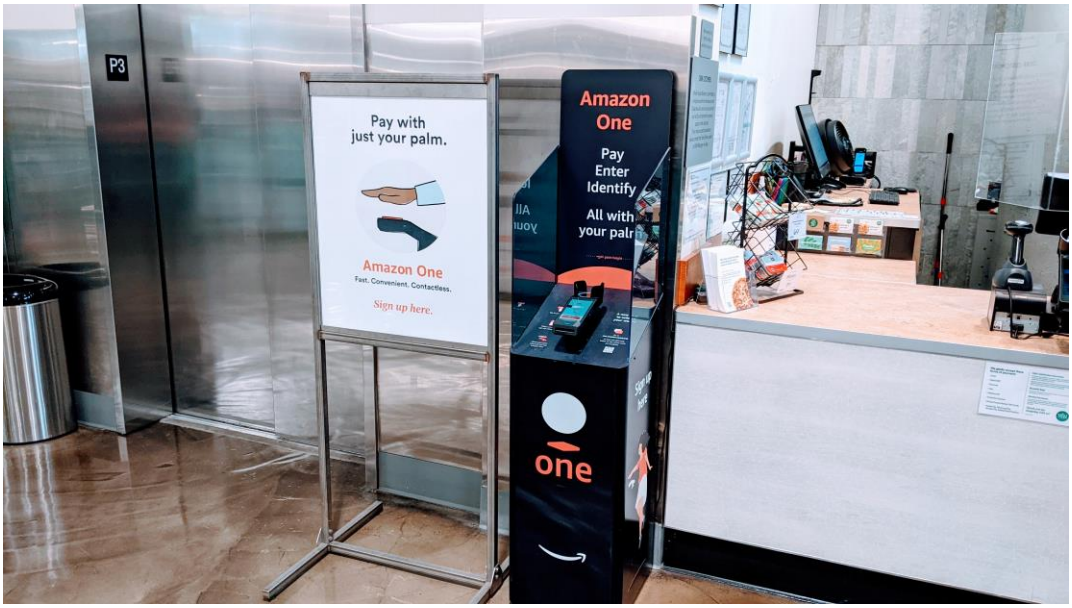
THIS IS *NOT* THE FUTURE I WANT TO EXPERIENCE



HTTPS://REDTEAMALLIANCE.COM

This is amazon (or any other retailer with a similar plan) taking biometric data from the user. Implants are not biometric… implants are controlled by the user and they are changeable.

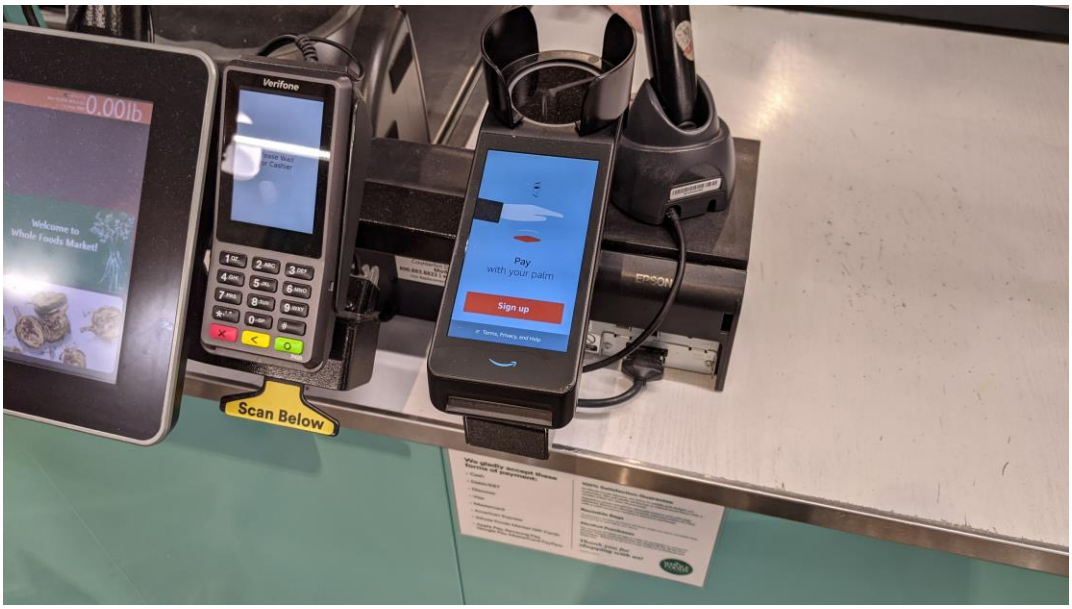
THIS IS *NOT* THE FUTURE I WANT TO EXPERIENCE



HTTPS://REDTEAMALLIANCE.COM

This is amazon (or any other retailer with a similar plan) taking biometric data from the user. Implants are not biometric… implants are controlled by the user and they are changeable.

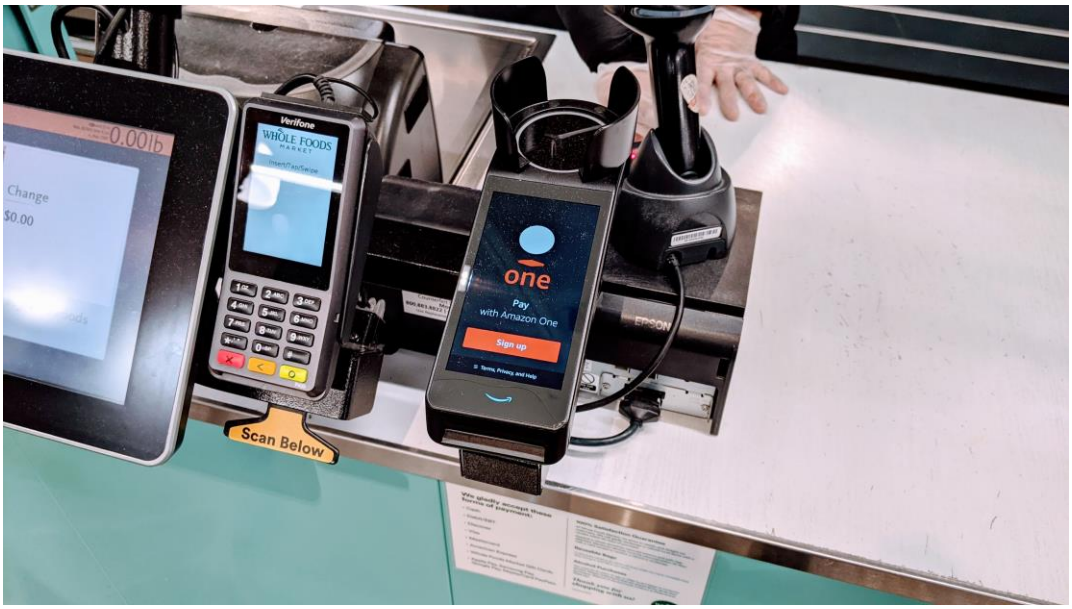
THIS IS *NOT* THE FUTURE I WANT TO EXPERIENCE



HTTPS://REDTEAMALLIANCE.COM

This is amazon (or any other retailer with a similar plan) taking biometric data from the user. Implants are not biometric… implants are controlled by the user and they are changeable.

This is *NOT* the Future I Want to Experience



HTTPS://REDTEAMALLIANCE.COM

This is amazon (or any other retailer with a similar plan) taking biometric data from the user. Implants are not biometric… implants are controlled by the user and they are changeable.

This is the Future I Want to Experience

This is the Future I Want to Experience

And Bold, Awesome People are Getting Us Closer!

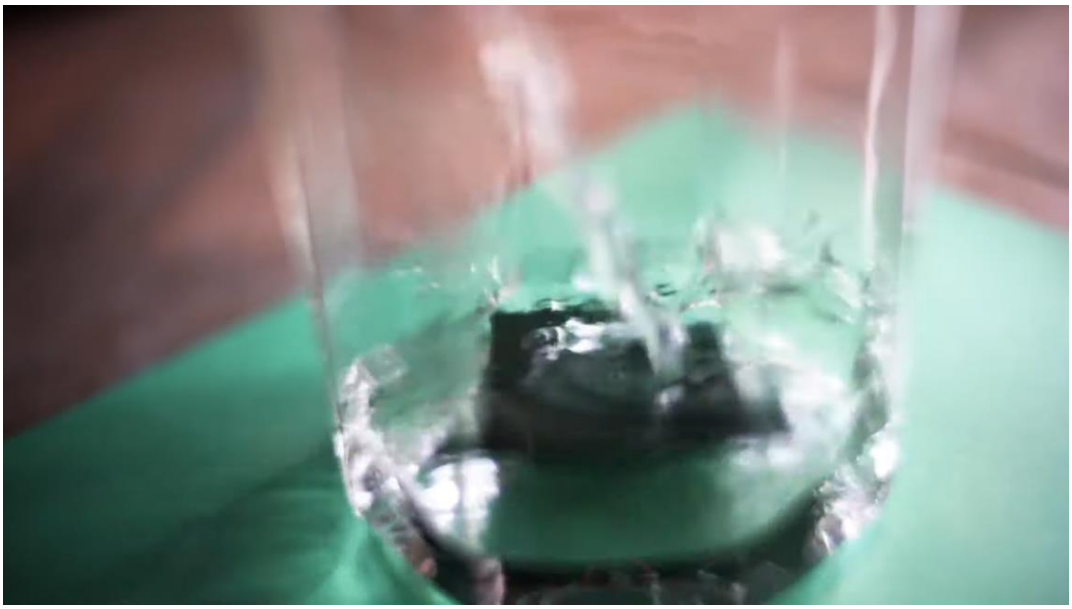
HTTPS://REDTEAMALLIANCE.COM

https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!

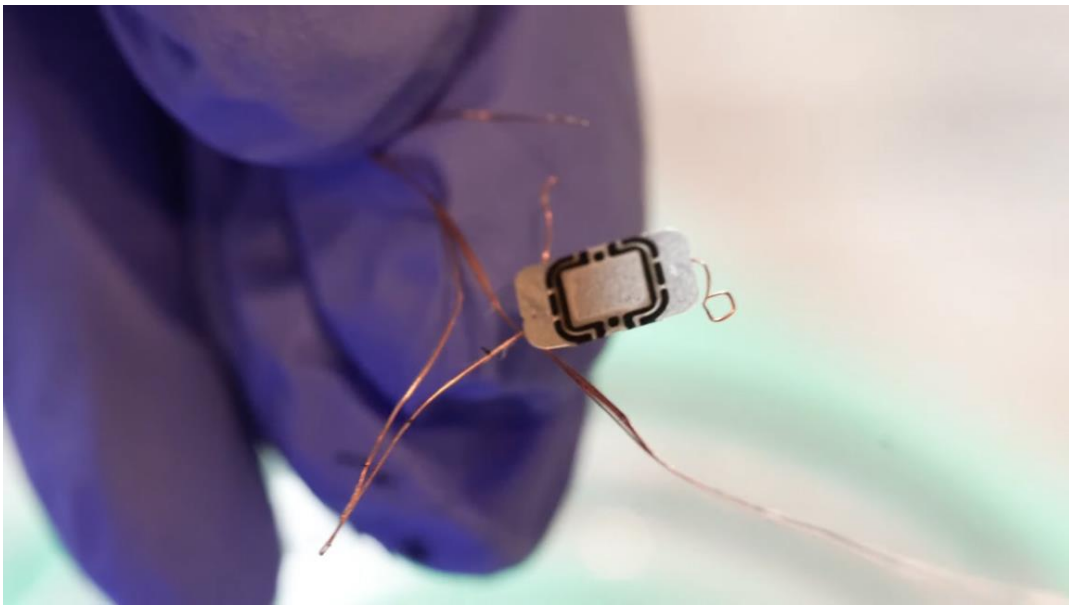
https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!



https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!



https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!

https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!

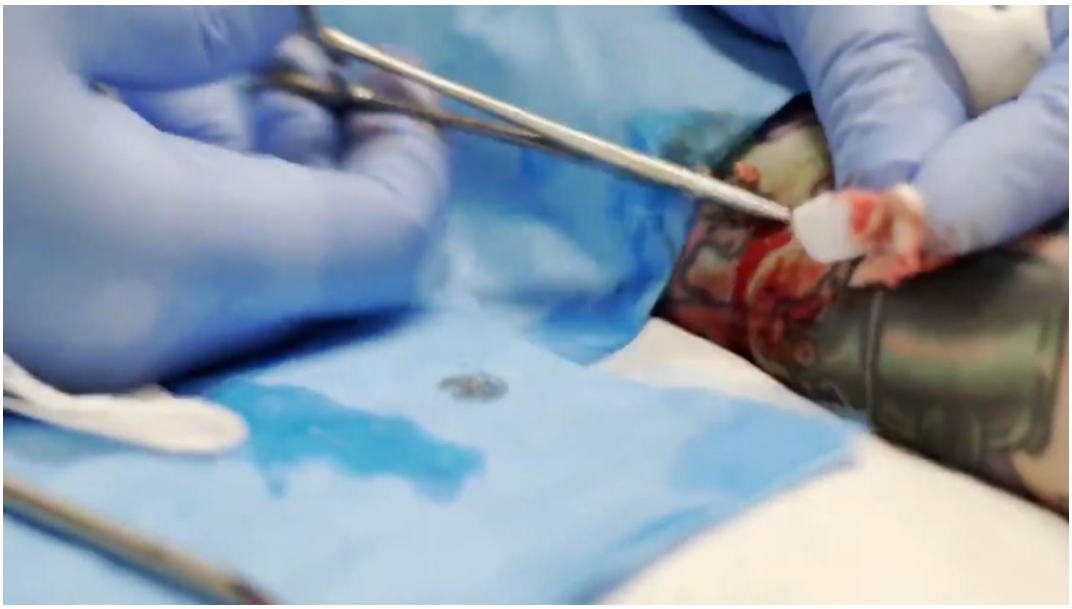
https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!

HTTPS://REDTEAMALLIANCE.COM

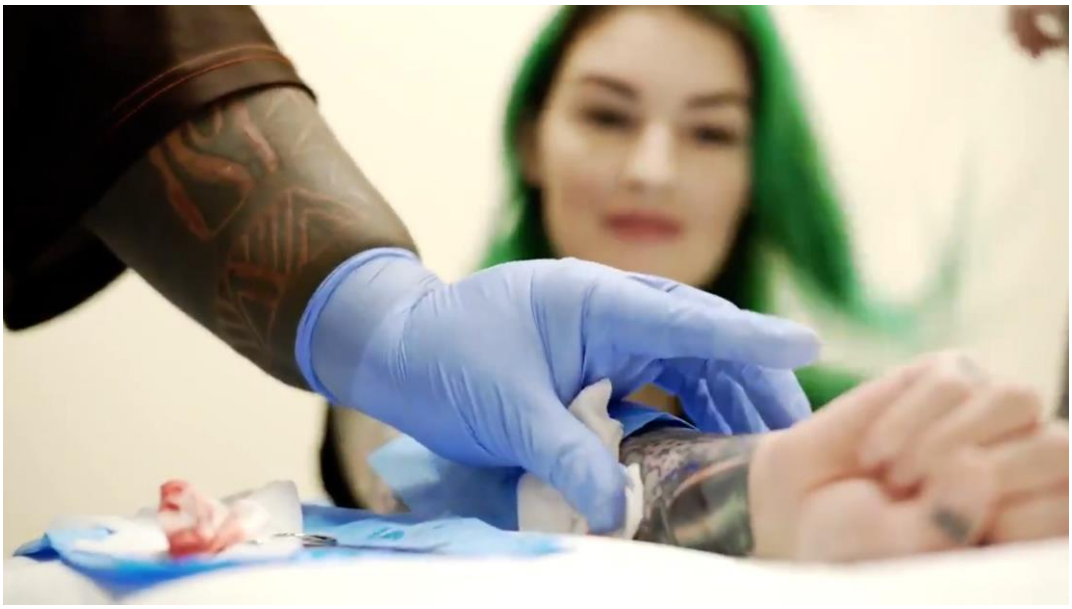
https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!



https://www.youtube.com/user/amieDoubleD/

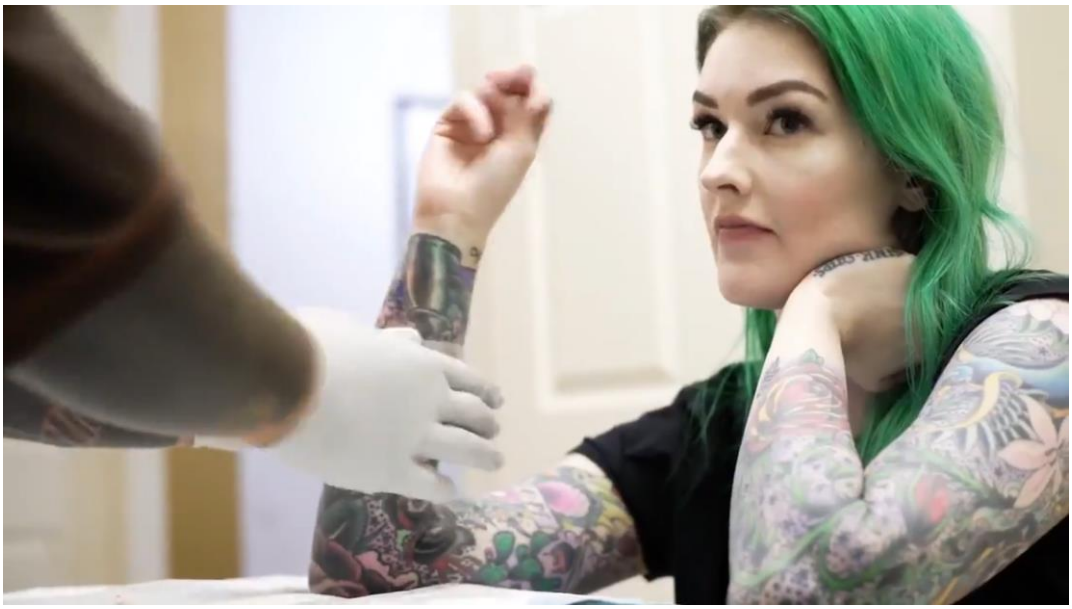
And Bold, Awesome People are Getting Us Closer!



HTTPS://REDTEAMALLIANCE.COM

https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!



HTTPS://REDTEAMALLIANCE.COM

https://www.youtube.com/user/amieDoubleD/

And Bold, Awesome People are Getting Us Closer!

HTTPS://REDTEAMALLIANCE.COM

https://www.youtube.com/user/amieDoubleD/

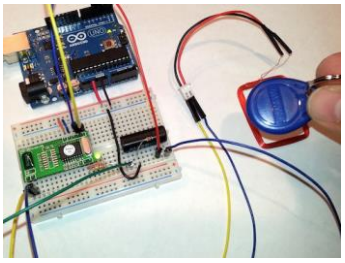
And Bold, Awesome People are Getting Us Closer!

HTTPS://REDTEAMALLIANCE.COM

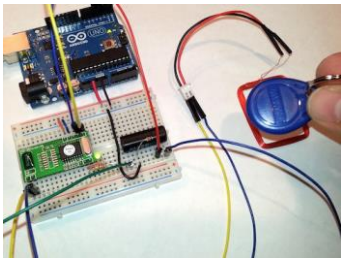
https://www.youtube.com/user/amieDoubleD/

Remember: The key issue is who *CONTROLS* the chips and data

Remember: The key issue is who *CONTROLS* the chips and data



Remember: The key issue is who *CONTROLS* the chips and data



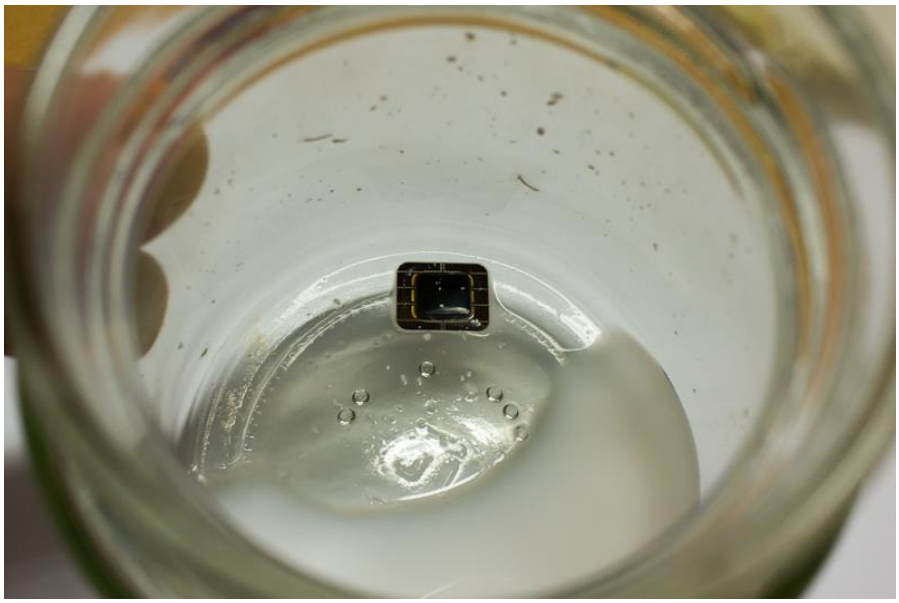
Custom Implants as a Service

HTTPS://REDTEAMALLIANCE.COM

customer often does acetone dissolve themselves
share photos, see if it's chip on board (COB) with plates that get in the way, or MOB package chips (MOB is a term from NXP)

$200 for "conversion"
- take cred
- pull chip
- test resonance
- test with BNA
- test performance before encapsulation
- encapsulate
- antenna shape is maximum width of 8mm at the widest (little black bowtie)
- allows for use of 4 gauge needle
- comes with fully gas plasma sterilized needle (low temp, doesn't harm the bio polymer) and lube, etc... all the things a professional would need
- (50% refund if it fails)
- (bulk rates at 22 units)

Custom Implants as a Service

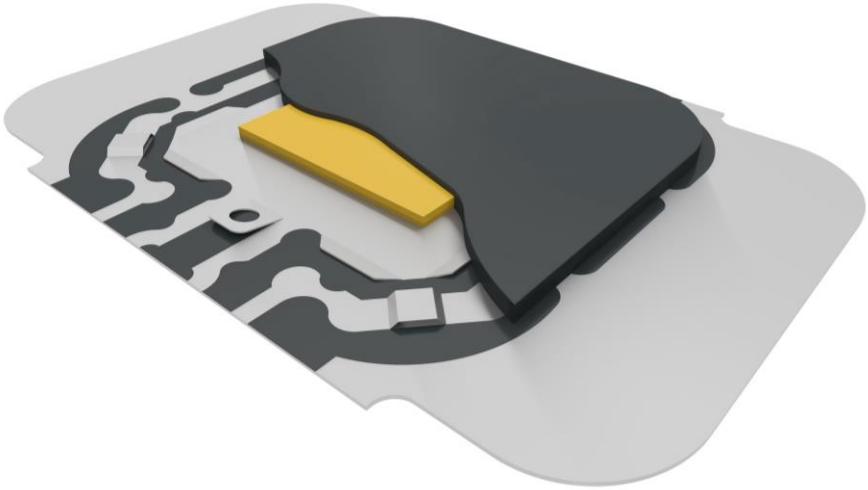


HTTPS://REDTEAMALLIANCE.COM

customer often does acetone dissolve themselves
share photos, see if it's chip on board (COB) with plates that get in the way, or MOB package chips (MOB is a term from NXP)

$200 for "conversion"
- take cred
- pull chip
- test resonance
- test with BNA
- test performance before encapsulation
- encapsulate
- antenna shape is maximum width of 8mm at the widest (little black bowtie)
- allows for use of 4 gauge needle
- comes with fully gas plasma sterilized needle (low temp, doesn't harm the bio polymer) and lube, etc... all the things a professional would need
- (50% refund if it fails)
- (bulk rates at 22 units)

Custom Implants as a Service

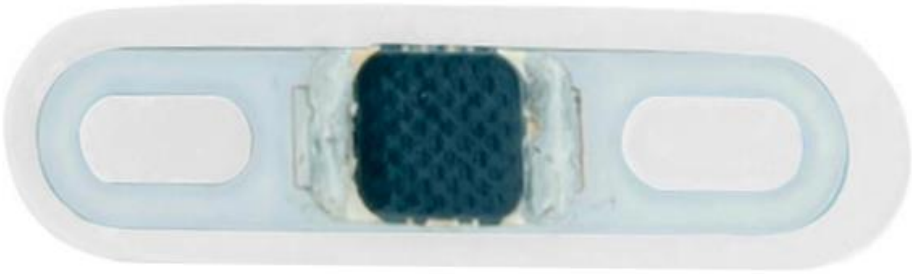


HTTPS://REDTEAMALLIANCE.COM

customer often does acetone dissolve themselves
share photos, see if it's chip on board (COB) with plates that get in the way, or MOB package chips (MOB is a term from NXP)

$200 for "conversion"
- take cred
- pull chip
- test resonance
- test with BNA
- test performance before encapsulation
- encapsulate
- antenna shape is maximum width of 8mm at the widest (little black bowtie)
- allows for use of 4 gauge needle
- comes with fully gas plasma sterilized needle (low temp, doesn't harm the bio polymer) and lube, etc... all the things a professional would need
- (50% refund if it fails)
- (bulk rates at 22 units)

Custom Implants as a Service



HTTPS://REDTEAMALLIANCE.COM

customer often does acetone dissolve themselves
share photos, see if it's chip on board (COB) with plates that get in the way, or MOB package chips (MOB is a term from NXP)

$200 for "conversion"
- take cred
- pull chip
- test resonance
- test with BNA
- test performance before encapsulation
- encapsulate
- antenna shape is maximum width of 8mm at the widest (little black bowtie)
- allows for use of 4 gauge needle
- comes with fully gas plasma sterilized needle (low temp, doesn't harm the bio polymer) and lube, etc... all the things a professional would need
- (50% refund if it fails)
- (bulk rates at 22 units)

Custom Implants as a Service

HTTPS://REDTEAMALLIANCE.COM

customer often does acetone dissolve themselves
share photos, see if it's chip on board (COB) with plates that get in the way, or MOB package chips (MOB is a term from NXP)

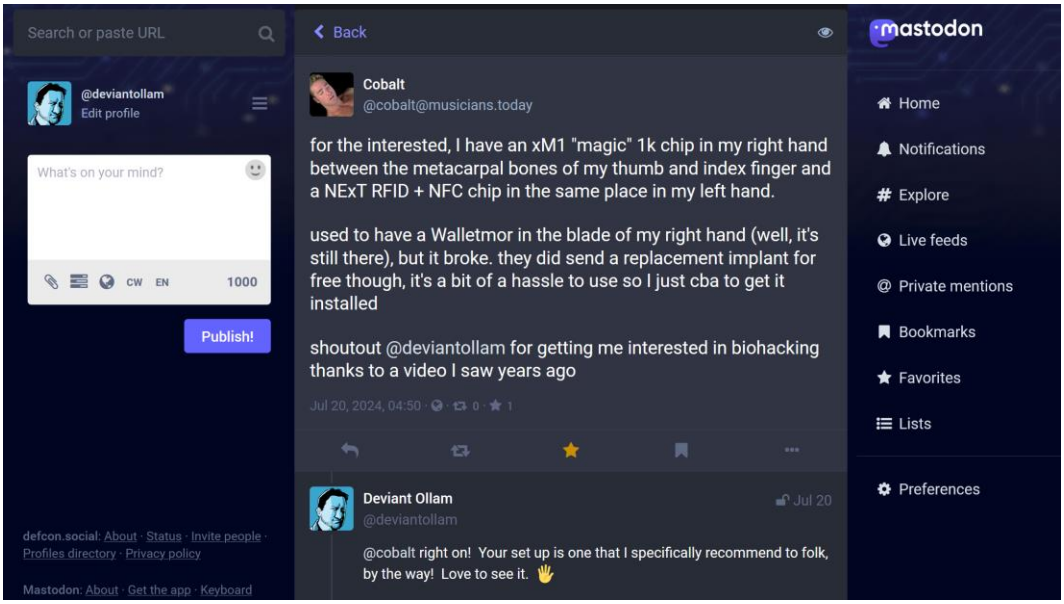
$200 for "conversion"
- take cred
- pull chip
- test resonance
- test with BNA
- test performance before encapsulation
- encapsulate
- antenna shape is maximum width of 8mm at the widest (little black bowtie)
- allows for use of 4 gauge needle
- comes with fully gas plasma sterilized needle (low temp, doesn't harm the bio polymer) and lube, etc... all the things a professional would need
- (50% refund if it fails)
- (bulk rates at 22 units)

COBALT'S IMPLANTS

HTTPS://REDTEAMALLIANCE.COM

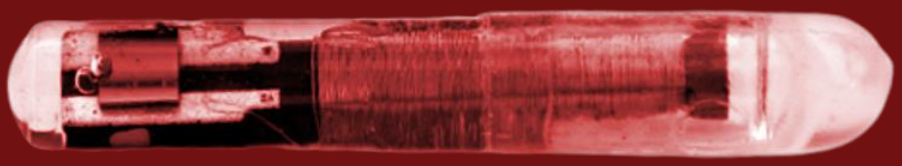
https://musicians.today/@cobalt/112817936307481374

COBALT'S IMPLANTS



https://musicians.today/@cobalt/112817936307481374

Common Questions and Concerns



"Does It Hurt?"

Juneau who's a better Alaskan than Sarah Palin
@Jun34u_sec

DHA Biohacker: "And they didn't give me ANY ANESTHESIA when I got these implants in!"

Me: "Oh, just like an IUD"

8:51 PM · Apr 6, 2022 · Twitter for Android

We do plenty of things that hurt… Most folk would say that it's compatible to a piercing, etc. But ask others who've had it done.

"Can I Use Them Right Away?"

HTTPS://REDTEAMALLIANCE.COM

It's common for the insertion point to swell slightly. This isn't a sign of a problem, it's just the body healing. The swelling can cause extra "distance" between the coil and any reader so for the first few days you might experience intermittent read/write difficulty. (This is less of an issue if you have a ferrite core antenna and an LF credential.)

"Can I Use Them Right Away?"

HTTPS://REDTEAMALLIANCE.COM

It's common for the insertion point to swell slightly. This isn't a sign of a problem, it's just the body healing. The swelling can cause extra "distance" between the coil and any reader so for the first few days you might experience intermittent read/write difficulty. (This is less of an issue if you have a ferrite core antenna and an LF credential.)

"Can I Use Them Right Away?"

HTTPS://REDTEAMALLIANCE.COM

It's common for the insertion point to swell slightly. This isn't a sign of a problem, it's just the body healing. The swelling can cause extra "distance" between the coil and any reader so for the first few days you might experience intermittent read/write difficulty. (This is less of an issue if you have a ferrite core antenna and an LF credential.)

"Are These Safe During Medical Procedures?"

HTTPS://REDTEAMALLIANCE.COM

Implantable RFID transponders have tested as compatible with MRI machines up to 7 Tesla field strength

But **magnetic** implants are **incompatible** with MRI machines and procedures

Think about it… long before humans did this, we've had pet chips. So there has been lots of testing both in field trials and clinical trials.

Non-ferrous, and data is found to still be readable and with good integrity.

There is SOME metal in these devices, however, which can cause artifacts in images acquired. If an implant is close to the region being imaged, the diagnosis may be compromised.

"Are These Safe During Medical Procedures?"

HTTPS://REDTEAMALLIANCE.COM

Deviant's friend Kara. Was having some trouble with balance and walking, eventually taking a hard fall.

Went in for consultation, they wanted to do an MRI. Question of whether she could go through the machine…. Because of implants in her hands.

"ARE THESE SAFE DURING MEDICAL PROCEDURES?"

DANGEROUS THINGS

MRI Compatibility of x-series transponders

Patients with a Dangerous Things x-series microtransponder may safely undergo MRI diagnostics in cylindrical systems up to 7-Tesla.

INSTRUCTIONS FOR PATIENTS UNDERGOING MRI:

- The patient should be monitored continuously throughout the MRI procedure using visual and audio means (e.g., video monitor with intercom link).

- Instruct the patient to alert the MR system operator of any unusual sensations or problems so that, if necessary, the MR system operator can immediately terminate the procedure.

- Provide the patient with a means to alert the MR system operator of any unusual sensations or problems.

- Do not perform MRI if the patient is sedated, anesthetized, confused or otherwise unable to communicate with the MR system operator.

- The presence of metal in the device is certain to cause artefacts in the images acquired, so if the device is close to the region being imaged, the diagnosis may be compromised. Removal of the device will be required if artefacts affect diagnostics.

CLINICAL TRIALS AND STUDIES:

The ability to read patient identification microchips relies on the use of radiofrequency pulses. Since radiofrequency pulses also form an integral part of the magnetic resonance imaging (MRI) process, the possibility of loss of microchip function during MRI scanning is of concern. Previous clinical trials have shown microchip function to be unaffected by MR imaging using a field strength of 1 Tesla and 1.5. As veterinary MRI scanners range widely in field strength, a study[1] was devised to determine whether exposure to lower or higher field strengths than 1 Tesla would affect the function of different types of microchip. In this phantom study, a total of 300 International Standards Organization (ISO)-approved microchips (100 each of three different types: ISO FDX-B 1.4 × 9 mm, ISO FDX-B 2.12 × 12 mm, ISO HDX 3.8 × 23 mm) were tested in a low field (0.5) and a high field scanner (3.0 Tesla). A total of 50 microchips of each type were tested in each scanner. The phantom was composed of a fluid-filled freezer pack onto which a plastic pillow and a cardboard strip with affixed microchips were positioned. Following an MRI scan protocol simulating a head study, all of the microchips were accurately readable. Neither 0.5 nor 3 Tesla imaging affected microchip function in this study.

HTTPS://REDTEAMALLIANCE.COM

Deviant's friend Kara. Was having some trouble with balance and walking, eventually taking a hard fall.

Went in for consultation, they wanted to do an MRI. Question of whether she could go through the machine…. Because of implants in her hands.

She spoke to Dev from the facility and he pointed her to that document, which was shared with doctors and clinical staff.

"Are These Safe During Medical Procedures?"

DANGEROUS THINGS

MRI Compatibility of x-series transponders

Patients with a Dangerous Things x-series microtransponder may safely undergo MRI diagnostics in cylindrical systems up to 7-Tesla.

INSTRUCTIONS FOR PATIENTS UNDERGOING MRI:

- The patient should be monitored continuously throughout the MRI procedure using visual and audio means (e.g., video monitor with intercom link).

- Instruct the patient to alert the MR syste… sensations or problems so that, if necessary, the MR system operator can …cedure.

- Provide the patient with a means to aler… unusual sensations or problems.

- Do not perform MRI if the patient is sed… otherwise unable to communicate with the MR system operator.

- The presence of metal in the device is … images acquired, so if the device is close to the region being imaged, the dia… emoval of the device will be required if artefacts affect diagnostics.

CLINICAL TRIALS AND STUDIES:

The ability to read patient identification microchips relies on the use of radiofrequency pulses. Since radiofrequency pulses also form an integral part of the magnetic resonance imaging (MRI) process, the possibility of loss of microchip function during MRI scanning is of concern. Previous clinical trials have shown microchip function to be unaffected by MR imaging using a field strength of 1 Tesla and 1.5. As veterinary MRI scanners range widely in field strength, a study[1] was devised to determine whether exposure to lower or higher field strengths than 1 Tesla would affect the function of different types of microchip. In this phantom study, a total of 300 International Standards Organization (ISO)-approved microchips (100 each of three different types: ISO FDX-B 1.4 × 9 mm, ISO FDX-B 2.12 × 12 mm, ISO HDX 3.8 × 23 mm) were tested in a low field (0.5) and a high field scanner (3.0 Tesla). A total of 50 microchips of each type were tested in each scanner. The phantom was composed of a fluid-filled freezer pack onto which a plastic pillow and a cardboard strip with affixed microchips were positioned. Following an MRI scan protocol simulating a head study, all of the microchips were accurately readable. Neither 0.5 nor 3 Tesla imaging affected microchip function in this study.

HTTPS://FORUM.DANGEROUSTHINGS.COM/UPLOADS/DEFAULT/ORIGINAL/1X/289AF3580C98807BDD9DE089A27D73F383CE7BCE.PDF

HTTPS://REDTEAMALLIANCE.COM

Deviant's friend Kara. Was having some trouble with balance and walking, eventually taking a hard fall.

Went in for consultation, they wanted to do an MRI. Question of whether she could go through the machine…. Because of implants in her hands.

She spoke to Dev from the facility and he pointed her to that document, which was shared with doctors and clinical staff.

https://forum.dangerousthings.com/uploads/default/original/1X/289af3580c98807bdd9de089a27d73f383ce7bce.pdf

"Are These Safe During Medical Procedures?"

HTTPS://REDTEAMALLIANCE.COM

They were satisfied and she was put in the imaging machine. Upon exit, her doctors were like, "OK, so we're going to admit you."

"Admit me to a regimen of care? Admit me for monitoring?" she asked. "No, I mean admit you for surgery. Now," they said… practically while scrubbing in.

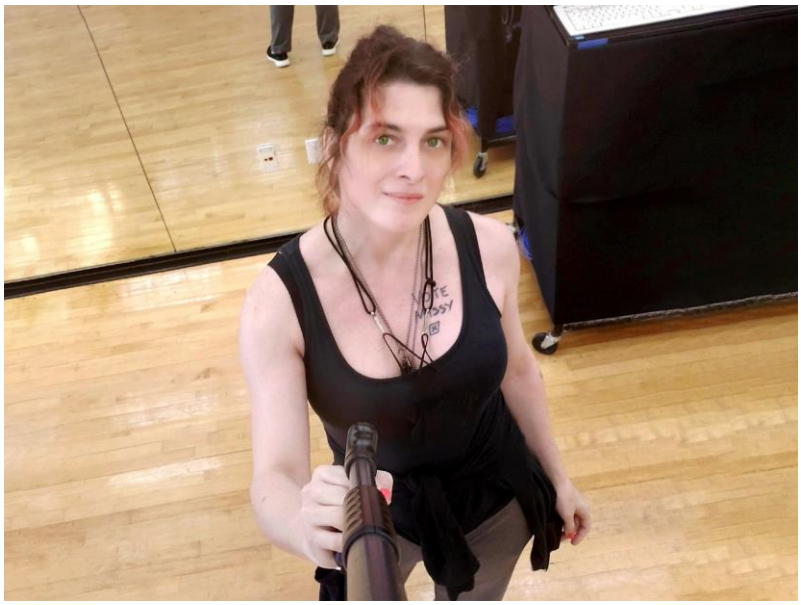
After the surgery, they told her about the scar tissue, the pressure against her spinal cord, and what a close call this was

"Are These Safe During Medical Procedures?"

HTTPS://REDTEAMALLIANCE.COM

As opposed to a lifetime of dizziness, pain, and likely becoming a paraplegic… this is her being discharged from the hospital a few weeks after her emergency surgery

"Are These Safe During Medical Procedures?"

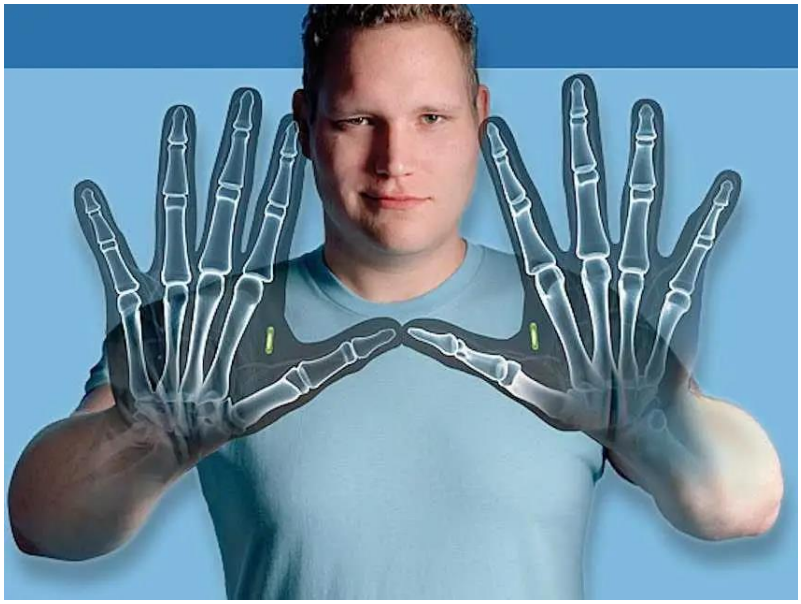


HTTPS://REDTEAMALLIANCE.COM

She still currently walks with a cane while continuing physical therapy… but she's alive.

She dodged possibly not being able to walk ever again or possibly dramatically shortening her life because she was able to get that MRI that day.

"Are These Safe During Medical Procedures?"

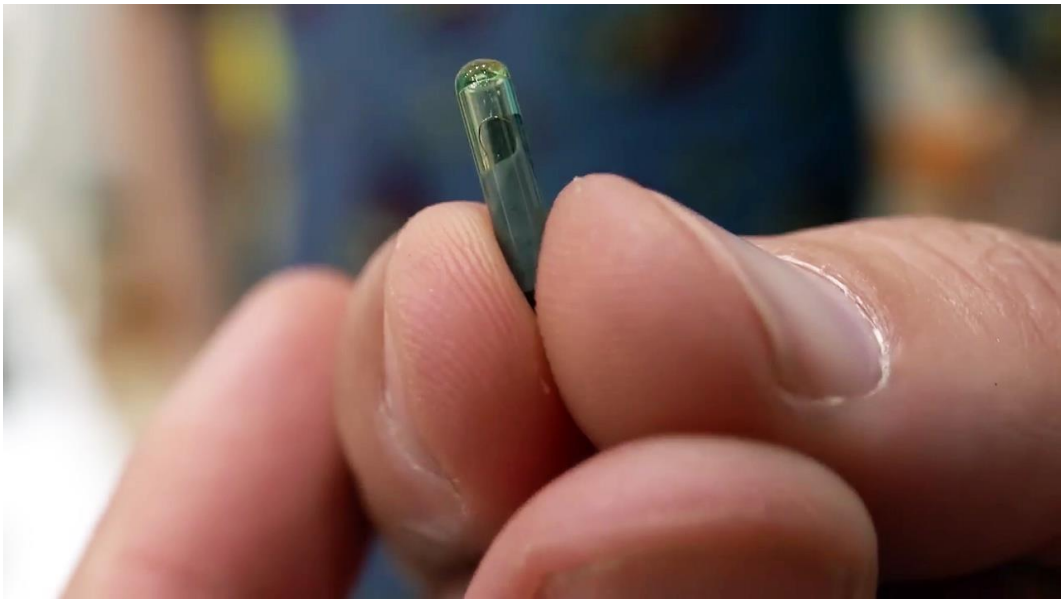


HTTPS://REDTEAMALLIANCE.COM

Amal's work and his kindness to put that document online -- publicly and for free so that anyone who needed this information could have it -- saved her

("take the time to write that blog entry or make that forum post or publish that proof-of-concept or submit to some hacker con CFP now… because you never know whose life your shared knowledge is going to impact years later")

"How Durable Are These?"



HTTPS://REDTEAMALLIANCE.COM

Bioglass (a variant of standard soda-lime glass as opposed to borosilicate glass, etc)

elicits the body collagenizing response
does not have biobond like animal tags
(causes inflamatory response -- cancer studies by antis -- and restricts removal)

CyberizeMe/BiohackMe -- makers of Firefly -- implants use flame-sealed process
(particulates all around the glass, forms a terrible tension point)
Dangerous Things -- implants use laser-sealed process

"How Durable Are These?"

HTTPS://REDTEAMALLIANCE.COM

Bioglass (a variant of standard soda-lime glass as opposed to borosilicate glass, etc)

elicits the body collagenizing response
does not have biobond like animal tags
(causes inflamatory response -- cancer studies by antis -- and restricts removal)

CyberizeMe/BiohackMe -- makers of Firefly -- implants use flame-sealed process
(particulates all around the glass, forms a terrible tension point)
Dangerous Things -- implants use laser-sealed process

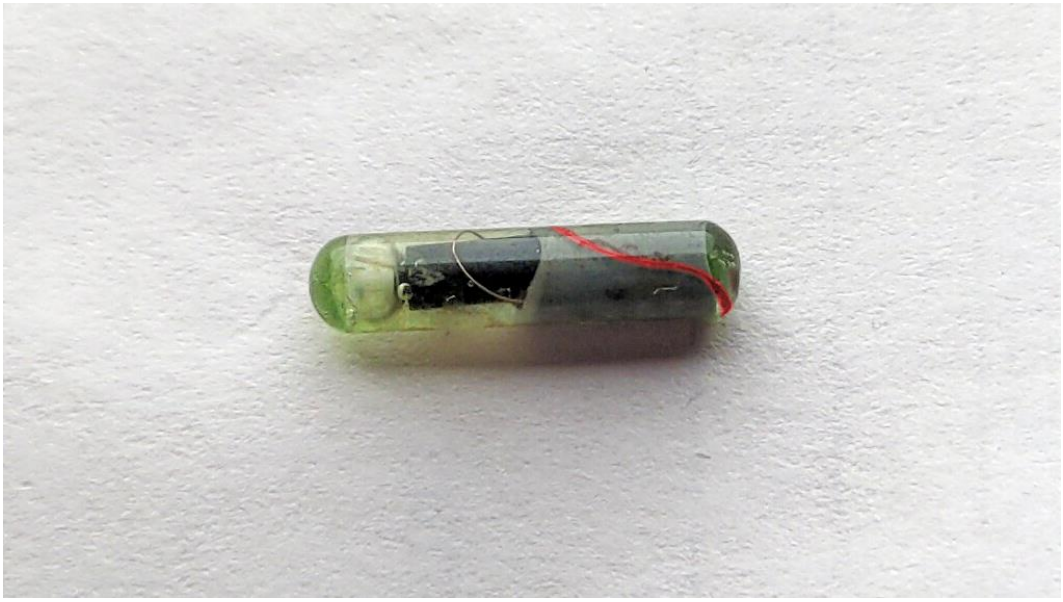
"How Durable Are These?"

HTTPS://REDTEAMALLIANCE.COM

bashNinja had a MIFARE chip stop working. These have been buggy for some folk, so he had it removed.

This is what was discovered…

"How Durable Are These?"



HTTPS://REDTEAMALLIANCE.COM

…hairline fracture. Could this have caused the failure? Maybe. Could this have happened in his hand? Doubtful. More than likely, this was pre-insertion.

Dangerous Things is inspecting things and checking out QA measures, etc. (unfortunately, no super easy way to inspect an implant before administering it)

Out of many thousands of implants, this is the only one we've ever heard of like this.

"How Secure Are These?"

HTTPS://REDTEAMALLIANCE.COM

So we need to talk about the difference between security ON the CHIP versus …

…integration with access control SYSTEMS

"How Secure Are These?"

HTTPS://REDTEAMALLIANCE.COM

So we need to talk about the difference between security ON the CHIP versus …

…integration with access control SYSTEMS

"How Secure Are These?"

HTTPS://REDTEAMALLIANCE.COM

So we need to talk about the difference between security ON the CHIP versus …

…integration with access control SYSTEMS

"How Secure Are These?"

```
 "0": "91DD1AE6B008040002EA1CF1517C6C1D",
 "1": "0DC015694D734D05428D2A03D510CD8D",
 "2": "52000400010000000000000000000000",
 "3": "00E990B9C9E8FF078069FFFFFFFFFFFF",
 "4": "30000C0000000000000000C100000002",
 "5": "30000C0000000000000000C100000002",
 "6": "00000000000000000000000000000000",
 "7": "2A2C13CC242AFF078069FFFFFFFFFFFF",
 "8": "00000000000000000000000000000000",
 "9": "00000000000000000000000000000000",
"10": "00000000000000000000000000000000",
"11": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"12": "00000000000000000000000000000000",
"13": "00000000000000000000000000000000",
"14": "00000000000000000000000000000000",
"15": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"16": "A64B787121DE00D9A64B752921620012",
"17": "A64B80BB21DE002BA64B80C021DE0030",
"18": "A64B7D7321620064A64B83F021DE0063",
"19": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"20": "A64B840521DE0079A64B82B8216200AE",
"21": "A64B84C121DE0035A64B836921620060",
"22": "A64B894921DE00C2A64B85FB216200F4",
"23": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"24": "00000000000000000000000000000000",
"25": "00000000000000000000000000000000",
"26": "00000000000000000000000000000000",
"27": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"28": "00000000000000000000000000000000",
"29": "00000000000000000000000000000000",
"30": "00000000000000000000000000000000",
"31": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"32": "00000000000000000000000000000000",
"33": "00000000000000000000000000000000",
"34": "00000000000000000000000000000000",
"35": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"36": "00000000000000000000000000000000",
"37": "00000000000000000000000000000000",
"38": "00000000000000000000000000000000",
"39": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"40": "00000000000000000000000000000000",
"41": "00000000000000000000000000000000",
"42": "00000000000000000000000000000000",
"43": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"44": "00000000000000000000000000000000",
"45": "00000000000000000000000000000000",
"46": "00000000000000000000000000000000",
"47": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"48": "00000000000000000000000000000000",
"49": "00000000000000000000000000000000",
"50": "00000000000000000000000000000000",
"51": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"52": "00000000000000000000000000000000",
"53": "00000000000000000000000000000000",
"54": "00000000000000000000000000000000",
"55": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"56": "00000000000000000000000000000000",
"57": "00000000000000000000000000000000",
"58": "00000000000000000000000000000000",
"59": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"60": "00000000000000000000000000000000",
"61": "00000000000000000000000000000000",
"62": "00000000000000000000000000000000",
"63": "00E990B9C9E8FF078069FFFFFFFFFFFF"
```

“How Secure Are These?”


```
"0": "91DD1AE6B008040002EA1CF1517C6C1D",
"1": "0DC015694D734D05428D2A03D510CD8D",
"2": "52000400010000000000000000000000",
"3": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"4": "30000C0000000000000000C100000002",
"5": "30000C0000000000000000C100000002",
"6": "00000000000000000000000000000000",
"7": "2A2C13CC242AFF078069FFFFFFFFFFFF",
"8": "00000000000000000000000000000000",
"9": "00000000000000000000000000000000",
"10": "00000000000000000000000000000000",
"11": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"12": "00000000000000000000000000000000",
"13": "00000000000000000000000000000000",
"14": "00000000000000000000000000000000",
"15": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"16": "A64B787121DE00D9A64B752921620012",
"17": "A64B80BB21DE002BA64B80C021DE0030",
"18": "A64B7D7321620064A64B83F021DE0063",
"19": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"20": "A64B840521DE0079A64B82B8216200AE",
"21": "A64B84C121DE0035A64B836921620060",
"22": "A64B894921DE00C2A64B85FB216200F4",
"23": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"24": "00000000000000000000000000000000",
"25": "00000000000000000000000000000000",
"26": "00000000000000000000000000000000",
"27": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"28": "00000000000000000000000000000000",
"29": "00000000000000000000000000000000",
"30": "00000000000000000000000000000000",
"31": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"32": "00000000000000000000000000000000",
"33": "00000000000000000000000000000000",
"34": "00000000000000000000000000000000",
"35": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"36": "00000000000000000000000000000000",
"37": "00000000000000000000000000000000",
"38": "00000000000000000000000000000000",
"39": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"40": "00000000000000000000000000000000",
"41": "00000000000000000000000000000000",
"42": "00000000000000000000000000000000",
"43": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"44": "00000000000000000000000000000000",
"45": "00000000000000000000000000000000",
"46": "00000000000000000000000000000000",
"47": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"48": "00000000000000000000000000000000",
"49": "00000000000000000000000000000000",
"50": "00000000000000000000000000000000",
"51": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"52": "00000000000000000000000000000000",
"53": "00000000000000000000000000000000",
"54": "00000000000000000000000000000000",
"55": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"56": "00000000000000000000000000000000",
"57": "00000000000000000000000000000000",
"58": "00000000000000000000000000000000",
"59": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"60": "00000000000000000000000000000000",
"61": "00000000000000000000000000000000",
"62": "00000000000000000000000000000000",
"63": "00E990B9C9E8FF078069FFFFFFFFFFFF"
```


Block 0 contains a Unique ID and some manufacturer information.

“How Secure Are These?”


```
"0": "91DD1AE6B008040002EA1CF1517C6C1D",
"1": "0DC015694D734D05428D2A03D510CD8D",
"2": "52000400010000000000000000000000",
"3": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"4": "30000C0000000000000000C100000002",
"5": "30000C0000000000000000C100000002",
"6": "00000000000000000000000000000000",
"7": "2A2C13CC242AFF078069FFFFFFFFFFFF",
"8": "00000000000000000000000000000000",
"9": "00000000000000000000000000000000",
"10": "00000000000000000000000000000000",
"11": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"12": "00000000000000000000000000000000",
"13": "00000000000000000000000000000000",
"14": "00000000000000000000000000000000",
"15": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"16": "A64B787121DE00D9A64B752921620012",
"17": "A64B80BB21DE002BA64B80C021DE0030",
"18": "A64B7D7321620064A64B83F021DE0063",
"19": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"20": "A64B840521DE0079A64B82B8216200AE",
"21": "A64B84C121DE0035A64B836921620060",
"22": "A64B894921DE00C2A64B85FB216200F4",
"23": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"24": "00000000000000000000000000000000",
"25": "00000000000000000000000000000000",
"26": "00000000000000000000000000000000",
"27": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"28": "00000000000000000000000000000000",
"29": "00000000000000000000000000000000",
"30": "00000000000000000000000000000000",
"31": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"32": "00000000000000000000000000000000",
"33": "00000000000000000000000000000000",
"34": "00000000000000000000000000000000",
"35": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"36": "00000000000000000000000000000000",
"37": "00000000000000000000000000000000",
"38": "00000000000000000000000000000000",
"39": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"40": "00000000000000000000000000000000",
"41": "00000000000000000000000000000000",
"42": "00000000000000000000000000000000",
"43": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"44": "00000000000000000000000000000000",
"45": "00000000000000000000000000000000",
"46": "00000000000000000000000000000000",
"47": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"48": "00000000000000000000000000000000",
"49": "00000000000000000000000000000000",
"50": "00000000000000000000000000000000",
"51": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"52": "00000000000000000000000000000000",
"53": "00000000000000000000000000000000",
"54": "00000000000000000000000000000000",
"55": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"56": "00000000000000000000000000000000",
"57": "00000000000000000000000000000000",
"58": "00000000000000000000000000000000",
"59": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"60": "00000000000000000000000000000000",
"61": "00000000000000000000000000000000",
"62": "00000000000000000000000000000000",
"63": "00E990B9C9E8FF078069FFFFFFFFFFFF"
```


All these other blocks of data are used for secure storage, however. They have specific keys that control how the data can be accessed, modified, etc

“How Secure Are These?”

And in these blocks here, this is where the card has the actual PACS payload and access control credential data stored

“How Secure Are These?”


```
"0": "91DD1AE6B008040002EA1CF1517C6C1D",
"1": "0DC015694D734D05428D2A03D510CD8D",
"2": "52000400010000000000000000000000",
"3": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"4": "30000C0000000000000000C100000002",
"5": "30000C0000000000000000C100000002",
"6": "00000000000000000000000000000000",
"7": "2A2C13CC242AFF078069FFFFFFFFFFFF",
"8": "00000000000000000000000000000000",
"9": "00000000000000000000000000000000",
"10": "00000000000000000000000000000000",
"11": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"12": "00000000000000000000000000000000",
"13": "00000000000000000000000000000000",
"14": "00000000000000000000000000000000",
"15": "FFFFFFFFFFFFFF078069FFFFFFFFFFFF",
"16": "A64B787121DE00D9A64B752921620012",
"17": "A64B80BB21DE002BA64B80C021DE0030",
"18": "A64B7D7321620064A64B83F021DE0063",
"19": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"20": "A64B840521DE0079A64B82B8216200AE",
"21": "A64B84C121DE0035A64B836921620060",
"22": "A64B894921DE00C2A64B85FB216200F4",
"23": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"24": "00000000000000000000000000000000",
"25": "00000000000000000000000000000000",
"26": "00000000000000000000000000000000",
"27": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"28": "00000000000000000000000000000000",
"29": "00000000000000000000000000000000",
"30": "00000000000000000000000000000000",
"31": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"32": "00000000000000000000000000000000",
"33": "00000000000000000000000000000000",
"34": "00000000000000000000000000000000",
"35": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"36": "00000000000000000000000000000000",
"37": "00000000000000000000000000000000",
"38": "00000000000000000000000000000000",
"39": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"40": "00000000000000000000000000000000",
"41": "00000000000000000000000000000000",
"42": "00000000000000000000000000000000",
"43": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"44": "00000000000000000000000000000000",
"45": "00000000000000000000000000000000",
"46": "00000000000000000000000000000000",
"47": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"48": "00000000000000000000000000000000",
"49": "00000000000000000000000000000000",
"50": "00000000000000000000000000000000",
"51": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"52": "00000000000000000000000000000000",
"53": "00000000000000000000000000000000",
"54": "00000000000000000000000000000000",
"55": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"56": "00000000000000000000000000000000",
"57": "00000000000000000000000000000000",
"58": "00000000000000000000000000000000",
"59": "00E990B9C9E8FF078069FFFFFFFFFFFF",
"60": "00000000000000000000000000000000",
"61": "00000000000000000000000000000000",
"62": "00000000000000000000000000000000",
"63": "00E990B9C9E8FF078069FFFFFFFFFFFF"
```


HTTPS://REDTEAMALLIANCE.COM

And that credential data is in the secured memory segment

“How Secure Are These?”

Now remember… Block 0 is not encrypted

the credential will share this with anyone who queries the card.

"How Secure Are These?"

HTTPS://REDTEAMALLIANCE.COM

the difference between security ON the CHIP versus …

…integration with access control SYSTEMS

"How Secure Are These?"

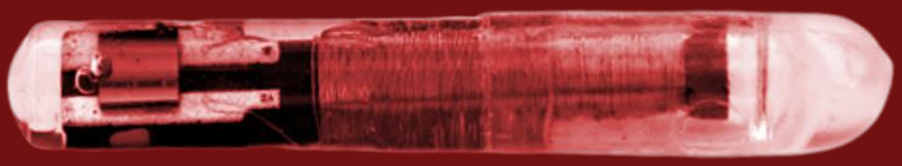
HTTPS://REDTEAMALLIANCE.COM

the difference between security ON the CHIP versus …

…integration with access control SYSTEMS

Be cautious of "CSN mode only" locks, etc.

The Security Risk of "CSN Mode" Authentication



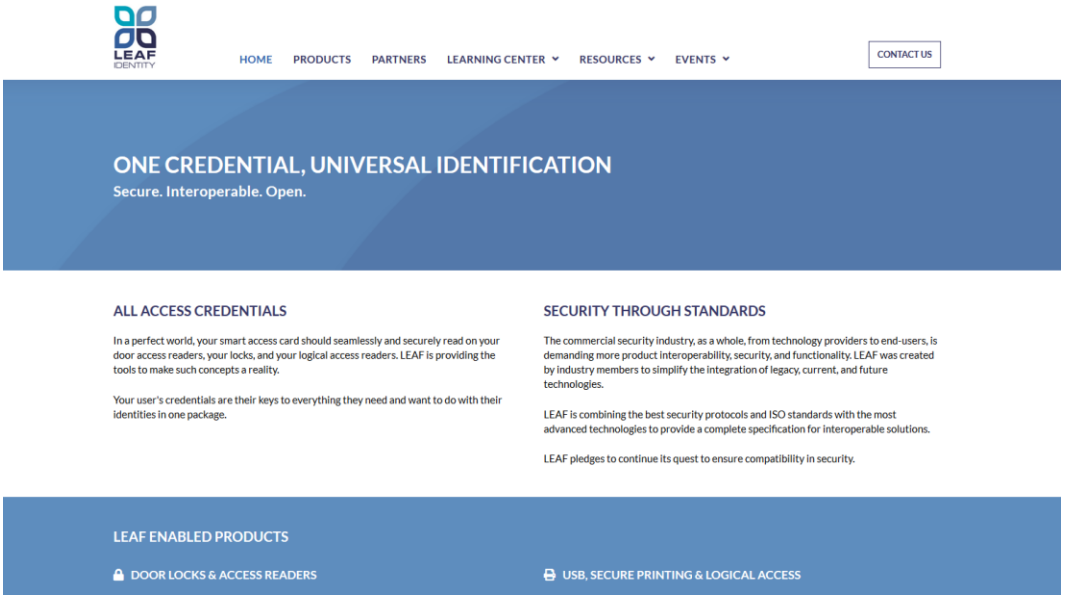
How Secure is This Process?

HTTPS://REDTEAMALLIANCE.COM

The difference between security ON the CHIP versus …

…integration with access control SYSTEMS

"How Secure Are These?"



HTTPS://REDTEAMALLIANCE.COM

There are efforts being made to push for more standards, especially as far as access control is concerned

The LEAF standard has the most promise here

"Can I Remove It?"

HTTPS://REDTEAMALLIANCE.COM

Per Deviant's friend Josh who removed a faulty xM1:

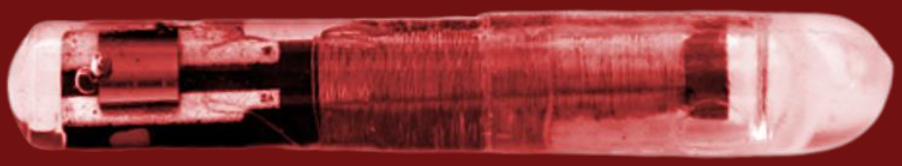
"It was mostly the case of making an incision at one of the short edges and giving it a 'ramp' to slide out of. Then, with some pressure, push it out of the opening enough to grab with tweezers or to make it completely fall out. I'd recommend some topical anesthetic. It wasn't an overall bad or unpleasant experience. Comparable to an x-Series install. Healing time wasn't too bad; the same for any cut given that it's only a small incision, after all."

"Can I Remove It?"

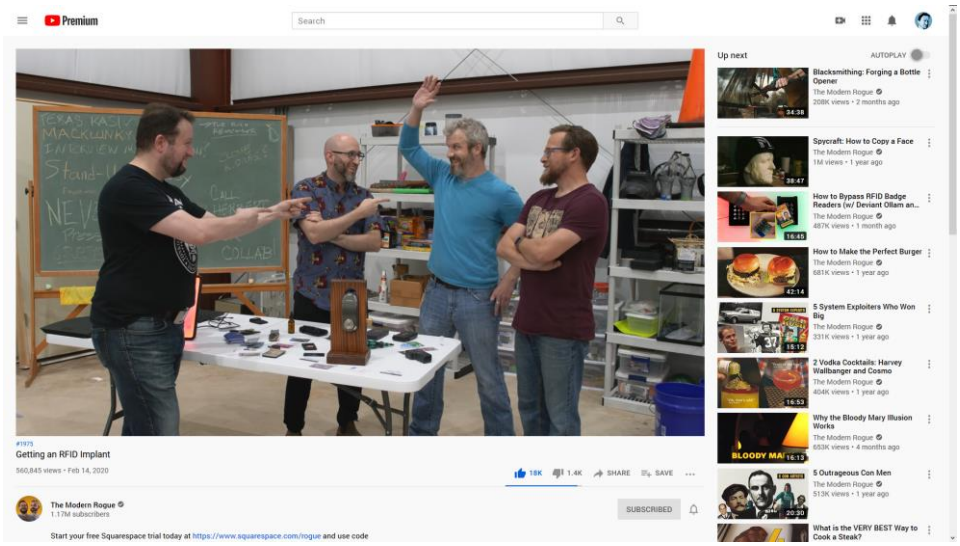
HTTPS://REDTEAMALLIANCE.COM

Other people have removed theirs over the years, mostly to upgrade to newer ones. Yes, it is possible.

Questions and Concerns From *Non*-Hackers

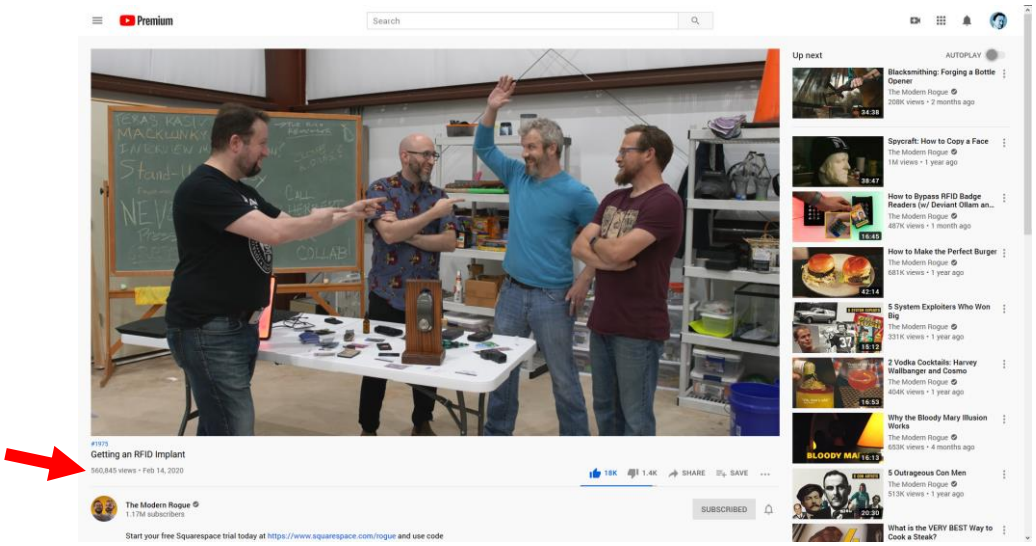


We Did This Video. It Was Fun.

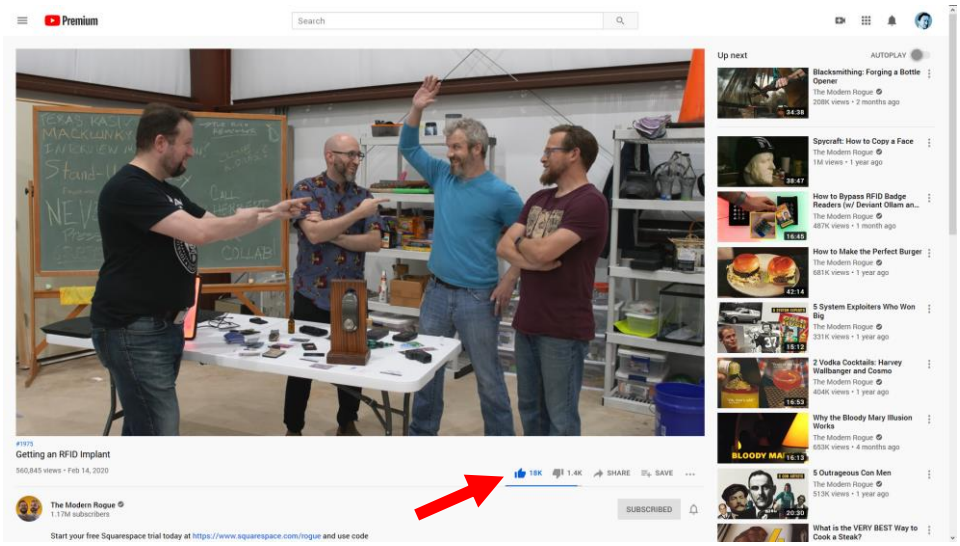


HTTPS://REDTEAMALLIANCE.COM

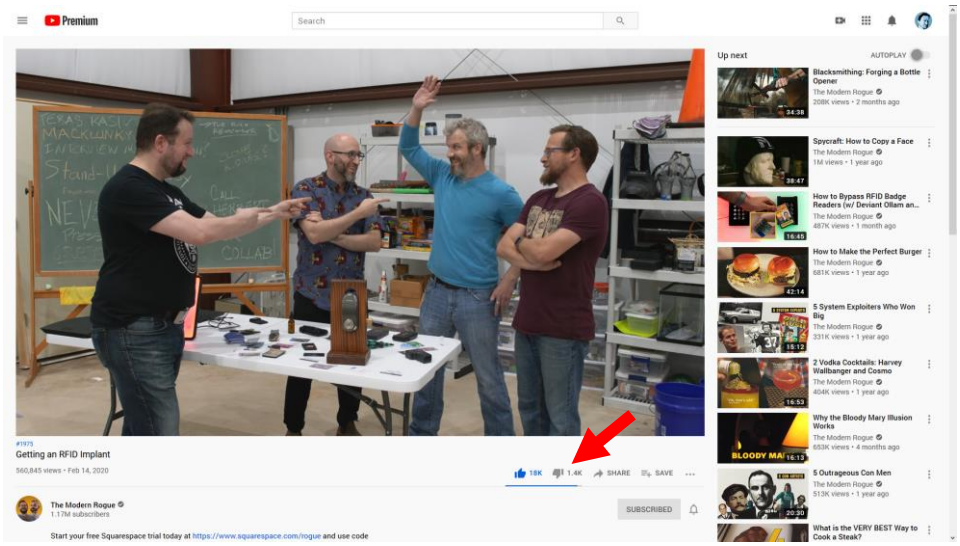
Lots of People Watched It



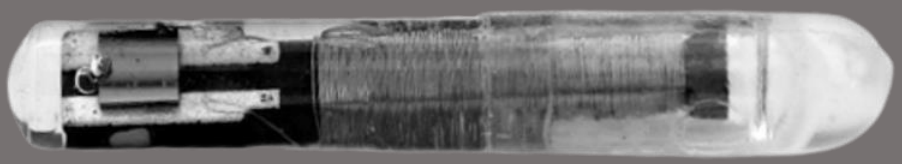
MOST OF THEM LIKED IT!



BUT A HANDFUL OF FOLK DIDN'T...

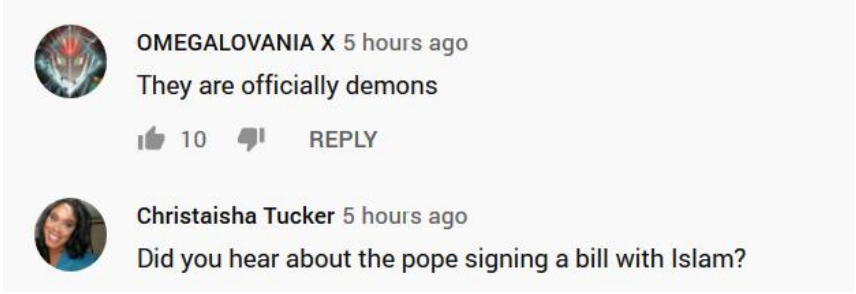


Behold: Internet Comments



Let's do a rundown / dramatic reading of **my top ten favorites**

COMMENTS FROM THE INTERNET - #10

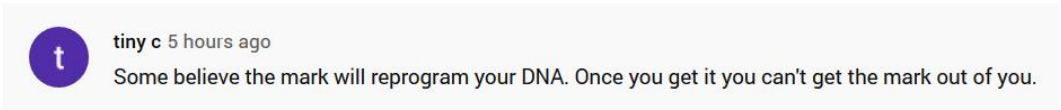


COMMENTS FROM THE INTERNET - #9

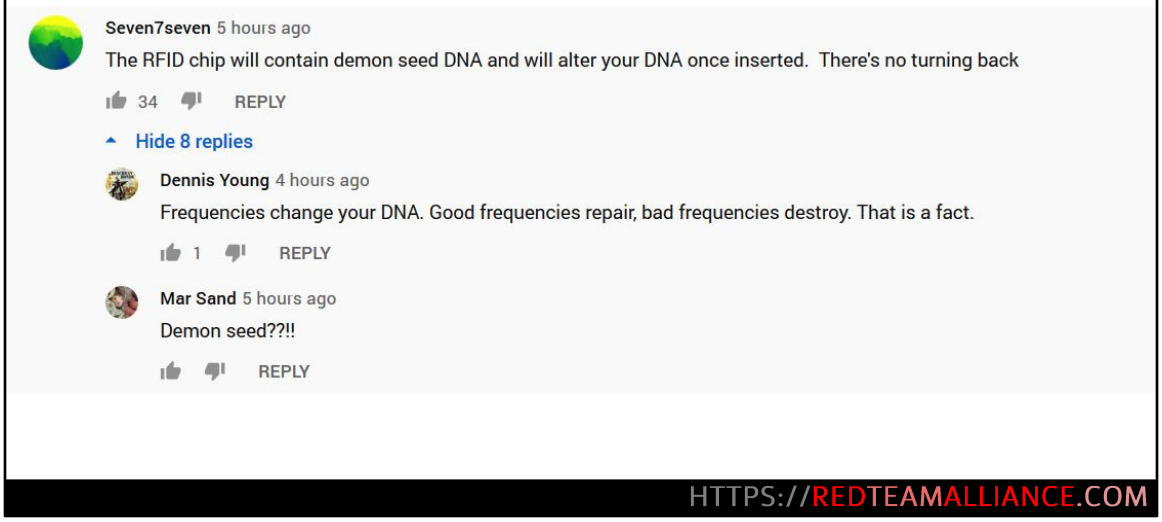
MoreCowbell 2 hours ago (edited)

Set the chips on FIRE! I woud never stick that thing in my body even before I woke up.

COMMENTS FROM THE INTERNET - #8

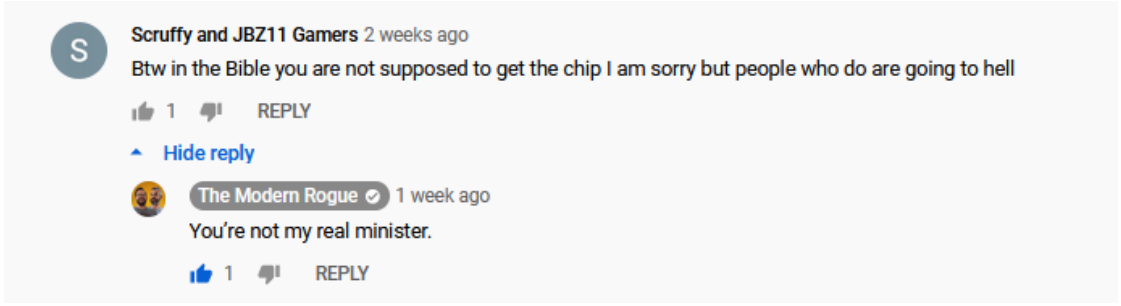


Comments From the Internet - #7

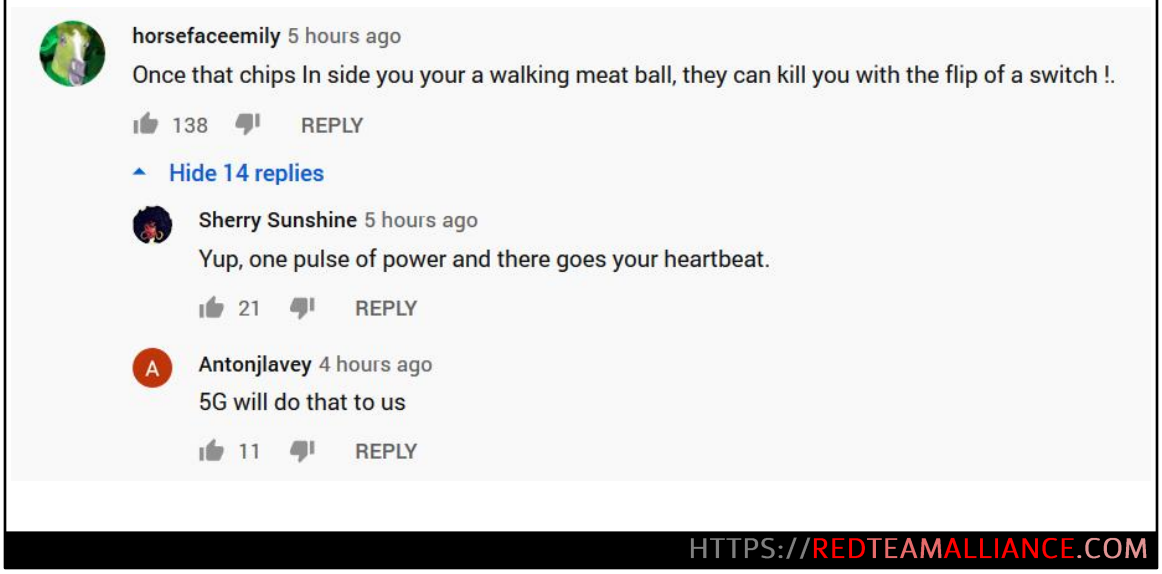


COMMENTS FROM THE INTERNET - #6

Comments From the Internet - #5



COMMENTS FROM THE INTERNET - #4



HTTPS://REDTEAMALLIANCE.COM

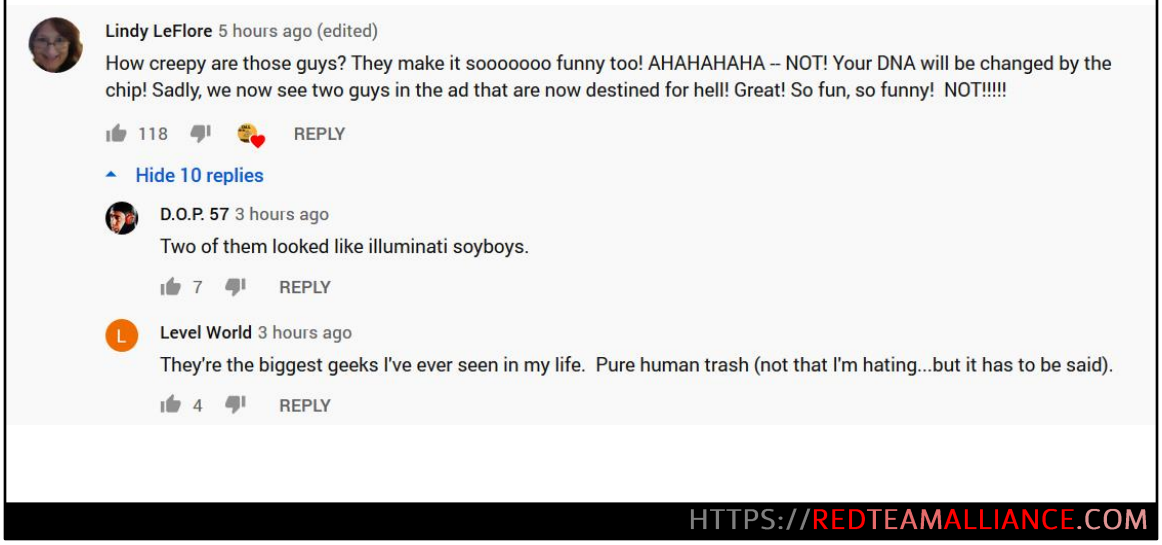
Comments From the Internet - #3

Th3lite 5 hours ago (edited)

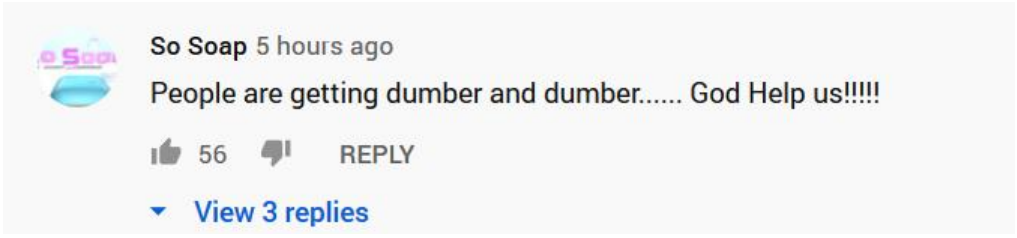
May the forces behind these evil agendas all be eaten alive by a sworn of lucust.

16 REPLY

Comments From the Internet - #2



COMMENTS FROM THE INTERNET - #1



COMMENTS FROM THE INTERNET - #1

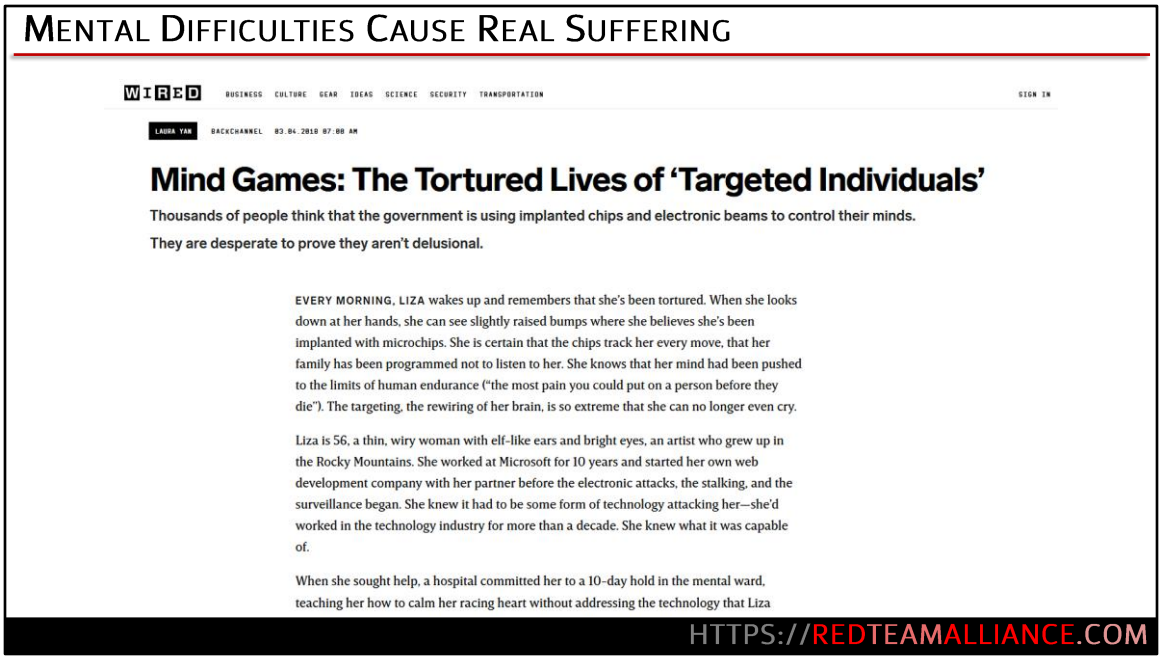
Comments From the Internet

HTTPS://REDTEAMALLIANCE.COM

So it's easy (terribly easy, as it turns out) to simply dismiss these folk all as scientifically-illiterate nutters and bible thumpers.

But we should recognize that there are people out there who are genuinely in pain every day because of mental difficulties… and these technologies -- and the conspiracy fantasies surrounding them -- feed their fears and delusions, while the internet helps them connect with one another and reinforce their misguidedness

MENTAL DIFFICULTIES CAUSE REAL SUFFERING



WIRED BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY TRANSPORTATION SIGN IN

LAURA YAN BACKCHANNEL 03.04.2018 07:00 AM

Mind Games: The Tortured Lives of 'Targeted Individuals'

Thousands of people think that the government is using implanted chips and electronic beams to control their minds. They are desperate to prove they aren't delusional.

EVERY MORNING, LIZA wakes up and remembers that she's been tortured. When she looks down at her hands, she can see slightly raised bumps where she believes she's been implanted with microchips. She is certain that the chips track her every move, that her family has been programmed not to listen to her. She knows that her mind had been pushed to the limits of human endurance ("the most pain you could put on a person before they die"). The targeting, the rewiring of her brain, is so extreme that she can no longer even cry.

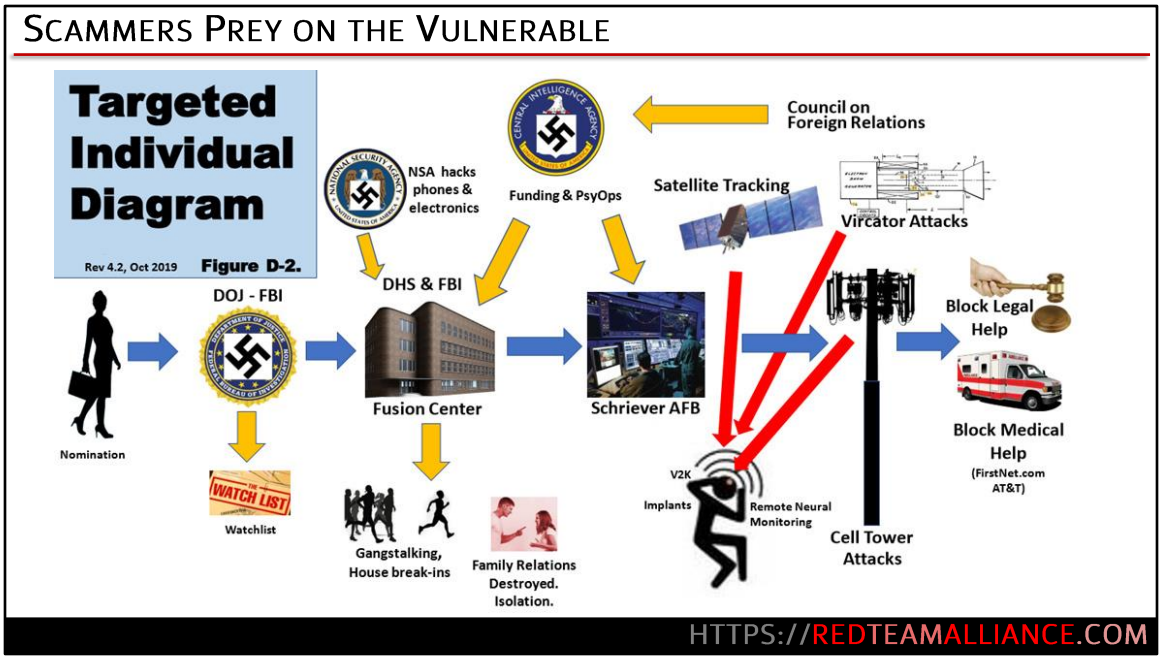
Liza is 56, a thin, wiry woman with elf-like ears and bright eyes, an artist who grew up in the Rocky Mountains. She worked at Microsoft for 10 years and started her own web development company with her partner before the electronic attacks, the stalking, and the surveillance began. She knew it had to be some form of technology attacking her—she'd worked in the technology industry for more than a decade. She knew what it was capable of.

When she sought help, a hospital committed her to a 10-day hold in the mental ward, teaching her how to calm her racing heart without addressing the technology that Liza

HTTPS://REDTEAMALLIANCE.COM

https://www.wired.com/story/mind-games-the-tortured-lives-of-targeted-individuals/

SCAMMERS PREY ON THE VULNERABLE



And there are scammers out there who prey on people that believe themselves to be "targeted" by radio waves and other technologies that they do not understand.

People take money from and further victimize these folk by playing into their beliefs

Scammers Prey on the Vulnerable

HTTPS://REDTEAMALLIANCE.COM

And there are scammers out there who prey on people that believe themselves to be "targeted" by radio waves and other technologies that they do not understand.

People take money from and further victimize these folk by playing into their beliefs

Scammers Prey on the Vulnerable

Forty-four percent of Republicans think Bill Gates wants to use coronavirus vaccine to microchip them: poll

By BRIAN NIEMIETZ
NEW YORK DAILY NEWS | MAY 22, 2020 | 3:51 PM

Bill Gates, a noted philanthropist, is up to no good in the eyes of 44% of Republicans in a new poll.(LUDOVIC MARIN/AP)

Hold onto your tin foil hats.

A poll taken this week found 44% of Republicans think Bill Gates is working on a coronavirus vaccine because he wants to plant a microchip in them and monitor their movements.

Yahoo News and YouGov found nearly half of Republicans believe that baseless conspiracy theory and may be resistant to using a vaccine that could end the pandemic. The poll also found that 19% of Democrats believe that story is credible while 52% know it is false. Only 26% of Republicans surveyed were certain the Microsoft founder is not hatching such a plot.

LATEST CORONAVIRUS

Coronavirus in New York, the U.S. and around the world: Latest Updates on May 24
27m

SEE IT: Packed pool party at Missouri's Lake of the Ozarks shows no one social distancing
1h

Rep. Val Demings warns Disney and other theme parks to reopen with care amid coronavirus
1h

MOST READ • CORONAVIRUS

SEE IT: Packed pool party at Missouri's Lake of the Ozarks shows no one social distancing
1h

In slight uptick, 109 dead from coronavirus in New York state Saturday: Gov. Cuomo
3h

Hackers Fight Snake Oil

HTTPS://REDTEAMALLIANCE.COM

We do this on the floor at RSA

We do this in our communities

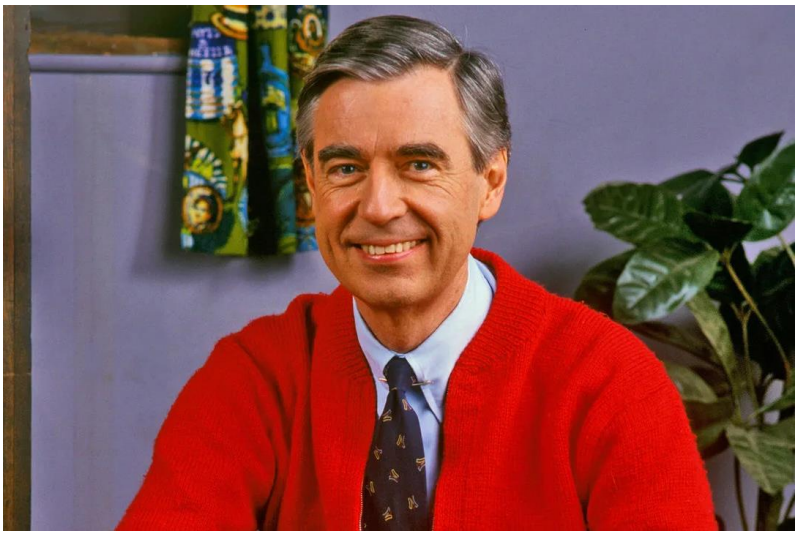
We can help here, too… but not with harsh criticism

Hackers Fight Snake Oil

HTTPS://REDTEAMALLIANCE.COM

While this in-your-face approach is appropriate and effective in fights against big entities, that is not exactly the landscape here

HELP THOSE WHO NEED HELP



HTTPS://REDTEAMALLIANCE.COM

Fred Rogers spoke of how the most vulnerable among us have “deep feelings” even if they seem immature

When they face crisis, Fred offered “a plea not to leave them isolated... And at the mercy of their own feelings and their own fantasies of loss and destruction.”

Striving to understand and better respond... That's a most important task

HELP THOSE WHO NEED HELP

https://forum.dangerousthings.com/t/so-you-think-youve-been-implanted-against-your-will/64

Amal did loads of amazing emotional work in this write-up

“Humans have evolved to imagine the future, they just haven't evolved yet to believe it.”

HELP THOSE WHO NEED HELP

HTTPS://REDTEAMALLIANCE.COM

We live in an increasingly connected yet also increasingly isolated society

President Johnson asked of our society and new technologies “how will we use our miracles?”

Help Those Who Need Help

HTTPS://REDTEAMALLIANCE.COM

People without access to proper safety nets slip through the cracks and can have their lives fall apart

Help Those Who Need Help

HTTPS://REDTEAMALLIANCE.COM

Destigmatize counseling and mental healthcare… and demand that legislators make costs no longer a barrier

Help Those Who Need Help

HTTPS://REDTEAMALLIANCE.COM

If you have the time and the spoons for it, do outreach in your communities and simply among your friends and families. People with good ties and healthy relationships are more likely to get help with delusions and they are far less susceptible to becoming swept up in internet conspiracy fantasies or bilked by scam "solutions" from charlatans

It's similar to how you have to deal with family members and loved ones who are regular consumers of outlets like Fox News…

1. *You have to deactivate their amygdala*
2. *Finding common ground through questions about shared values*
3. *Act like you don't understand and ask them to explain*
4. *Eventually, ask about what the motivations could be for alleged boogeymen "How would that strategy work?" "How would they go about doing that?" "How would that play out… what kind of laws and policies would it take?"*

Be good to one another and be close to those who matter to you

THANK YOU VERY MUCH!