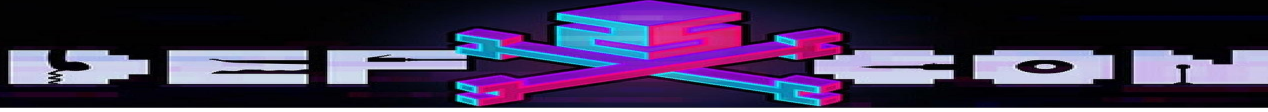


Exploiting Old Mag-stripe Information with New Technology

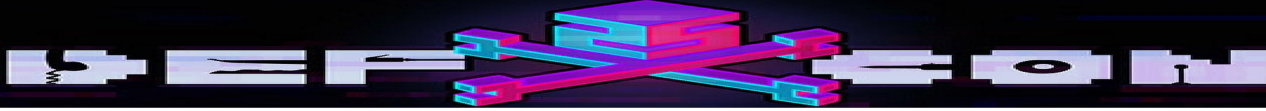
Salvador Mendoza
Twitter: [@Netxing](#)
Blog: [salmg.net](#)



About Me

- Security Researcher
- Samsung Pay:
Tokenized Numbers,
Flaws and Issues





Analyzing previous talks/tools

- **Major Malfunction DEFCON 14**

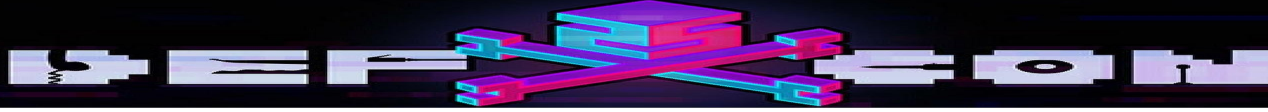
Magstripe Madness

- **Samy Kamkar**

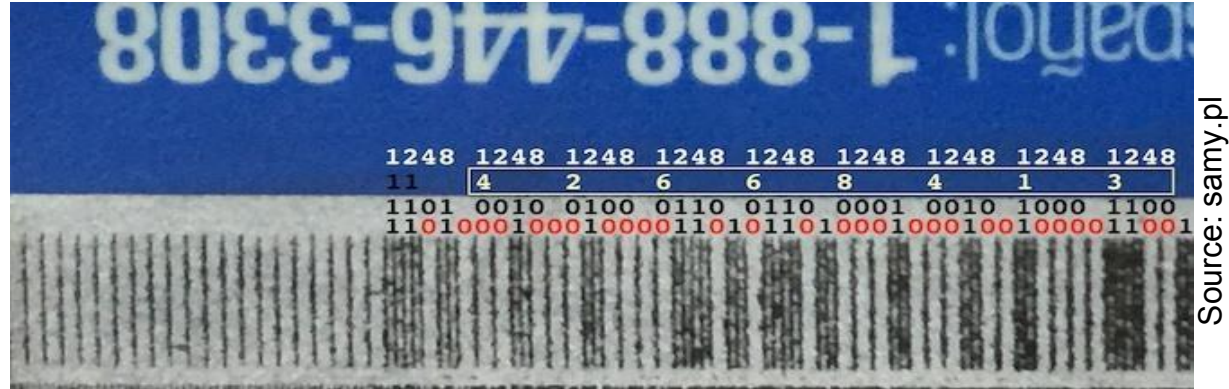
MagSpoof - 2015

- **Weston Hecker DEFCON 24**

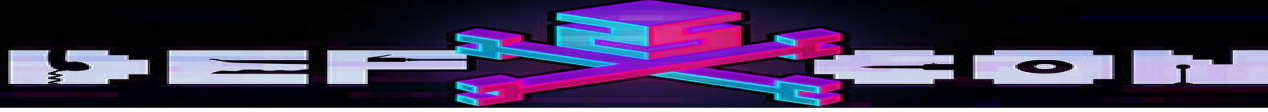
Hacking Hotel Keys and Point of Sale Systems



Intro to Magnetic Stripe Information

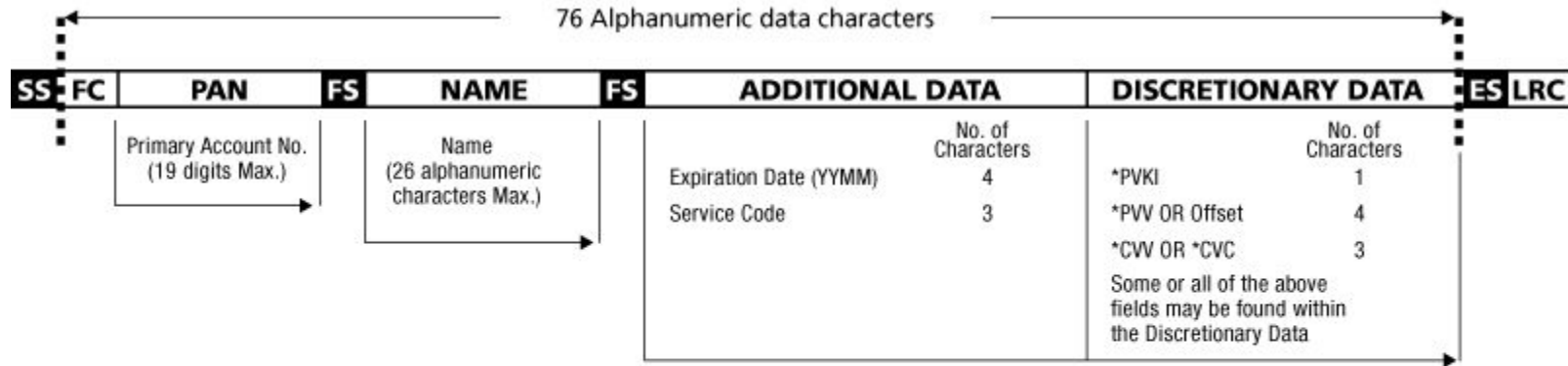


- Type of card capable of storing data by modifying the magnetism of tiny iron-based magnetic particles on a band of magnetic material on the card
- TL;DR → Track1 = [UPPERCASE,numbers] Track 2/3 = Numbers



Magstripe Composition

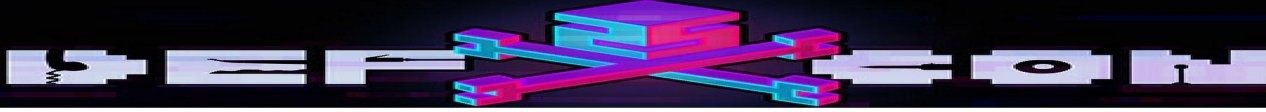
%B4929555123456789^MALFUNCTION/MAJOR ^0902201010000000000000970000000?



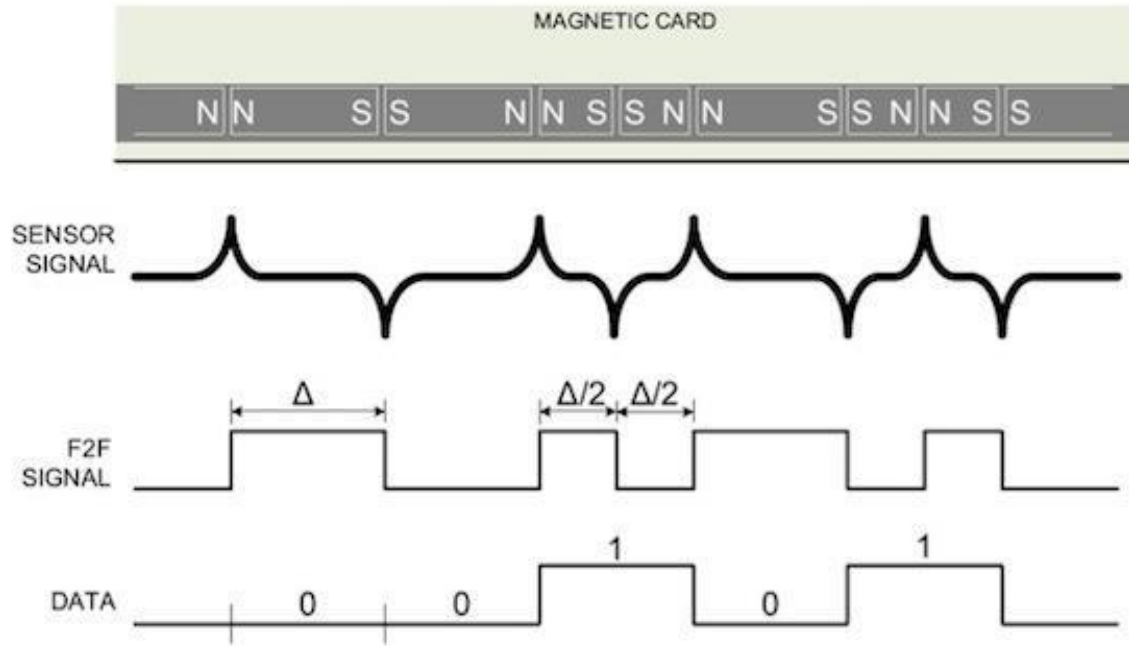
Shaded area identifies control characters

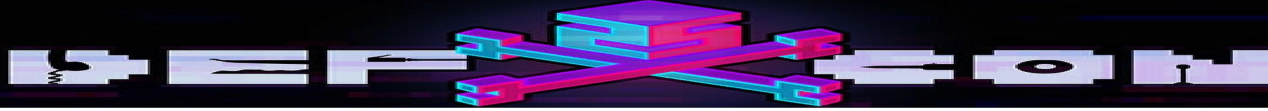
SS Start Sentinel	%	FC Format Code
FS Field Separator	^	LRC Longitudinal Redundancy Check Character
ES End Sentinel	?	

* (PVKI) PIN Verification Key Indicator
* (PVV) PIN Verification Value
* (CVV) Card Verification Value
* (CVC) Card Validation Code



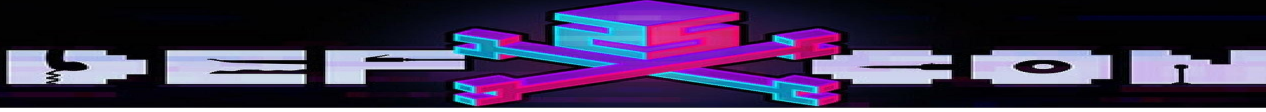
Magstripe info, Parity, and Waves



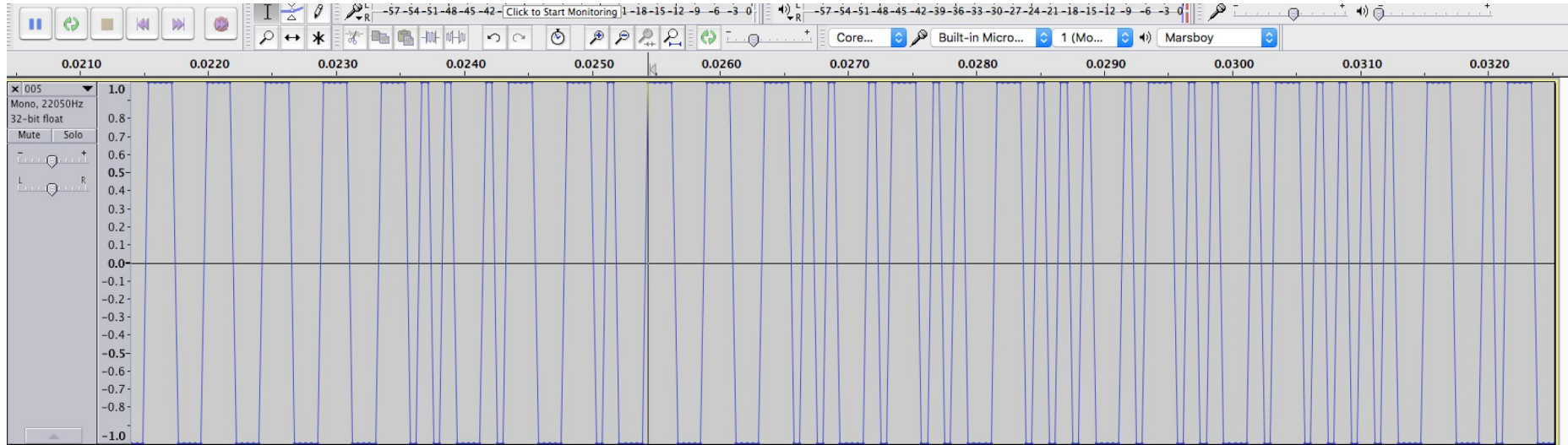


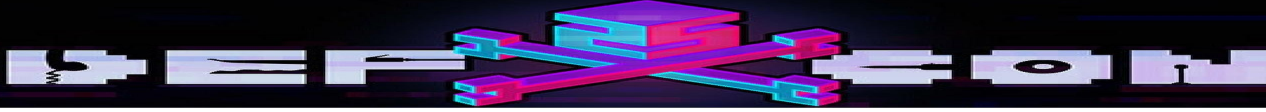
Magstripe info, Parity, and Waves

--Data Bits--				Parity	Character	Function
b1	b2	b3	b4	b5		
0	0	0	0	1	0 (0H)	Data
1	0	0	0	0	1 (1H)	"
0	1	0	0	0	2 (2H)	"
1	1	0	0	1	3 (3H)	"
0	0	1	0	0	4 (4H)	"
1	0	1	0	1	5 (5H)	"
0	1	1	0	1	6 (6H)	"
1	1	1	0	0	7 (7H)	"
0	0	0	1	0	8 (8H)	"
1	0	0	1	1	9 (9H)	"
0	1	0	1	1	: (AH)	Control
1	1	0	1	0	; (BH)	Start Sentinel
0	0	1	1	1	< (CH)	Control
1	0	1	1	0	= (DH)	Field Separator
0	1	1	1	0	> (EH)	Control
1	1	1	1	1	? (FH)	End Sentinel

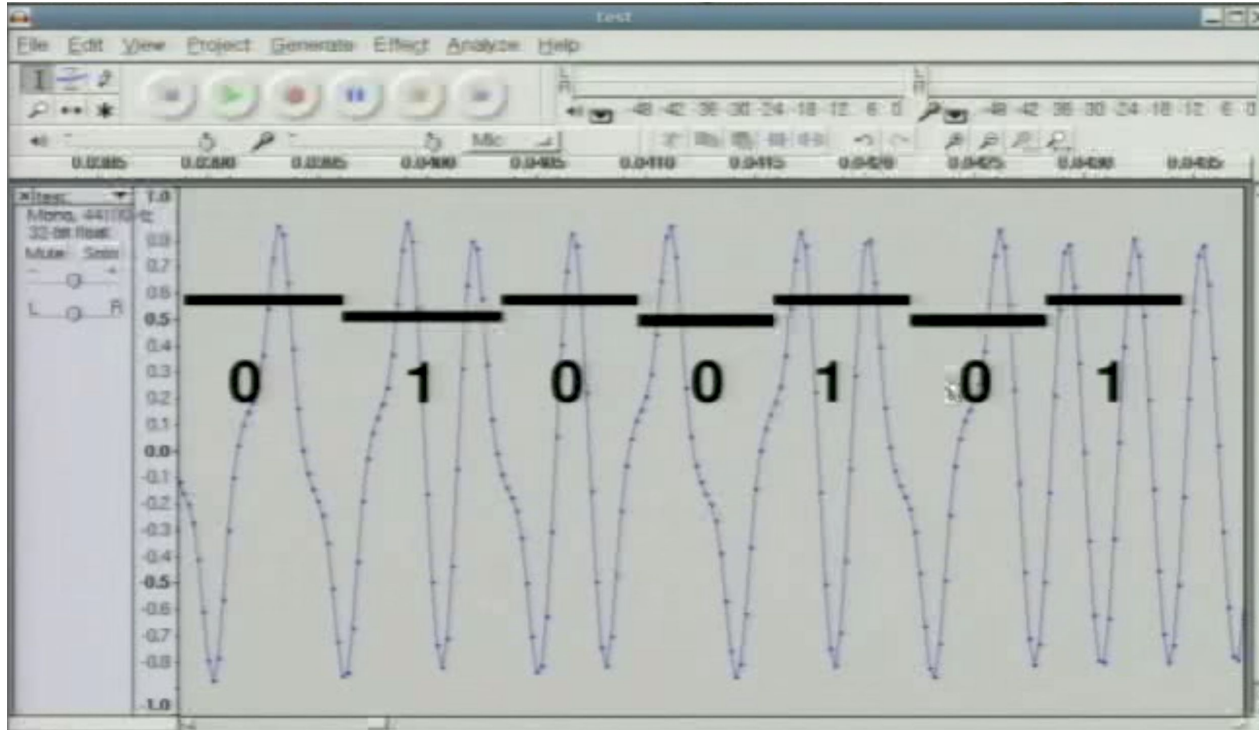


Magstripe Signal

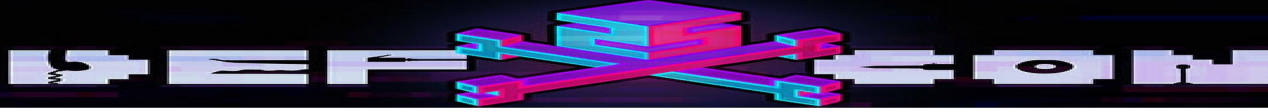




Major Malfunction DEFCON 14



<https://www.youtube.com/watch?v=ITihB1c3dHw>



BlueSpooof Descendancy

MagSpooof

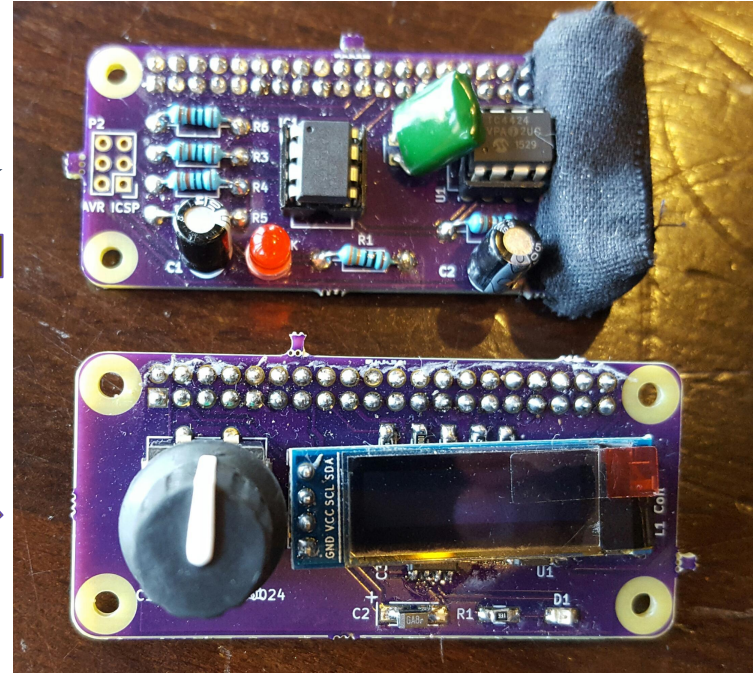


<https://www.samy.pl>

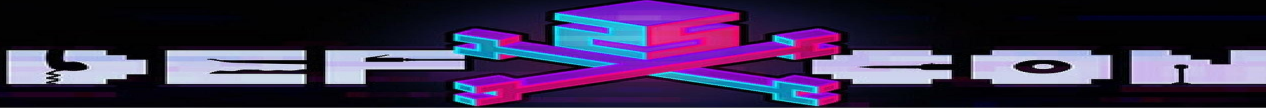
MagSpooofPI

SamyKam

First Prototypes

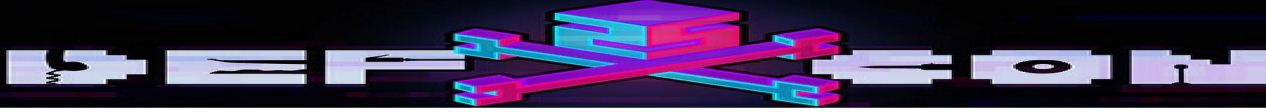


Designed PCB by @electronicats

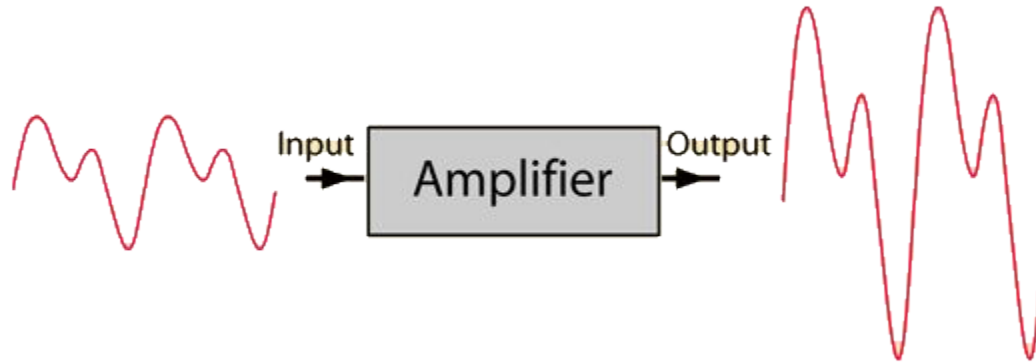


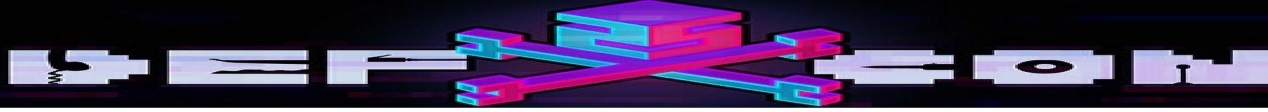
Weston Hecker - DEFCON 24





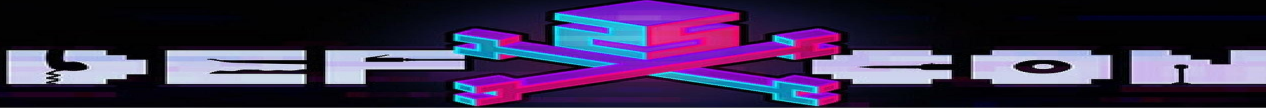
Sound Amplifier



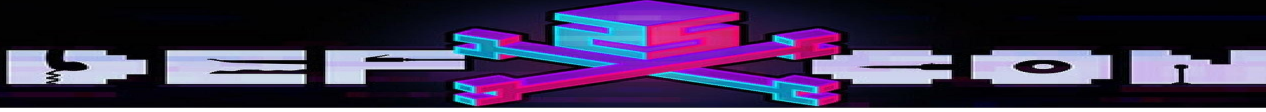


Raspberry Pi + Amplifier + Coil



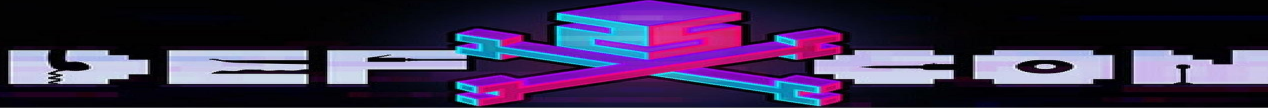


Raspberry Pi - Demo



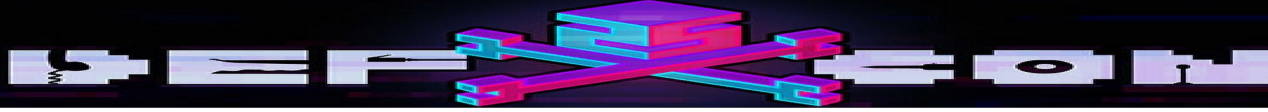
Bluetooth Technology



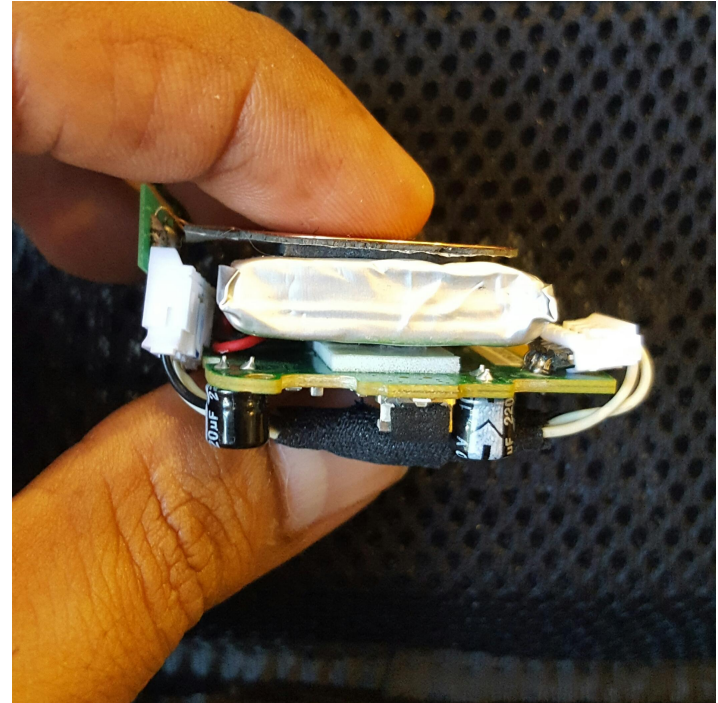


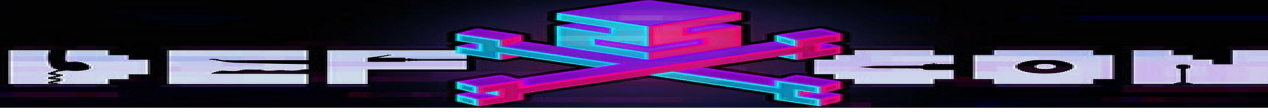
Bluetooth Speaker





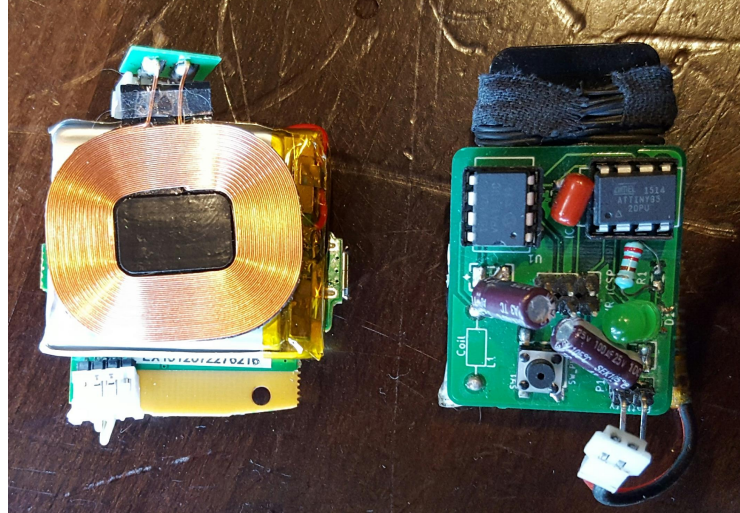
Bluetooth Speaker





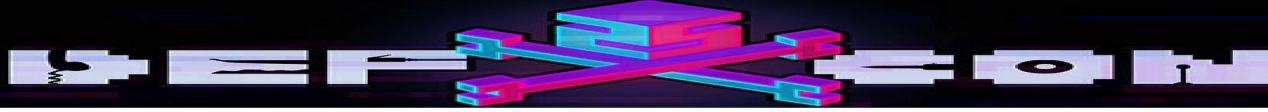
MagSpoof Cousin

BlueSpoof

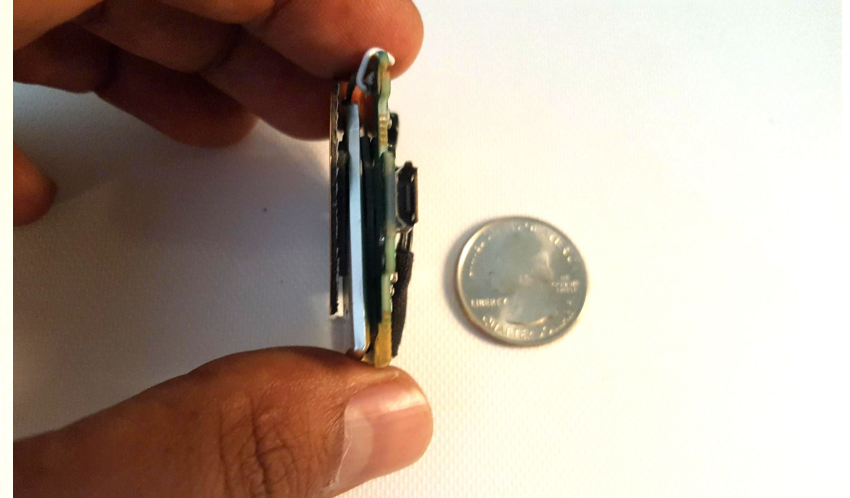
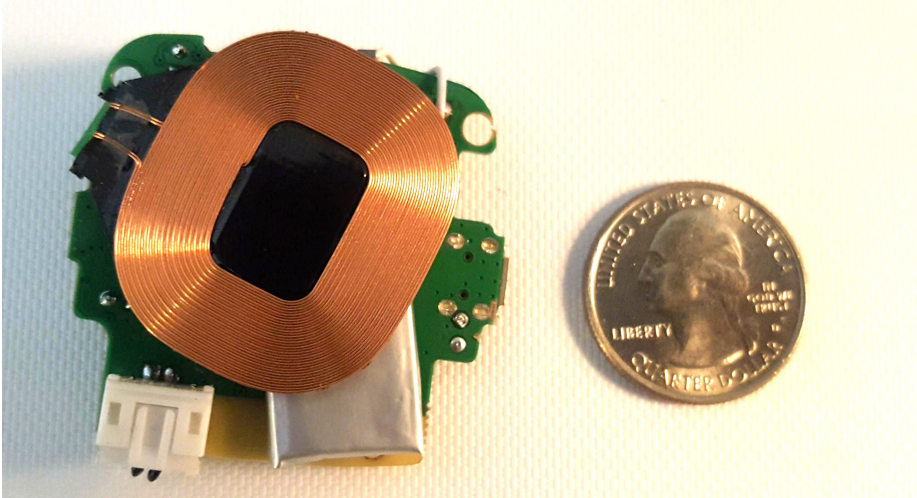


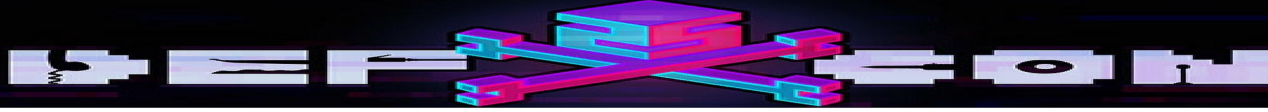
Electronic Cats(@electronicats)
design

MagSpoof



BlueSpooof

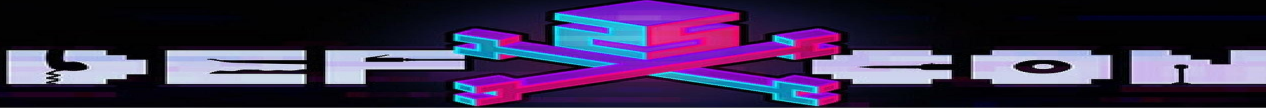




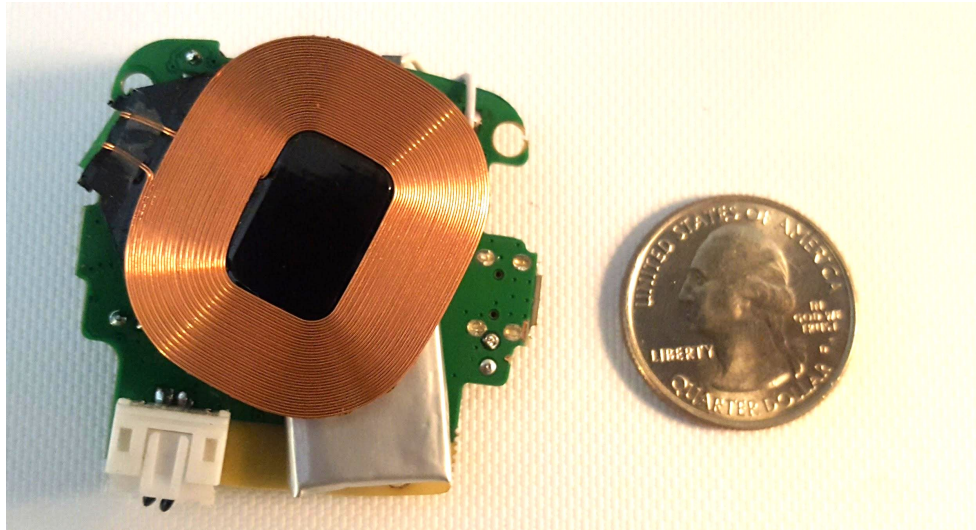
BlueSpooof tool - Characteristics

- Cheap < \$20
- Easy to implement
- Escalable
- 3.7 V Battery
- Fast transmission
- Accurate

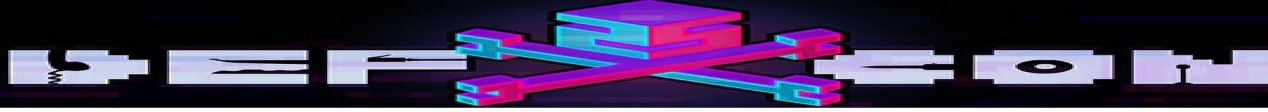




BlueSpooof - Demo



<https://www.youtube.com/watch?v=elzqLhLnCek>



Multiple Targets?



Token 1



Token 2





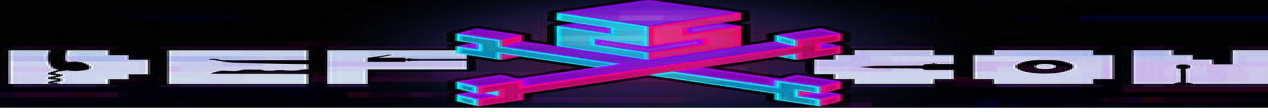
Controlling Multiple Speakers?

Python Sound Device Library

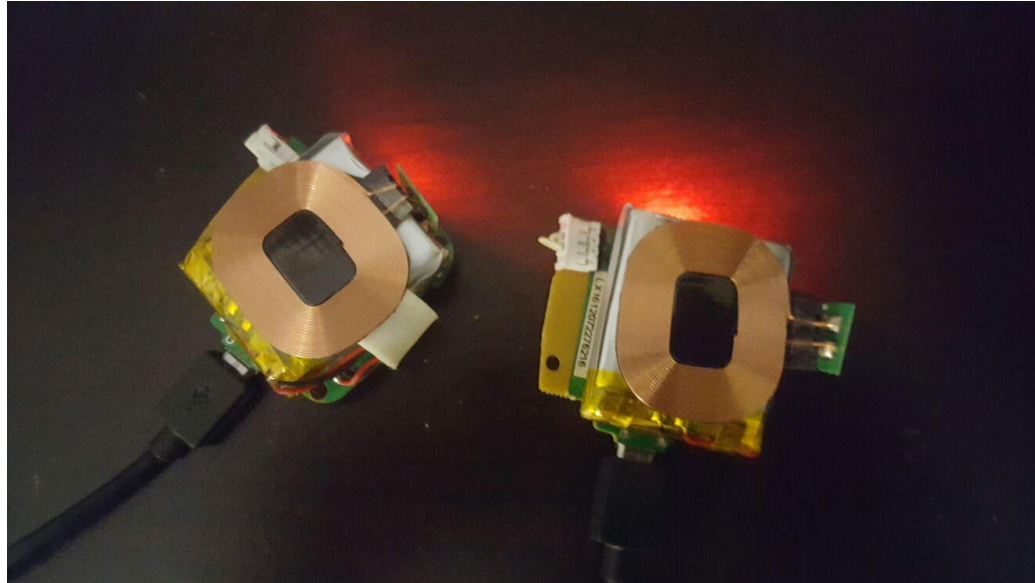
```
[salvador@Sal-M:~/Desktop/defcon 25]$ python -m sounddevice
> 0 Built-in Microphone, Core Audio (2 in, 0 out)
  1 Built-in Output, Core Audio (0 in, 2 out)
  2 token-, Core Audio (1 in, 0 out)
  3 token-, Core Audio (0 in, 2 out)
  4 Marsboy, Core Audio (1 in, 0 out)
< 5 Marsboy, Core Audio (0 in, 2 out)
```

<https://pypi.python.org/pypi/sounddevice>





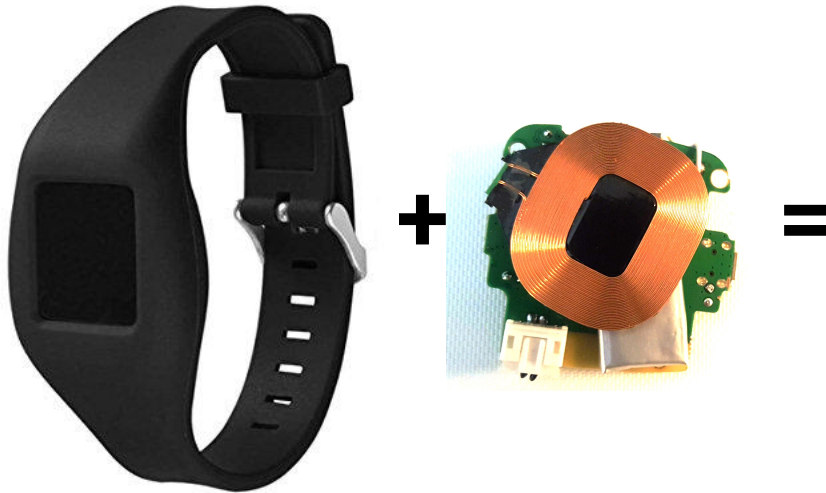
Attack with Multiple Bluetooth Speakers?

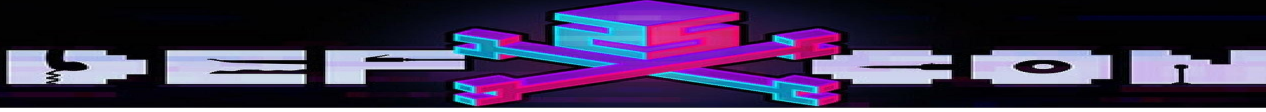


Demo

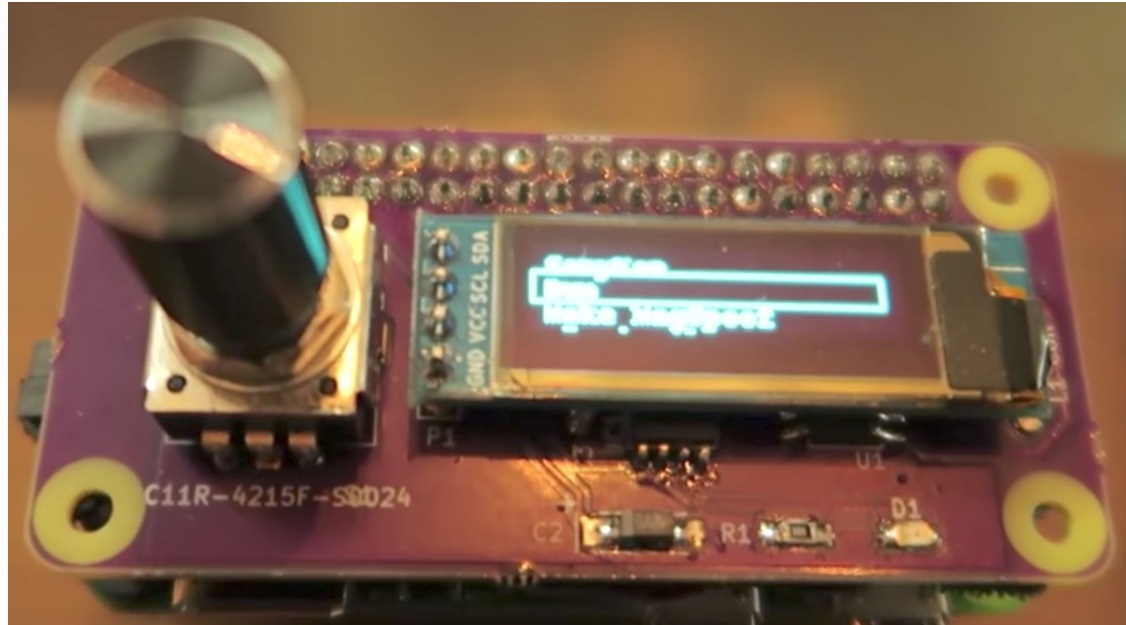
<https://www.youtube.com/watch?v=5hInVNLUC8s>

Bonus Take-Away Project: iWey





SamyKam



<https://salmg.net/2017/01/16/samykam/>



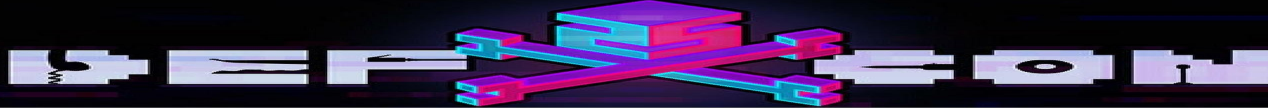
Greetz, Hugs & Stuff

Samy Kamkar (@samykamkar)

Electronic Cats (@electronicats)

RMHT (raza-mexicana.org)

Los Razos!



Questions?

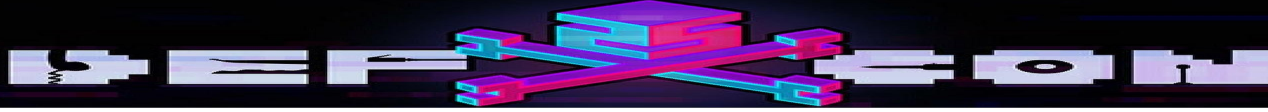


Salvador Mendoza

Twitter: [@Netxing](https://twitter.com/Netxing)

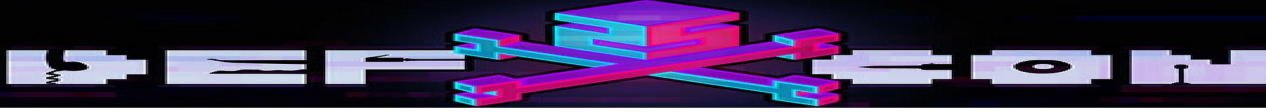
Blog: salmg.net

sal@salmg.net



Thank you!

**Happy Hacking
Anniversary!**



Resources

Samy Kamkar: samy.pl/magspooft

Electronic Cats: twitter.com/electronicats

Major Malfunction: youtube.com/watch?v=ITihB1c3dHw

Weston Hecker: youtube.com/watch?v=mV_0k9Fh590