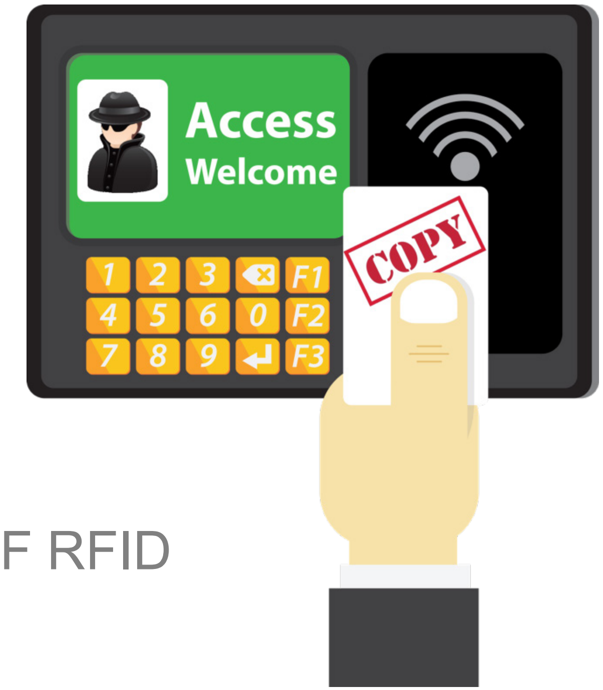


RFIDiggity

Pentester Guide to Hacking HF/NFC and UHF RFID

05 Apr 2016 – InfoSec World 2016 – Orlando, FL

INFOSEC WORLD
CONFERENCE & EXPO 2016

Presented by:
Francis Brown
Bishop Fox
www.bishopfox.com

BISHOP FOX

NEW Tools - Demos

BISHOP FOX

BADGE ATTACKS

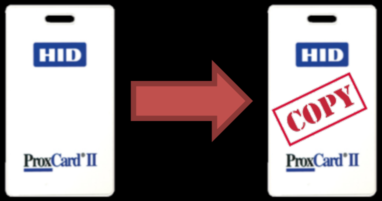
ICLASS BADGE READING/CLONING

Methodology

3 STEP APPROACH

1. **Silently steal badge info**

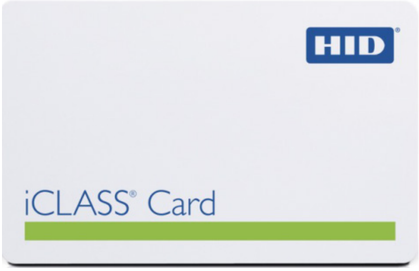
2. **Create card clone**

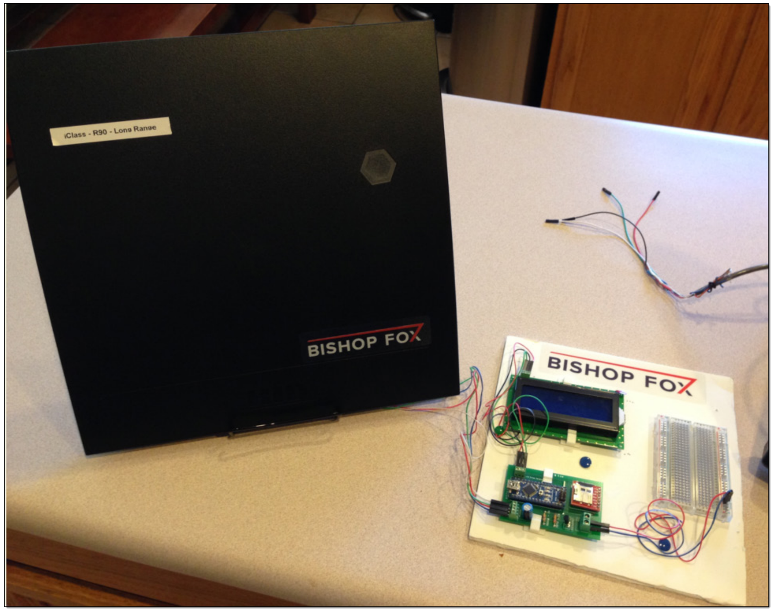


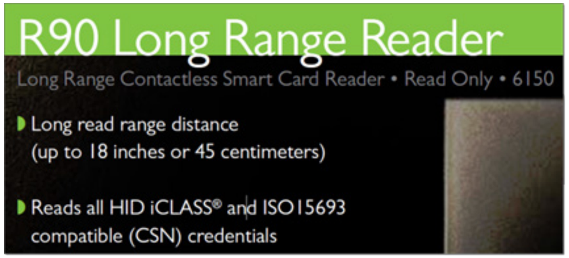
3. **Enter and plant backdoor**

Tastic RFID Thief

LONG RANGE RFID STEALER



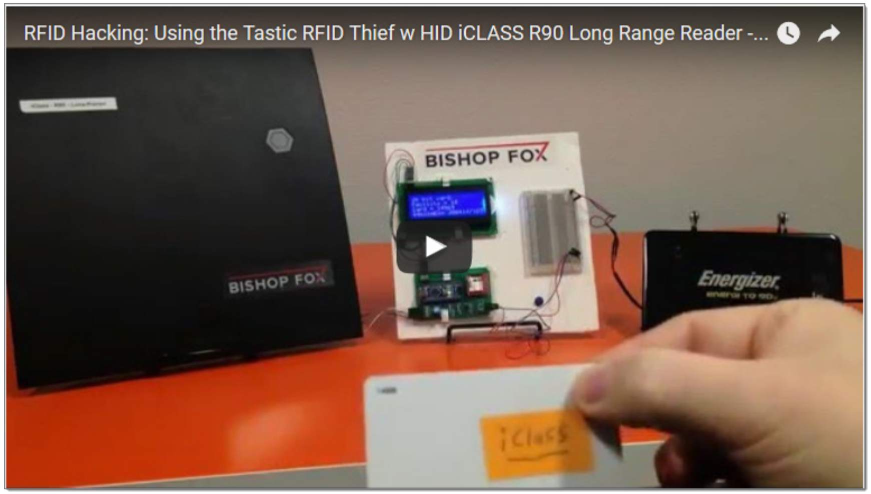




R90 Long Range Reader

Long Range Contactless Smart Card Reader • Read Only • 6150

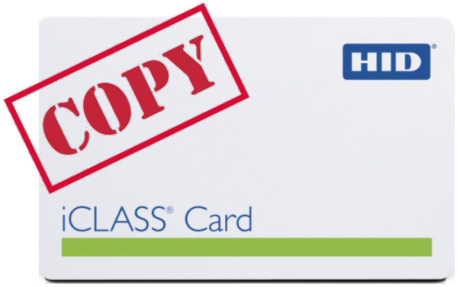
- Long read range distance (up to 18 inches or 45 centimeters)
- Reads all HID iCLASS® and ISO15693 compatible (CSN) credentials

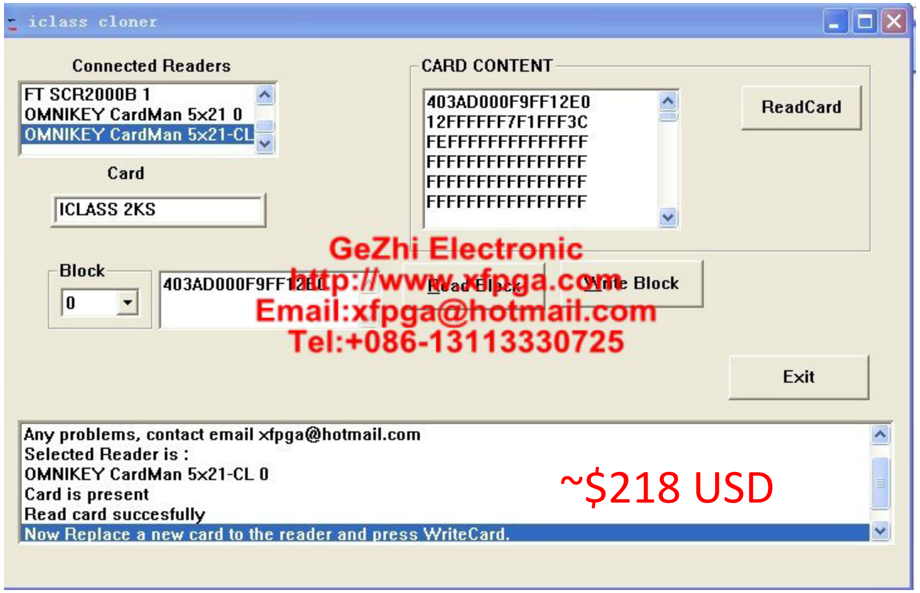


RFID Hacking: Using the Tastic RFID Thief w HID iCLASS R90 Long Range Reader -...

iCLASS Cloner

XFPGA.COM - FROM CHINA





iclass cloner

Connected Readers

FT SCR2000B 1
OMNIKEY CardMan 5x21 0
OMNIKEY CardMan 5x21-CL

Card: ICLASS 2KS

CARD CONTENT

```
403AD000F9FF12E0
12FFFFFF7F1FFF3C
FEFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF
```

ReadCard

Block: 0

403AD000F9FF12E0

Read Block | Write Block | Exit

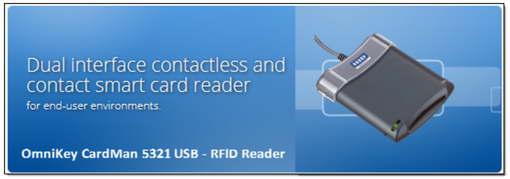
GeZhi Electronic
http://www.xfpga.com
Email:xfpga@hotmail.com
Tel:+086-13113330725

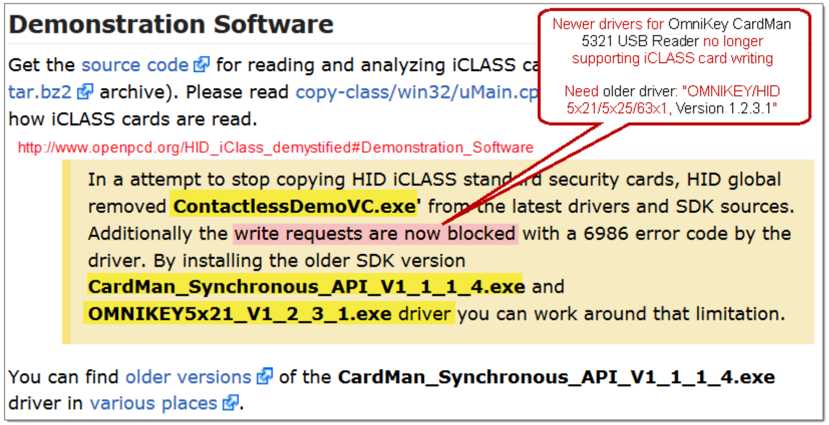
```
Any problems, contact email xfpga@hotmail.com
Selected Reader is :
OMNIKEY CardMan 5x21-CL 0
Card is present
Read card succesfully
Now Replace a new card to the reader and press WriteCard.
```

~$218 USD

- http://www.xfpga.com/html_products/iclass-card-cloner-en-82.html
- Read/Write iCLASS cards using "Standard Security" only (not "High" or "Elite")
- Requires older 32bit driver, and won't let you run in a VM (so Win32 actual install necessary)
- Built from original ContactlessDemoVC.exe
- USB hardware licensing dongle shipped

Uses: OmniKey CardMan 5321 USB - RFID Reader (13.56 Mhz)


Dual interface contactless and contact smart card reader
for end-user environments.
OmniKey CardMan 5321 USB - RFID Reader



Demonstration Software

Get the source code for reading and analyzing iCLASS ca
tar.bz2 archive). Please read copy-class/win32/uMain.cp
how iCLASS cards are read.

Newer drivers for OmniKey CardMan 5321 USB Reader no longer supporting iCLASS card writing

Need older driver: "OMNIKEY/HID 5x21/5x25/63x1, Version 1.2.3.1"

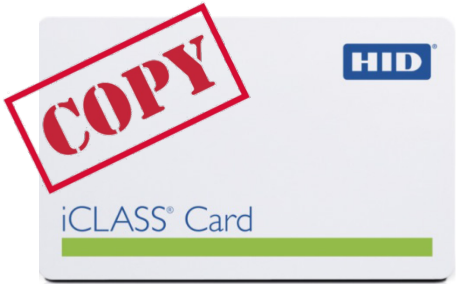
http://www.openpcd.org/HID_iClass_demystified#Demonstration_Software

> In a attempt to stop copying HID iCLASS standard security cards, HID global removed **ContactlessDemoVC.exe**' from the latest drivers and SDK sources. Additionally the write requests are now blocked with a 6986 error code by the driver. By installing the older SDK version **CardMan_Synchronous_API_V1_1_1_4.exe** and **OMNIKEY5x21_V1_2_3_1.exe** driver you can work around that limitation.

You can find older versions of the **CardMan_Synchronous_API_V1_1_1_4.exe** driver in various places.

iCLASS Cloner

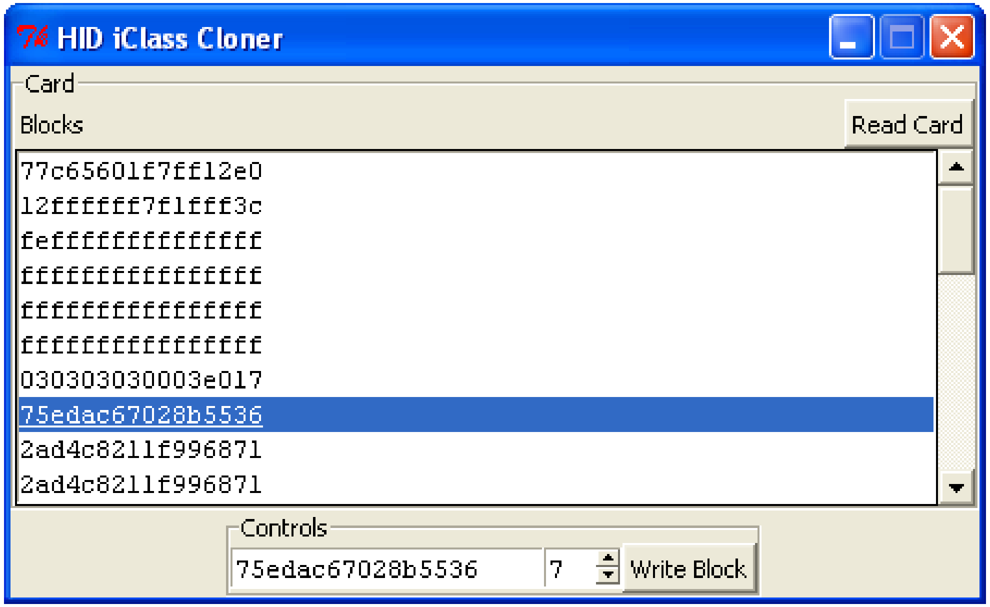
NEW – Bishop Fox – FREE Edition



UPDATE

Read / Write to HID iCLASS Cards:

- https://blog.kchung.co/reverse-engineering-hid-iclass-master-keys/
- https://github.com/ColdHeat/iclass



```
77c65601f7ff12e0
12ffffff7f1fff3c
feffffffffffffff
ffffffffffffffff
ffffffffffffffff
ffffffffffffffff
030303030003e017
75edac67028b5536
2ad4c8211f996871
2ad4c8211f996871
```

Controls: 75edac67028b5536 | 7 | Write Block

AS SEEN ON TV

Tastic RFID Thief

LONG RANGE RFID STEALER

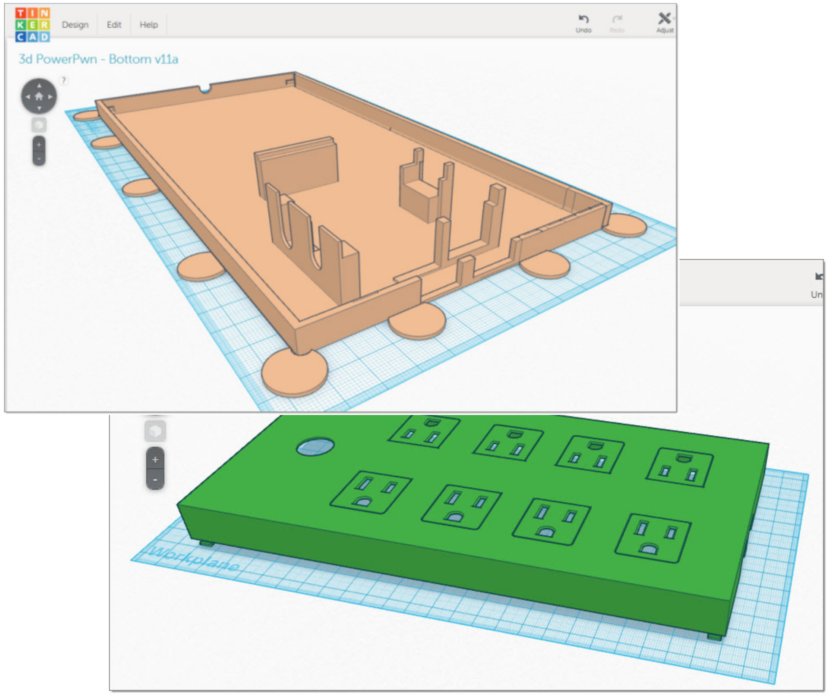
BADGE ATTACKS

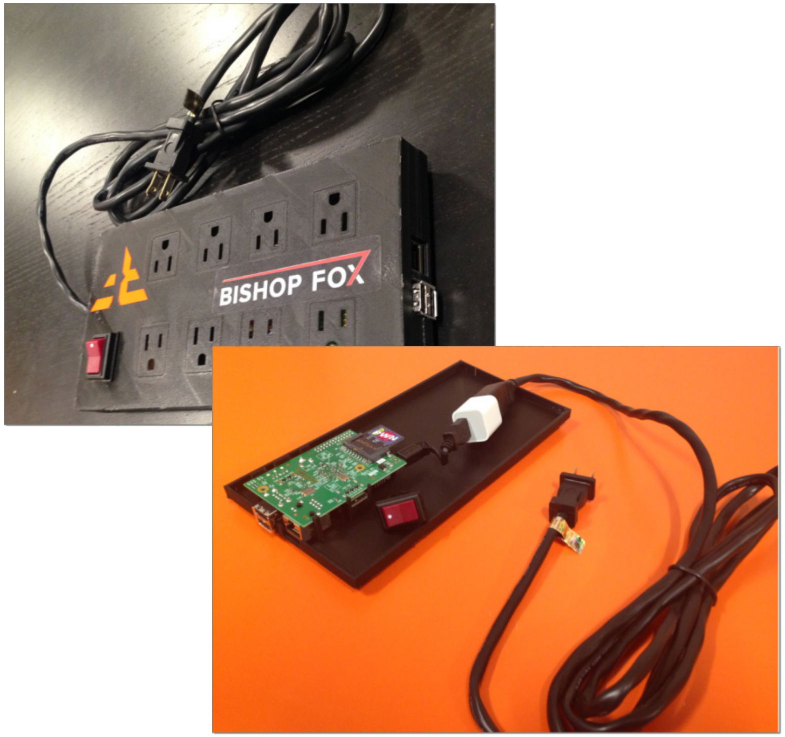
BACKDOOR DEVICES

Raspberry Pi

MAINTAINING ACCESS

- Raspberry Pi – cheap alternative (~$35) to Pwn Plug/Power Pwn
  - Tastic 3D Case for RaspPi Backdoor Hidden Backdoor Device



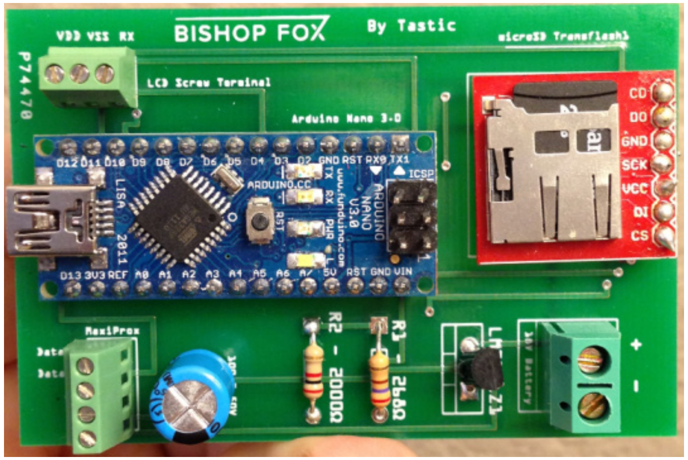


READER ATTACKS

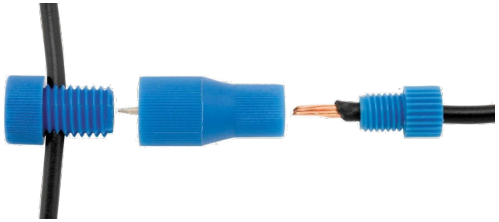
BADGE READER MITM IMPLANTS

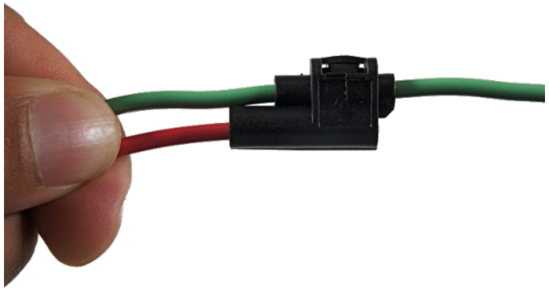
Reader Attacks

TASTIC–MITM ATTACK



+

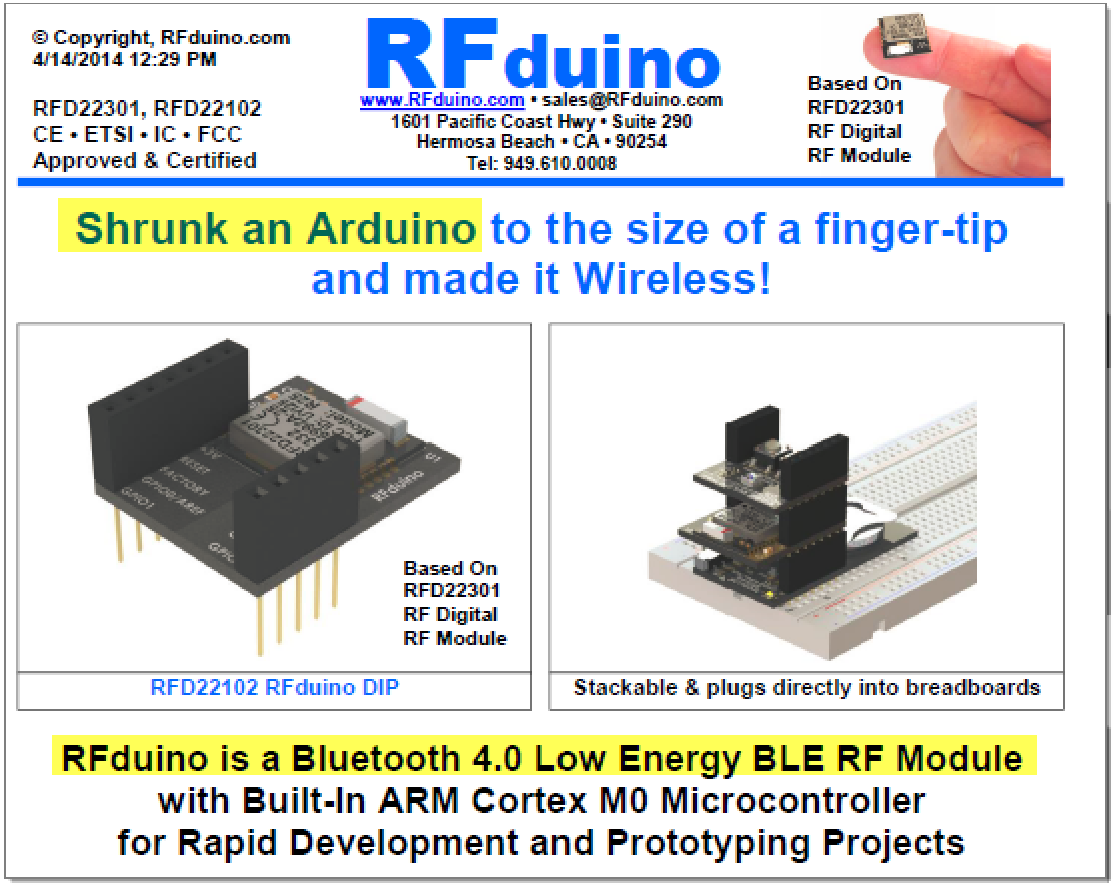




- Insert in door reader of target building – record badge #s
- Tastic RFID Thief's PCB could be used similiarly for MITM attack

Reader Attacks

TASTIC–MITM ATTACK



© Copyright, RFduino.com
4/14/2014 12:29 PM

RFD22301, RFD22102
CE • ETSI • IC • FCC
Approved & Certified

RFduino

www.RFduino.com • sales@RFduino.com
1601 Pacific Coast Hwy • Suite 290
Hermosa Beach • CA • 90254
Tel: 949.610.0008

Based On
RFD22301
RF Digital
RF Module

Shrunk an Arduino to the size of a finger-tip and made it Wireless!

Based On
RFD22301
RF Digital
RF Module

RFD22102 RFduino DIP

Stackable & plugs directly into breadboards

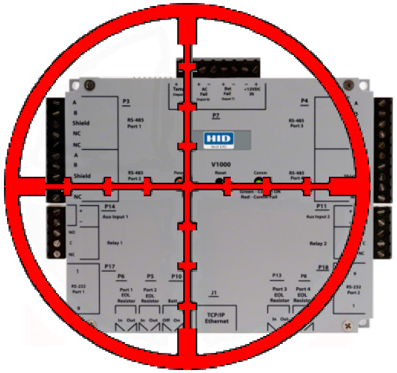
RFduino is a Bluetooth 4.0 Low Energy BLE RF Module with Built-In ARM Cortex M0 Microcontroller for Rapid Development and Prototyping Projects

CONTROLLER ATTACKS

VERTX CONTROLLER SEACH/EXPLOIT

Controller Attacks

JACKED IN

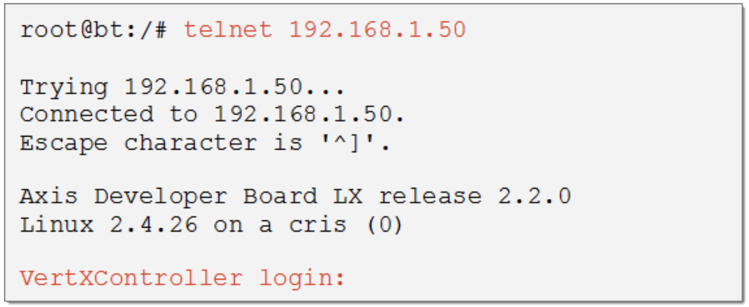


Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

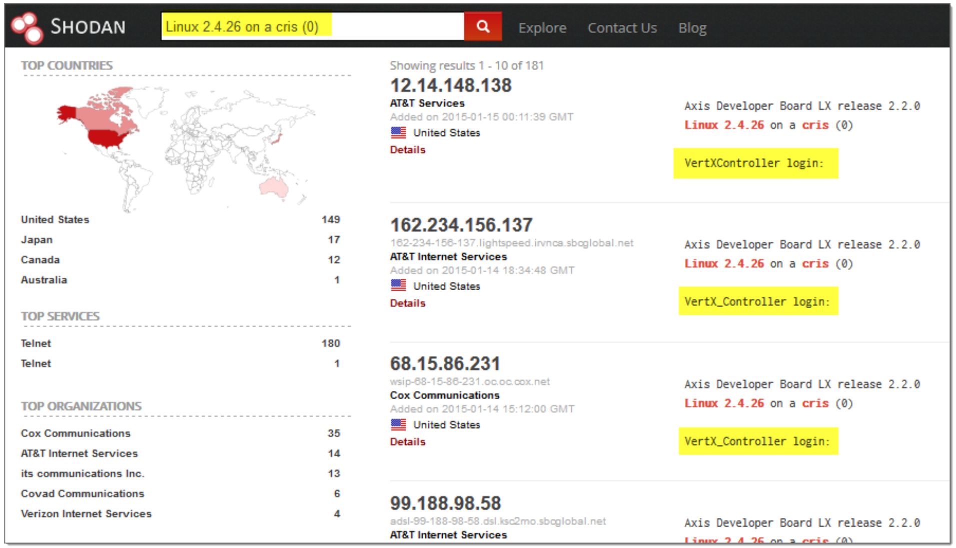
- HID VertX Controller – Default Open Ports:
  - FTP (21), Telnet (23), HTTP (80)

- HID VertX Controller – Connect via FTP / Telnet / HTTP with Default Admin Creds: **root/pass**

- Banner grabbing for HID VertX controller discovery
  - Can also find using SHODAN search engine



```
root@bt:/# telnet 192.168.1.50

Trying 192.168.1.50...
Connected to 192.168.1.50.
Escape character is '^]'.

Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertXController login:
```



TOP COUNTRIES

United States	149
Japan	17
Canada	12
Australia	1

TOP SERVICES

Telnet	180
Telnet	1

TOP ORGANIZATIONS

Cox Communications	35
AT&T Internet Services	14
its communications Inc.	13
Covad Communications	6
Verizon Internet Services	4

Showing results 1 - 10 of 181

12.14.148.138
AT&T Services
Added on 2015-01-15 00:11:39 GMT
United States
Details

```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertXController login:
```

162.234.156.137
162-234-156-137.lightspeed.irvnca.sbcglobal.net
AT&T Internet Services
Added on 2015-01-14 18:34:48 GMT
United States
Details

```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:
```

68.15.86.231
wsip-68-15-86-231.oc.oc.cox.net
Cox Communications
Added on 2015-01-14 15:12:00 GMT
United States
Details

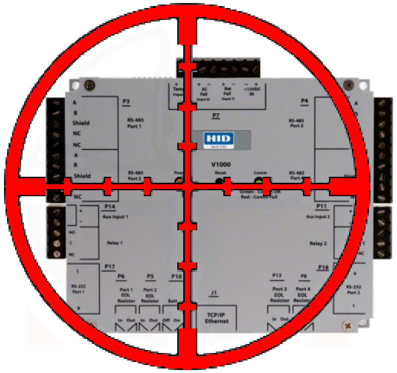
```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:
```

99.188.98.58
adsl-99-188-98-58.dsl.ksc2mo.sbcglobal.net
AT&T Internet Services

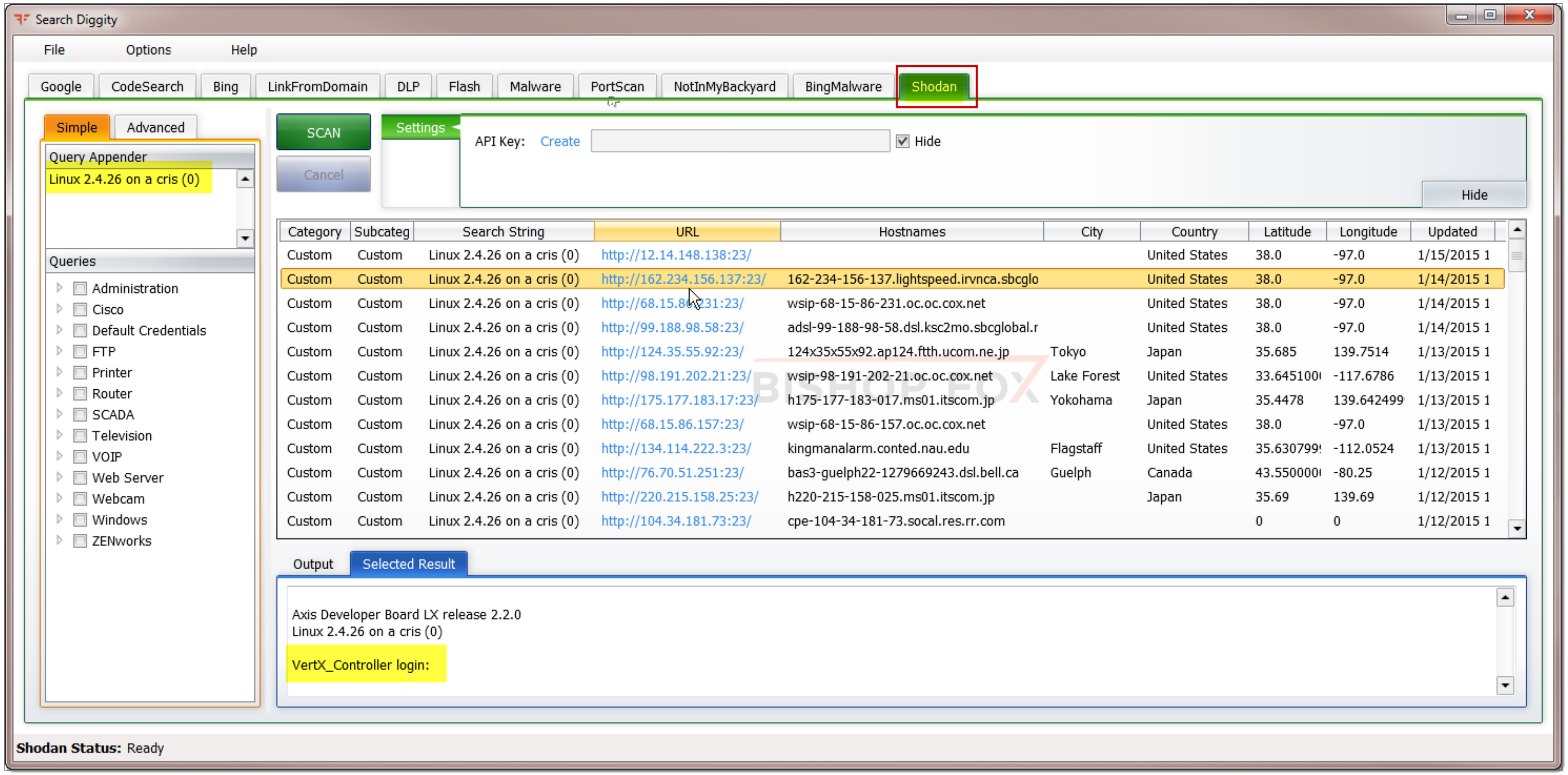
```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)
```

Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network



Query Appender

Linux 2.4.26 on a cris (0)

Queries

- □ Administration
- □ Cisco
- □ Default Credentials
- □ FTP
- □ Printer
- □ Router
- □ SCADA
- □ Television
- □ VOIP
- □ Web Server
- □ Webcam
- □ Windows
- □ ZENworks

API Key: Create ☑ Hide

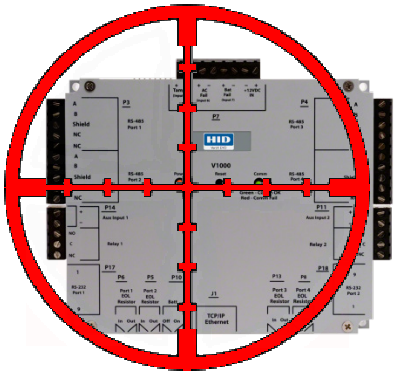
Category	Subcateg	Search String	URL	Hostnames	City	Country	Latitude	Longitude	Updated
Custom	Custom	Linux 2.4.26 on a cris (0)	http://12.14.148.138:23/			United States	38.0	-97.0	1/15/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://162.234.156.137:23/	162-234-156-137.lightspeed.irvnca.sbcglo		United States	38.0	-97.0	1/14/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://68.15.86.231:23/	wsip-68-15-86-231.oc.oc.cox.net		United States	38.0	-97.0	1/14/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://99.188.98.58:23/	adsl-99-188-98-58.dsl.ksc2mo.sbcglobal.r		United States	38.0	-97.0	1/14/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://124.35.55.92:23/	124x35x55x92.ap124.ftth.ucom.ne.jp	Tokyo	Japan	35.685	139.7514	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://98.191.202.21:23/	wsip-98-191-202-21.oc.oc.cox.net	Lake Forest	United States	33.645100	-117.6786	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://175.177.183.17:23/	h175-177-183-017.ms01.itscom.jp	Yokohama	Japan	35.4478	139.642499	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://68.15.86.157:23/	wsip-68-15-86-157.oc.oc.cox.net		United States	38.0	-97.0	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://134.114.222.3:23/	kingmanalarm.conted.nau.edu	Flagstaff	United States	35.630799	-112.0524	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://76.70.51.251:23/	bas3-guelph22-1279669243.dsl.bell.ca	Guelph	Canada	43.550000	-80.25	1/12/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://220.215.158.25:23/	h220-215-158-025.ms01.itscom.jp		Japan	35.69	139.69	1/12/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://104.34.181.73:23/	cpe-104-34-181-73.socal.res.rr.com			0	0	1/12/2015 1

```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:
```

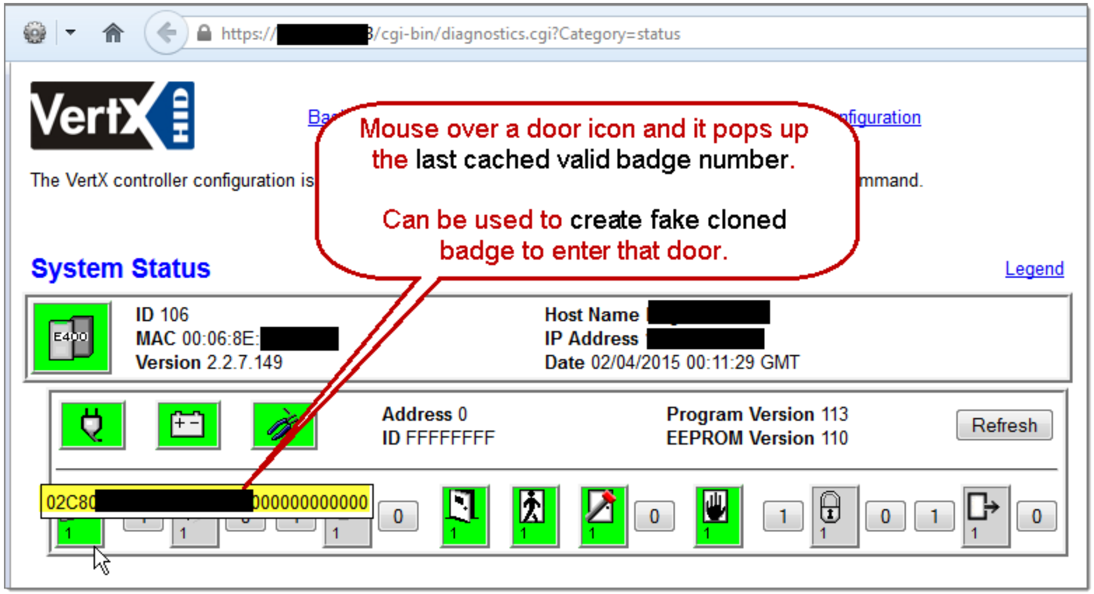
Shodan Status: Ready

Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network



https://[redacted]3/cgi-bin/diagnostics.cgi?Category=status

The VertX controller configuration is ... mmand.

System Status

ID 106
MAC 00:06:8E:[redacted]
Version 2.2.7.149

Host Name [redacted]
IP Address [redacted]
Date 02/04/2015 00:11:29 GMT

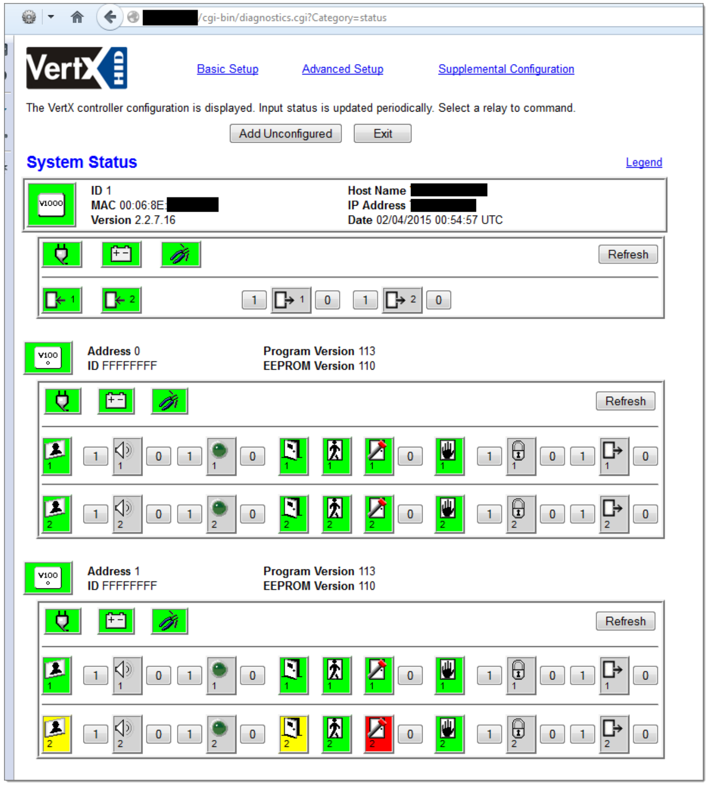
Address 0
ID FFFFFFFF

Program Version 113
EEPROM Version 110

02C80[redacted]000000000000

Mouse over a door icon and it pops up the last cached valid badge number.

Can be used to create fake cloned badge to enter that door.



[redacted]/cgi-bin/diagnostics.cgi?Category=status

The VertX controller configuration is displayed. Input status is updated periodically. Select a relay to command.

System Status

ID 1
MAC 00:06:8E:[redacted]
Version 2.2.7.16

Host Name [redacted]
IP Address [redacted]
Date 02/04/2015 00:54:57 UTC

Address 0
ID FFFFFFFF

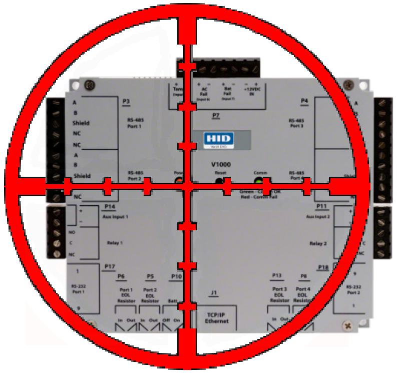
Program Version 113
EEPROM Version 110

Address 1
ID FFFFFFFF

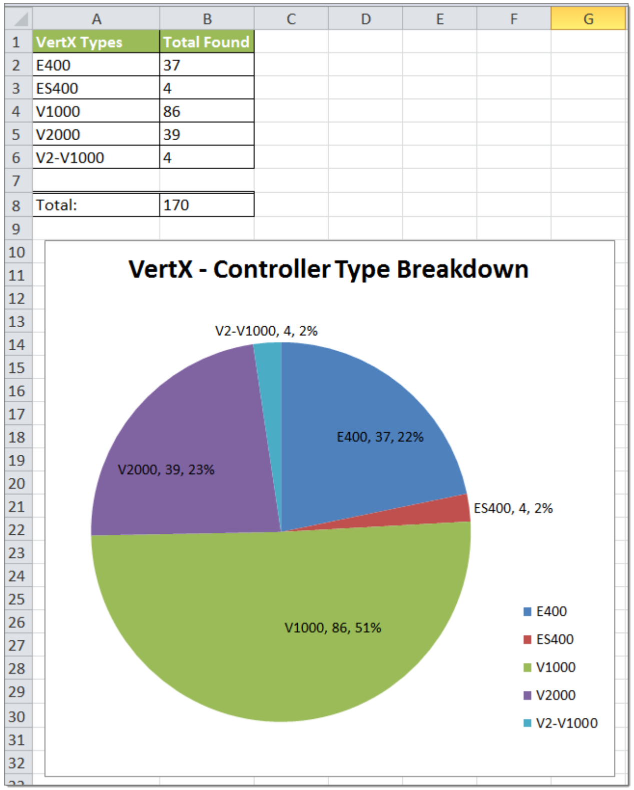
Program Version 113
EEPROM Version 110

Controller Attacks

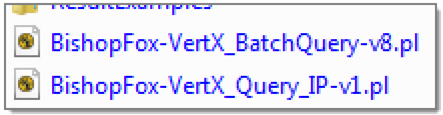
JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

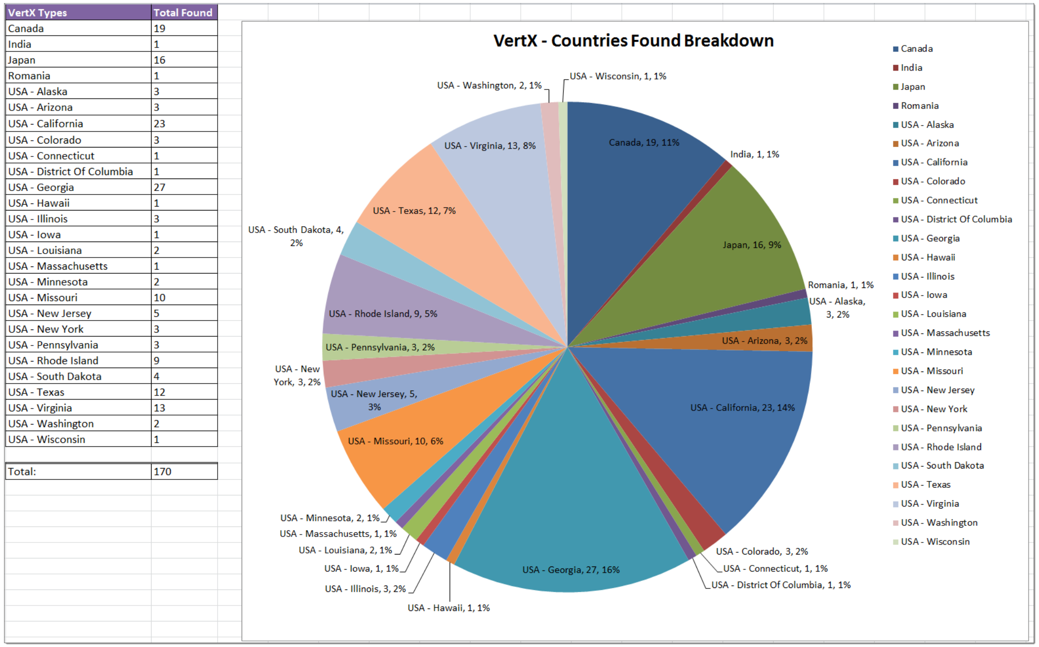


VertX Types	Total Found
E400	37
ES400	4
V1000	86
V2000	39
V2-V1000	4
Total:	170



BishopFox-VertX_BatchQuery-v8.pl

BishopFox-VertX_Query_IP-v1.pl



VertX Types	Total Found
Canada	19
India	1
Japan	16
Romania	1
USA - Alaska	3
USA - Arizona	3
USA - California	23
USA - Colorado	3
USA - Connecticut	1
USA - District Of Columbia	1
USA - Georgia	27
USA - Hawaii	1
USA - Illinois	3
USA - Iowa	1
USA - Louisiana	2
USA - Massachusetts	1
USA - Minnesota	2
USA - Missouri	10
USA - New Jersey	5
USA - New York	3
USA - Pennsylvania	3
USA - Rhode Island	9
USA - South Dakota	4
USA - Texas	12
USA - Virginia	13
USA - Washington	2
USA - Wisconsin	1
Total:	170

Introduction/Background

GETTING UP TO SPEED

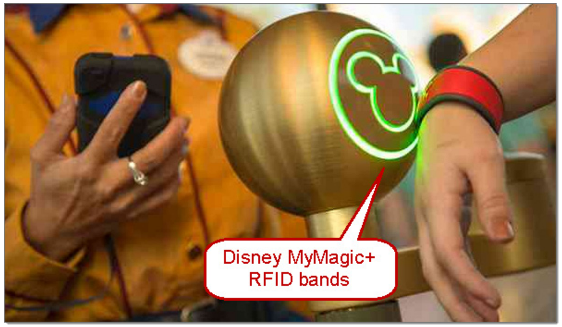
Badge Basics

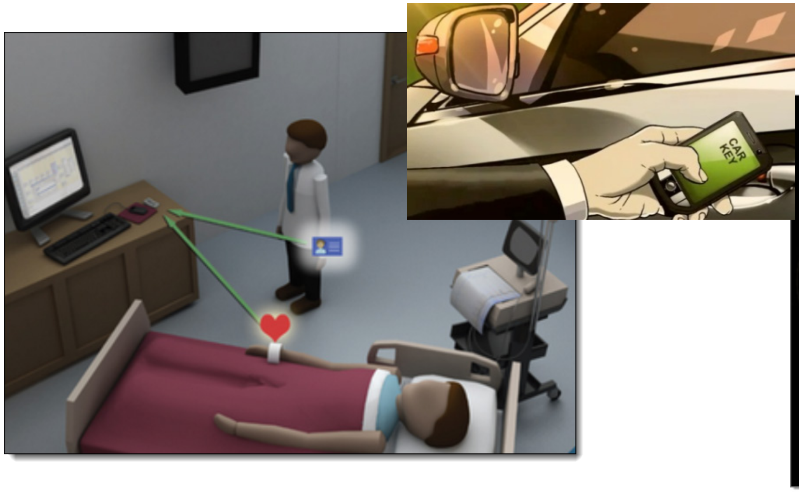
FREQUENCIES

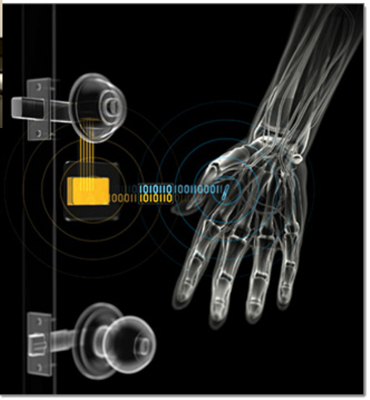
Frequency	Range	Distance	Common Usage	Card Types	Standards
Low Frequency (LF)	120kHz – 140kHz	<3 ft. (Commonly under 1.5ft)	Access control systems; animal tagging; car immobilizer	HID Prox, Indala Prox, Kantech ioProx, Hitag 1/2/S, Casi-Rusco, EM4X, Honeywell Nexwatch, G-Prox II, AWID, Pyramid Prox, Keri Prox, Q5, TI-RFID Systems, VeriChip	ISO 11784 / ISO 11785 ISO 14223 (Animals) ISO 18000-2
High Frequency (HF)	13.56MHz	3-10ft **Maybe up to ~35 ft*	Contactless smart cards; access control systems; loyalty card; credit cards; payment card; mobile payments; ski pass; e-Passport; public transportation systems	iCLASS, MIFARE/DESFire, LEGIC, Sony Felicia, Calypso, Tag-it, Topaz, Sielox, SRIX4K, CryptoRF, JCOP	ISO 15963 - Vicinity Card ISO 14443A ISO 14443B ISO 18000-3 ISO 18092 - NFC ISO 21481 – NFCIP-2 EPC Class 1 (13.56MHz)
Ultra-High Frequency (UHF)	860MHz – 960MHz (Regional) Also: 433MHz	~30ft **Up to miles with strong antenna and line of sight*	Supply chain; inventory tracking; Walmart; baggage handling; toll collecting; Enhanced Driver's License; U.S. Passport Card (not book); Trusted traveler cards; ski pass	EPC Gen 2	EPC Class 0 EPC Class 1 (860-930MHz) EPC UHF Gen 2 ISO 18000-6C ISO 18000-63 INCITS 371.2

RFID Other Usage

WHERE ELSE?



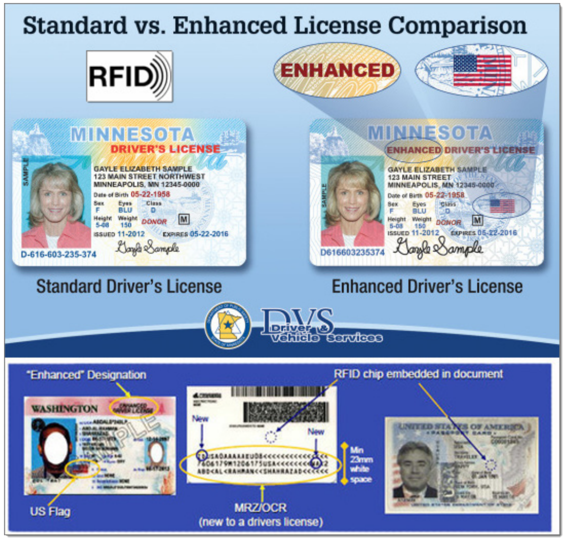




RFID Other Usage

WHERE ELSE?

RFID card needed to access encrypted hard drive


Standard vs. Enhanced License Comparison

Standard Driver's License

Enhanced Driver's License

"Enhanced" Designation

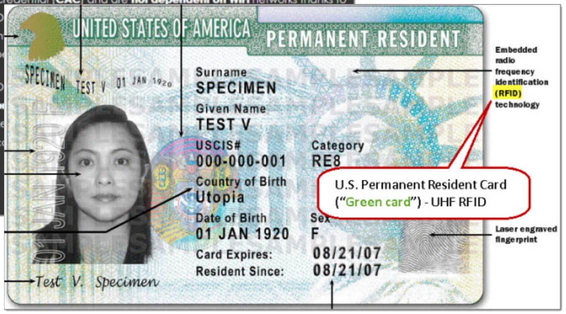
RFID chip embedded in document

US Flag

MRZ/OCR
(new to a drivers license)

MORE WAYS TO UNLOCK DOORS

OKIDOKEYS' Smart-Locks work across a **unique multi-technology platform including**: Bluetooth 4.0 (**BLE**), Near Field Communication (**NFC**), Radio Frequency Identification (**RFID**), Crypto Acoustic Credential (**CAC**) and are **not dependent on WiFi** networks thanks to


U.S. Permanent Resident Card ("Green card") - UHF RFID

Embedded radio frequency identification (RFID) technology

Laser engraved fingerprint

Hotel RFID Keys

Marriott REWARDS.

Operating Instructions:
Touch keycard to lens to unlock

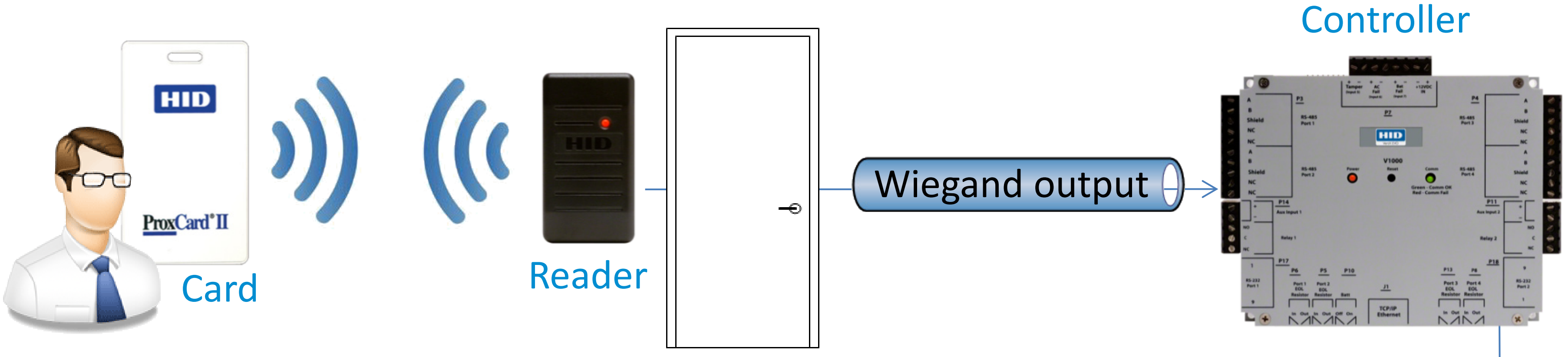
For your safety:

- Use safety deposit box for valuables.
- Secure deadbolt and door guard when in room.
- Use viewport to identify all visitors.
- Employees are required to wear name tags.
- Evacuate immediately when fire alarm sounds.
- Safeguard and keep your door key with you at all times.
- Ensure that all windows and doors are locked.

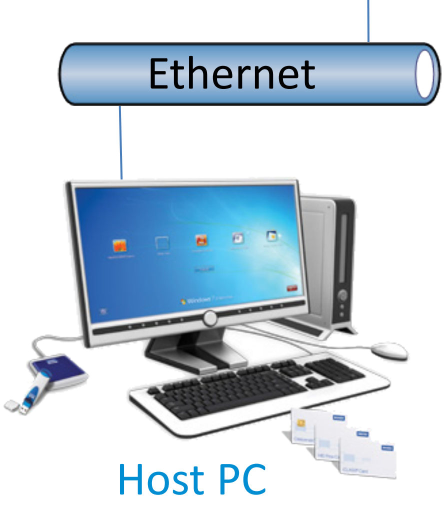
www.rfidhotel.com

How a Card Is Read

POINTS OF ATTACK



Card	• Broadcasts 26-37 bit card number
Reader	• Converts card data to “Wiegand Protocol” for transmission to the controller • No access decisions are made by reader
Controller	• Binary card data “format” is decoded • Makes decision to grant access (or not)
Host PC	• Add/remove card holders, access privileges • Monitor system events in real time



HID Global – How a HID Card is “Read” (PDF)
https://info.hidglobal.com/WP-How-an-HID-Card-is-Read_Request.html

RFID Hacking Gear

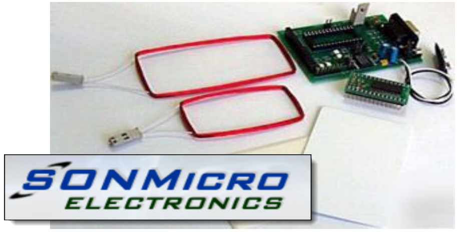
PENTEST TOOLKIT

RFID Hacking Gear

SUMMARY OF WHAT WE HAVE

Tastic RFID Thief

- T55x7 Cards
- Q5 cards (T5555)



SONMicro - 125 KHz RFID Evaluation Kit - Deluxe

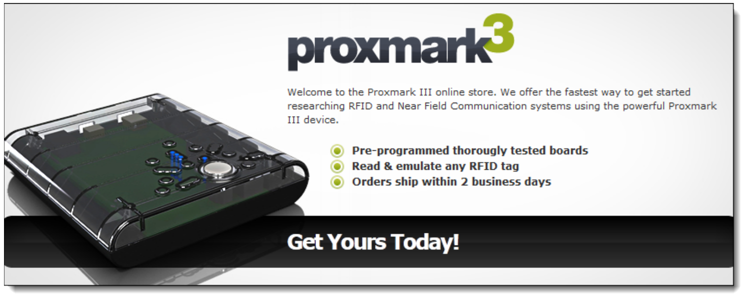
pcProx® 125 kHz & AIR ID® 13.56 MHz Card Analyzer

Intelligent portable Card Analyzers for determination of proximity & contactless smart cards

RFIDeas – HF and LF USB Tools

ACG LAHF USB	125/134.2 kHz & 13.56 MHz	USB	EM4x02 EM4x50 EM4x05 (ISO 11784/5 FDX-B) Hitag 1 / 2 / S Q5 TI 64 bit R/O & R/W TI 1088 bit Multipage ISO 14443 A/B, ISO 15693, ISO 18000-3, NFC, I-CODE	

rfidiot.org



proxmark3

Welcome to the Proxmark III online store. We offer the fastest way to get started researching RFID and Near Field Communication systems using the powerful Proxmark III device.

- Pre-programmed thorougly tested boards
- Read & emulate any RFID tag
- Orders ship within 2 business days

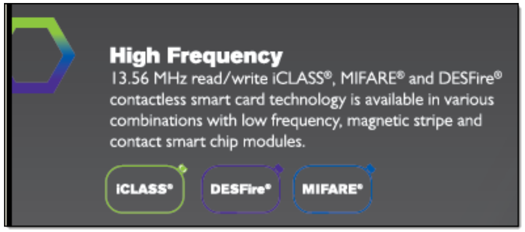
Get Yours Today!

Proxmark3

RFIDiots Compatible - ACG LAHF USB – Hig h and Low Frequency Antenna

RFID Hacking Gear

HF - HIGH FREQUENCY (13.56 MHz)



High Frequency
13.56 MHz read/write iCLASS®, MIFARE® and DESFire® contactless smart card technology is available in various combinations with low frequency, magnetic stripe and contact smart chip modules.

iCLASS®
DESFire®
MIFARE®

In The Box	HF PCB antenna with 3' USB cable
Dimensions	8.3cm x 5.5cm x 1cm
Weight	16g
Impedance	1.5Ω
Approximate Range	3 - 5cm

High Frequency PCB Antenna

Our high frequency PCB antenna ("HFA") is specifically designed for the Proxmark III. It is tuned to operate at 13.56MHz and is capable of snooping the UID of a Mifare 1k classic card at a distance of 3cm.

The antenna can be switched to match either a 100pF or 47pF capacitor on the HF circuit of the Proxmark. When connected to a working Proxmark, the antenna registers approximately 8-9V (as produced by the `tune` command). Our HFA can be used to interact with the following tags:

- Mifare
- ISO14443A / ISO14443B
- ISO15693
- EPA
- Legic
- iClass

The antenna is the size of a credit card and ships with a 3' Hirose USB cable that is used to connect it to a Proxmark. Antennas are connected to the 5-pin USB port on the Proxmark using the USB cable included.

Proxmark3 - HF Antenna

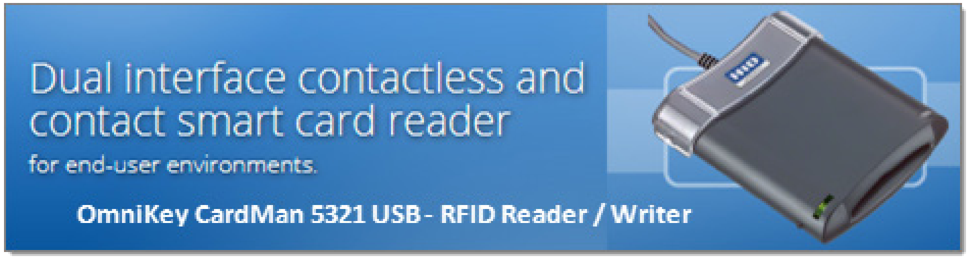
Identive SCM SCL3711 USB 13.56 MHz Reader/Writer

- Works with `libnfc` library, PN533 chip

rfidiot.org

ACG LAHF USB	125/134.2 kHz & 13.56 MHz	USB	EM4x02 EM4x50 EM4x05 (ISO 11784/5 FDX-B) Hitag 1 / 2 / S Q5 TI 64 bit R/O & R/W TI 1088 bit Multipage ISO 14443 A/B, ISO 15693, ISO 18000-3, NFC, I-CODE	

RFIDiots Compatible - ACG LAHF USB – Hig h and Low Frequency Antenna

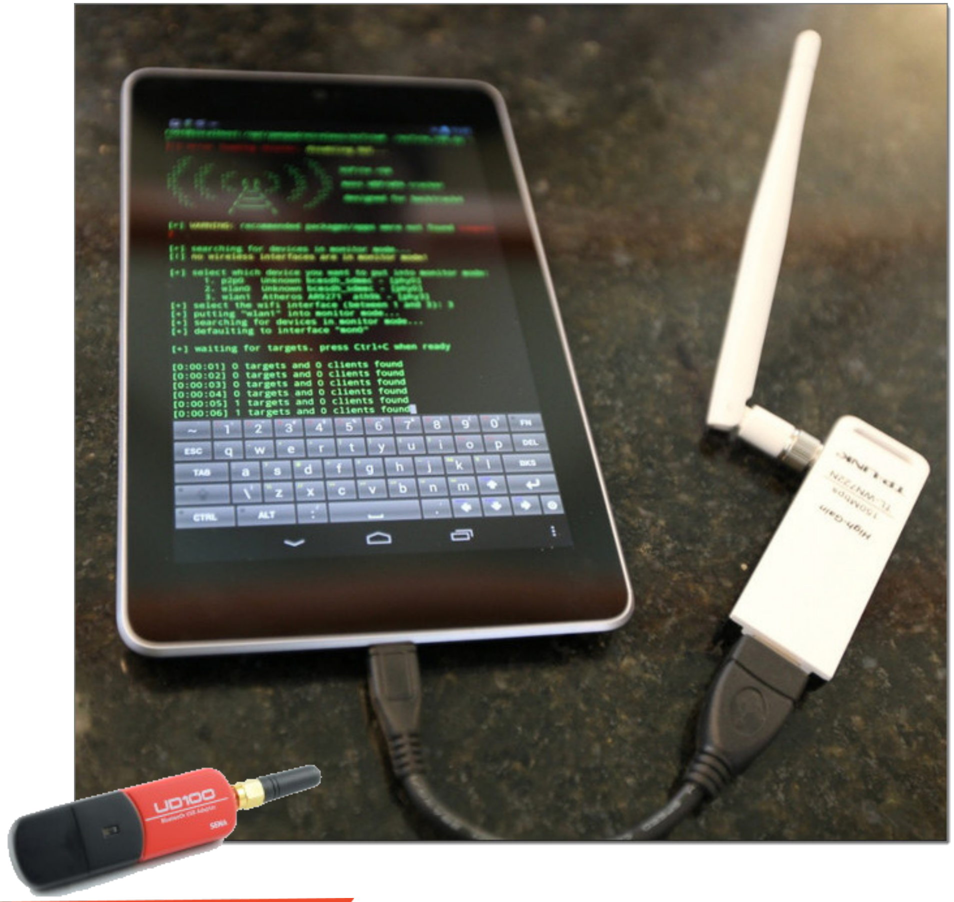


Dual interface contactless and contact smart card reader
for end-user environments.

OmniKey CardMan 5321 USB - RFID Reader / Writer

Pwn Pad 2014

NEXUS 7 PENTEST DEVICE



```
[illegible]
[+] WARNING: recommended packages/apps were not found
[+] searching for devices in monitor mode...
[!] no wireless interfaces are in monitor mode!
[+] select which device you want to put into monitor mode:
    1. p2p0   Unknown bcmsdh_sdmmc - [phy0]
    2. wlan0  Unknown bcmsdh_sdmmc - [phy0]
    3. wlan1  Atheros AR9271  ath9k - [phy1]
[+] select the wifi interface (between 1 and 3): 3
[+] putting "wlan1" into monitor mode...
[+] searching for devices in monitor mode...
[+] defaulting to interface "mon0"

[+] waiting for targets. press Ctrl+C when ready

[0:00:01] 0 targets and 0 clients found
[0:00:02] 0 targets and 0 clients found
[0:00:03] 0 targets and 0 clients found
[0:00:04] 0 targets and 0 clients found
[0:00:05] 1 targets and 0 clients found
[0:00:06] 1 targets and 0 clients found
```

Toolkit includes:

Wireless Tools

- Aircrack-ng
- Kismet
- Wifite
- Reaver
- MDK3
- EAPeak
- Asleap
- FreeRADIUS-WPE
- Hostapd

Bluetooth Tools:

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools

Web Tools

- Nikto
- W3af

Network Tools

- NET-SNMP
- Nmap
- Netcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng
- SSLstrip
- Hamster & Ferret
- Metasploit
- SET
- Easy-Creds
- John (JTR)
- Hydra
- Pyrit
- Scapy

BISHOP FOX

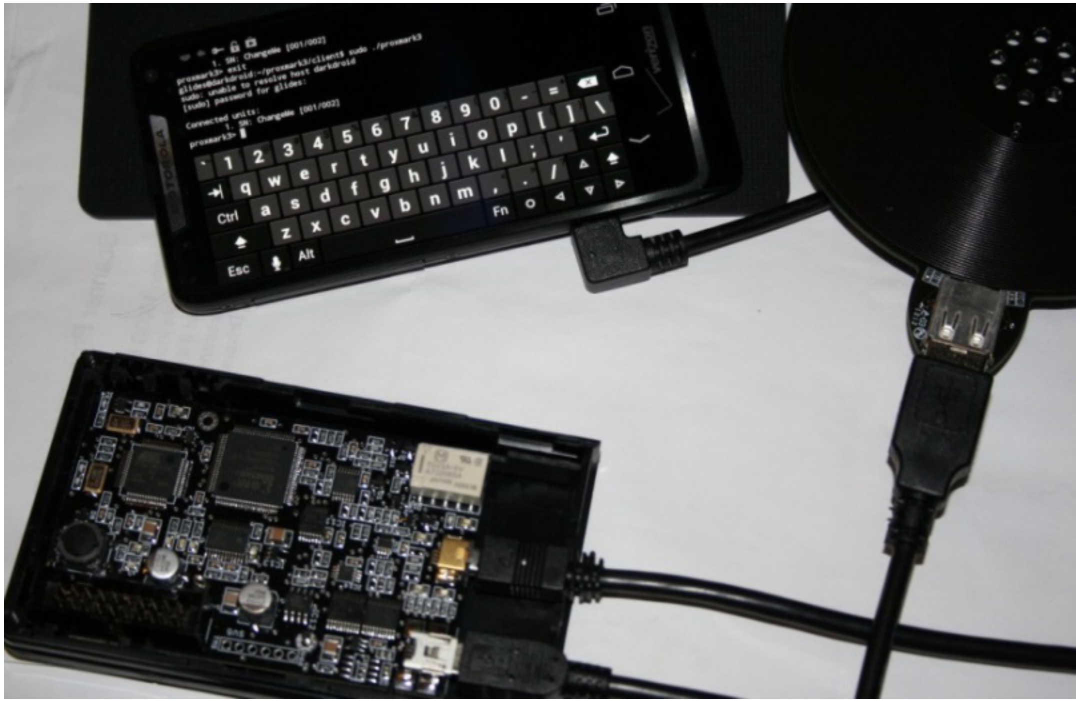
Kali NetHunter

NEXUS 7 PENTEST DEVICE

Nexus7 (2013 – WiFi) – Android Tablet – **Non**-PwnPad2014

Proxmark3 on Android

MOBILERFID HACKING



```
    1. SN: ChangeMe [001/002]
proxmark3> exit
glides@darkdroid:~/proxmark3/client$ sudo ./proxmark3
sudo: unable to resolve host darkdroid
[sudo] password for glides:

Connected units:
    1. SN: ChangeMe [001/002]
proxmark3> ▮
```

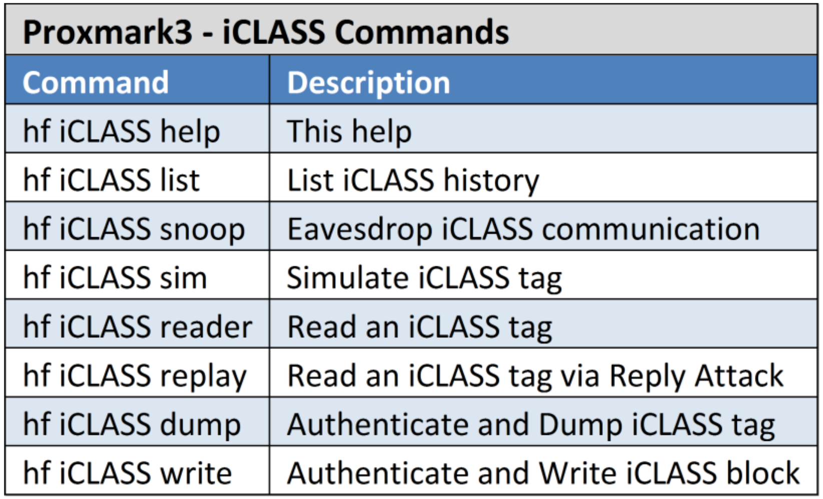
RFID Hacking Tools

PENTEST TOOLKIT

Proxmark3

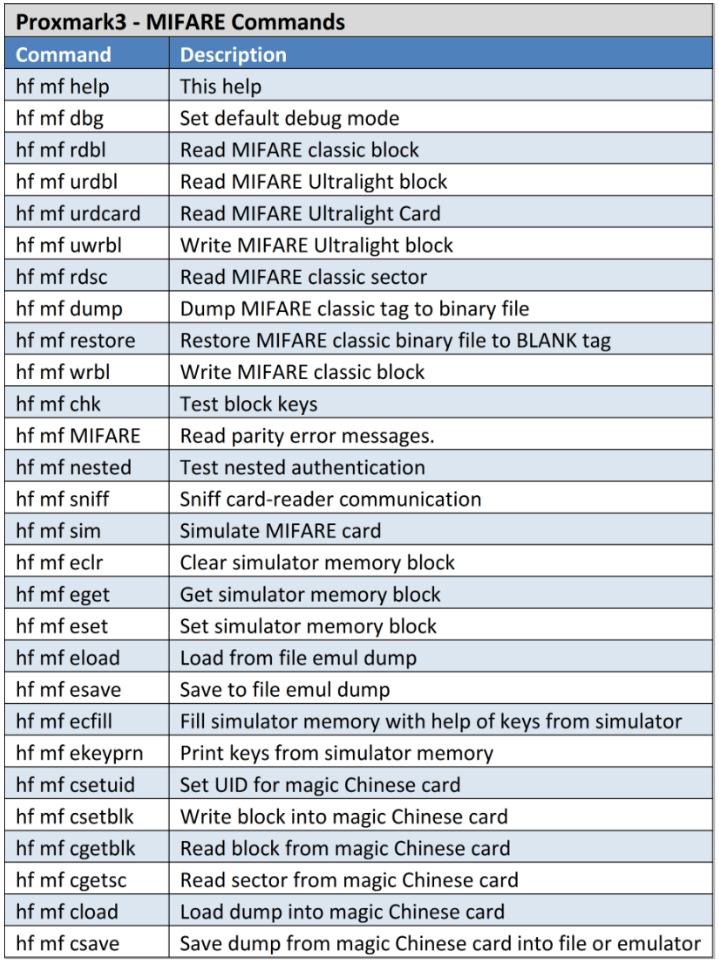
RFID HACKING TOOLS

- RFID Hacking swiss army knife
- Read/simulate/clone RFID cards



Proxmark3 - iCLASS Commands

Command	Description
hf iCLASS help	This help
hf iCLASS list	List iCLASS history
hf iCLASS snoop	Eavesdrop iCLASS communication
hf iCLASS sim	Simulate iCLASS tag
hf iCLASS reader	Read an iCLASS tag
hf iCLASS replay	Read an iCLASS tag via Reply Attack
hf iCLASS dump	Authenticate and Dump iCLASS tag
hf iCLASS write	Authenticate and Write iCLASS block



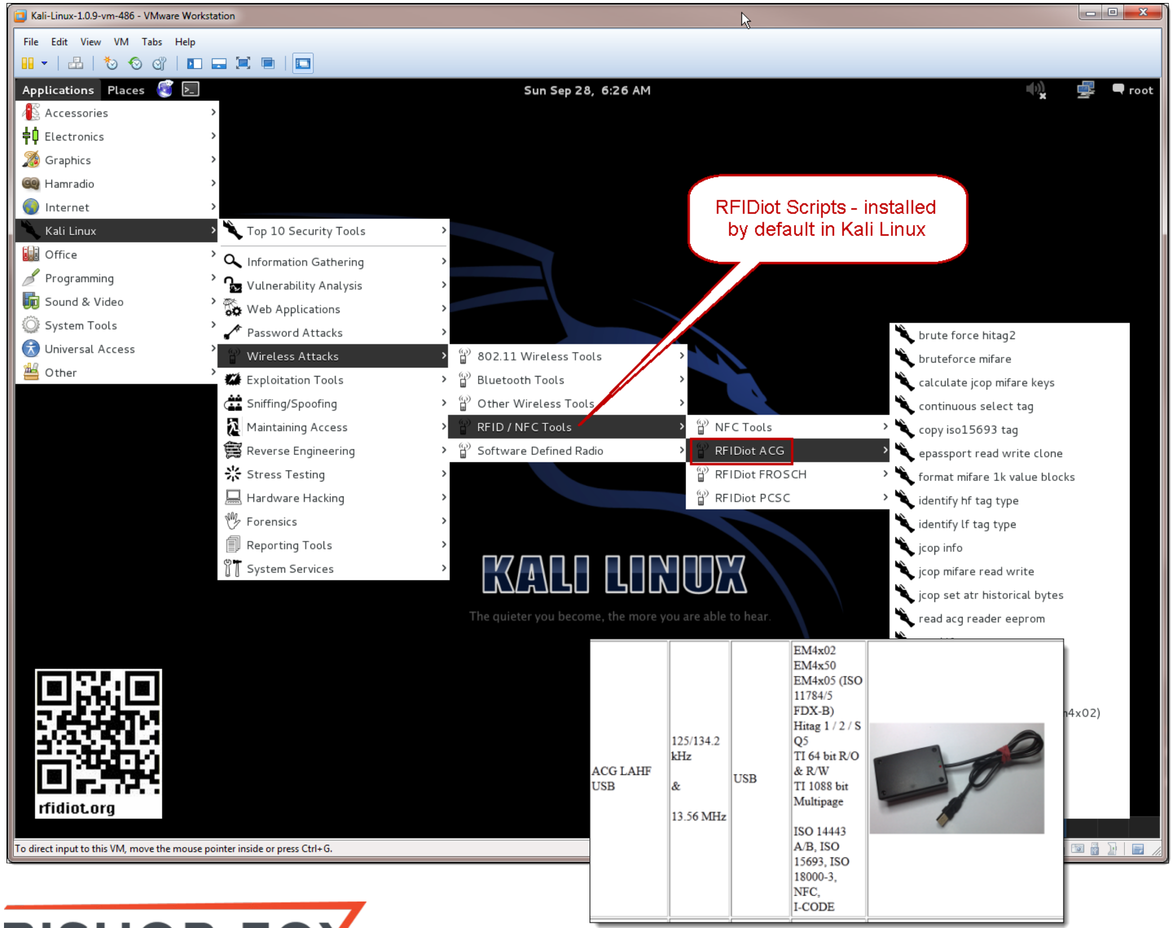
Proxmark3 - MIFARE Commands

Command	Description
hf mf help	This help
hf mf dbg	Set default debug mode
hf mf rdbl	Read MIFARE classic block
hf mf urdbl	Read MIFARE Ultralight block
hf mf urdcard	Read MIFARE Ultralight Card
hf mf uwrbl	Write MIFARE Ultralight block
hf mf rdsc	Read MIFARE classic sector
hf mf dump	Dump MIFARE classic tag to binary file
hf mf restore	Restore MIFARE classic binary file to BLANK tag
hf mf wrbl	Write MIFARE classic block
hf mf chk	Test block keys
hf mf MIFARE	Read parity error messages.
hf mf nested	Test nested authentication
hf mf sniff	Sniff card-reader communication
hf mf sim	Simulate MIFARE card
hf mf eclr	Clear simulator memory block
hf mf eget	Get simulator memory block
hf mf eset	Set simulator memory block
hf mf eload	Load from file emul dump
hf mf esave	Save to file emul dump
hf mf ecfill	Fill simulator memory with help of keys from simulator
hf mf ekeyprn	Print keys from simulator memory
hf mf csetuid	Set UID for magic Chinese card
hf mf csetblk	Write block into magic Chinese card
hf mf cgetblk	Read block from magic Chinese card
hf mf cgetsc	Read sector from magic Chinese card
hf mf cload	Load dump into magic Chinese card
hf mf csave	Save dump from magic Chinese card into file or emulator

RFIDiot Scripts

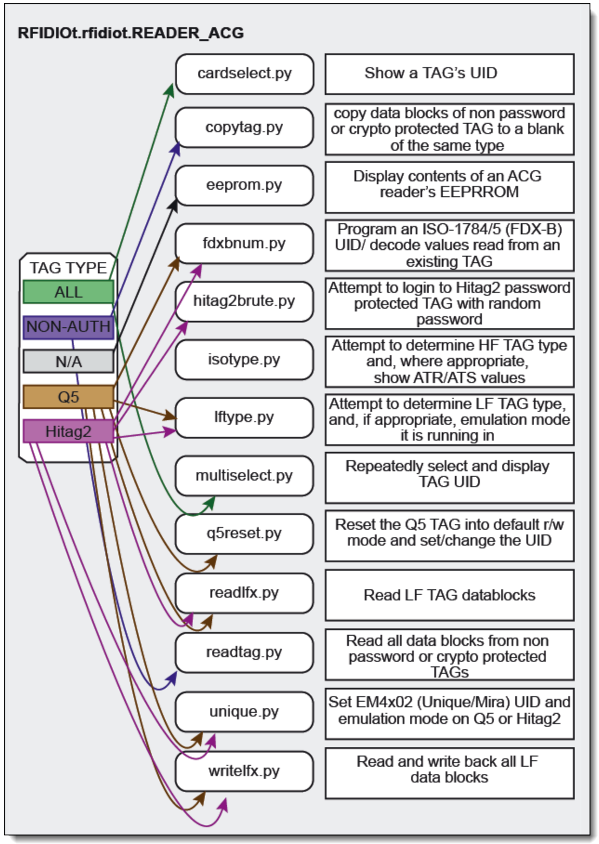
RFID HACKING TOOLS

rfidiot.org



RFIDiot Scripts - installed by default in Kali Linux

ACG LAHF USB	125/134.2 kHz & 13.56 MHz	USB	EM4x02 EM4x50 EM4x05 (ISO 11784/5 FDX-B) Hitag 1 / 2 / S Q5 TI 64 bit R/O & R/W TI 1088 bit Multipage ISO 14443 A/B, ISO 15693, ISO 18000-3, NFC, I-CODE	



RFIDIOt.rfidiot.READER_ACG

cardselect.py	Show a TAG's UID
copytag.py	copy data blocks of non password or crypto protected TAG to a blank of the same type
eeprom.py	Display contents of an ACG reader's EEPRROM
fdxbnum.py	Program an ISO-1784/5 (FDX-B) UID/ decode values read from an existing TAG
hitag2brute.py	Attempt to login to Hitag2 password protected TAG with random password
isotype.py	Attempt to determine HF TAG type and, where appropriate, show ATR/ATS values
lftype.py	Attempt to determine LF TAG type, and, if appropriate, emulation mode it is running in
multiselect.py	Repeatedly select and display TAG UID
q5reset.py	Reset the Q5 TAG into default r/w mode and set/change the UID
readlfx.py	Read LF TAG datablocks
readtag.py	Read all data blocks from non password or crypto protected TAGs
unique.py	Set EM4x02 (Unique/Mira) UID and emulation mode on Q5 or Hitag2
writelfx.py	Read and write back all LF data blocks

BISHOP FOX

RFIDeas Tools

RF IDEAS

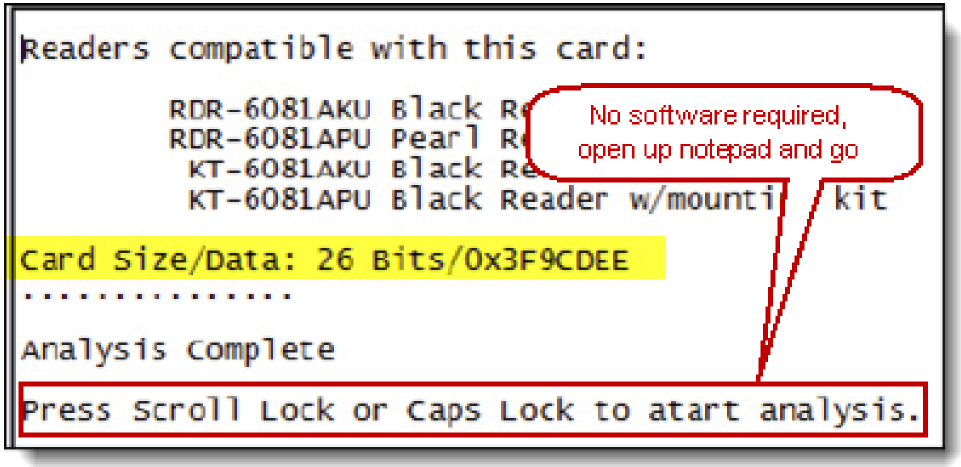
RFID HACKING TOOLS

pcProx® 125 kHz & AIR ID® 13.56 MHz Card Analyzer

$269.00

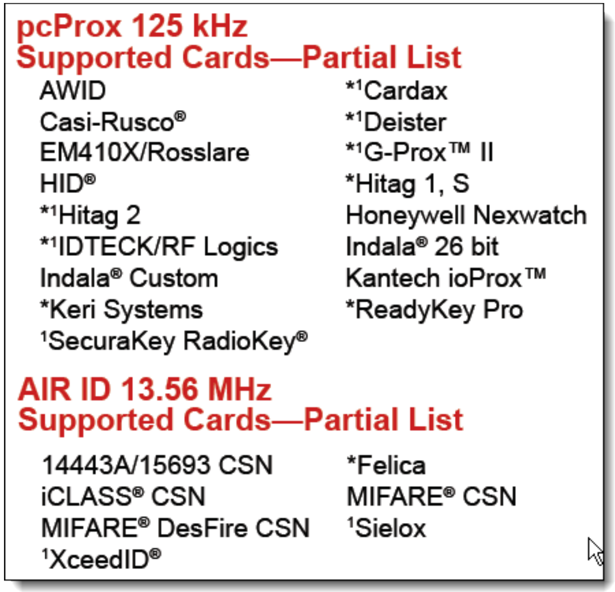
Intelligent portable Card Analyzers for determination of proximity & contactless smart cards

- No software required
- Identifies card type and data
- Great for badges w/o visual indicators of card type



```
Readers compatible with this card:

        RDR-6081AKU Black Re
        RDR-6081APU Pearl Re
         KT-6081AKU Black Re
         KT-6081APU Black Reader w/mounti    kit

Card Size/Data: 26 Bits/0x3F9CDEE
...............

Analysis Complete

Press Scroll Lock or Caps Lock to atart analysis.
```

No software required, open up notepad and go



pcProx 125 kHz Supported Cards—Partial List

AWID	*[1]Cardax
Casi-Rusco®	*[1]Deister
EM410X/Rosslare	*[1]G-Prox™ II
HID®	*Hitag 1, S
*[1]Hitag 2	Honeywell Nexwatch
*[1]IDTECK/RF Logics	Indala® 26 bit
Indala® Custom	Kantech ioProx™
*Keri Systems	*ReadyKey Pro
[1]SecuraKey RadioKey®	

AIR ID 13.56 MHz Supported Cards—Partial List

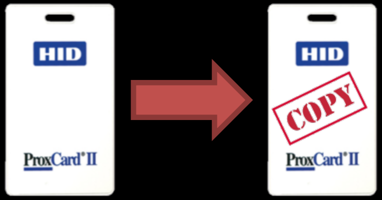
14443A/15693 CSN	*Felica
iCLASS® CSN	MIFARE® CSN
MIFARE® DesFire CSN	[1]Sielox
[1]XceedID®	

Methodology

3 STEP APPROACH

1. Silently steal badge info

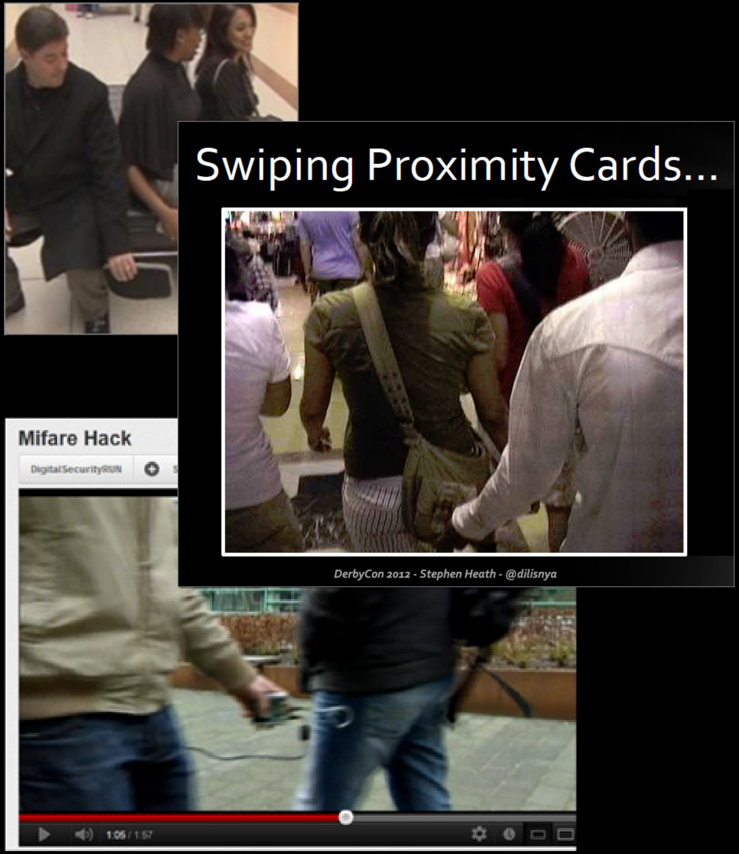
2. Create card clone



3. Enter and plant backdoor

Distance Limitations

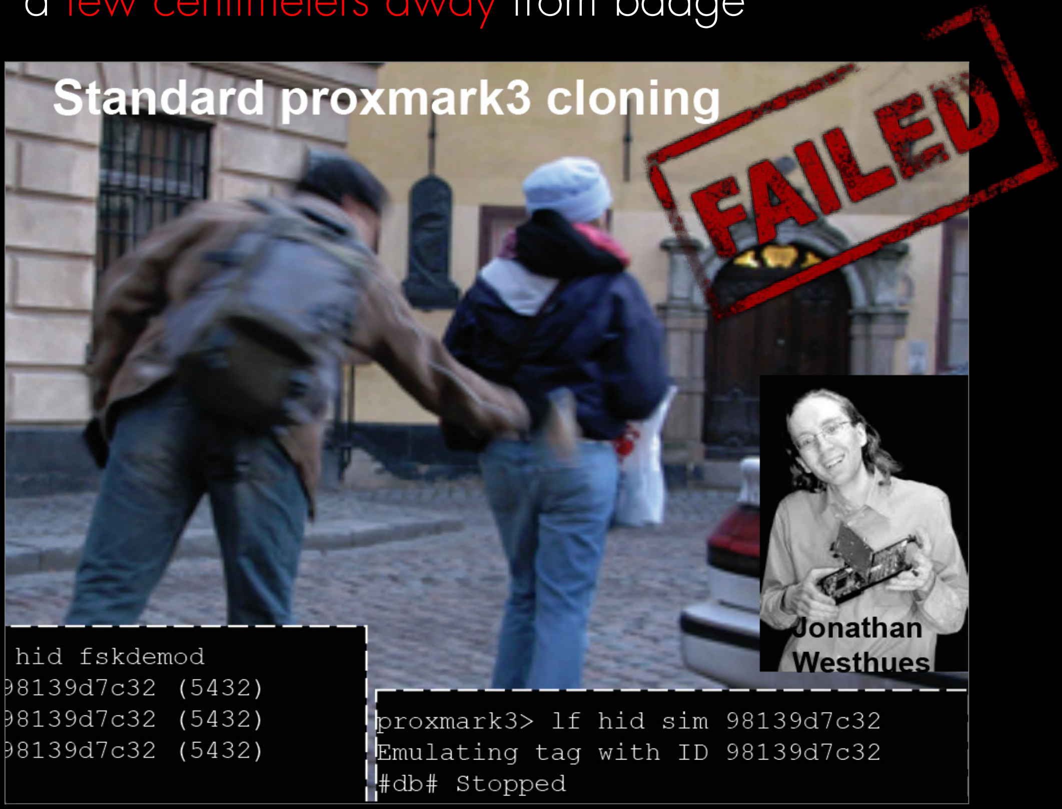
A$$ GRABBING METHOD



Swiping Proximity Cards…

DerbyCon 2012 - Stephen Heath - @dilisnya

Existing RFID hacking tools only work when a few centimeters away from badge



Standard proxmark3 cloning

FAILED

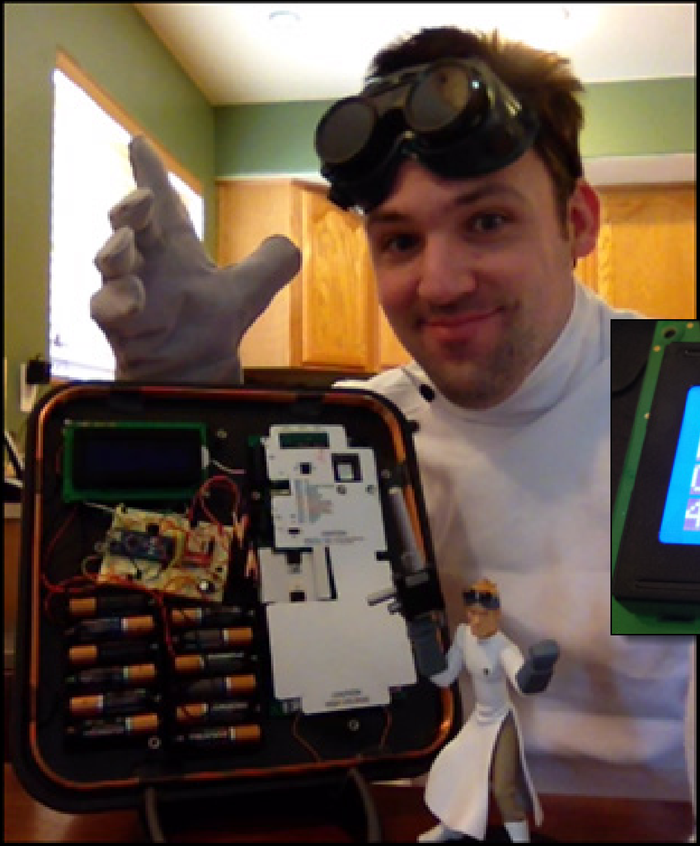
```
hid fskdemod
98139d7c32 (5432)
98139d7c32 (5432)
98139d7c32 (5432)
```

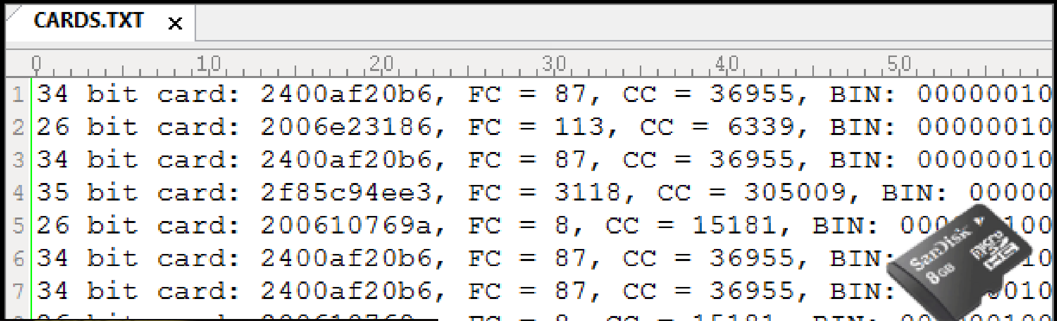
```
proxmark3> lf hid sim 98139d7c32
Emulating tag with ID 98139d7c32
#db# Stopped
```

Tastic Solution

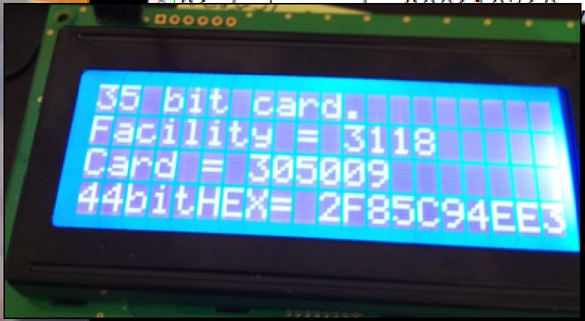
Hacker inside

LONG RANGE RFID STEALER

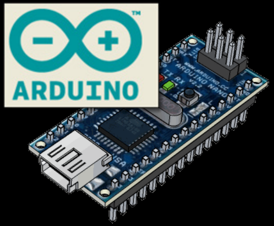


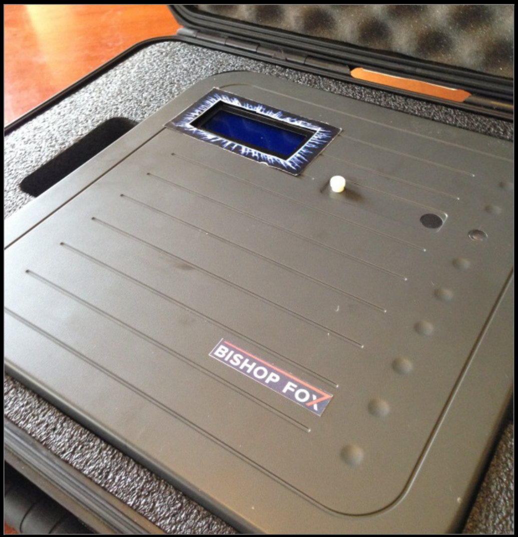


```
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
26 bit card: 2006e23186, FC = 113, CC = 6339, BIN: 00000010
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
35 bit card: 2f85c94ee3, FC = 3118, CC = 305009, BIN: 00000
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 000000100
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 000000100
```



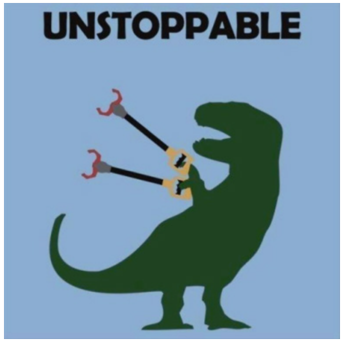
```
35 bit card.
Facility = 3118
Card = 305009
44bitHEX= 2F85C94EE3
```



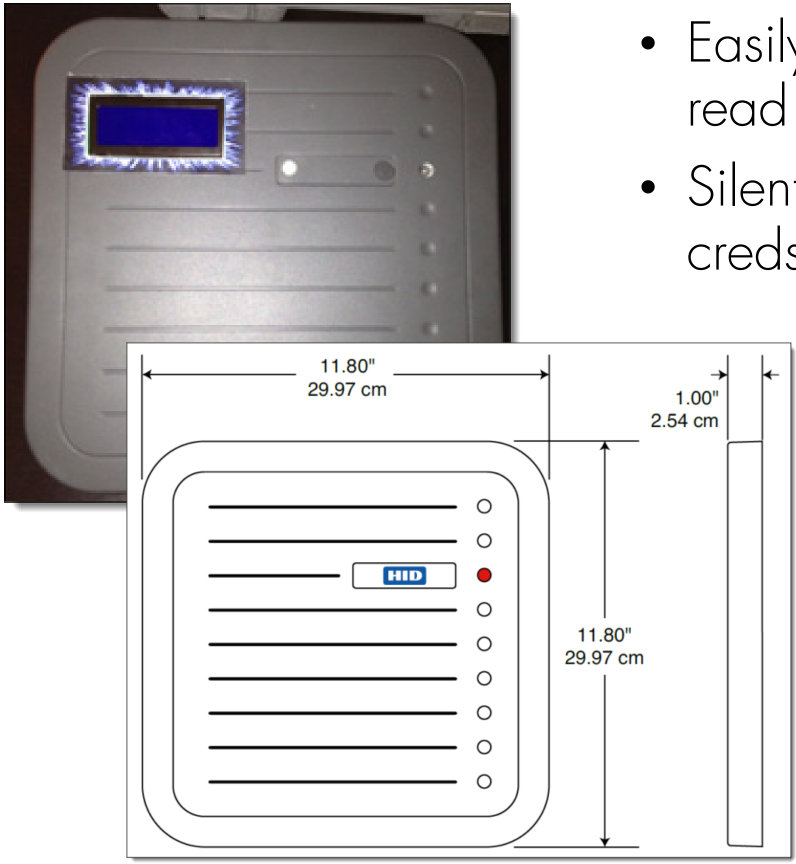


Tastic RFID Thief

LONG RANGE RFID STEALER



- Easily hide in briefcase or messenger bag, read badges from up to 3 feet away
- Silent powering and stealing of RFID badge creds to be cloned later using T55x7 cards



Tastic RFID Thief

LONG RANGE RFID STEALER

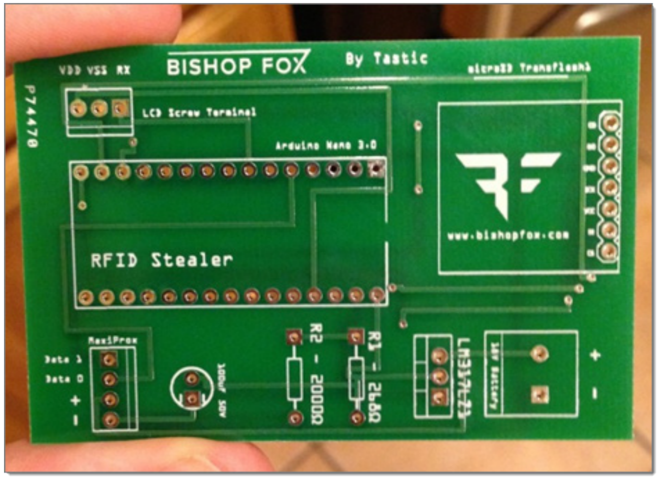
AS SEEN ON TV

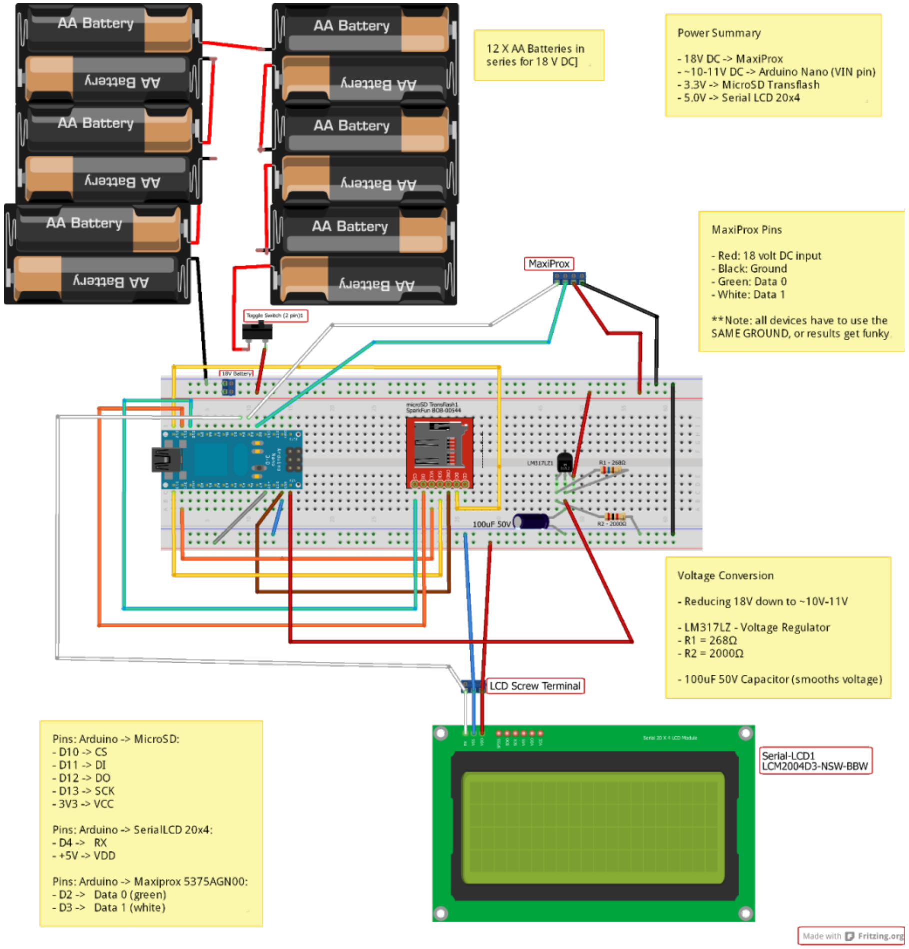
FRITZING

Tastic RFID Thief

LONG RANGE RFID STEALER

- Designed using Fritzing
- Exports to Extended-Gerber
- Order PCB at www.4pcb.com
    - $33 for 1 PCB
    - Much cheaper in bulk





12 X AA Batteries in series for 18 V DC]

Power Summary

- 18V DC -> MaxiProx
- ~10-11V DC -> Arduino Nano (VIN pin)
- 3.3V -> MicroSD Transflash
- 5.0V -> Serial LCD 20x4

MaxiProx Pins

- Red: 18 volt DC input
- Black: Ground
- Green: Data 0
- White: Data 1

**Note: all devices have to use the SAME GROUND, or results get funky

Voltage Conversion

- Reducing 18V down to ~10V-11V

- LM317LZ - Voltage Regulator
- R1 = 268Ω
- R2 = 2000Ω

- 100uF 50V Capacitor (smooths voltage)

Pins: Arduino -> MicroSD:
- D10 -> CS
- D11 -> DI
- D12 -> DO
- D13 -> SCK
- 3V3 -> VCC

Pins: Arduino -> SerialLCD 20x4:
- D4 -> RX
- +5V -> VDD

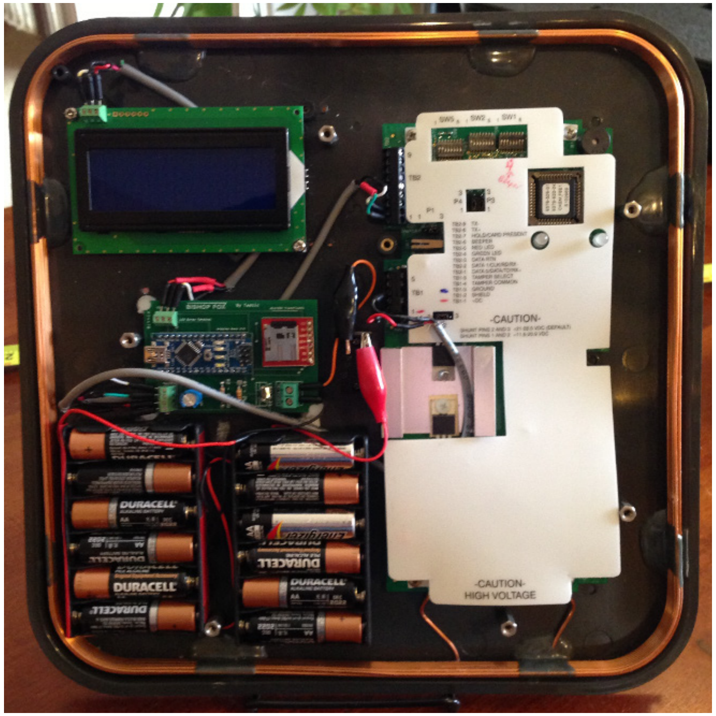
Pins: Arduino -> Maxiprox 5375AGN00:
- D2 -> Data 0 (green)
- D3 -> Data 1 (white)

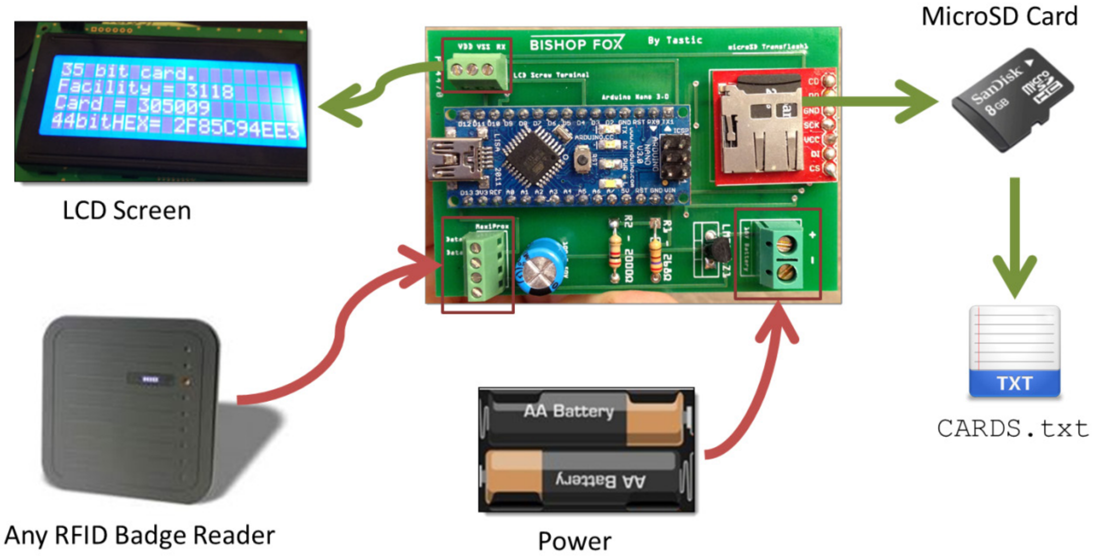
Custom PCB

TASTIC RFID THIEF

Hacker inside

Custom PCB – easy to plug into any type of RFID badge reader





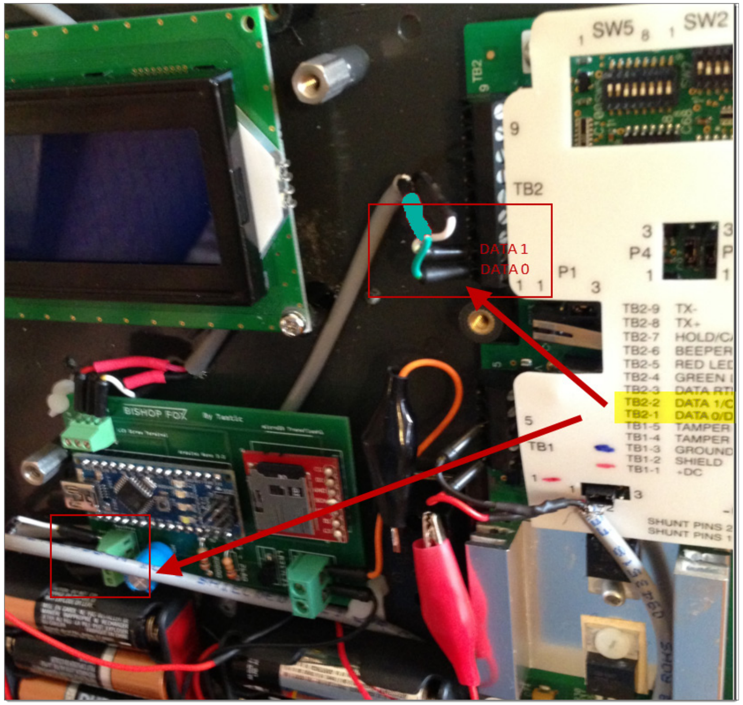
```
35 bit card.
Facility = 3118
Card = 305009
44bitHEX= 2F85C94EE3
```

Wiegand Input

TASTIC RFID THIEF

Tastic Custom PCB – reads from Wiegand output of RFID badge reader:

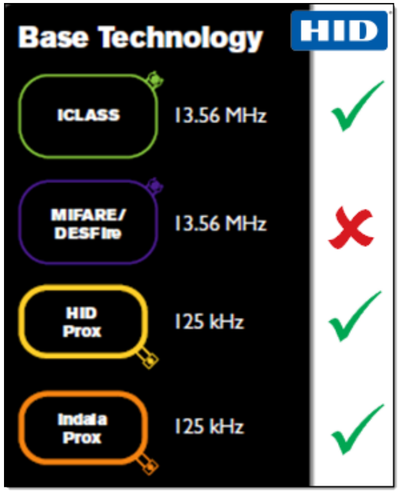
- Outputs a badge binary number by sending electrical pulses for '0' and '1' on wires Data 0 and Data 1
- Wiegand Interface consists of 3 lines: "Data 0", "Data 1", "Data Return" (Ground)
- To send a '0'-bit, a pulse is sent on DATA 0 (Green)
- To send a '1'-bit, a pulse is sent on DATA 1 (White)
- Every HID reader has a Wiegand output available



Wiegand Interface
https://en.wikipedia.org/wiki/Wiegand_interface

Commercial Readers

TASTIC RFID THIEF

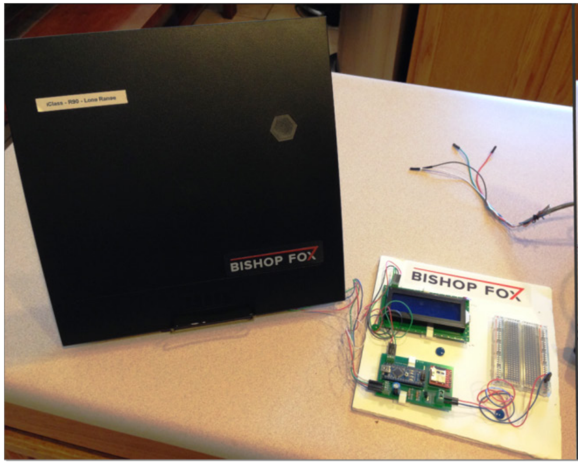


Base Technology		HID
ICLASS	13.56 MHz	✓
MIFARE/ DESFire	13.56 MHz	✗
HID Prox	125 kHz	✓
Indala Prox	125 kHz	✓

Long-range commercial RFID readers to weaponize:

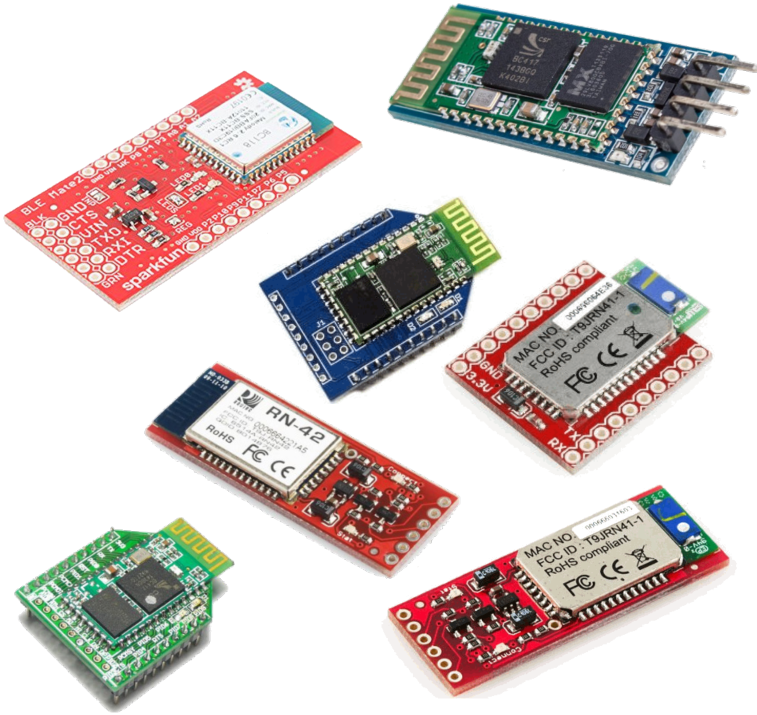
RFID Product Family	Frequency	Long Range Reader	URL
HID Prox	Low Frequency	HID MaxiProx 5375	https://www.hidglobal.com/products/readers/hid-proximity/5375
Indala Prox	Low Frequency	Indala Long-Range Reader 620	http://www.hidglobal.com/products/readers/indala/620
iCLASS	High Frequency	iCLASS - R90 Long Range reader	http://www.hidglobal.com/products/readers/iCLASS/r90

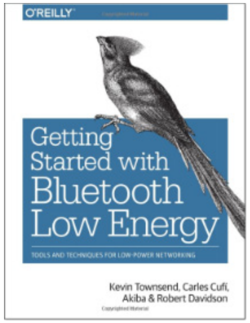
3 out of 4 HID RFID product families covered



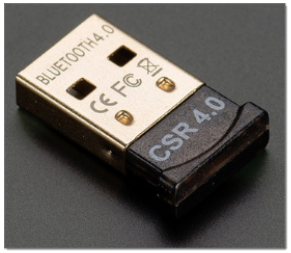
Bluetooth – Other

- Bluetooth Modules:
  - SparkFun BLE Mate 2
  - Bluetooth Mate Gold - Sparkfun
  - Bluetooth Module Breakout - Roving Networks (RN-41)
  - Bluetooth Modem - BlueSMiRF Silver (RN-42)
  - Bluetooth Bee for Arduino - Seeedstudio
  - Bluetooth Bee Standalone with built-in Arduino
  - KEDSUM Arduino Wireless Bluetooth Transceiver Module
- Bluetooth 4.0 USB Module (v2.1 Back-Compatible)
- SENA UD100 industrial Bluetooth USB adapter
  - PwnPad 2014 - supports packet injection (up to 1000')



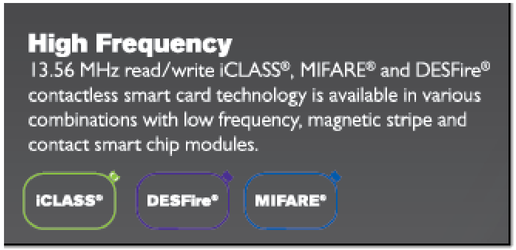


O'REILLY
Getting Started with Bluetooth Low Energy
Kevin Townsend, Carles Cufí, Akiba & Robert Davidson



Commercial Readers

TASTIC RFID THIEF

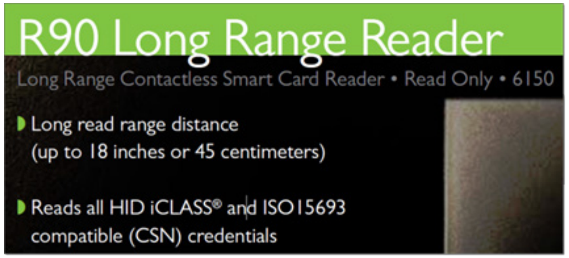


High Frequency
13.56 MHz read/write iCLASS®, MIFARE® and DESFire® contactless smart card technology is available in various combinations with low frequency, magnetic stripe and contact smart chip modules.

iCLASS®
DESFire®
MIFARE®

~$345 on ebay

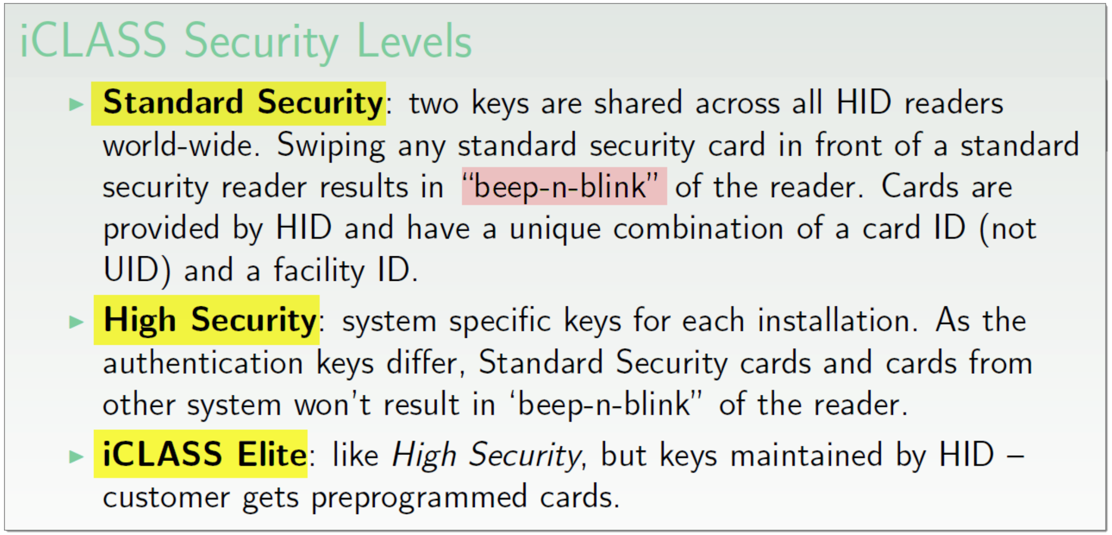
- HID iCLASS – R90 – Long Range Reader
  - Tastic PCB in R90 will pick up iCLASS card if target company is using default "Standard Security".



R90 Long Range Reader

Long Range Contactless Smart Card Reader • Read Only • 6150

- Long read range distance (up to 18 inches or 45 centimeters)
- Reads all HID iCLASS® and ISO15693 compatible (CSN) credentials



iCLASS Security Levels

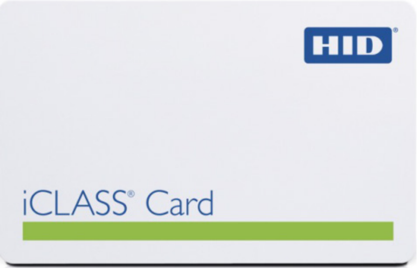
- **Standard Security**: two keys are shared across all HID readers world-wide. Swiping any standard security card in front of a standard security reader results in "beep-n-blink" of the reader. Cards are provided by HID and have a unique combination of a card ID (not UID) and a facility ID.
- **High Security**: system specific keys for each installation. As the authentication keys differ, Standard Security cards and cards from other system won't result in 'beep-n-blink" of the reader.
- **iCLASS Elite**: like *High Security*, but keys maintained by HID – customer gets preprogrammed cards.

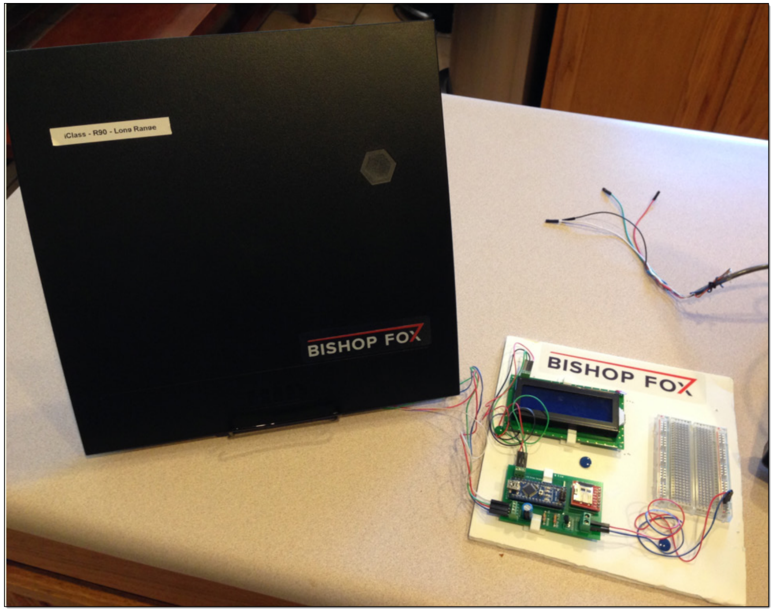
BISHOP FOX

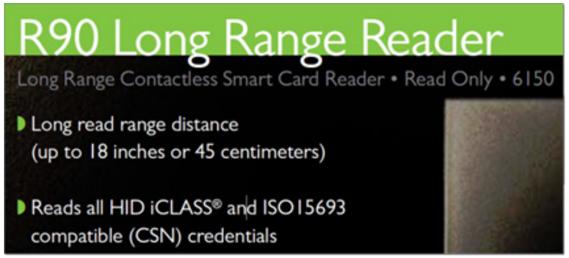
Chaos27th-Analyzing a Modern Cryptographic RFID System-Dec2010
http://events.ccc.de/congress/2010/Fahrplan/events/4114.en.html

Tastic RFID Thief

LONG RANGE RFID STEALER

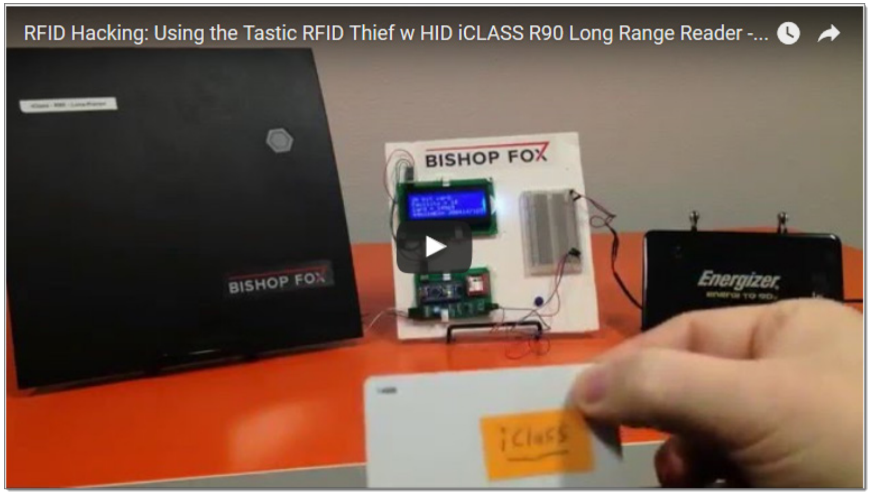





R90 Long Range Reader

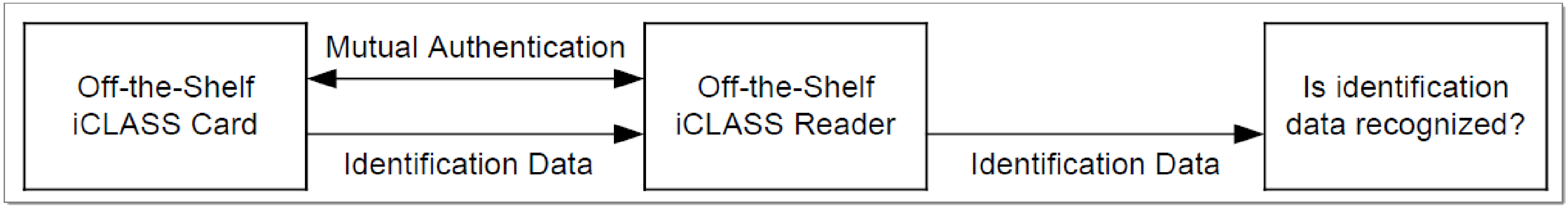
Long Range Contactless Smart Card Reader • Read Only • 6150

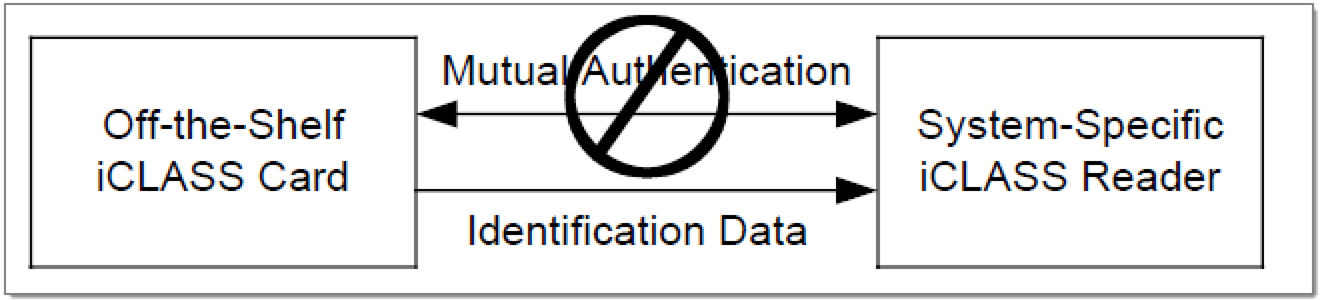
- Long read range distance (up to 18 inches or 45 centimeters)
- Reads all HID iCLASS® and ISO15693 compatible (CSN) credentials


RFID Hacking: Using the Tastic RFID Thief w HID iCLASS R90 Long Range Reader -...

iCLASS

TASTIC RFID THIEF

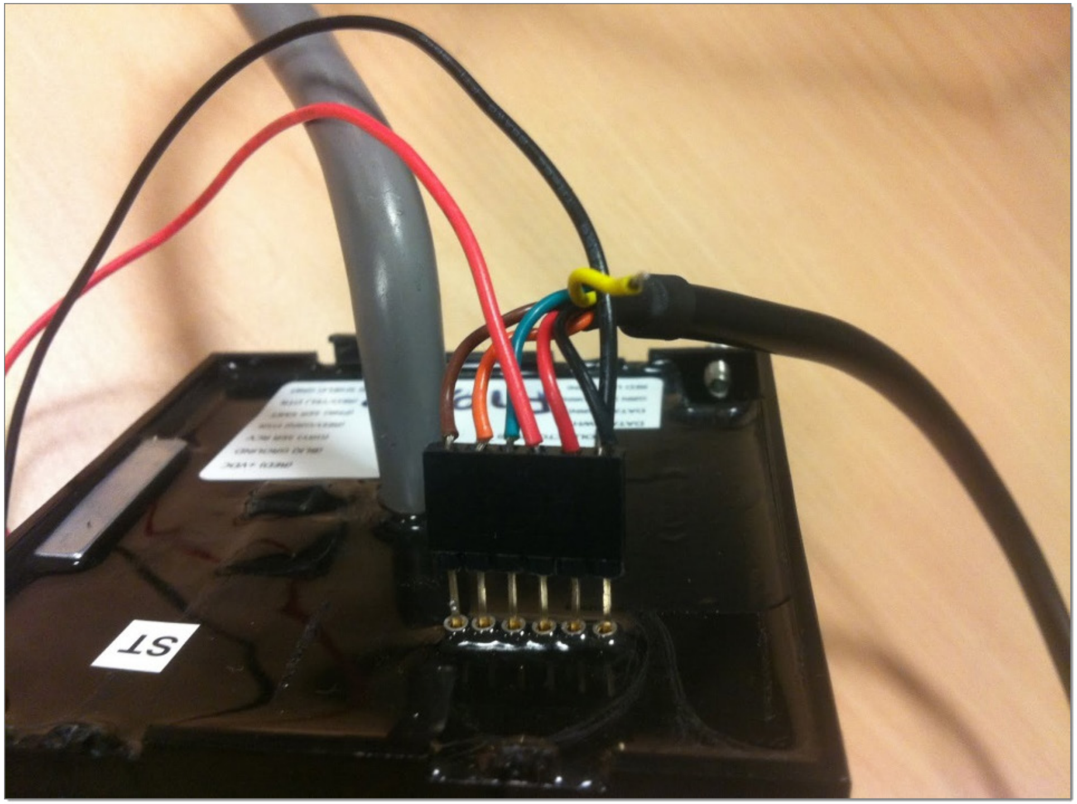

Off-the-Shelf iCLASS Card
Mutual Authentication
Identification Data
Off-the-Shelf iCLASS Reader
Identification Data
Is identification data recognized?



Chaos27th-Analyzing a Modern Cryptographic RFID System-Dec2010
http://events.ccc.de/congress/2010/Fahrplan/events/4114.en.html

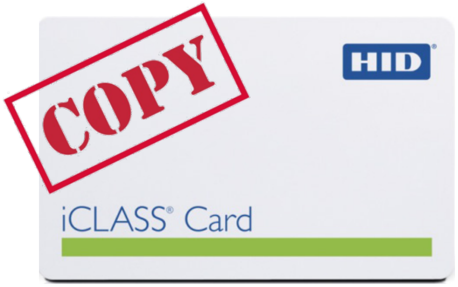
iCLASS – Dumping Key

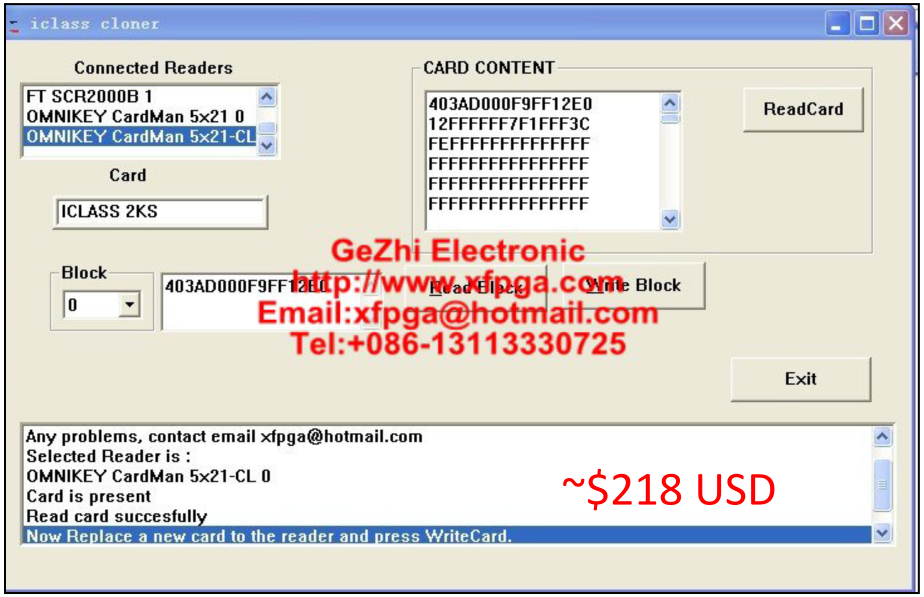
READER ATTACK



iCLASS Cloner

XFPGA.COM - FROM CHINA





Connected Readers

FT SCR2000B 1
OMNIKEY CardMan 5x21 0
OMNIKEY CardMan 5x21-CL 0

Card: ICLASS 2KS

CARD CONTENT

```
403AD000F9FF12E0
12FFFFFF7F1FFF3C
FEFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFF
```

Block: 0 — 403AD000F9FF12E0

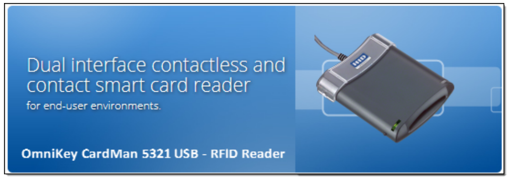
GeZhi Electronic
http://www.xfpga.com
Email:xfpga@hotmail.com
Tel:+086-13113330725

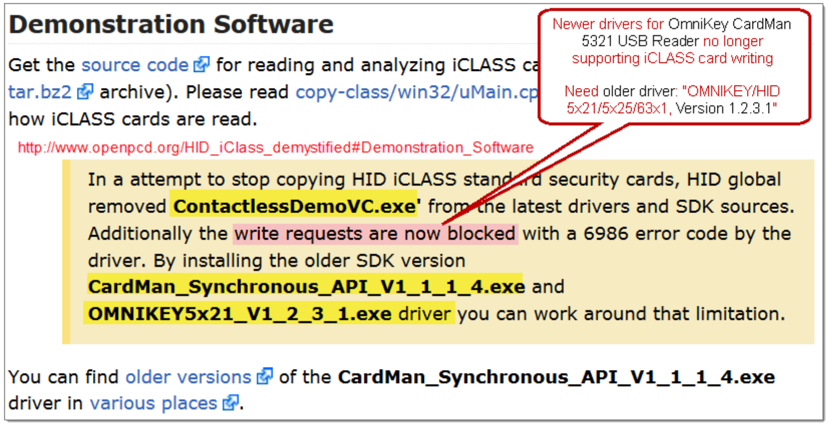
```
Any problems, contact email xfpga@hotmail.com
Selected Reader is :
OMNIKEY CardMan 5x21-CL 0
Card is present
Read card succesfully
Now Replace a new card to the reader and press WriteCard.
```

~$218 USD

- http://www.xfpga.com/html_products/iclass-card-cloner-en-82.html
- Read/Write iCLASS cards using "Standard Security" only (not "High" or "Elite")
- Requires older 32bit driver, and won't let you run in a VM (so Win32 actual install necessary)
- Built from original ContactlessDemoVC.exe
- USB hardware licensing dongle shipped

Uses: OmniKey CardMan 5321 USB - RFID Reader (13.56 Mhz)


Dual interface contactless and contact smart card reader
for end-user environments.
OmniKey CardMan 5321 USB - RFID Reader



Demonstration Software

Get the source code for reading and analyzing iCLASS ca tar.bz2 archive). Please read copy-class/win32/uMain.cp how iCLASS cards are read.

Newer drivers for OmniKey CardMan 5321 USB Reader no longer supporting iCLASS card writing

Need older driver: "OMNIKEY/HID 5x21/5x25/63x1, Version 1.2.3.1"

http://www.openpcd.org/HID_iClass_demystified#Demonstration_Software

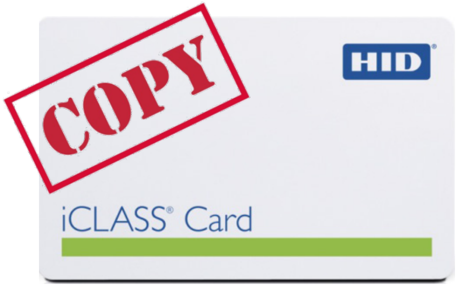
> In a attempt to stop copying HID iCLASS standard security cards, HID global removed **ContactlessDemoVC.exe**' from the latest drivers and SDK sources. Additionally the write requests are now blocked with a 6986 error code by the driver. By installing the older SDK version **CardMan_Synchronous_API_V1_1_1_4.exe** and **OMNIKEY5x21_V1_2_3_1.exe** driver you can work around that limitation.

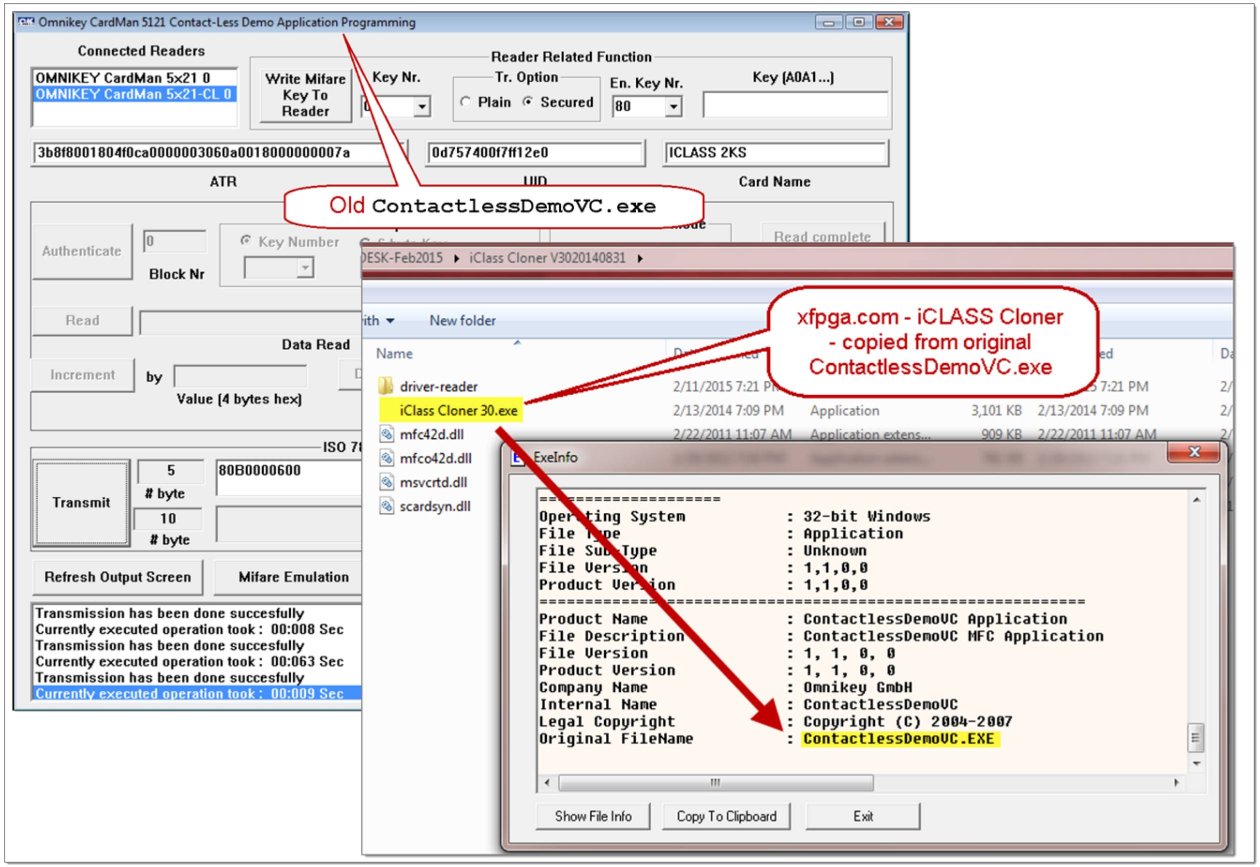
You can find older versions of the **CardMan_Synchronous_API_V1_1_1_4.exe** driver in various places.

BISHOP FOX

iCLASS Cloner

XFPGA.COM - FROM CHINA





Omnikey CardMan 5121 Contact-Less Demo Application Programming

Connected Readers: OMNIKEY CardMan 5x21 0; OMNIKEY CardMan 5x21-CL 0

Reader Related Function — Tr. Option: ○ Plain ● Secured; En. Key Nr.: 80; Key (A0A1...)

ATR: 3b8f8001804f0ca0000003060a0018000000007a

UID: 0d757400f7ff12e0

Card Name: ICLASS 2KS

Transmit: 5 # byte, 80B0000600; 10 # byte

```
Transmission has been done succesfully
Currently executed operation took :  00:008 Sec
Transmission has been done succesfully
Currently executed operation took :  00:063 Sec
Transmission has been done succesfully
Currently executed operation took :  00:009 Sec
```

Old ContactlessDemoVC.exe

DESK-Feb2015 ▸ iClass Cloner V3020140831 ▸

Name	Date modified	Type	Size	
driver-reader	2/11/2015 7:21 PM			7:21 PM
iClass Cloner 30.exe	2/13/2014 7:09 PM	Application	3,101 KB	2/13/2014 7:09 PM
mfc42d.dll	2/22/2011 11:07 AM	Application extens...	909 KB	2/22/2011 11:07 AM
mfco42d.dll				
msvcrtd.dll				
scardsyn.dll				

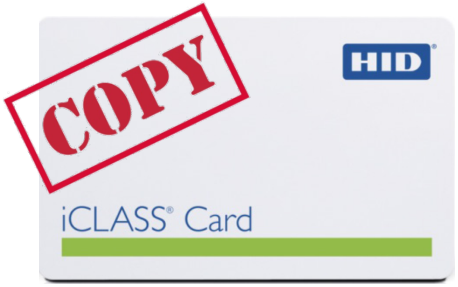
xfpga.com - iCLASS Cloner - copied from original ContactlessDemoVC.exe

ExeInfo

```
====================
Operating System           : 32-bit Windows
File Type                  : Application
File Sub-Type              : Unknown
File Version               : 1,1,0,0
Product Version            : 1,1,0,0
============================================================
Product Name               : ContactlessDemoVC Application
File Description           : ContactlessDemoVC MFC Application
File Version               : 1, 1, 0, 0
Product Version            : 1, 1, 0, 0
Company Name               : Omnikey GmbH
Internal Name              : ContactlessDemoVC
Legal Copyright            : Copyright (C) 2004-2007
Original FileName          : ContactlessDemoVC.EXE
```

iCLASS Cloner

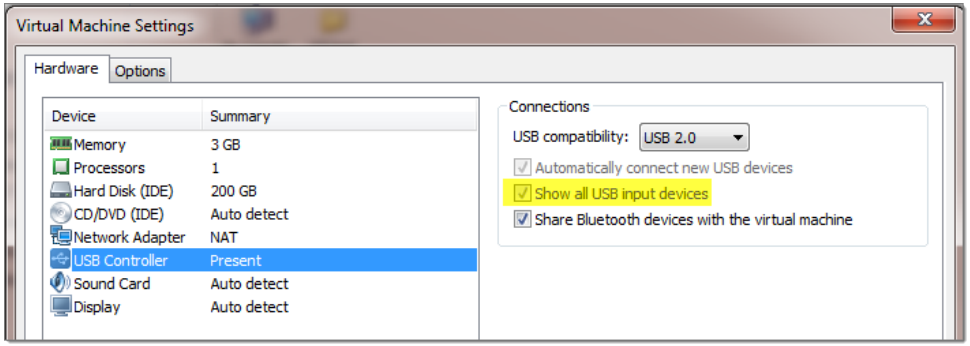
XFPGA.COM - FROM CHINA



VMWare settings – 32bit MS Windows Vmware image with old HID drivers installed:

- To avoid VMWare restrictions on xfpga software, add to your `.vmx` file:
  - `isolation.tools.getVersion.disable = "TRUE"`

- Enable all USB devices:



Device	Summary
Memory	3 GB
Processors	1
Hard Disk (IDE)	200 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Connections

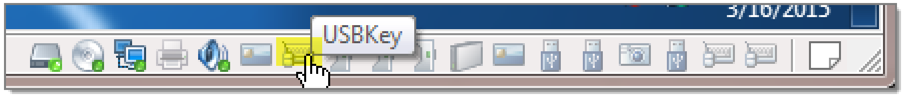
USB compatibility: USB 2.0

☑ Automatically connect new USB devices

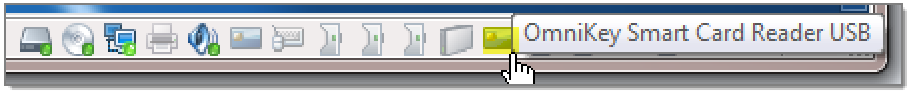
☑ Show all USB input devices

☑ Share Bluetooth devices with the virtual machine

- USB license dongle pass through:

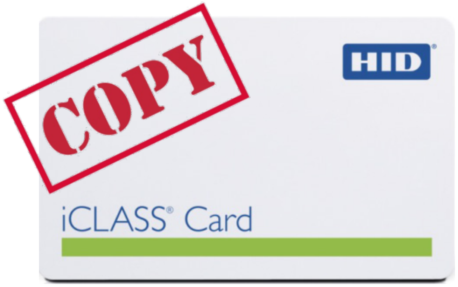


- Omnikey USB pass through:



iCLASS Cloner

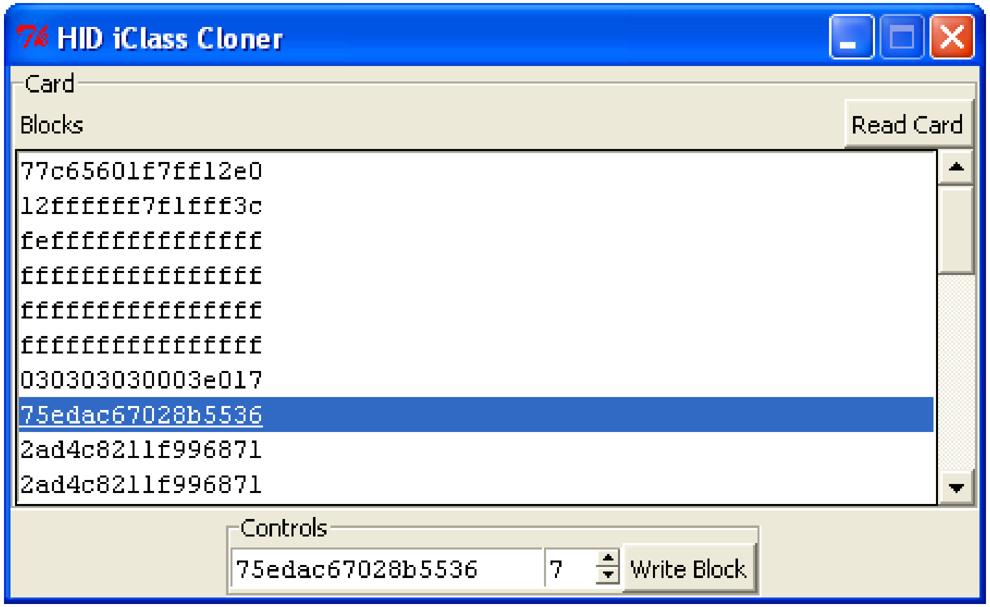
NEW – Bishop Fox – FREE Edition



UPDATE

Read / Write to HID iCLASS Cards:

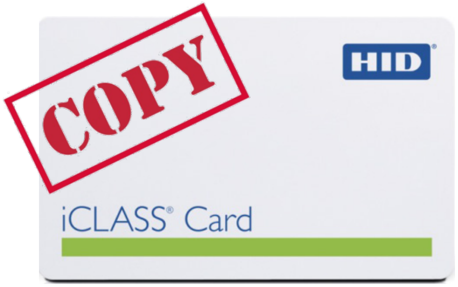
- https://blog.kchung.co/reverse-engineering-hid-iclass-master-keys/
- https://github.com/ColdHeat/iclass



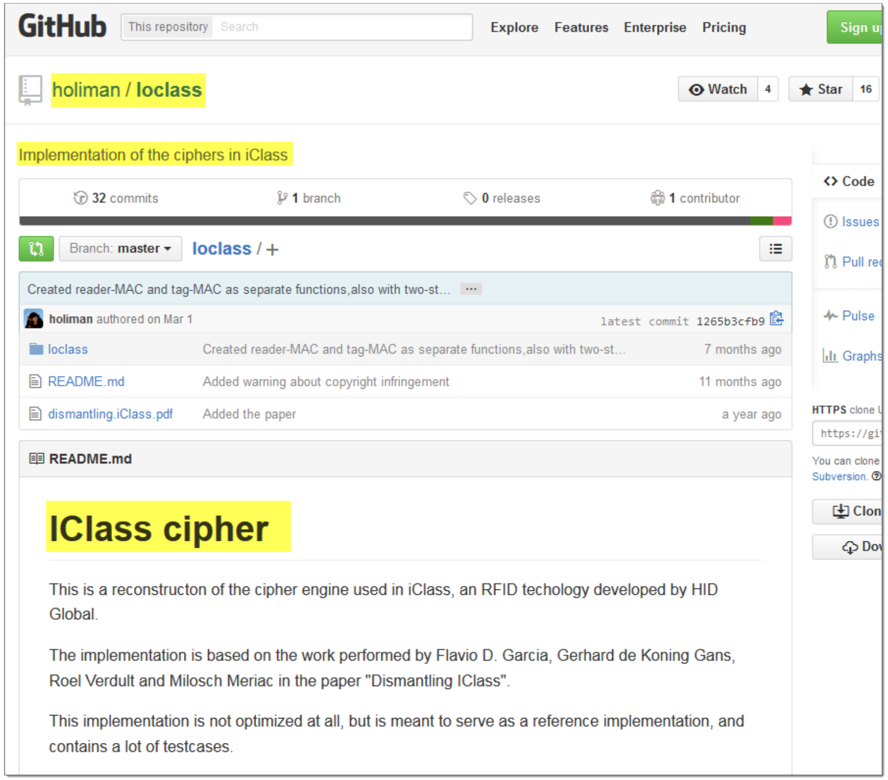
```
77c65601f7ff12e0
12ffffff7f1fff3c
feffffffffffffff
ffffffffffffffff
ffffffffffffffff
ffffffffffffffff
030303030003e017
75edac67028b5536
2ad4c8211f996871
2ad4c8211f996871
```

Controls: 75edac67028b5536 | 7

iCLASS Cloning



Ioclass – Implementation of iCLASS Ciphers



holiman / loclass

Implementation of the ciphers in iClass

32 commits | 1 branch | 0 releases | 1 contributor

Branch: master ▾ loclass / +

Created reader-MAC and tag-MAC as separate functions,also with two-st… …

holiman authored on Mar 1 latest commit 1265b3cfb9

loclass	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
README.md	Added warning about copyright infringement	11 months ago
dismantling.iClass.pdf	Added the paper	a year ago

HTTPS clone

https://gi

You can clone
Subversion.

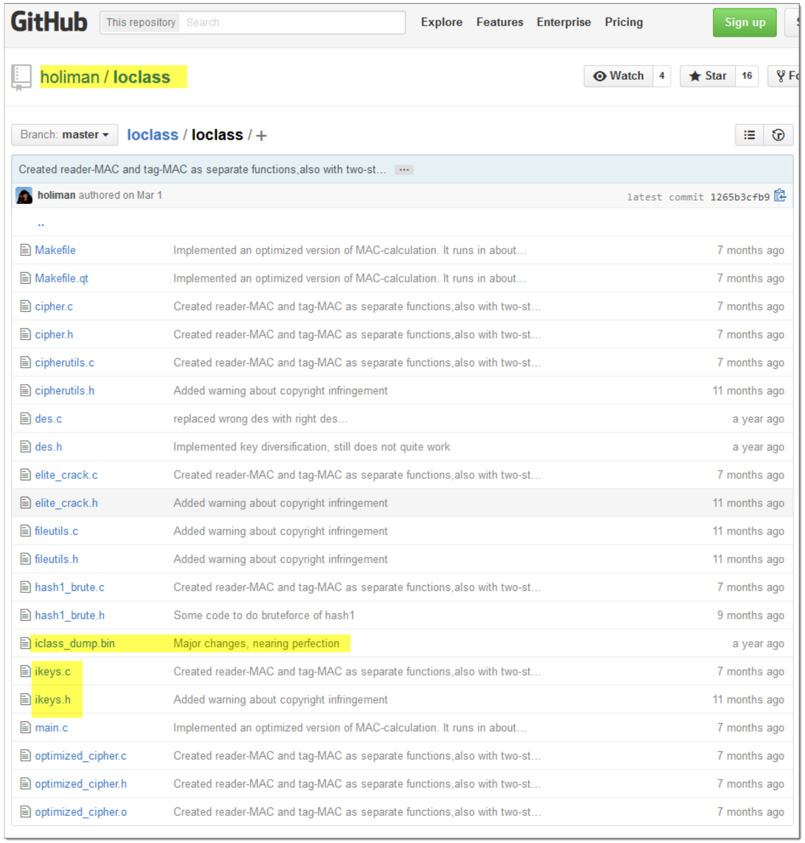
README.md

IClass cipher

This is a reconstructon of the cipher engine used in iClass, an RFID techology developed by HID Global.

The implementation is based on the work performed by Flavio D. Garcia, Gerhard de Koning Gans, Roel Verdult and Milosch Meriac in the paper "Dismantling IClass".

This implementation is not optimized at all, but is meant to serve as a reference implementation, and contains a lot of testcases.



holiman / loclass

Branch: master ▾ loclass / loclass / +

Created reader-MAC and tag-MAC as separate functions,also with two-st… …

holiman authored on Mar 1 latest commit 1265b3cfb9

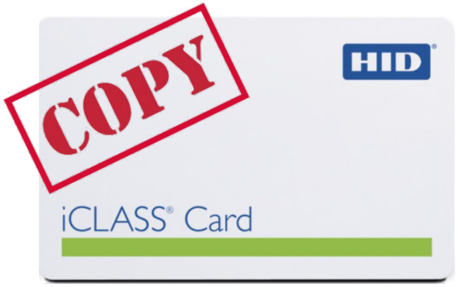
..

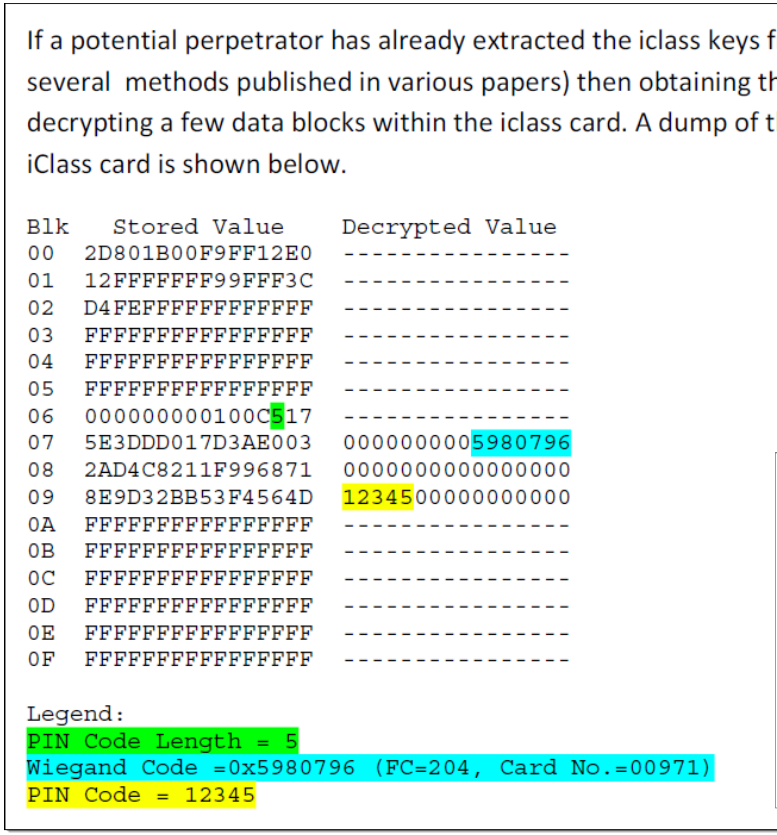
Makefile	Implemented an optimized version of MAC-calculation. It runs in about…	7 months ago
Makefile.qt	Implemented an optimized version of MAC-calculation. It runs in about…	7 months ago
cipher.c	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
cipher.h	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
cipherutils.c	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
cipherutils.h	Added warning about copyright infringement	11 months ago
des.c	replaced wrong des with right des…	a year ago
des.h	Implemented key diversification, still does not quite work	a year ago
elite_crack.c	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
elite_crack.h	Added warning about copyright infringement	11 months ago
fileutils.c	Added warning about copyright infringement	11 months ago
fileutils.h	Added warning about copyright infringement	11 months ago
hash1_brute.c	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
hash1_brute.h	Some code to do bruteforce of hash1	9 months ago
iclass_dump.bin	Major changes, nearing perfection	a year ago
ikeys.c	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
ikeys.h	Added warning about copyright infringement	11 months ago
main.c	Implemented an optimized version of MAC-calculation. It runs in about…	7 months ago
optimized_cipher.c	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
optimized_cipher.h	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago
optimized_cipher.o	Created reader-MAC and tag-MAC as separate functions,also with two-st…	7 months ago

- http://martin.swende.se/blog/Elite-Hacking.html
- https://github.com/holiman/loclass

bioCLASS Bypass

FINGERPRINT AND PIN





If a potential perpetrator has already extracted the iclass keys from an iClass reader (using one of several methods published in various papers) then obtaining the PIN is as simple as reading and decrypting a few data blocks within the iclass card. A dump of the first sixteen data blocks of a typical iClass card is shown below.

```
Blk   Stored Value      Decrypted Value
00   2D801B00F9FF12E0   ----------------
01   12FFFFFFF99FFF3C   ----------------
02   D4FEFFFFFFFFFFFF   ----------------
03   FFFFFFFFFFFFFFFF   ----------------
04   FFFFFFFFFFFFFFFF   ----------------
05   FFFFFFFFFFFFFFFF   ----------------
06   000000000100C517   ----------------
07   5E3DDD017D3AE003   0000000005980796
08   2AD4C8211F996871   0000000000000000
09   8E9D32BB53F4564D   1234500000000000
0A   FFFFFFFFFFFFFFFF   ----------------
0B   FFFFFFFFFFFFFFFF   ----------------
0C   FFFFFFFFFFFFFFFF   ----------------
0D   FFFFFFFFFFFFFFFF   ----------------
0E   FFFFFFFFFFFFFFFF   ----------------
0F   FFFFFFFFFFFFFFFF   ----------------

Legend:
PIN Code Length = 5
Wiegand Code =0x5980796 (FC=204, Card No.=00971)
PIN Code = 12345
```

HID iCLASS - RWKLB575 - Biometric Keypad Reader / Writer

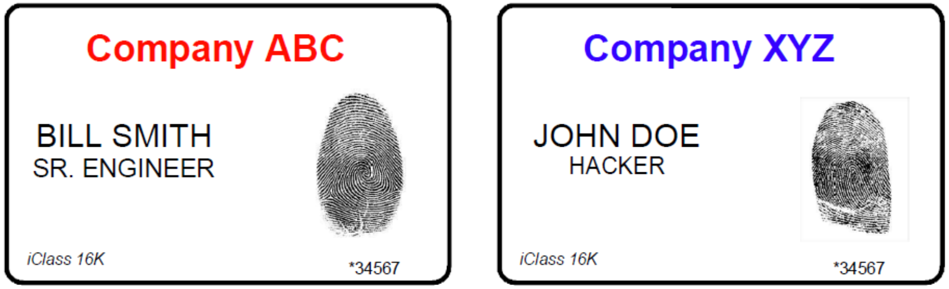
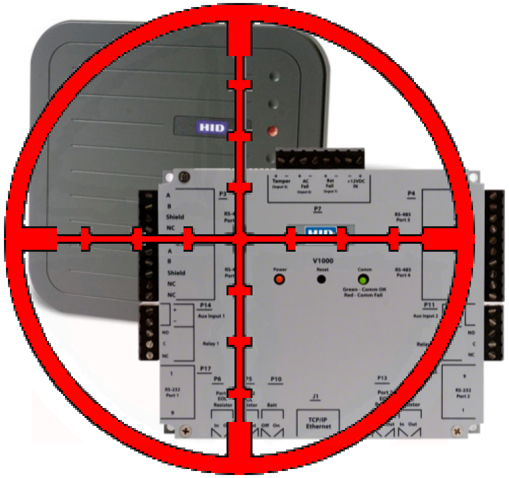


Figure 4. Different cards, yet they are considered identical from the bioCLASS reader and backend controller perspective.

BISHOP FOX

Proxclone.com - HID_bioCLASS-Enhanced_Security_or_Costly_Placebo - 27Mar2013
http://www.proxclone.com/pdfs/HID_bioCLASS-Enhanced_Security_or_Costly_Placebo.pdf

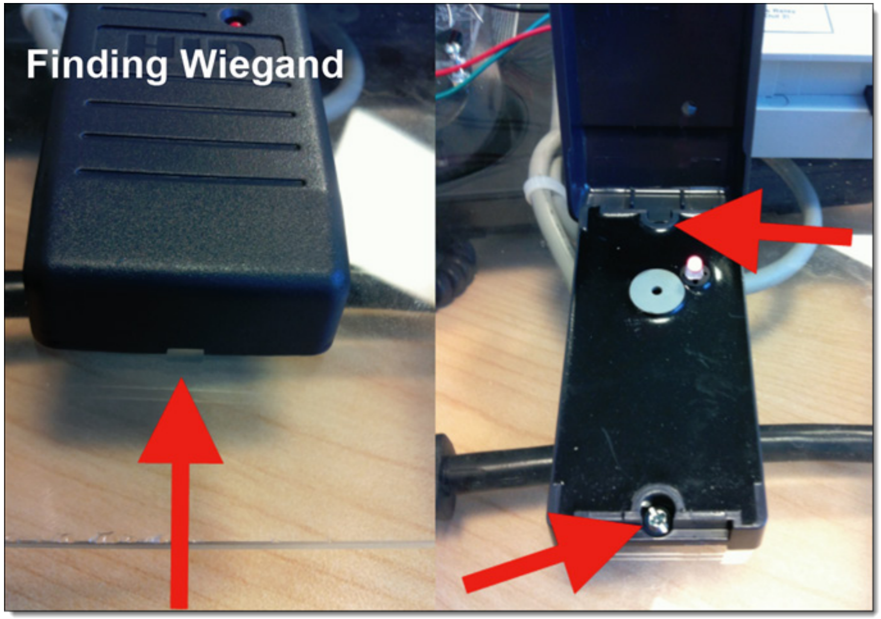


Reader and Controller Attacks

DIRECT APPROACH

Reader Attacks

JACKED IN



- Dump private keys, valid badge info, and more in few seconds
- Plant backdoor devices in reader
- Brute-force badge numbers over the wire via Wiegand (5x faster)

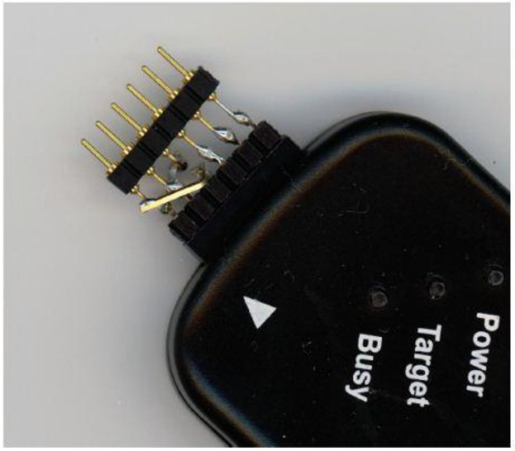
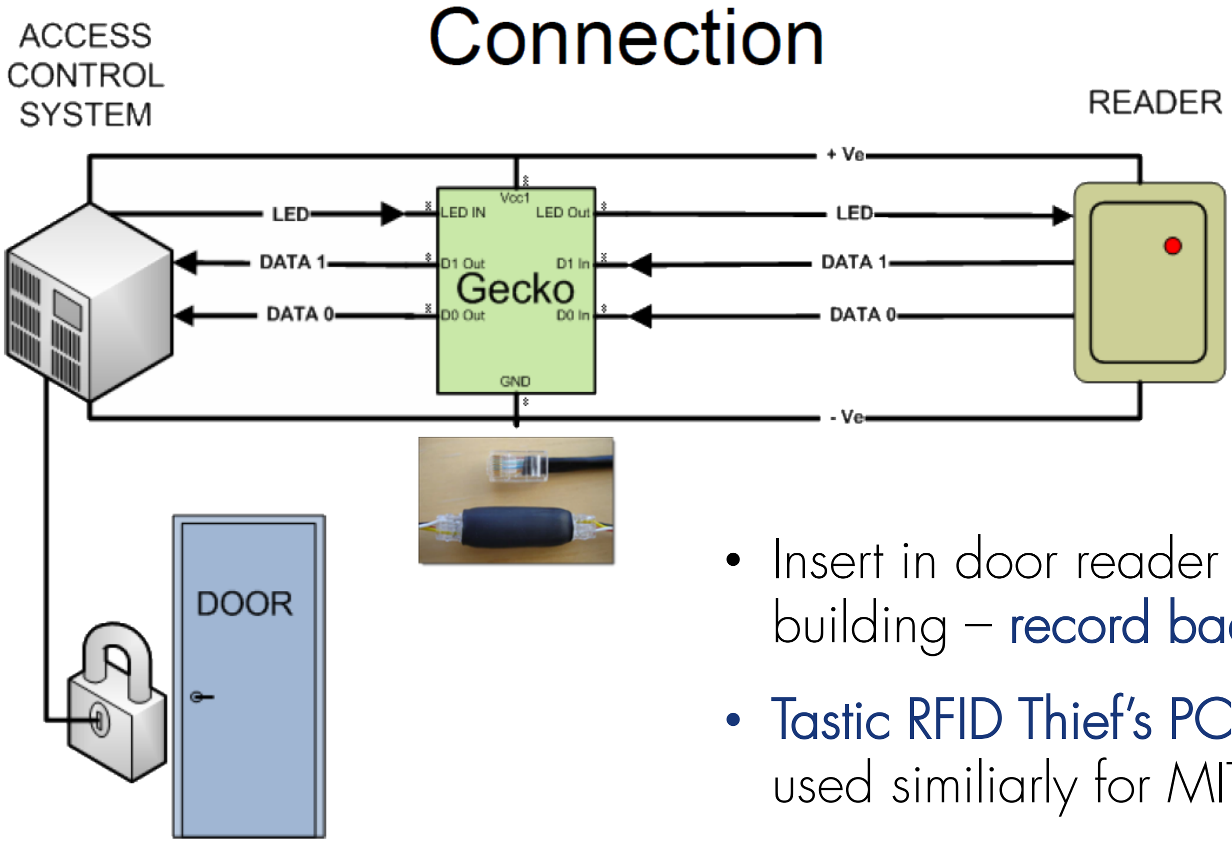


Fig. 3. Programming interface adapter for PICkit2 to switch Pin 1 with Pin 3.

Reader Attacks

GECKO–MITM ATTACK

Never publicly released

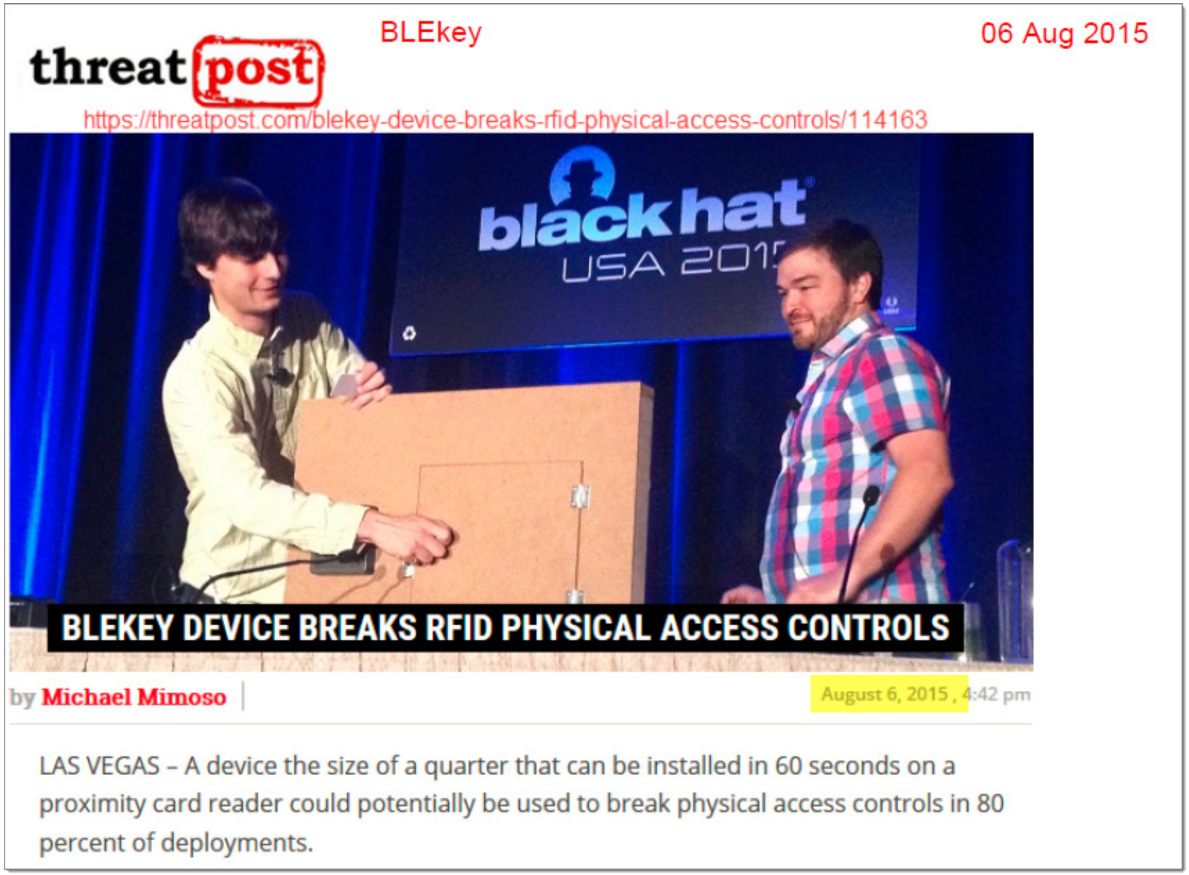


- Insert in door reader of target building – record badge #s
- Tastic RFID Thief's PCB could be used similiarly for MITM attack

Black Hat D.C. 2008 - Biometric and Token-Based Access Control Systems - Franken
http://www.blackhat.com/presentations/bh-dc-08/Franken/Presentation/bh-dc-08-franken.pdf

Reader Attacks

BLEKEY–MITM ATTACK



threatpost

BLEkey

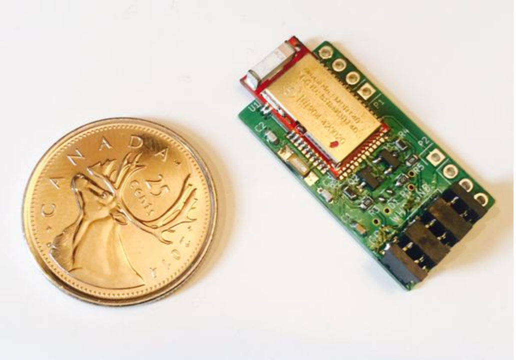
06 Aug 2015

https://threatpost.com/blekey-device-breaks-rfid-physical-access-controls/114163

BLEKEY DEVICE BREAKS RFID PHYSICAL ACCESS CONTROLS

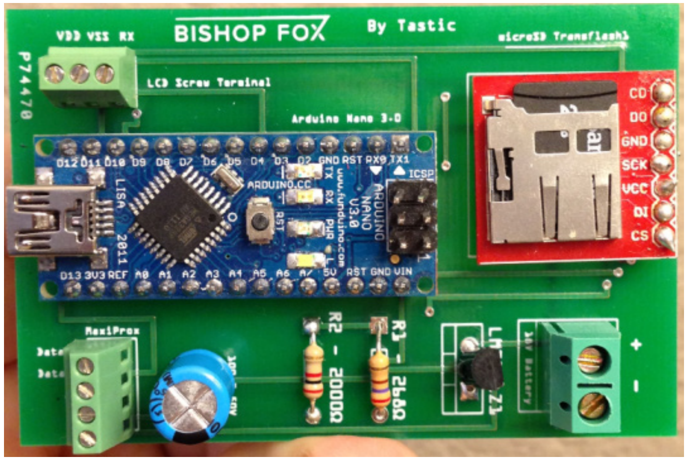
by Michael Mimoso | August 6, 2015 , 4:42 pm

LAS VEGAS – A device the size of a quarter that can be installed in 60 seconds on a proximity card reader could potentially be used to break physical access controls in 80 percent of deployments.

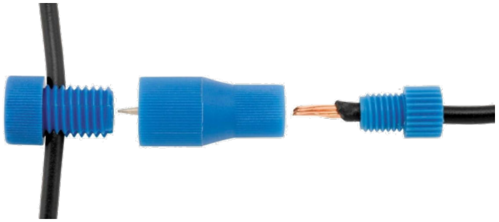


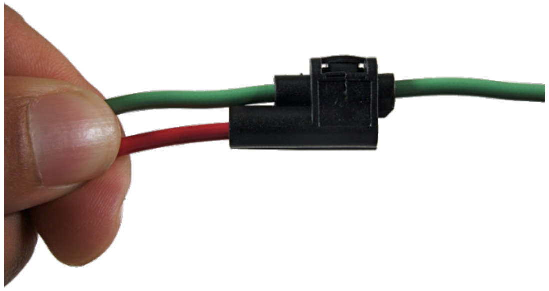
Reader Attacks

TASTIC–MITM ATTACK



+

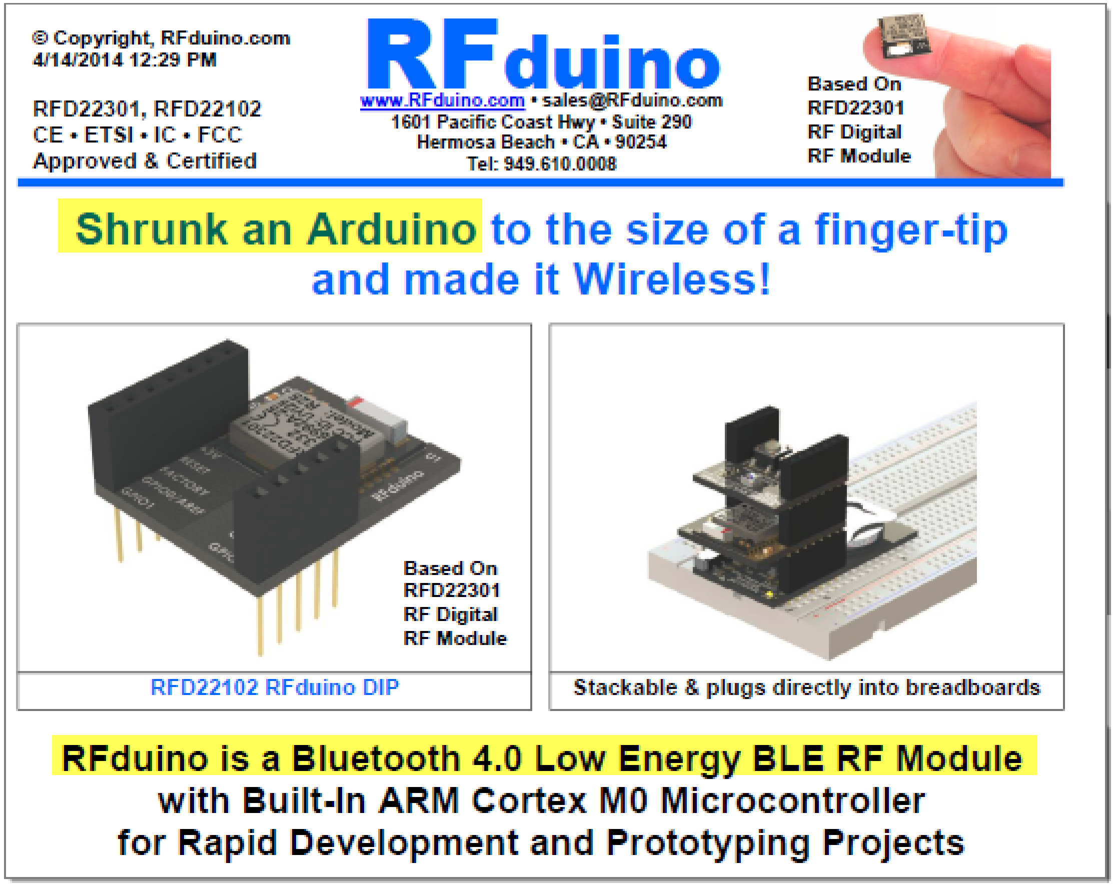




- Insert in door reader of target building – record badge #s
- Tastic RFID Thief's PCB could be used similiarly for MITM attack

Reader Attacks

TASTIC–MITM ATTACK



© Copyright, RFduino.com
4/14/2014 12:29 PM

RFD22301, RFD22102
CE • ETSI • IC • FCC
Approved & Certified

RFduino

www.RFduino.com • sales@RFduino.com
1601 Pacific Coast Hwy • Suite 290
Hermosa Beach • CA • 90254
Tel: 949.610.0008

Based On
RFD22301
RF Digital
RF Module

Shrunk an Arduino to the size of a finger-tip and made it Wireless!

Based On
RFD22301
RF Digital
RF Module

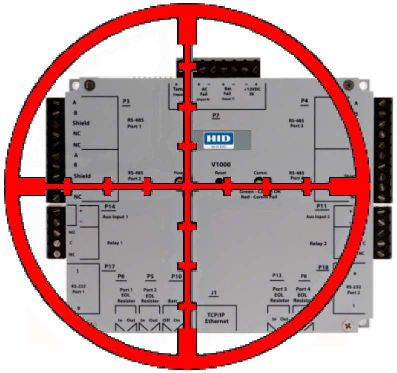
RFD22102 RFduino DIP

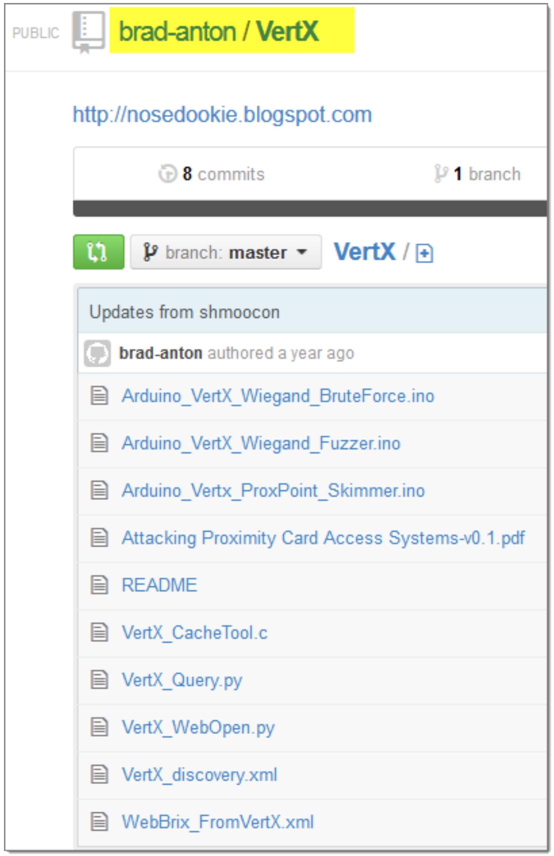
Stackable & plugs directly into breadboards

RFduino is a Bluetooth 4.0 Low Energy BLE RF Module with Built-In ARM Cortex M0 Microcontroller for Rapid Development and Prototyping Projects

Controller Attacks

JACKED IN





PUBLIC brad-anton / VertX

http://nosedookie.blogspot.com

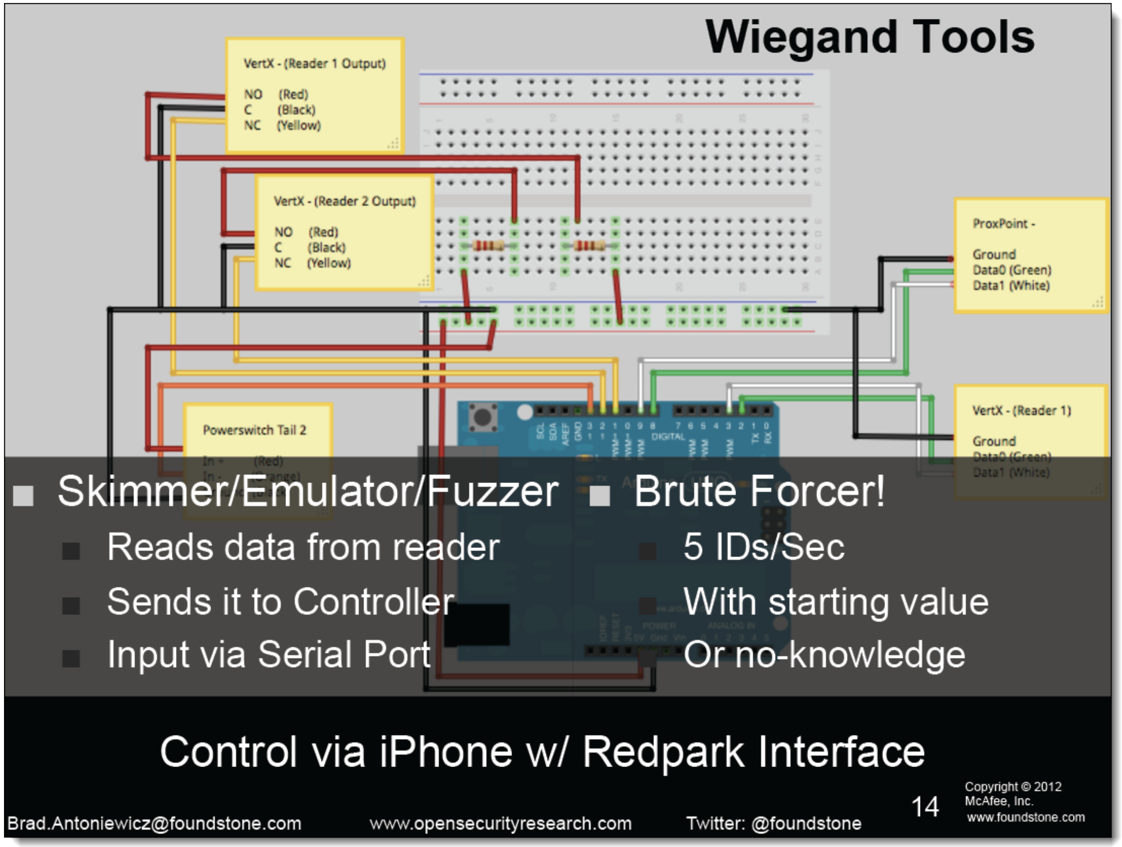
8 commits 1 branch

branch: master VertX / +

Updates from shmoocon

brad-anton authored a year ago

- Arduino_VertX_Wiegand_BruteForce.ino
- Arduino_VertX_Wiegand_Fuzzer.ino
- Arduino_Vertx_ProxPoint_Skimmer.ino
- Attacking Proximity Card Access Systems-v0.1.pdf
- README
- VertX_CacheTool.c
- VertX_Query.py
- VertX_WebOpen.py
- VertX_discovery.xml
- WebBrix_FromVertX.xml



Wiegand Tools

- Skimmer/Emulator/Fuzzer
  - Reads data from reader
  - Sends it to Controller
  - Input via Serial Port
- Brute Forcer!
  - 5 IDs/Sec
  - With starting value
  - Or no-knowledge

Control via iPhone w/ Redpark Interface

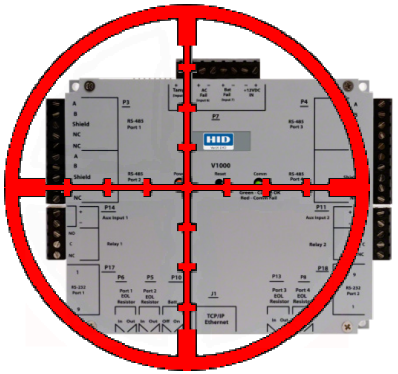
Brad.Antoniewicz@foundstone.com www.opensecurityresearch.com Twitter: @foundstone 14 Copyright © 2012 McAfee, Inc. www.foundstone.com

BISHOP FOX

Shmoocon 2012 - Attacking Proximity Card Systems - Brad Antoniewicz
http://www.shmoocon.org/2012/videos/Antoniewicsz-AttackingCardAccess.m4v

Controller Attacks

JACKED IN



RFID Reader / Controller Attack Tools – by Brad Antoniewicz

Open the Badge Reader to Attack the Controller Directly via Wiegand Interface:

- Arduino Wiegand BruteForcer – `Arduino_VertX_Wiegand_BruteForce.ino`
  - 5 IDs per Second Brute-force Badge Guessing
- Arduino Wiegand Skimmer and Emulator - `Arduino_Vertx_ProxPoint_Skimmer.ino`
- Arduino Wiegand Fuzzer - `Arduino_VertX_Wiegand_Fuzzer.ino`

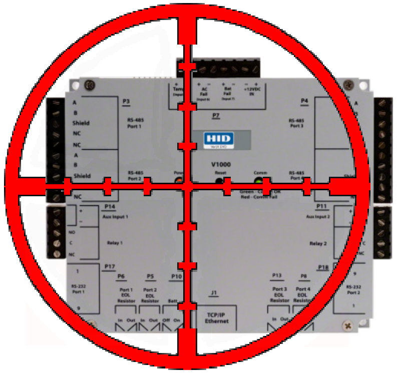
Attacking the VertX Controller Over the Network:

- `VertX_Query.py` – HID VertX Controller Discovery and Query Tool
- `VertX_WebOpen.py` – Physically Open Door via HTTP GET Request to the WebUI
- `VertX_CacheTool.c` – HID VertX V2000 Cache Dump and Insertion Tool

Shmoocon 2012 - Attacking Proximity Card Systems - Brad Antoniewicz
http://www.shmoocon.org/2012/videos/Antoniewicsz-AttackingCardAccess.m4v
http://blog.opensecurityresearch.com/2012/12/hacking-wiegand-serial-protocol.html

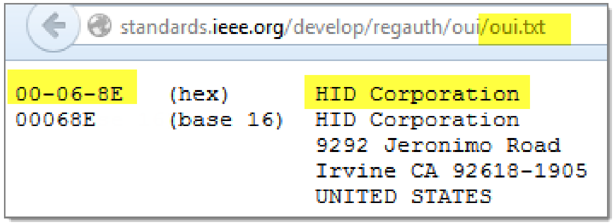
Controller Attacks

JACKED IN

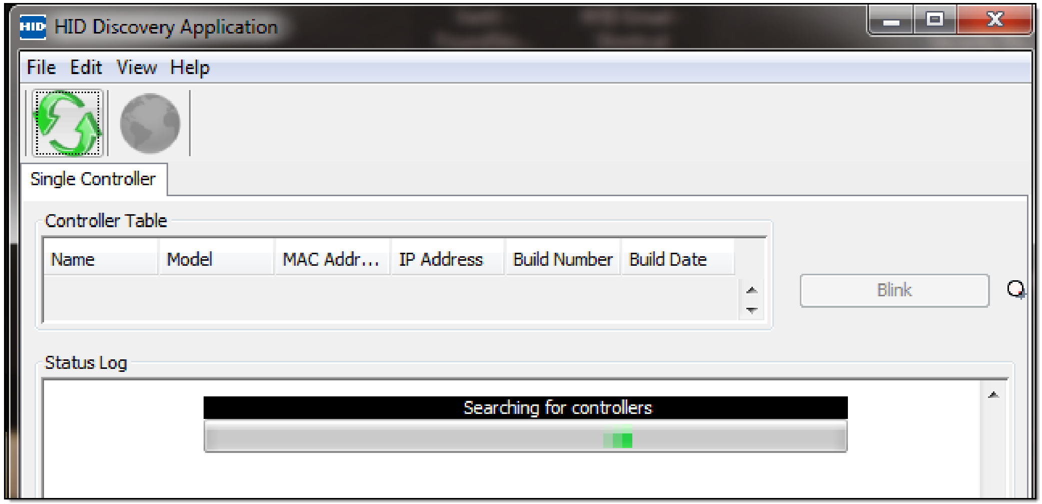


MAC Address - Targetting HID Controllers Over Network

- HID Global – MAC Address OUI: 00:06:8E:*:*:*
- Scan network for MAC Addresses starting with 00:06:8E: directly, or use HID's controller discovery GUI tool:
  - https://www.hidglobal.com/drivers/15654


standards.ieee.org/develop/regauth/oui/oui.txt

```
00-06-8E     (hex)        HID Corporation
00068E       (base 16)    HID Corporation
                          9292 Jeronimo Road
                          Irvine CA 92618-1905
                          UNITED STATES
```



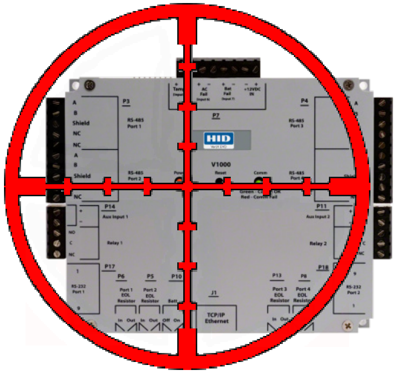
Name	Model	MAC Addr...	IP Address	Build Number	Build Date

Searching for controllers

BISHOP FOX

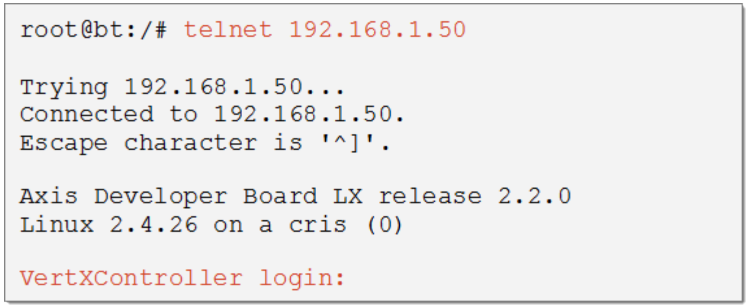
Controller Attacks

JACKED IN

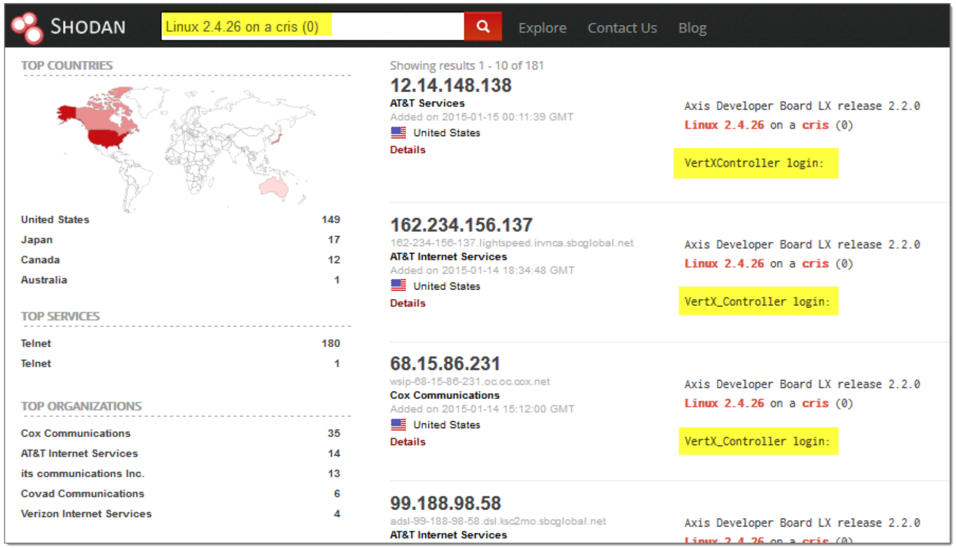


Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

- HID VertX Controller – Default Open Ports:
  - FTP (21), Telnet (23), HTTP (80)
- HID VertX Controller – Connect via FTP / Telnet / HTTP with Default Admin Creds: **`root/pass`**
- Banner grabbing for HID VertX controller discovery
  - Can also find using SHODAN search engine



```
root@bt:/# telnet 192.168.1.50

Trying 192.168.1.50...
Connected to 192.168.1.50.
Escape character is '^]'.

Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertXController login:
```



TOP COUNTRIES

United States	149
Japan	17
Canada	12
Australia	1

TOP SERVICES

Telnet	180
Telnet	1

TOP ORGANIZATIONS

Cox Communications	35
AT&T Internet Services	14
its communications Inc.	13
Covad Communications	6
Verizon Internet Services	4

Showing results 1 - 10 of 181

12.14.148.138
AT&T Services
Added on 2015-01-15 00:11:39 GMT
United States
Details

```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertXController login:
```

162.234.156.137
162-234-156-137.lightspeed.irvnca.sbcglobal.net
AT&T Internet Services
Added on 2015-01-14 18:34:48 GMT
United States
Details

```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:
```

68.15.86.231
wsip-68-15-86-231.oc.oc.cox.net
Cox Communications
Added on 2015-01-14 15:12:00 GMT
United States
Details

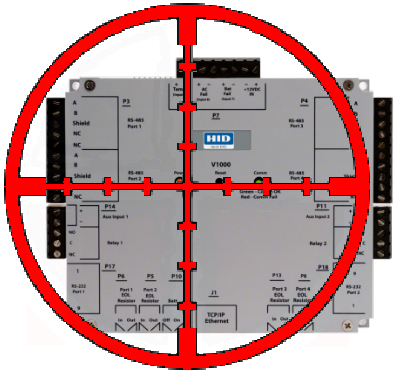
```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:
```

99.188.98.58
adsl-99-188-98-58.dsl.ksc2mo.sbcglobal.net
AT&T Internet Services

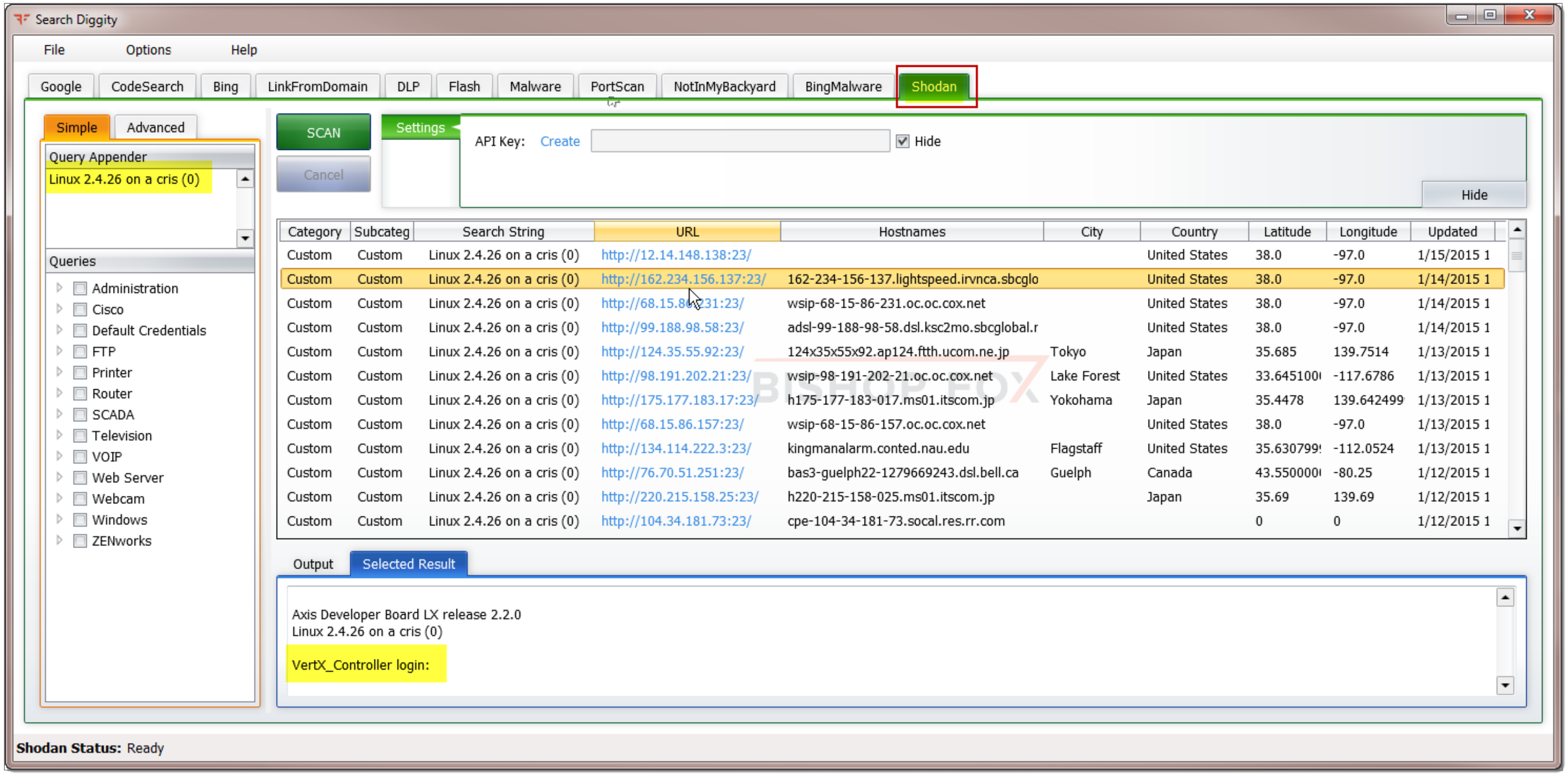
```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)
```

Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network



Query Appender: Linux 2.4.26 on a cris (0)

API Key: ☑ Hide

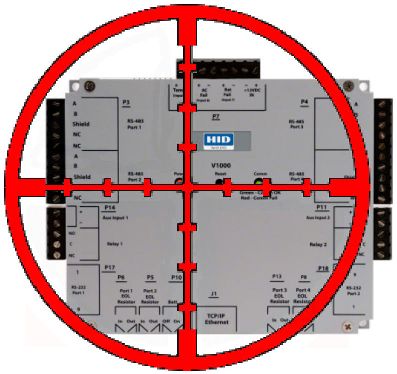
Category	Subcateg	Search String	URL	Hostnames	City	Country	Latitude	Longitude	Updated
Custom	Custom	Linux 2.4.26 on a cris (0)	http://12.14.148.138:23/			United States	38.0	-97.0	1/15/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://162.234.156.137:23/	162-234-156-137.lightspeed.irvnca.sbcglo		United States	38.0	-97.0	1/14/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://68.15.86.231:23/	wsip-68-15-86-231.oc.oc.cox.net		United States	38.0	-97.0	1/14/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://99.188.98.58:23/	adsl-99-188-98-58.dsl.ksc2mo.sbcglobal.r		United States	38.0	-97.0	1/14/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://124.35.55.92:23/	124x35x55x92.ap124.ftth.ucom.ne.jp	Tokyo	Japan	35.685	139.7514	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://98.191.202.21:23/	wsip-98-191-202-21.oc.oc.cox.net	Lake Forest	United States	33.645100(	-117.6786	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://175.177.183.17:23/	h175-177-183-017.ms01.itscom.jp	Yokohama	Japan	35.4478	139.642499	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://68.15.86.157:23/	wsip-68-15-86-157.oc.oc.cox.net		United States	38.0	-97.0	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://134.114.222.3:23/	kingmanalarm.conted.nau.edu	Flagstaff	United States	35.630799!	-112.0524	1/13/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://76.70.51.251:23/	bas3-guelph22-1279669243.dsl.bell.ca	Guelph	Canada	43.550000(	-80.25	1/12/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://220.215.158.25:23/	h220-215-158-025.ms01.itscom.jp		Japan	35.69	139.69	1/12/2015 1
Custom	Custom	Linux 2.4.26 on a cris (0)	http://104.34.181.73:23/	cpe-104-34-181-73.socal.res.rr.com			0	0	1/12/2015 1

```
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:
```

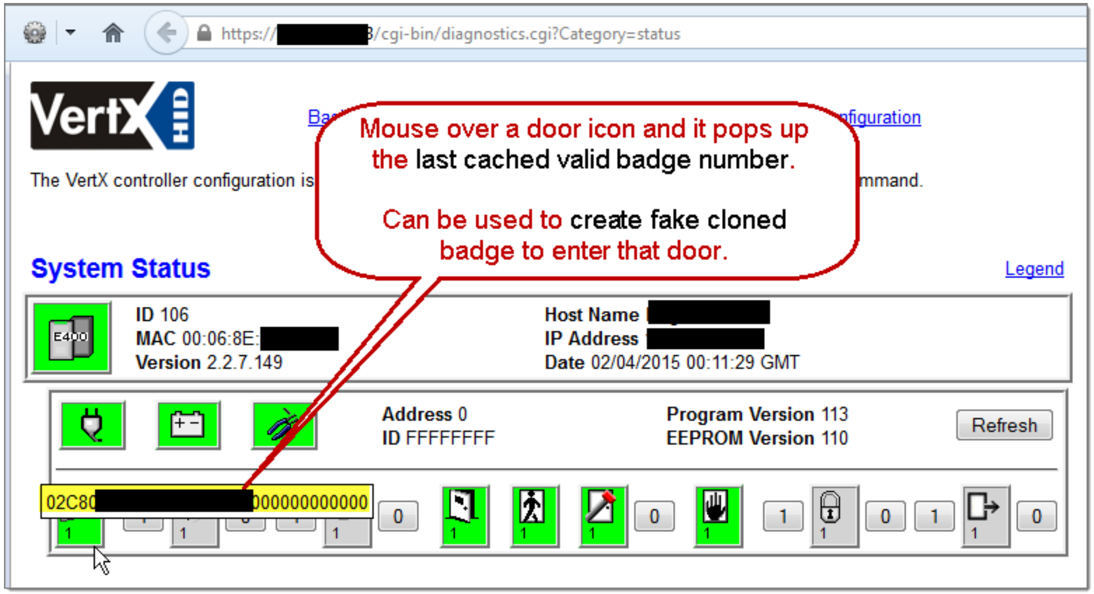
Shodan Status: Ready

Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network



https://[redacted]/cgi-bin/diagnostics.cgi?Category=status

Ba nfiguration

The VertX controller configuration is mmand.

Mouse over a door icon and it pops up the last cached valid badge number.

Can be used to create fake cloned badge to enter that door.

System Status

Legend

ID 106
MAC 00:06:8E:[redacted]
Version 2.2.7.149

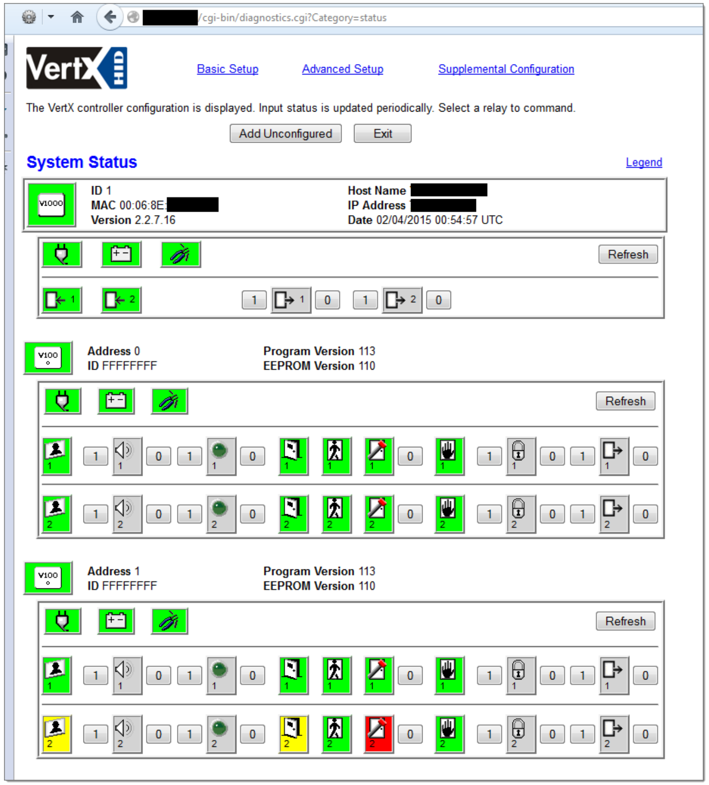
Host Name [redacted]
IP Address [redacted]
Date 02/04/2015 00:11:29 GMT

Address 0
ID FFFFFFFF

Program Version 113
EEPROM Version 110

Refresh

02C80[redacted]000000000000



[redacted]/cgi-bin/diagnostics.cgi?Category=status

Basic Setup   Advanced Setup   Supplemental Configuration

The VertX controller configuration is displayed. Input status is updated periodically. Select a relay to command.

Add Unconfigured   Exit

System Status

Legend

ID 1
MAC 00:06:8E:[redacted]
Version 2.2.7.16

Host Name [redacted]
IP Address [redacted]
Date 02/04/2015 00:54:57 UTC

Refresh

Address 0
ID FFFFFFFF

Program Version 113
EEPROM Version 110

Refresh

Address 1
ID FFFFFFFF

Program Version 113
EEPROM Version 110

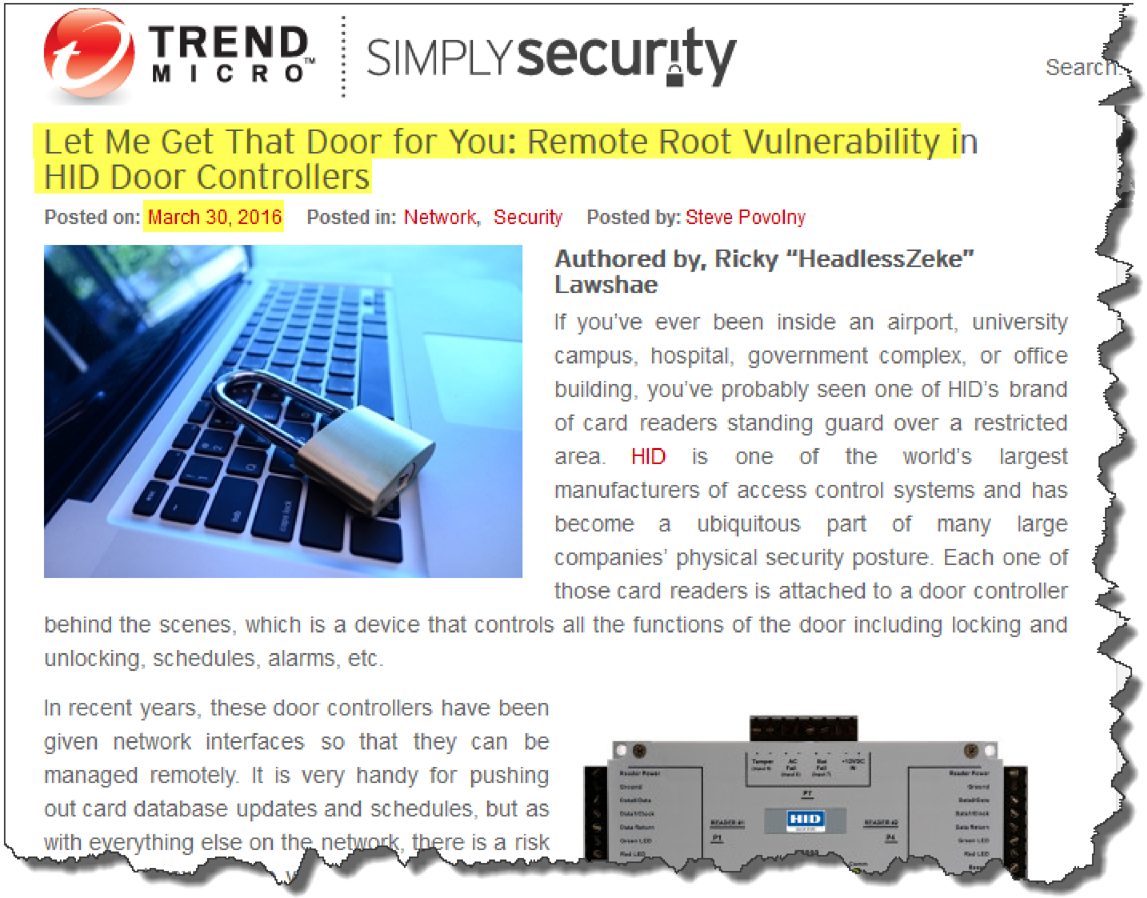
Refresh

BISHOP FOX

Controller Attacks

JACKED IN

Mar 2016



TREND MICRO | SIMPLYsecurity

Search

Let Me Get That Door for You: Remote Root Vulnerability in HID Door Controllers

Posted on: March 30, 2016 Posted in: Network, Security Posted by: Steve Povolny

Authored by, Ricky "HeadlessZeke" Lawshae

If you've ever been inside an airport, university campus, hospital, government complex, or office building, you've probably seen one of HID's brand of card readers standing guard over a restricted area. HID is one of the world's largest manufacturers of access control systems and has become a ubiquitous part of many large companies' physical security posture. Each one of those card readers is attached to a door controller behind the scenes, which is a device that controls all the functions of the door including locking and unlocking, schedules, alarms, etc.

In recent years, these door controllers have been given network interfaces so that they can be managed remotely. It is very handy for pushing out card database updates and schedules, but as with everything else on the network, there is a risk

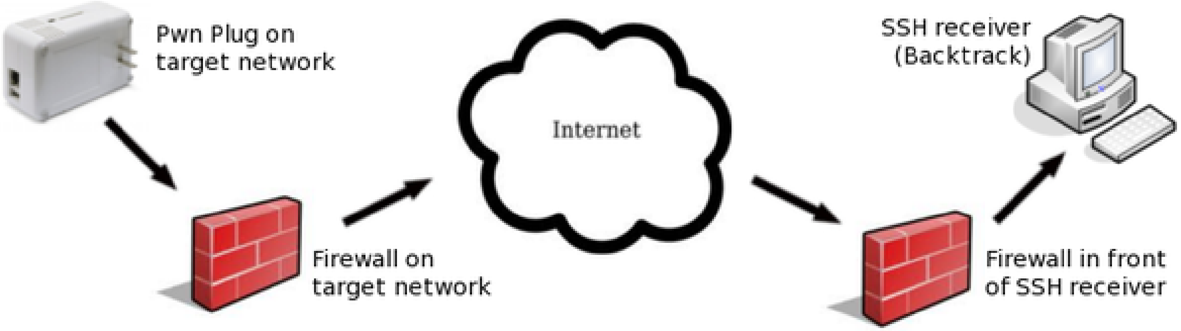
Backdoors and Other Fun

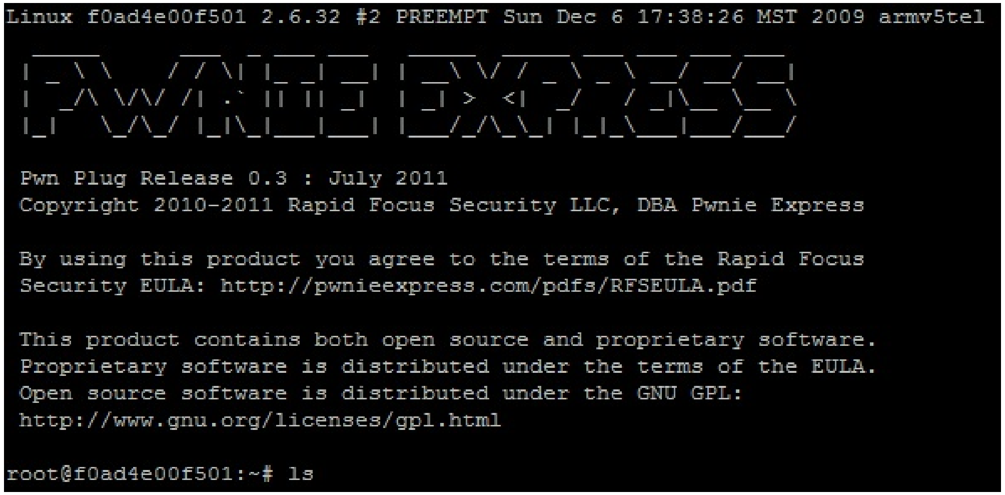
LITTLE DIFFERENCES

Pwn Plug

MAINTAINING ACCESS

THE Pwn Plug.
The Industry's First Commercial Pentesting Drop Box.
Air Freshener?
Printer PSU? ...nope
FEATURES:
Covert tunneling
SSH access over 3G/GSM cell networks
NAC/802.1x bypass
and more!
Discover the glory of Universal Plug & Pwn
PWNIE EXPRESS
@pwnieexpress.com


Pwn Plug on target network
Firewall on target network
Internet
Firewall in front of SSH receiver
SSH receiver (Backtrack)



```
Linux f0ad4e00f501 2.6.32 #2 PREEMPT Sun Dec 6 17:38:26 MST 2009 armv5tel
 ___ __      ___  _ ___ ___   _____  _____ ___ ___ ___ 
| _ \\ \    / / \| |_ _| __| | __\ \/ / _ \ _ \ __/ __/ __|
|  _/ \ \/\/ /| .` || || _|  | _| >  <|  _/   / _|\__ \__ \
|_|    \_/\_/ |_|\_|___|___| |___/_/\_\_| |_|_\___|___/___/

 Pwn Plug Release 0.3 : July 2011
 Copyright 2010-2011 Rapid Focus Security LLC, DBA Pwnie Express

 By using this product you agree to the terms of the Rapid Focus
 Security EULA: http://pwnieexpress.com/pdfs/RFSEULA.pdf

 This product contains both open source and proprietary software.
 Proprietary software is distributed under the terms of the EULA.
 Open source software is distributed under the GNU GPL:
 http://www.gnu.org/licenses/gpl.html

root@f0ad4e00f501:~# ls
```

Pwn Plug

MAINTAINING ACCESS

- Pwn Plug Elite: $995.00
- Power Pwn: $1,995.00

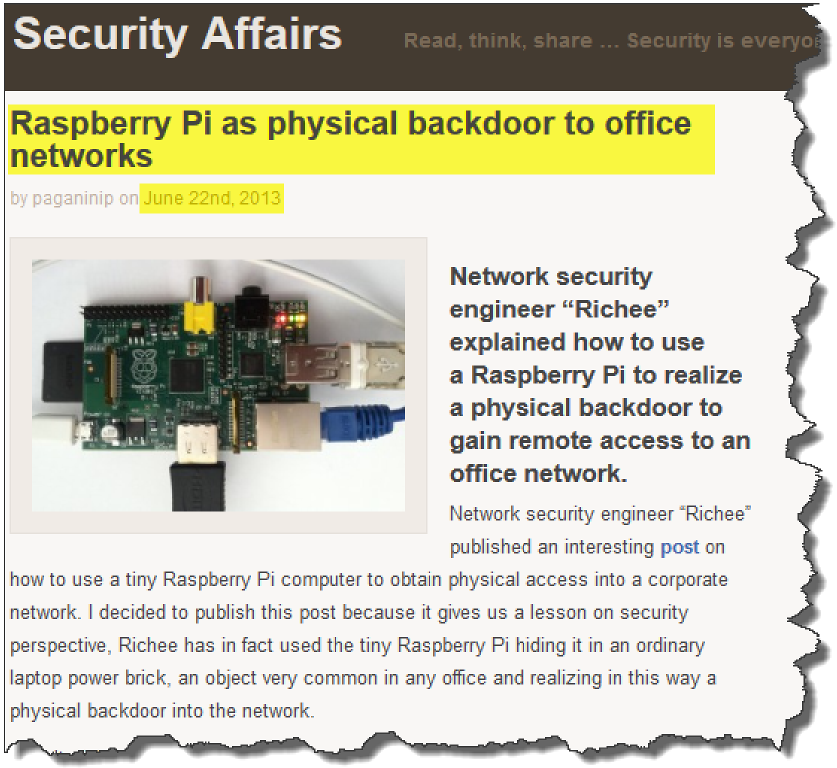
First release of Pwn Plug

New: Power Pwn

Raspberry Pi

MAINTAINING ACCESS

- Raspberry Pi - credit card sized, single-board computer – cheap $35



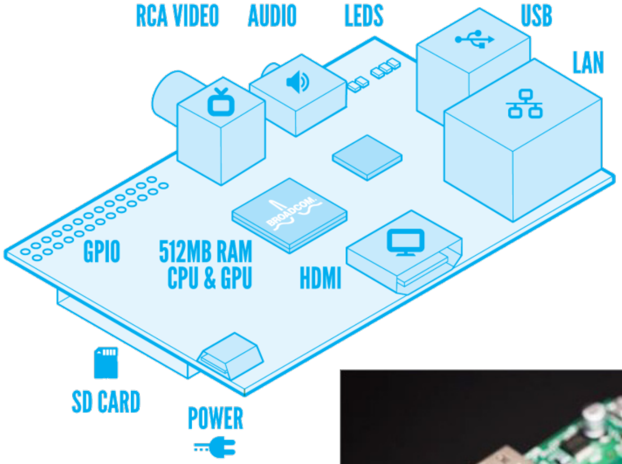
Security Affairs   Read, think, share … Security is everyo

Raspberry Pi as physical backdoor to office networks

by paganinip on June 22nd, 2013

Network security engineer "Richee" explained how to use a Raspberry Pi to realize a physical backdoor to gain remote access to an office network.

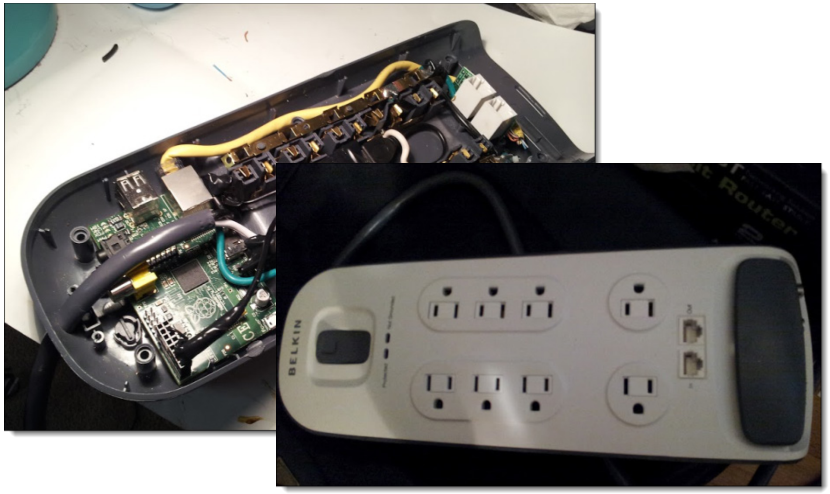
Network security engineer "Richee" published an interesting post on how to use a tiny Raspberry Pi computer to obtain physical access into a corporate network. I decided to publish this post because it gives us a lesson on security perspective, Richee has in fact used the tiny Raspberry Pi hiding it in an ordinary laptop power brick, an object very common in any office and realizing in this way a physical backdoor into the network.

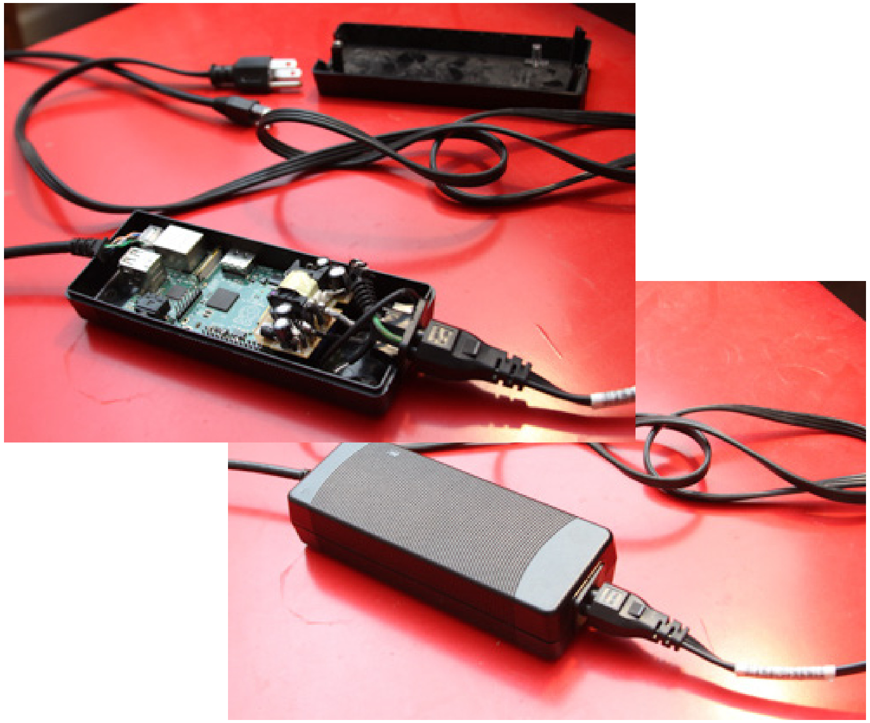


Raspberry Pi

MAINTAINING ACCESS

- Raspberry Pi – cheap alternative (~$35) to Pwn Plug/Power Pwn
  - Pwnie Express – Raspberry Pwn
  - Rogue Pi – RPi Pentesting Dropbox
  - Pwn Pi v3.0

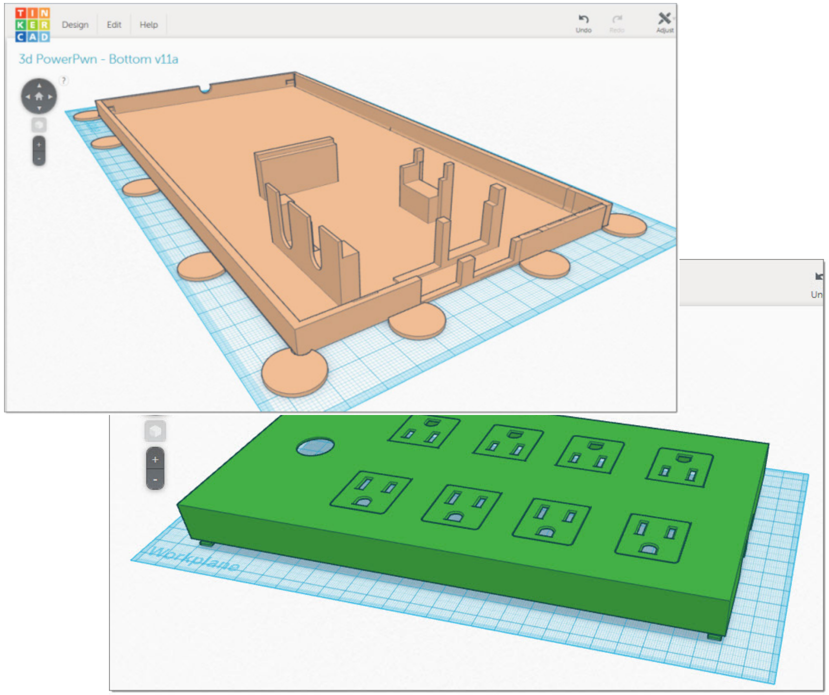


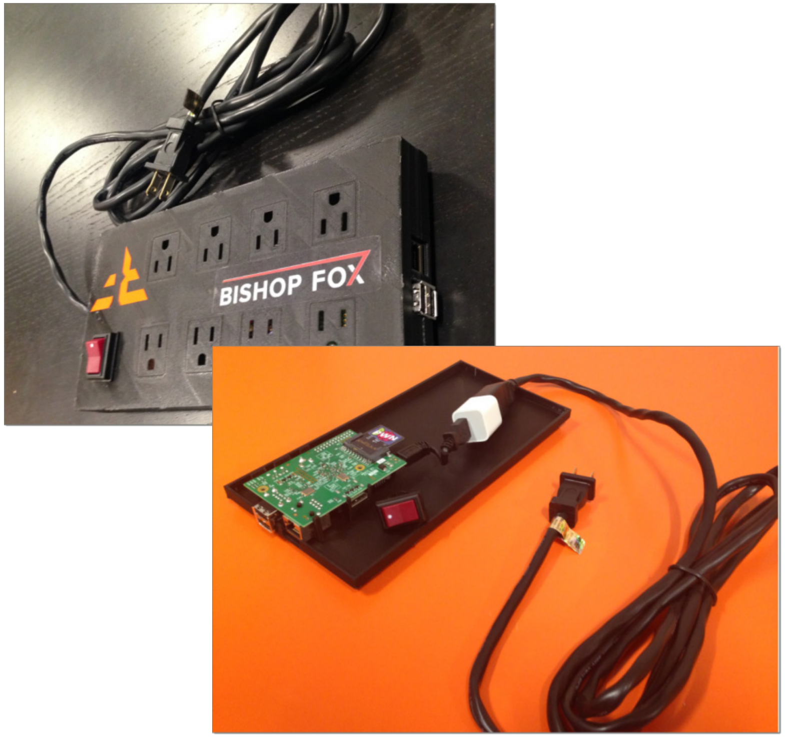


Raspberry Pi

MAINTAINING ACCESS

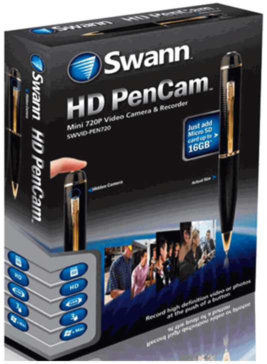
- Raspberry Pi – cheap alternative (~$35) to Pwn Plug/Power Pwn
  - Tastic 3D Case for RaspPi Backdoor Hidden Backdoor Device





Little Extra Touches

GO A LONG WAY


Swann
HD PenCam
Mini 720P Video Camera & Recorder
SWVID-PEN720
Just add Micro SD card up to 16GB

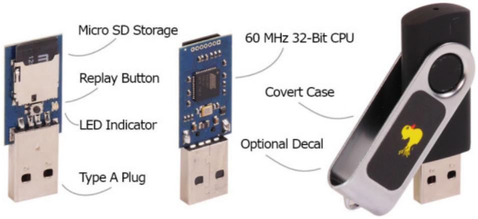
HD PenCam - Mini 720p Video

Lock picks and pick guns

Fake polo shirts for target company
(get logo from target website)

[redacted]

[redacted]



USB Rubber Ducky Delux

[redacted]

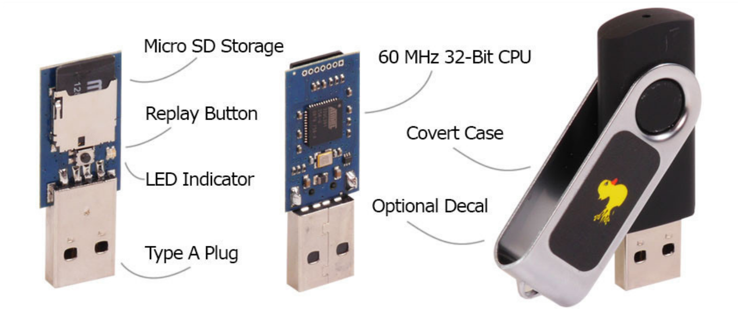
[redacted]

Label Printer and Badge Accessories

Fargo DTC515 Full Color ID Card ID Badge Printer

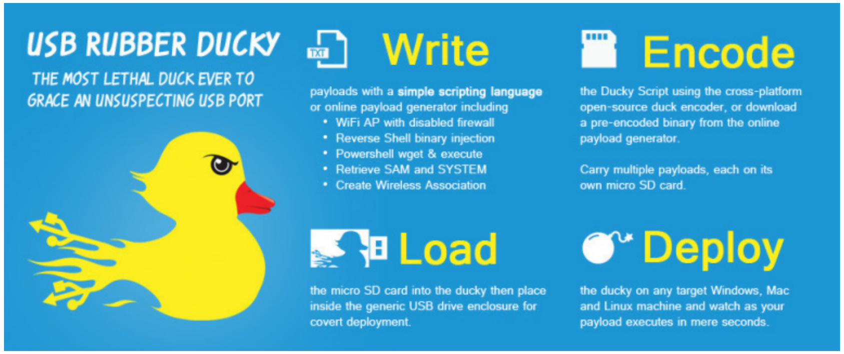
USB Rubber Ducky Delux

QUICK PHYSICAL OWNAGE



"If it quacks like a keyboard and types like a keyboard, it must be a keyboard."

"Humans use keyboards, and computers trust humans."



Write

payloads with a **simple scripting language** or online payload generator including

- WiFi AP with disabled firewall
- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

Encode

the Ducky Script using the cross-platform open-source duck encoder, or download a pre-encoded binary from the online payload generator.

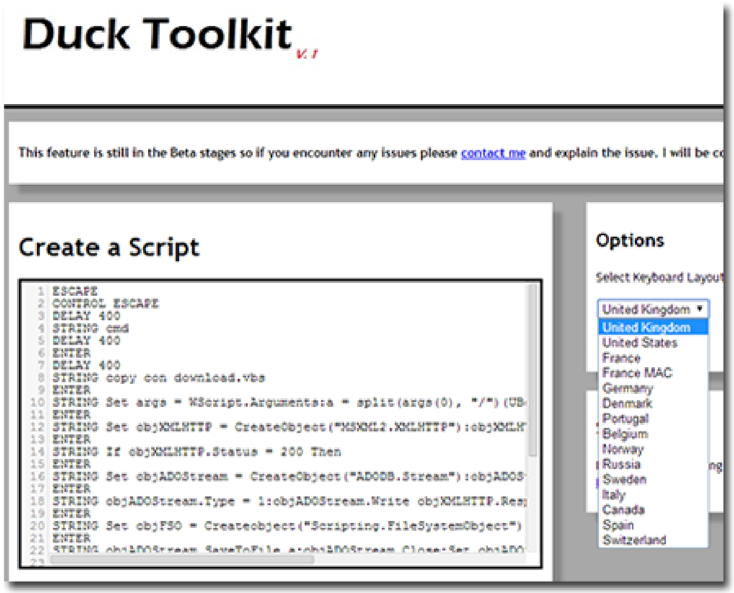
Carry multiple payloads, each on its own micro SD card.

Load

the micro SD card into the ducky then place inside the generic USB drive enclosure for covert deployment.

Deploy

the ducky on any target Windows, Mac and Linux machine and watch as your payload executes in mere seconds.



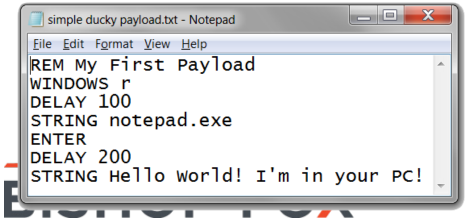
This feature is still in the Beta stages so if you encounter any issues please contact me and explain the issue. I will be co

Create a Script

```
ESCAPE
CONTROL ESCAPE
DELAY 400
STRING cmd
DELAY 400
ENTER
DELAY 400
STRING copy con download.vbs
ENTER
STRING Set args = WScript.Arguments:a = split(args(0), "/")(UB
ENTER
STRING Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP"):objXMLH
ENTER
STRING If objXMLHTTP.Status = 200 Then
ENTER
STRING Set objADOStream = CreateObject("ADODB.Stream"):objADOS
ENTER
STRING objADOStream.Type = 1:objADOStream.Write objXMLHTTP.Res
ENTER
STRING Set objFSO = Createobject("Scripting.FileSystemObject")
ENTER
STRING objADOStream.SaveToFile a:objADOStream.Close:Set objADO
```

Options

Select Keyboard Layout: United Kingdom


simple ducky payload.txt - Notepad
File Edit Format View Help

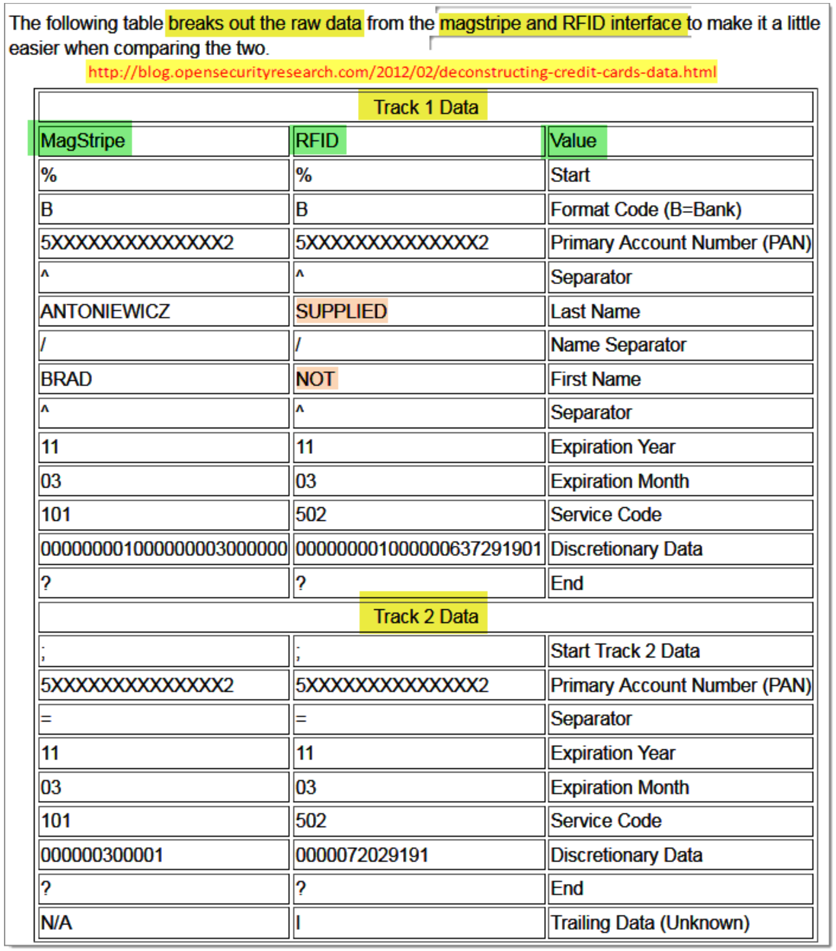
```
REM My First Payload
WINDOWS r
DELAY 100
STRING notepad.exe
ENTER
DELAY 200
STRING Hello World! I'm in your PC!
```

Credit Cards

CONTACTLESS PAYMENTS

Credit Card RFID

NFC



The following table breaks out the raw data from the magstripe and RFID interface to make it a little easier when comparing the two.

http://blog.opensecurityresearch.com/2012/02/deconstructing-credit-cards-data.html

	Track 1 Data	
MagStripe	RFID	Value
%	%	Start
B	B	Format Code (B=Bank)
5XXXXXXXXXXXXXX2	5XXXXXXXXXXXXXX2	Primary Account Number (PAN)
^	^	Separator
ANTONIEWICZ	SUPPLIED	Last Name
/	/	Name Separator
BRAD	NOT	First Name
^	^	Separator
11	11	Expiration Year
03	03	Expiration Month
101	502	Service Code
0000000010000000003000000	0000000010000000637291901	Discretionary Data
?	?	End
	Track 2 Data	
;	;	Start Track 2 Data
5XXXXXXXXXXXXXX2	5XXXXXXXXXXXXXX2	Primary Account Number (PAN)
=	=	Separator
11	11	Expiration Year
03	03	Expiration Month
101	502	Service Code
000000300001	0000072029191	Discretionary Data
?	?	End
N/A	I	Trailing Data (Unknown)

BISHOP FOX

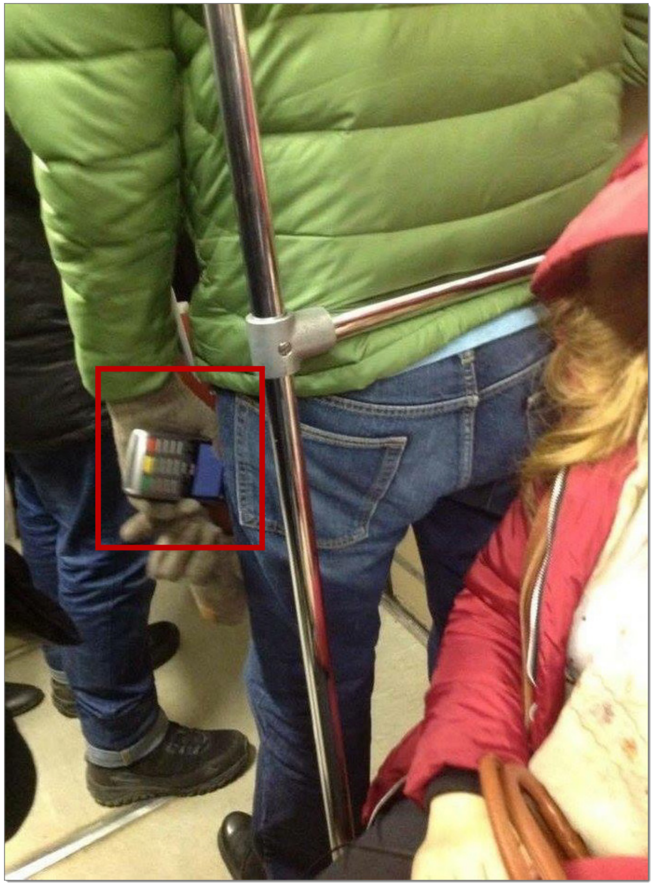
Credit Card RFID

SKIMMING

NEWS

Feb 2016

- Point of Sale (PoS) – keep under ~$30 and tap your wallet



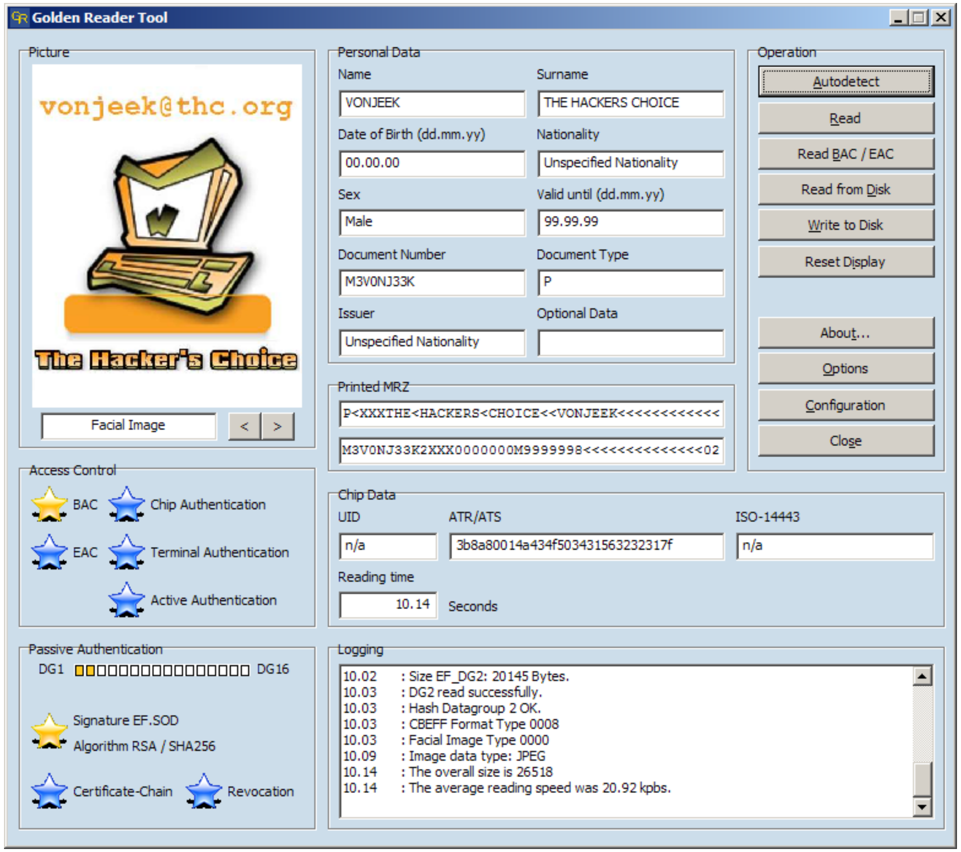
BISHOP FOX

Passports (Book)

RFID IN ID

Passport Books

RFID



Personal Data

Name: VONJEEK	Surname: THE HACKERS CHOICE
Date of Birth (dd.mm.yy): 00.00.00	Nationality: Unspecified Nationality
Sex: Male	Valid until (dd.mm.yy): 99.99.99
Document Number: M3V0NJ33K	Document Type: P
Issuer: Unspecified Nationality	Optional Data:

Printed MRZ

```
P<XXXTHE<HACKERS<CHOICE<<VONJEEK<<<<<<<<<<<<
M3V0NJ33K2XXX0000000M9999998<<<<<<<<<<<<<<02
```

Signature EF.SOD
Algorithm RSA / SHA256

Chip Data

UID: n/a
ATR/ATS: 3b8a80014a434f503431563232317f
ISO-14443: n/a
Reading time: 10.14 Seconds

Logging

```
10.02     : Size EF_DG2: 20145 Bytes.
10.03     : DG2 read successfully.
10.03     : Hash Datagroup 2 OK.
10.03     : CBEFF Format Type 0008
10.03     : Facial Image Type 0000
10.09     : Image data type: JPEG
10.14     : The overall size is 26518
10.14     : The average reading speed was 20.92 kpbs.
```

Biometric Passport Security Issues

The biometric passport has been designed to have non-traceable computer chip characteristics as well as a number of preventative technologies including *Passive Authentication* (PA) and *Active Authentication* (AA)

Table 1. *Personal data encrypted in biometric passport*

Passport Type	Date of Birth
Country Code	Sex type
Passport Number	Place of Birth
Surname	Valid from to dates
First and middle names	Country of Authority
Nationality	Signature

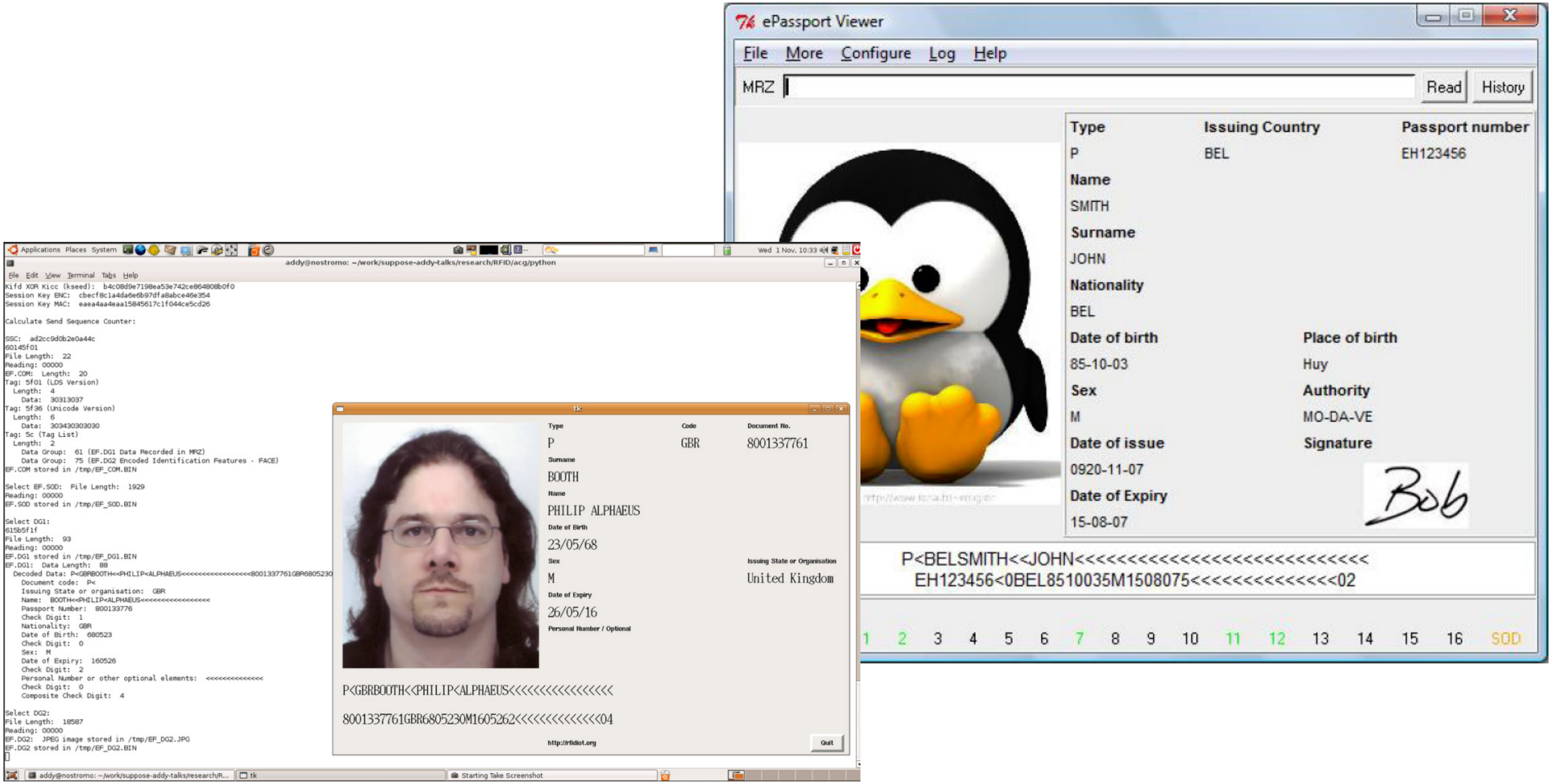
mrpkey.py

Readers: ACS HF, ACS LAHF, PCSC
TAGS: ISO-14443 ePassport/eID, JCOP JMRTD/vonJeek, NFC vonJeek

Read/Write/Clone contents of Machine Readable Travel Document.

Passport Books

RFID



ePassport Viewer
File More Configure Log Help
MRZ
Read
History

Type: P
Issuing Country: BEL
Passport number: EH123456
Name: SMITH
Surname: JOHN
Nationality: BEL
Date of birth: 85-10-03
Place of birth: Huy
Sex: M
Authority: MO-DA-VE
Date of issue: 0920-11-07
Signature: Bob
Date of Expiry: 15-08-07

```
P<BELSMITH<<JOHN<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
EH123456<0BEL8510035M1508075<<<<<<<<<<<<<<02
```

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 SOD
Applications Places System
addy@nostromo: ~/work/suppose-addy-talks/research/RFID/acg/python
File Edit View Terminal Tabs Help

```
Kifd XOR Kicc (kseed):  b4c08d9e7198ea53e742ce864808b0f0
Session Key ENC:  cbecf8c1a4da6e6b97dfa8abce46e354
Session Key MAC:  eaea4aa4eaa15845617c1f044ce5cd26

Calculate Send Sequence Counter:

SSC:  ad2cc9d0b2e0a44c
60145f01
File Length:  22
Reading: 00000
EF.COM:  Length:  20
Tag: 5f01 (LDS Version)
  Length:  4
    Data:  30313037
Tag: 5f36 (Unicode Version)
  Length:  6
    Data:  303430303030
Tag: 5c (Tag List)
  Length:  2
    Data Group:  61 (EF.DG1 Data Recorded in MRZ)
    Data Group:  75 (EF.DG2 Encoded Identification Features - FACE)
EF.COM stored in /tmp/EF_COM.BIN

Select EF.SOD:  File Length:  1929
Reading: 00000
EF.SOD stored in /tmp/EF_SOD.BIN

Select DG1:
615b5f1f
File Length:  93
Reading: 00000
EF.DG1 stored in /tmp/EF_DG1.BIN
EF.DG1:  Data Length:  88
  Decoded Data: P<GBRBOOTH<<PHILIP<ALPHAEUS<<<<<<<<<<<<<<<<<8001337761GBR6805230
    Document code:  P<
    Issuing State or organisation:  GBR
    Name:  BOOTH<<PHILIP<ALPHAEUS<<<<<<<<<<<<<<<<<
    Passport Number:  800133776
    Check Digit:  1
    Nationality:  GBR
    Date of Birth:  680523
    Check Digit:  0
    Sex:  M
    Date of Expiry:  160526
    Check Digit:  2
    Personal Number or other optional elements:  <<<<<<<<<<<<<<
    Check Digit:  0
    Composite Check Digit:  4

Select DG2:
File Length:  18587
Reading: 00000
EF.DG2:  JPEG image stored in /tmp/EF_DG2.JPG
EF.DG2 stored in /tmp/EF_DG2.BIN
```

Type: P
Code: GBR
Document No.: 8001337761
Surname: BOOTH
Name: PHILIP ALPHAEUS
Date of Birth: 23/05/68
Sex: M
Issuing State or Organisation: United Kingdom
Date of Expiry: 26/05/16
Personal Number / Optional

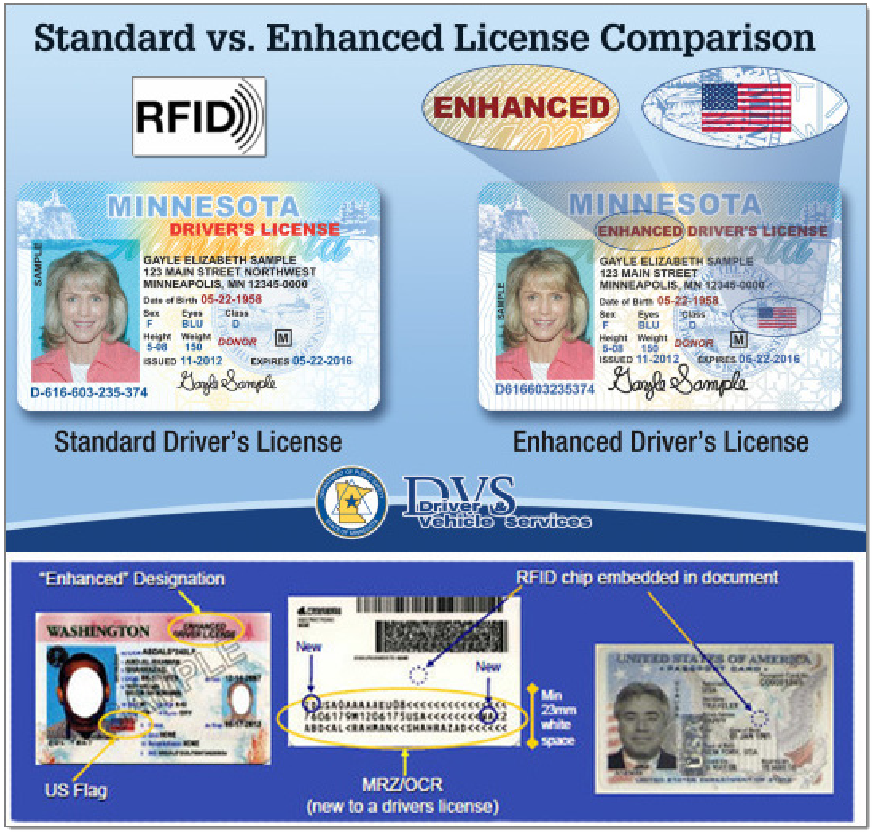
```
P<GBRBOOTH<<PHILIP<ALPHAEUS<<<<<<<<<<<<<<<<<
8001337761GBR6805230M1605262<<<<<<<<<<<<<<04
```

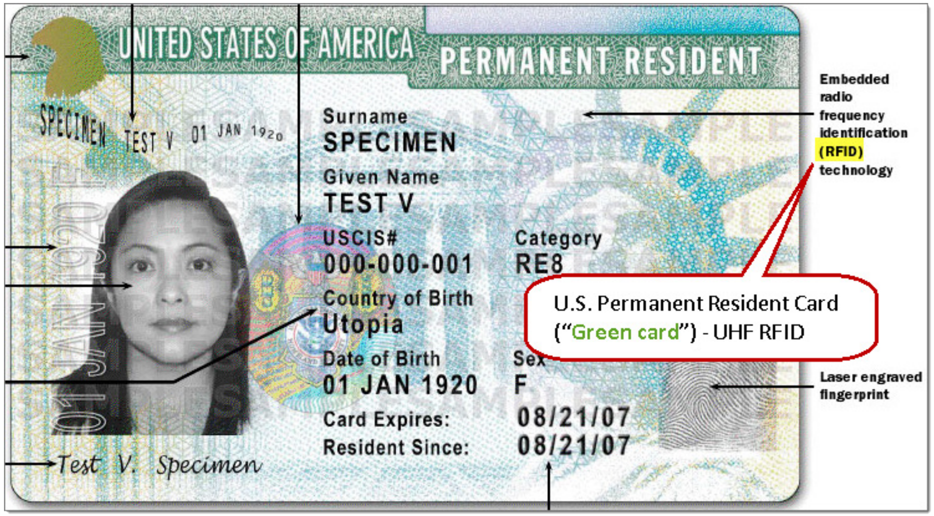
UHF Hacking

ULTRA

Enhanced Licenses

RFID

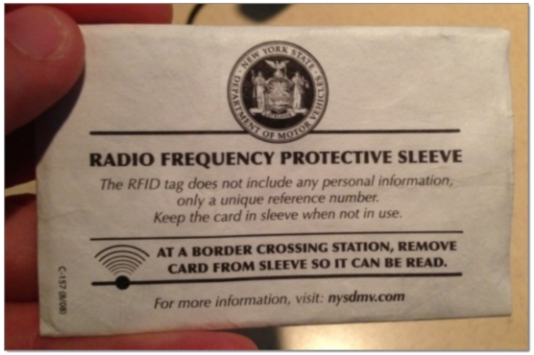

Standard vs. Enhanced License Comparison
RFID
ENHANCED
MINNESOTA
DRIVER'S LICENSE
ENHANCED DRIVER'S LICENSE
Standard Driver's License
Enhanced Driver's License
DVS Driver & Vehicle Services
"Enhanced" Designation
RFID chip embedded in document
US Flag
MRZ/OCR
(new to a drivers license)
Min 23mm white space



Embedded radio frequency identification (RFID) technology

U.S. Permanent Resident Card ("Green card") - UHF RFID

Laser engraved fingerprint



RADIO FREQUENCY PROTECTIVE SLEEVE

The RFID tag does not include any personal information, only a unique reference number. Keep the card in sleeve when not in use.

AT A BORDER CROSSING STATION, REMOVE CARD FROM SLEEVE SO IT CAN BE READ.

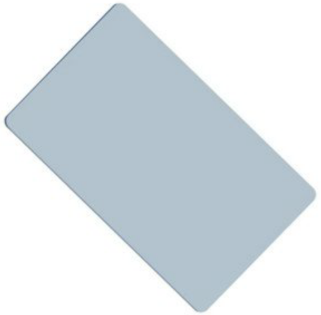
For more information, visit: nysdmv.com

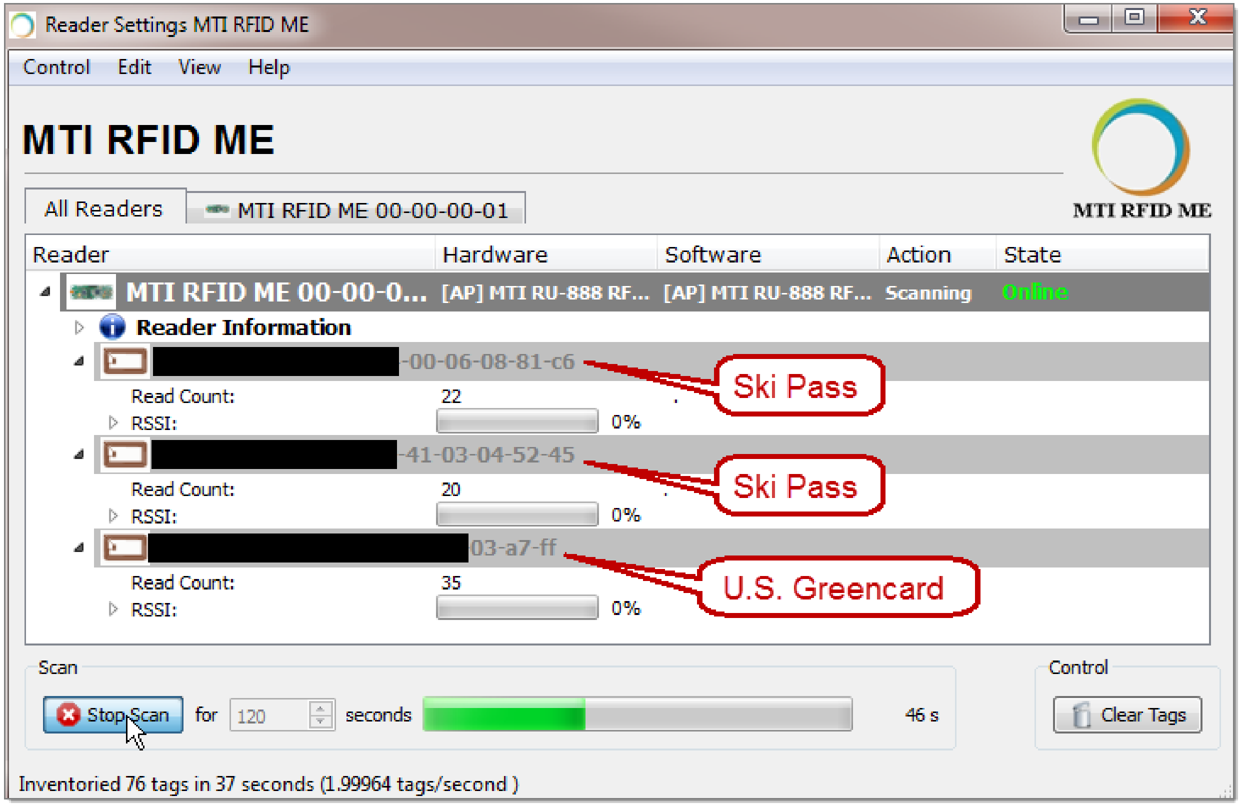
UHF - RFID Gear

ULTRAHIGH FREQUENCY

RFID ME: USB Dongle UHF Reader /Writer

50 pcs UHF ISO18000-6C EPC Class1 Gen2860-960Mhz Long-range Passive RFID tag card





MTI RFID ME

Reader	Hardware	Software	Action	State
MTI RFID ME 00-00-0...	[AP] MTI RU-888 RF...	[AP] MTI RU-888 RF...	Scanning	Online
Reader Information				
[redacted]-00-06-08-81-c6				
Read Count:	22			
RSSI:	0%			
[redacted]-41-03-04-52-45				
Read Count:	20			
RSSI:	0%			
[redacted]03-a7-ff				
Read Count:	35			
RSSI:	0%			

Ski Pass

Ski Pass

U.S. Greencard

Scan: Stop Scan for 120 seconds 46 s

Control: Clear Tags

Inventoried 76 tags in 37 seconds (1.99964 tags/second)

BISHOP FOX

UHF Custom Tools

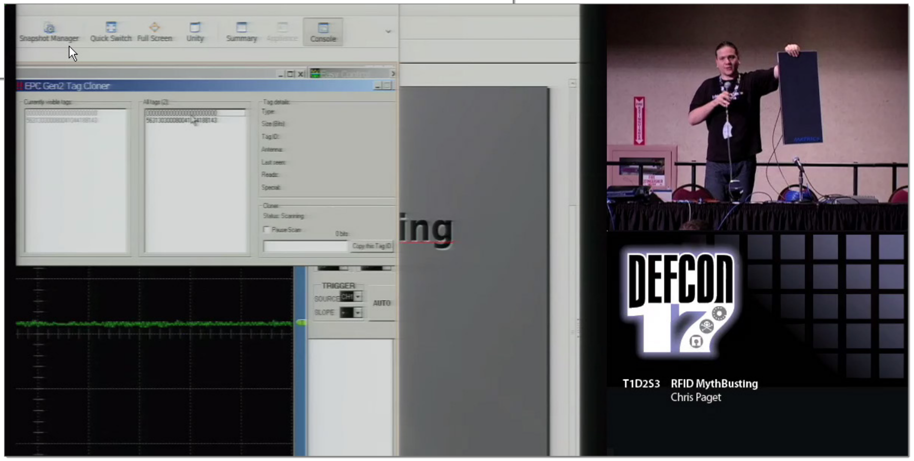
RFID

- 1W of RF power → 70W
  - 18dB power increase
  - 9dB range increase (radar range equation)
- 6dBi antenna → 13dBi antenna
  - 7dB antenna gain increase
  - 3.5dB range increase
- Overall, 9 + 3.5 = 12.5dB range increase
- 30 feet reference range + 12.5dB == 565 feet

Final Read Range

Reading EPC Gen2 tag on this tiny person, 217 feet away

217 feet

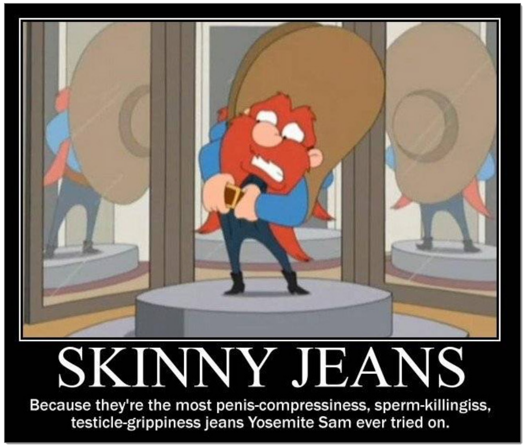


Defenses

AVOID BEING PROBED

Defenses

FLY GEAR


SKINNY JEANS
Because they're the most penis-compressiness, sperm-killingiss, testicle-grippiness jeans Yosemite Sam ever tried on.

- RFID Blocking Skinny Jeans
- RFID Blocking Vests, Blazers, and Clothes
- RFID Blocking Bags and Backpacks

Defenses

RECOMMENDATIONS

- Consider implementing a more secure, active RFID system (e.g. "*contactless smart cards*") that incorporates encryption, mutual authentication, and message replay protection.

- Consider systems that also support 2-factor authentication, using elements such as a PIN pad or biometric inputs.

- Consider implementing physical security intrusion and anomaly detection software.

- Implement "feel tests" by guards to ensure badges are not fake printed badges

HID Global - Best Practices in Access Control White Paper (PDF)
https://www.hidglobal.com/node/16181

Defenses

RECOMMENDATIONS

- Instruct employees not to wear their badges in prominent view when outside the company premises.
- Utilize RFID card shields when the badge is not in use to prevent drive-by card sniffing attacks.
- Physically protect the RFID badge readers by using security screws that require special tools to remove the cover and access security components.
- Employ the tamper detect mechanisms to prevent badge reader physical tampering. All readers and doors should be monitored by CCTV.

WORLD'S MOST
SECURE FASTENER
Unique keyway shape is designed for each customer.
And only that customer has the matched driver bit.

HID Global - Physical Reader Security, Tamper, and Supervisor Features (PDF)
http://www.hidglobal.com/physical-reader-security-tamper-and-supervisor-features

Defenses

RECOMMENDATIONS

- Cryptographic distance-bounding protocols that measure accurately the round-trip delay of the radio signal countermeasure to relay attacks.

- Open Supervised Device Protocol (OSDP) w/ Secure Channel Protocol (SCP) for secure initial pairing of readers/controllers to prevent MITM attacks.

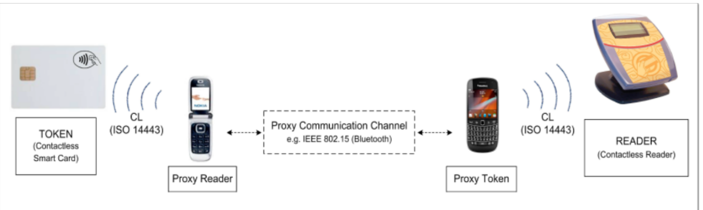
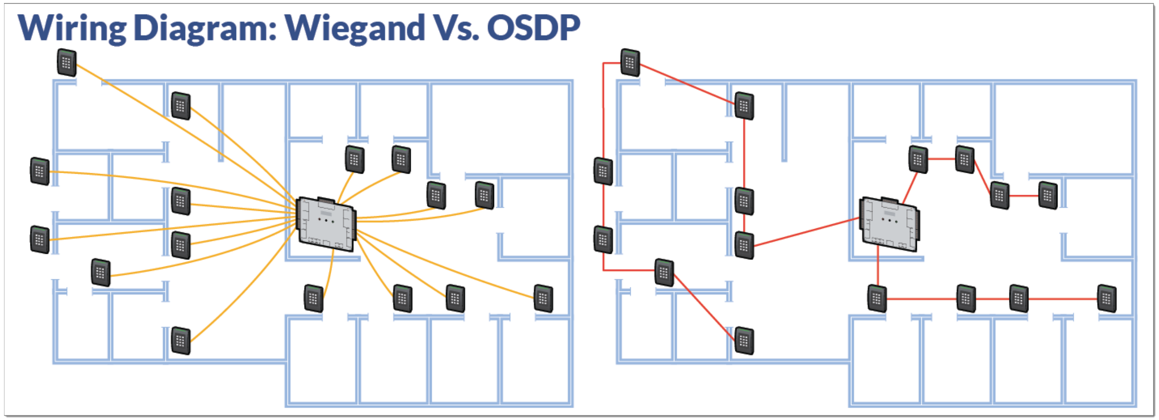
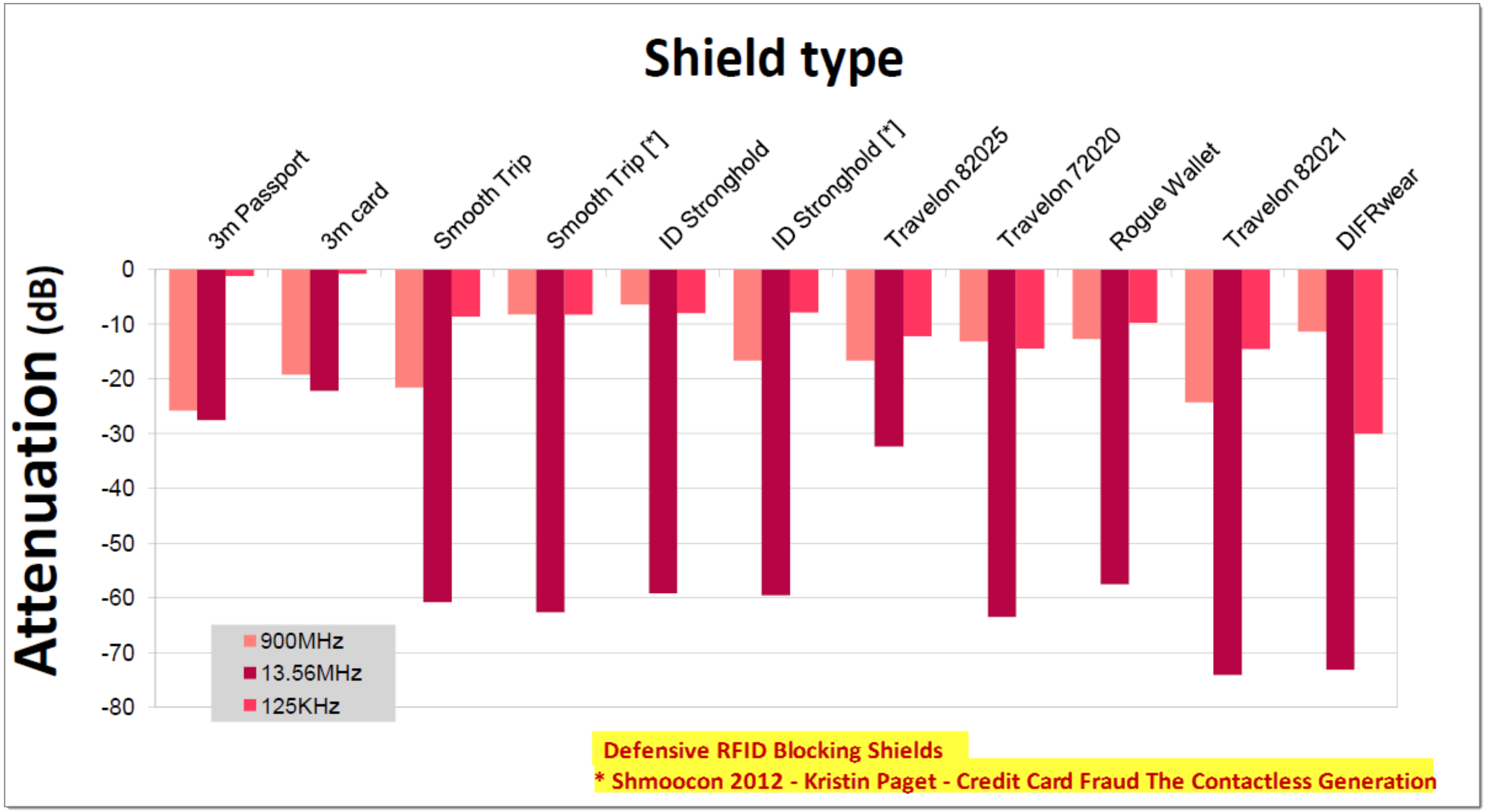


Figure 2: Practical relay setup using only NFC mobile phones.



Defenses (Broken)

SOME DON'T...EXAMPLE...



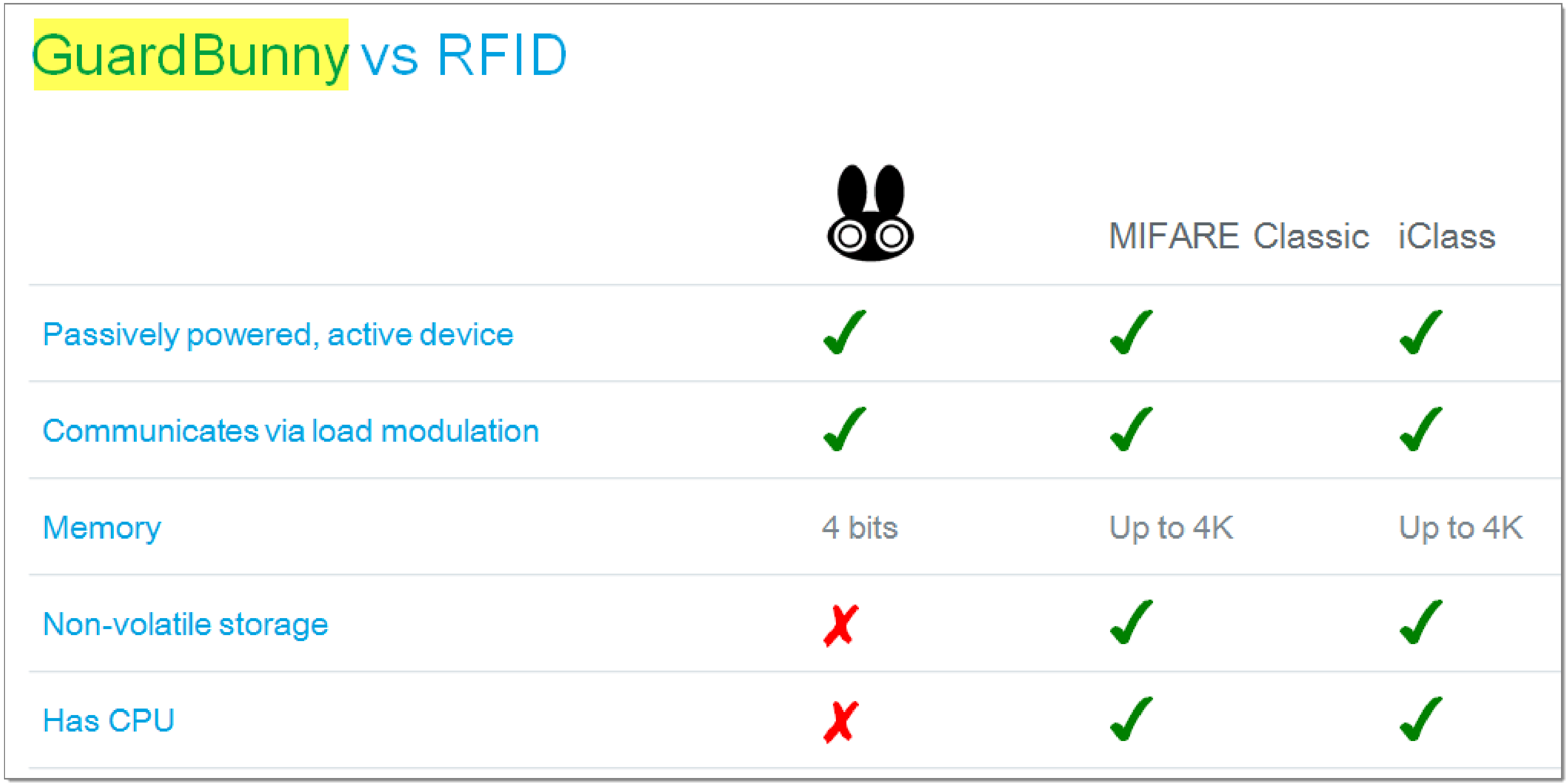
Defensive RFID Blocking Shields

* Shmoocon 2012 - Kristin Paget - Credit Card Fraud The Contactless Generation

Shmoocon 2012 - Kristin Paget - Credit Card Fraud: The Contactless Generation
http://www.shmoocon.org/2012/presentations/Paget_shmoocon2012-credit-cards.pdf

Defenses

ACTIVE BLOCKING



GuardBunny vs RFID

		MIFARE Classic	iClass
Passively powered, active device	✓	✓	✓
Communicates via load modulation	✓	✓	✓
Memory	4 bits	Up to 4K	Up to 4K
Non-volatile storage	✗	✓	✓
Has CPU	✗	✓	✓

Thank You

Bishop Fox – see for more info:
http://www.bishopfox.com/resources/tools/rfid-hacking/

BISHOP FOX