RFIDiggity

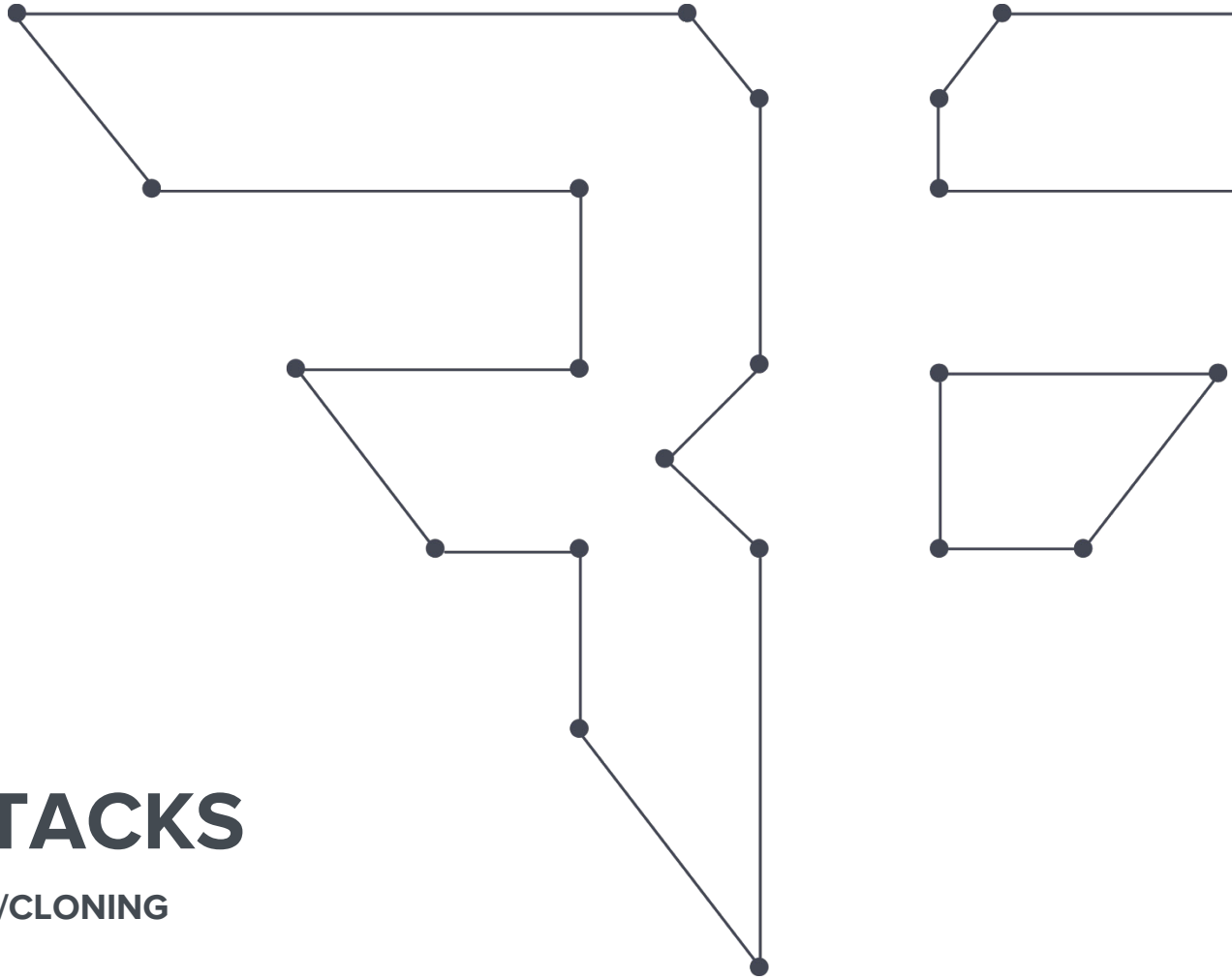
Pentester Guide to Hacking HF/NFC and UHF RFID

09 Aug 2015 – DEF CON 23 (2015) – Las Vegas, NV

Presented by:
Francis Brown &
Shubham Shah
Bishop Fox
www.bishopfox.com

BISHOP FOX

NEW Tools - Demos



BADGE ATTACKS

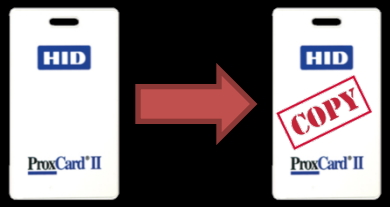
ICLASS BADGE READING/CLONING

Methodology

3 STEP APPROACH

1. **Silently steal badge info**

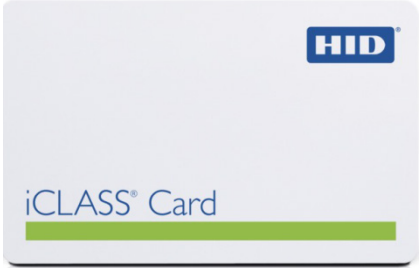
2. **Create card clone**

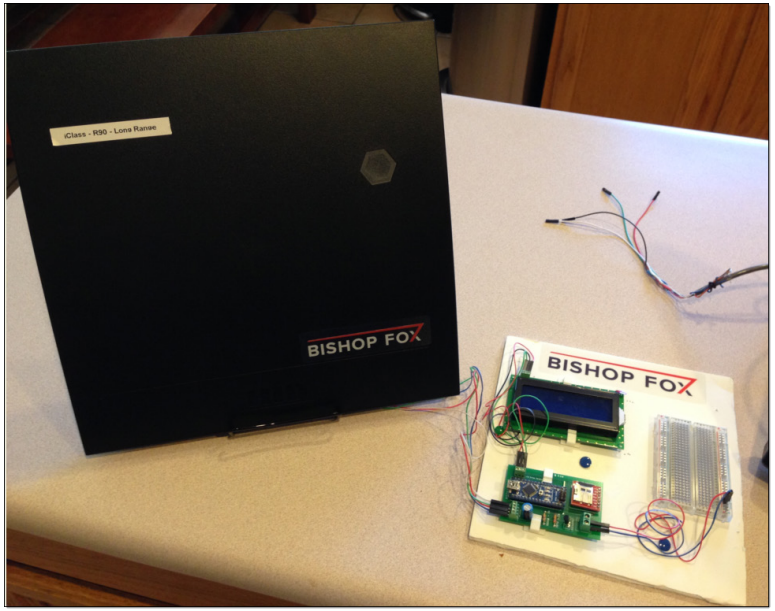


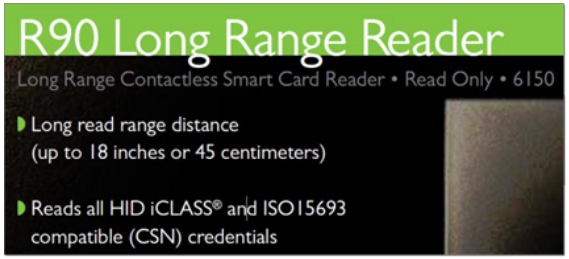
3. **Enter and plant backdoor**

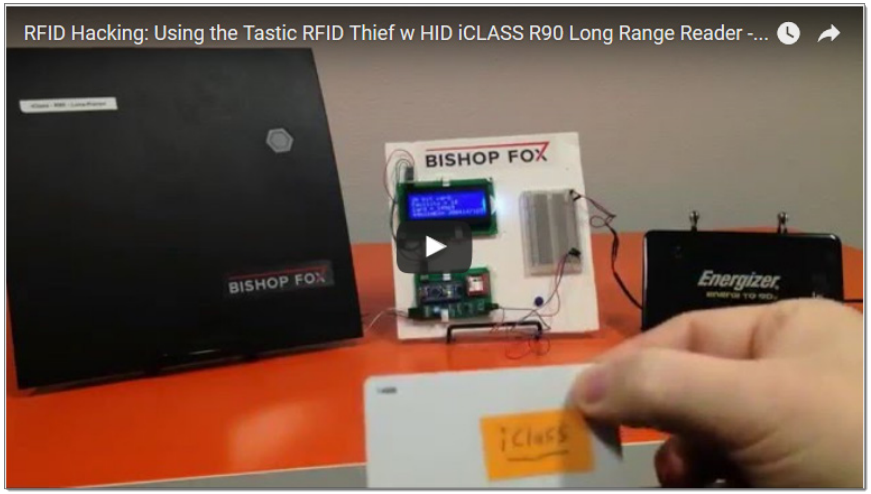
Tastic RFID Thief

LONG RANGE RFID STEALER



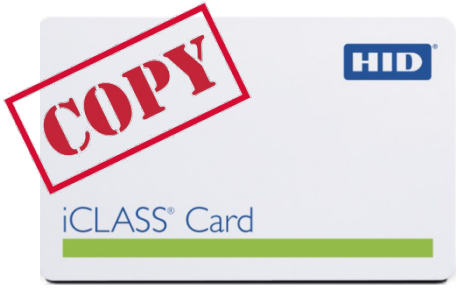






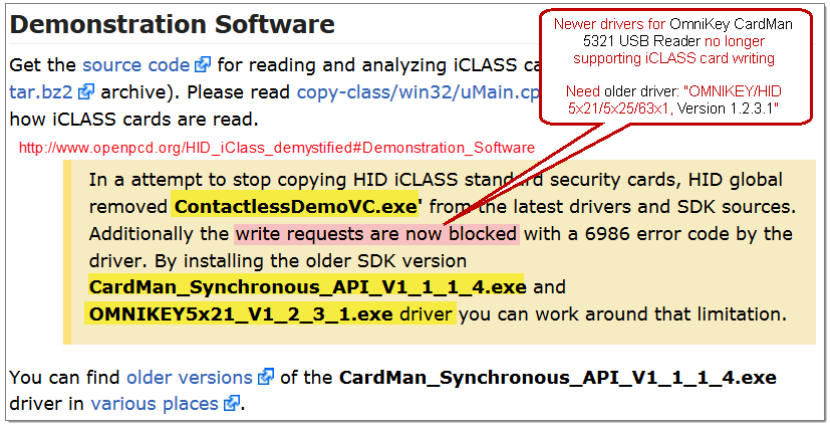
iCLASS Cloner

XFPGA.COM - FROM CHINA



~$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



Demonstration Software

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"

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.

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.

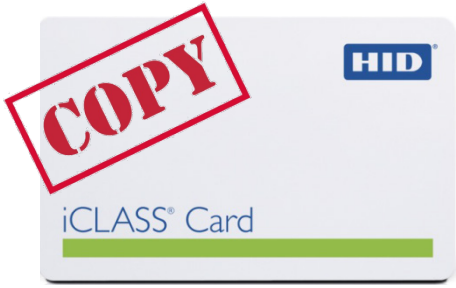
You can find older versions of the **CardMan_Synchronous_API_V1_1_1_4.exe** driver in various places.

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

BISHOP FOX

iCLASS Cloner

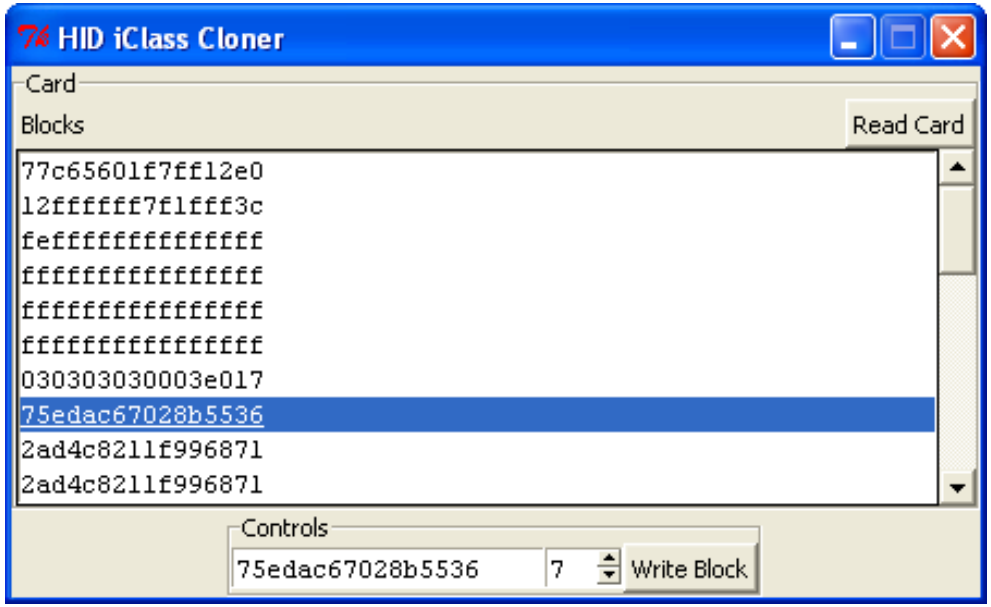
NEW – Bishop Fox – FREE Edition



UPDATE

Read / Write to HID iCLASS Cards:

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



Tastic RFID Thief

LONG RANGE RFID STEALER

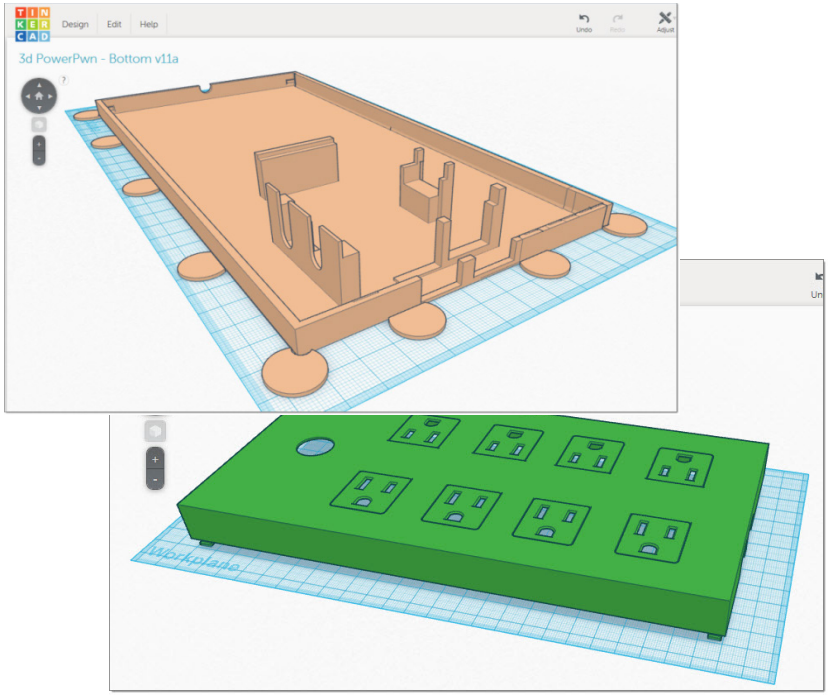
BADGE ATTACKS

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

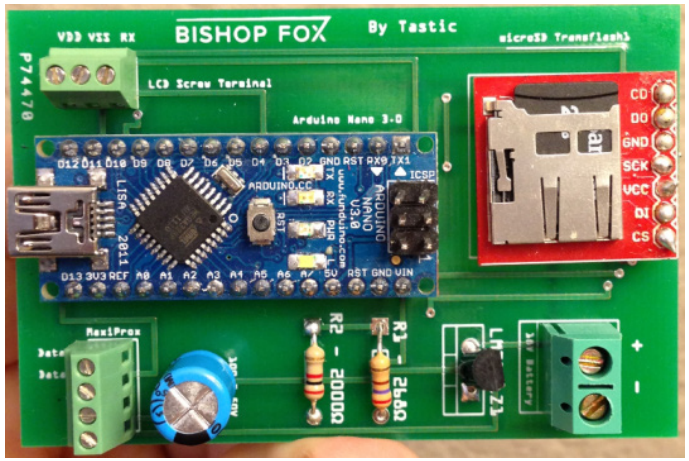


READER ATTACKS

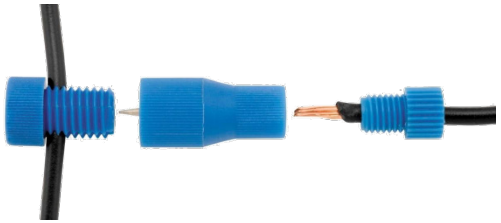
BADGE READER MITM IMPLANTS

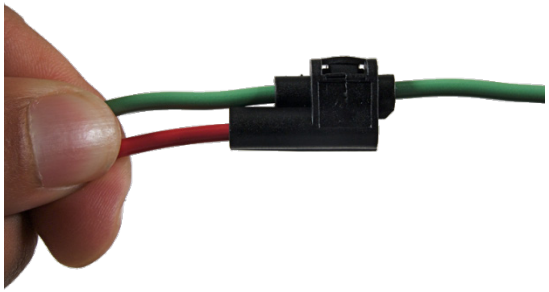
Reader Attacks

TASTIC–MITM ATTACK



+

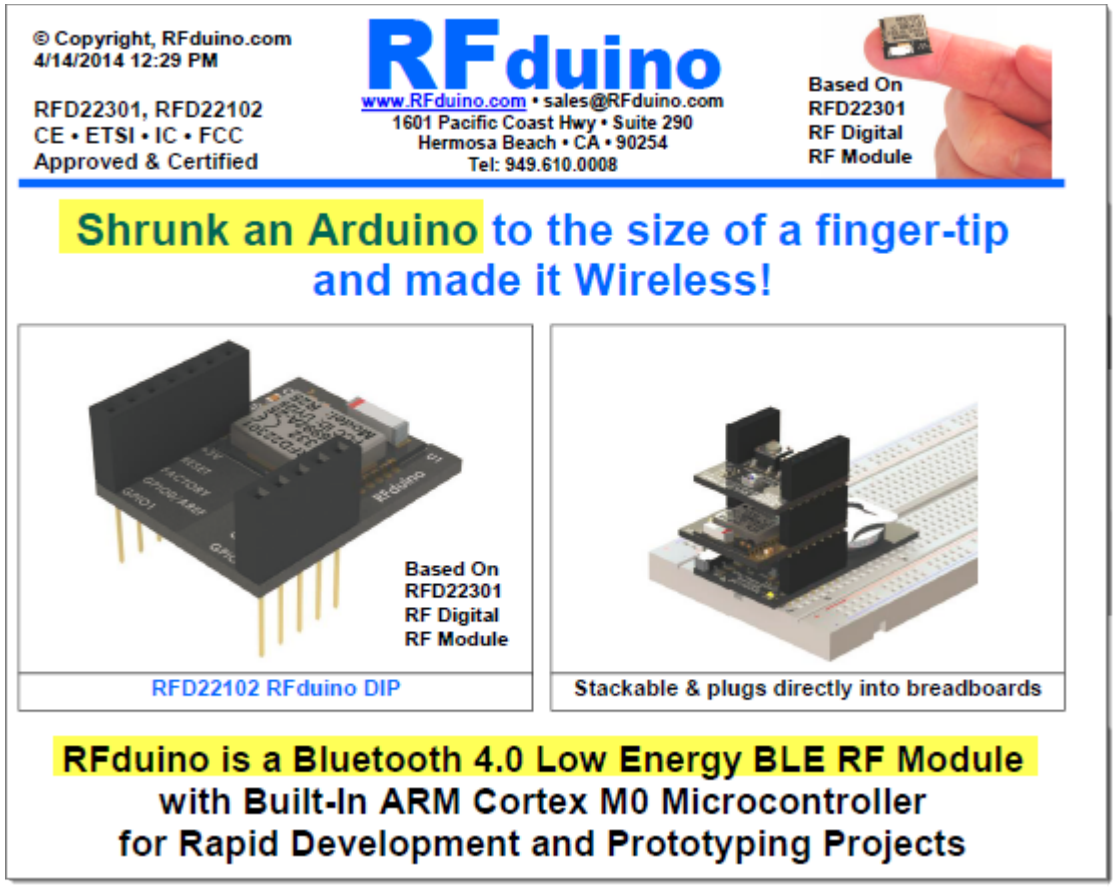


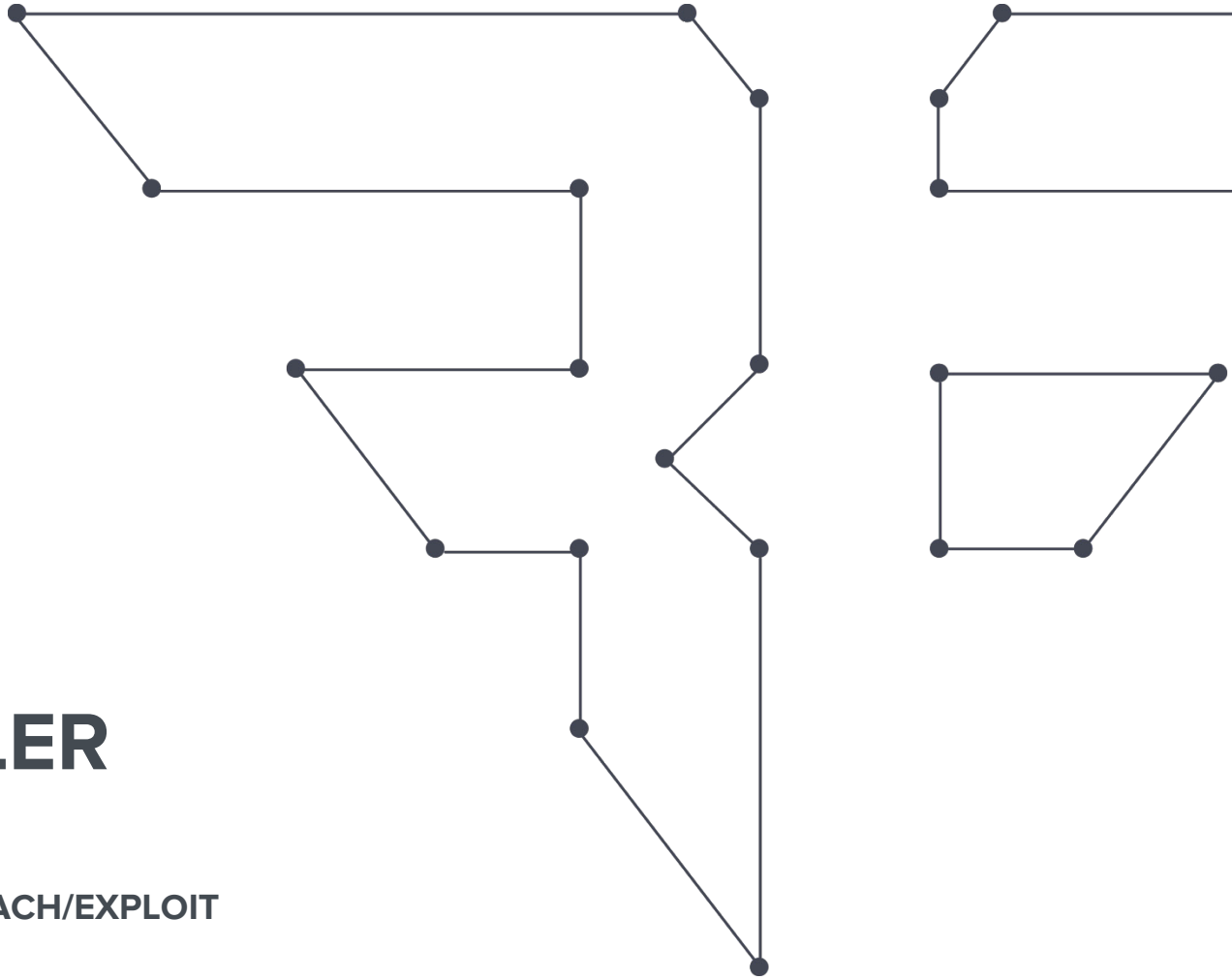


- Insert in door reader of target building – record badge #s
- Tastic RFID Thief's PCB could be used similiarly for MITM attack

Reader Attacks

TASTIC–MITM ATTACK



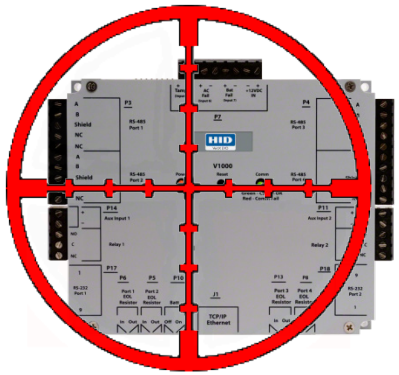


CONTROLLER ATTACKS

VERTX CONTROLLER SEACH/EXPLOIT

Controller Attacks

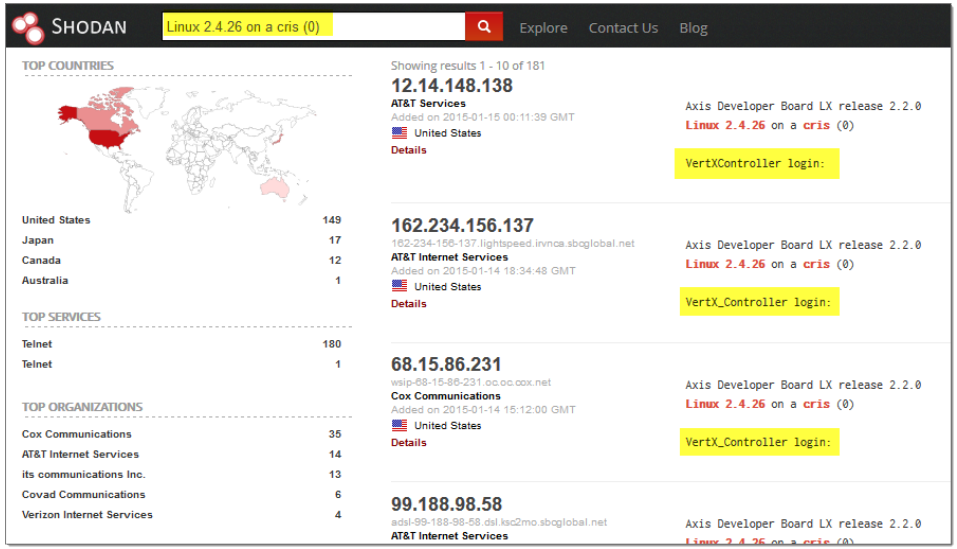
JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

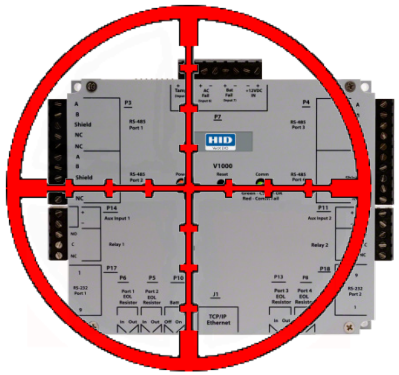
- HID VertX Controller – Default Open Ports:
  - FTP (21), Telnet (23), HTTP (80)
- HID VertX Controller – Connect via FTP / Telnet / HTTP with Default Admin Creds: **`root/pass`**
- Banner grabbing for HID VertX controller discovery
  - Can also find using SHODAN search engine

```
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:
```



Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

Search Diggity

File Options Help

Google | CodeSearch | Bing | LinkFromDomain | DLP | Flash | Malware | PortScan | NotInMyBackyard | BingMalware | Shodan

Simple | Advanced

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

SCAN | Cancel | Settings

API Key: Create [ ] Hide

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://68.15.8[illegible]31:23/	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[illegible]	-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[illegible]	-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[illegible]	-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

Output | Selected Result

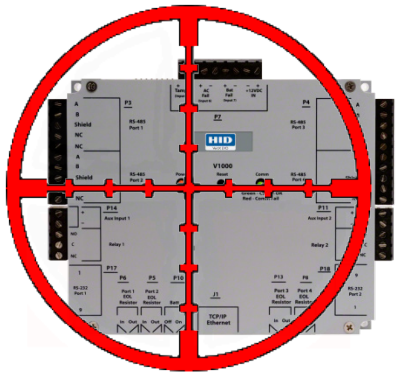
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:

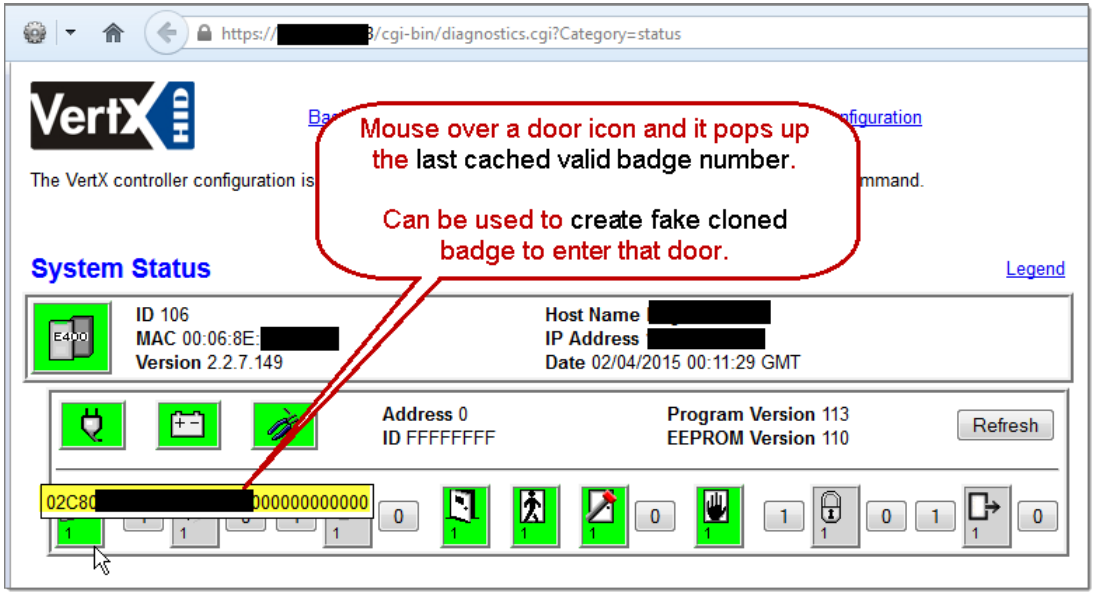
Shodan Status: Ready

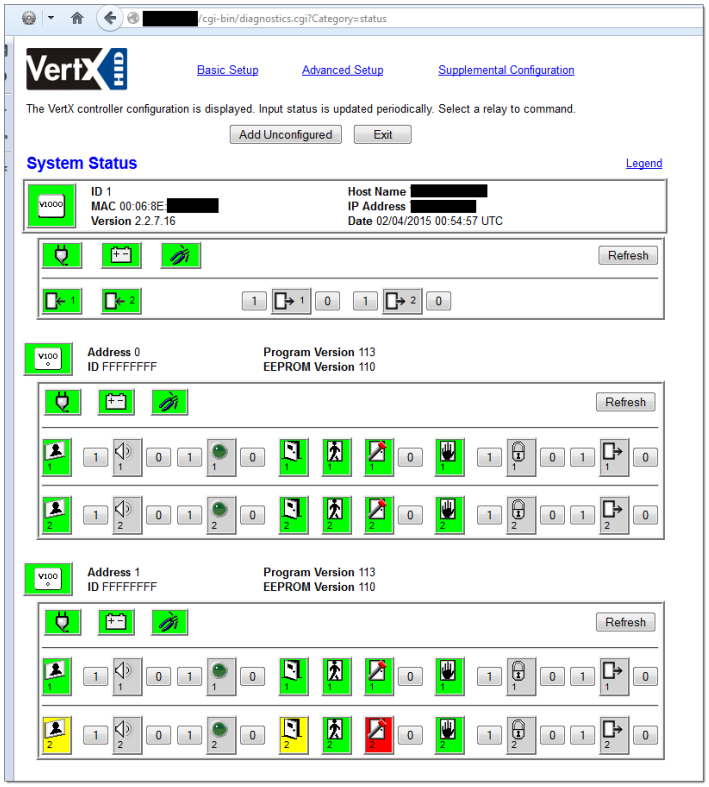
Controller Attacks

JACKED IN



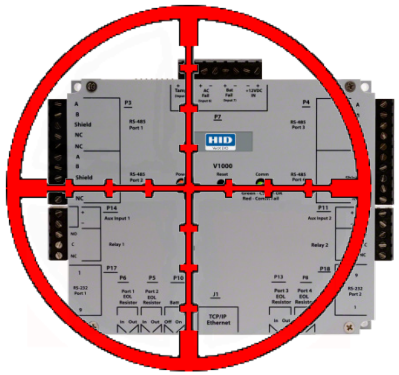
Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network





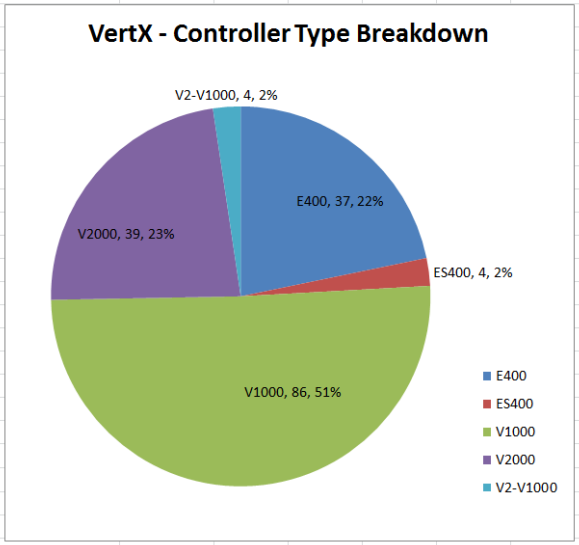
Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

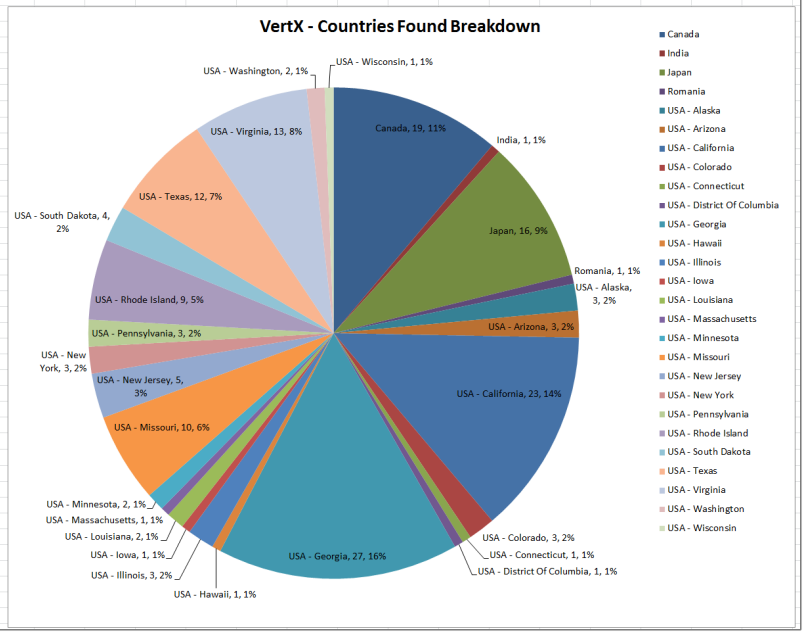
VertX Types	Total Found
E400	37
ES400	4
V1000	86
V2000	39
V2-V1000	4
Total:	170



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



BISHOP FOX

Introduction/Background

GETTING UP TO SPEED

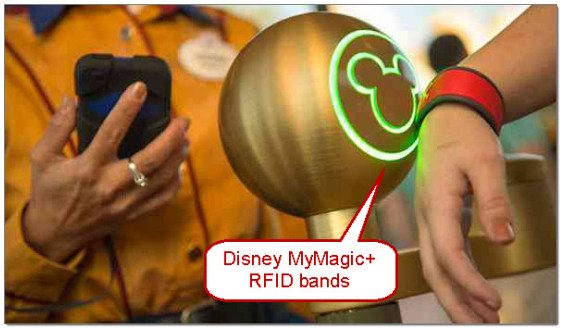
Badge Basics

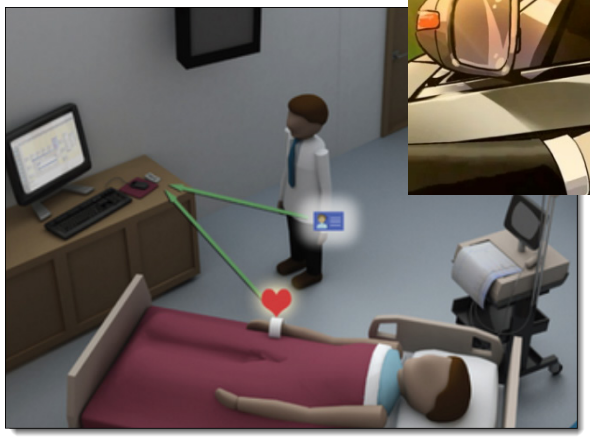
FREQUENCIES

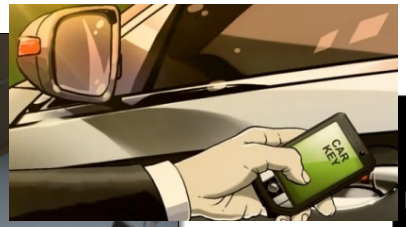
Frequency	Range	Distance	Common Usage	Card Types	Standards
Low Frequency (LF)	120kHz – 140kHz	<3 ft. (Commonly under 1.5ft)	Access control systems; animal tagging; car immobilizer	HID Prox, Indala Prox, Kantech ioProx, Hitag 1/2/S, Casi-Rusco, EM4X, Honeywell Nexwatch, G-Prox II, AWID, Pyramid Prox, 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

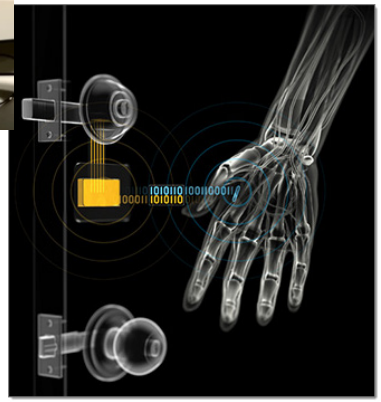
RFID Other Usage

WHERE ELSE?





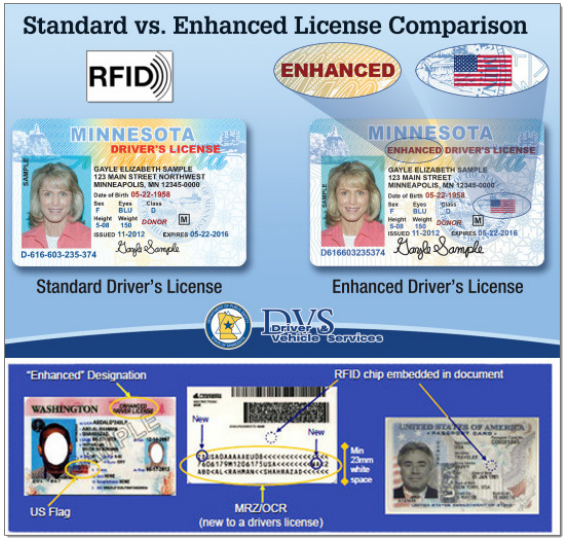




BISHOP FOX

RFID Other Usage

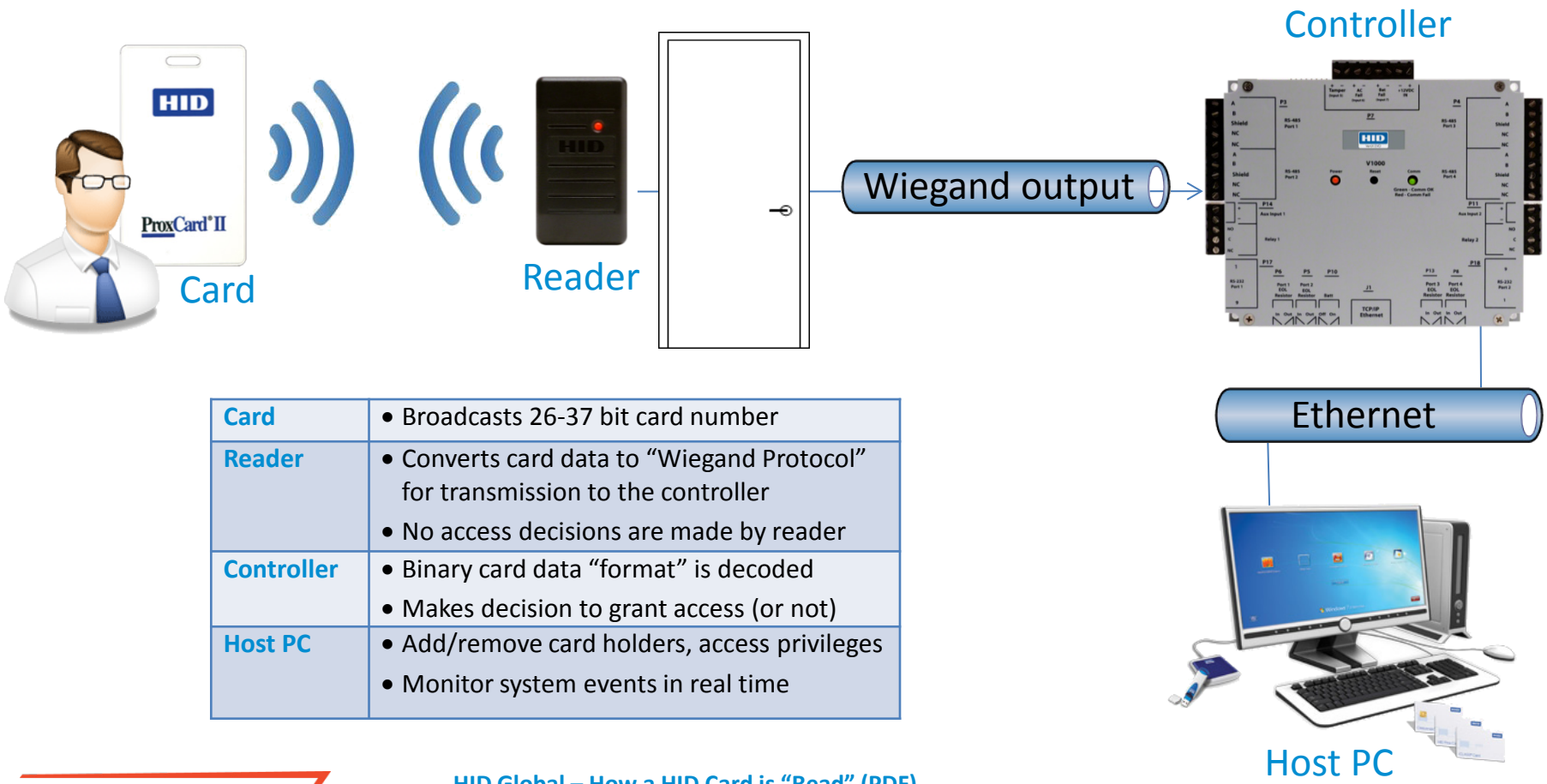
WHERE ELSE?



BISHOP FOX

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

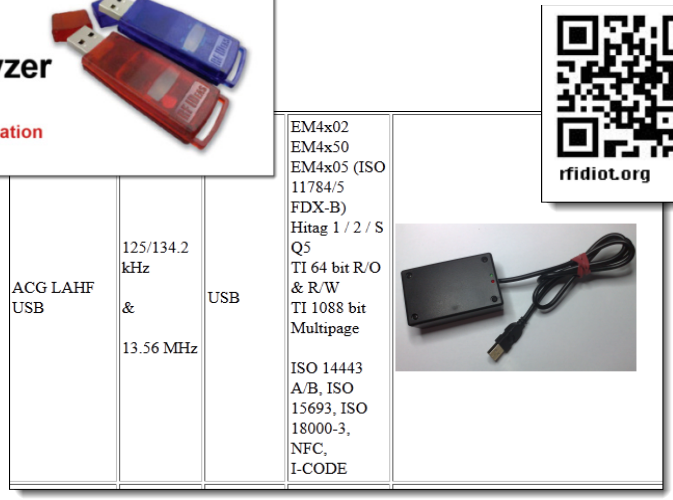
Tastic RFID Thief

- T55x7 Cards
- Q5 cards (T5555)

SONMicro - 125 KHz RFID Evaluation Kit - Deluxe

RFIDeas – HF and LF USB Tools

Proxmark3



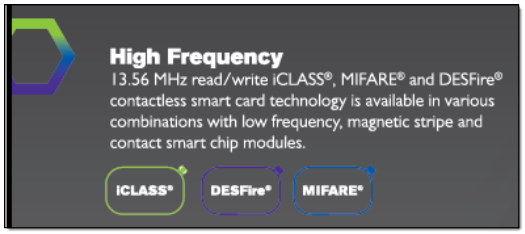
ACG LAHF USB	125/134.2 kHz & 13.56 MHz	USB	EM4x02 EM4x50 EM4x05 (ISO 11784/5 FDX-B) Hitag 1 / 2 / S Q5 TI 64 bit R/O & R/W TI 1088 bit Multipage ISO 14443 A/B, ISO 15693, ISO 18000-3, NFC, I-CODE	

rfidiot.org

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

RFID Hacking Gear

HF - HIGH FREQUENCY (13.56 MHz)



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

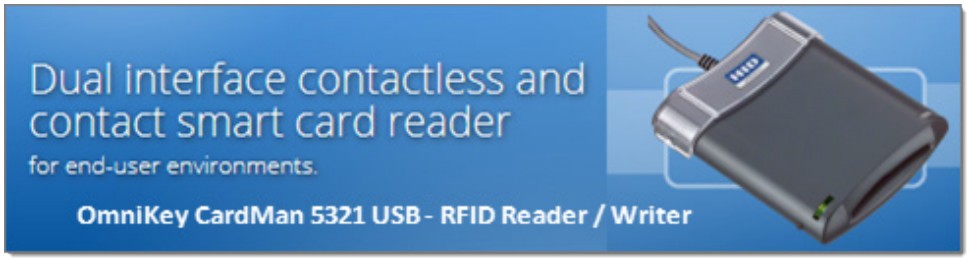
The antenna is the size of a credit card and ships with a 3' Hirose USB cable that is used to connect it to a Proxmark. Antennas are connected to the 5-pin USB port on the Proxmark using the USB cable included.

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

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

Pwn Pad 2014

NEXUS 7 PENTEST DEVICE

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

RFID Hacking Tools

PENTEST TOOLKIT

Proxmark3

RFID HACKING TOOLS

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

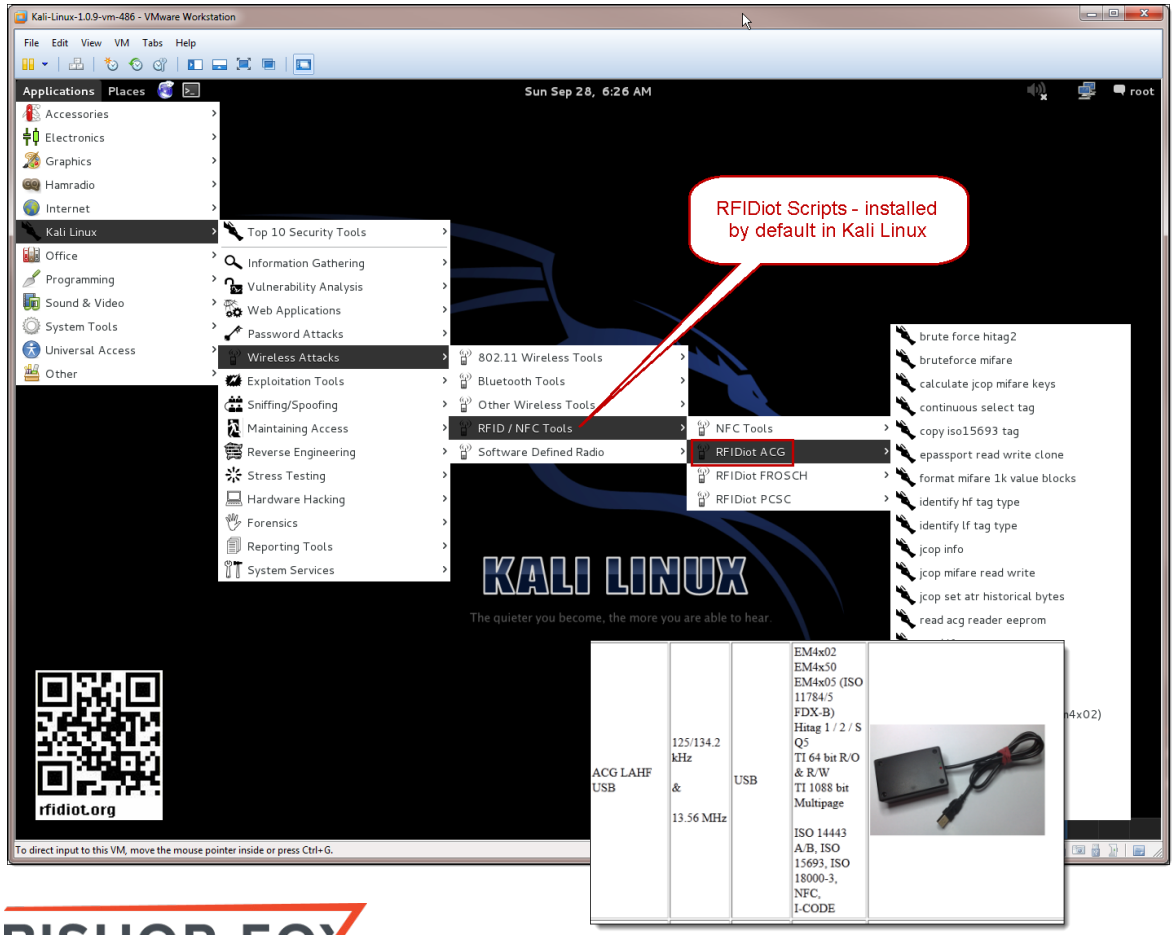
Proxmark3 - iCLASS Commands	
Command	**Description**
hf iCLASS help	This help
hf iCLASS list	List iCLASS history
hf iCLASS snoop	Eavesdrop iCLASS communication
hf iCLASS sim	Simulate iCLASS tag
hf iCLASS reader	Read an iCLASS tag
hf iCLASS replay	Read an iCLASS tag via Reply Attack
hf iCLASS dump	Authenticate 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

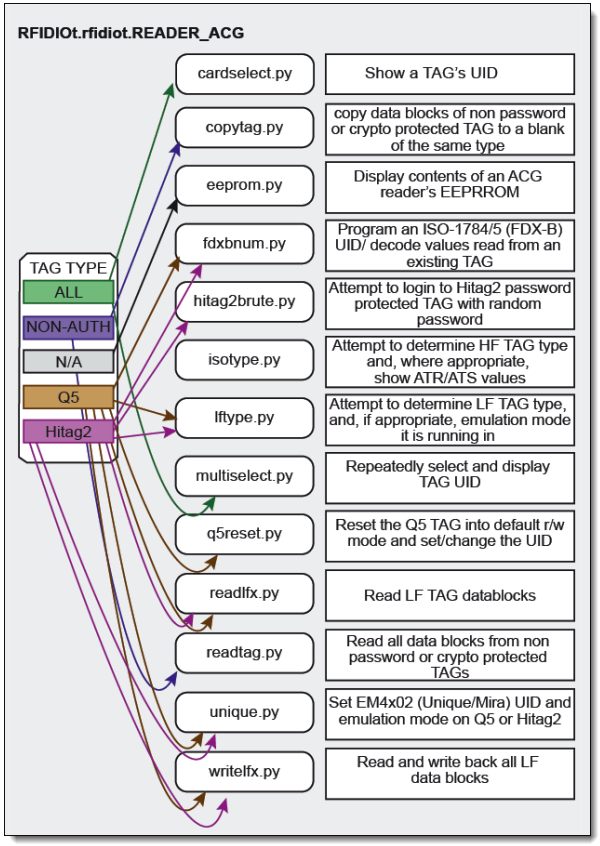
RFIDiot Scripts

RFID HACKING TOOLS

rfidiot.org



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	



BISHOP FOX

RFIDeas Tools

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 R
        RDR-6081APU Pearl R
         KT-6081AKU Black R
         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®	

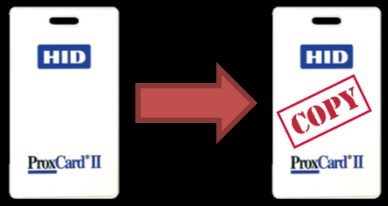
BISHOP FOX

Methodology

3 STEP APPROACH

1. **Silently steal badge info**

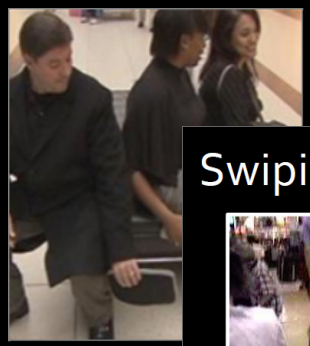
2. **Create card clone**

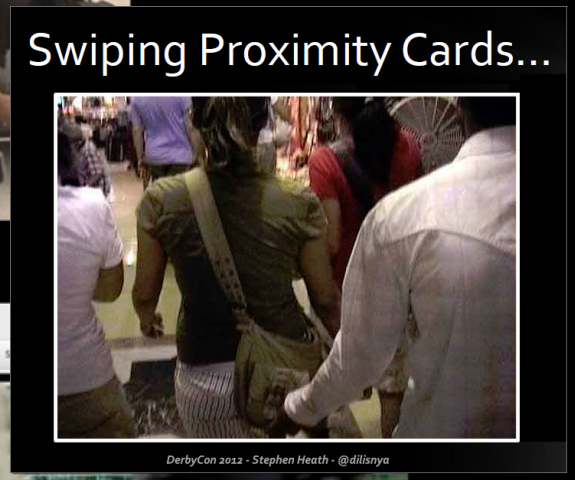


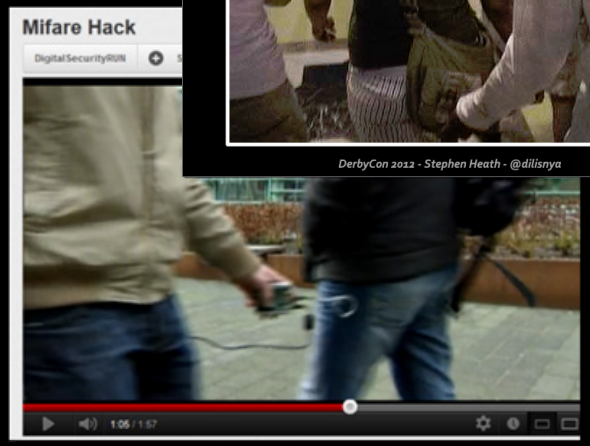
3. **Enter and plant backdoor**

Distance Limitations

A$$ GRABBING METHOD







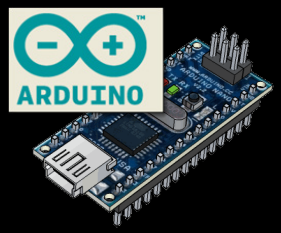
Existing RFID hacking tools only work when a few centimeters away from badge

Tastic Solution

LONG RANGE RFID STEALER

CARDS.TXT

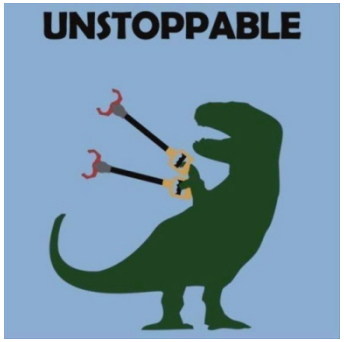
```
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
26 bit card: 2006e23186, FC = 113, CC = 6339, BIN: 00000010
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
35 bit card: 2f85c94ee3, FC = 3118, CC = 305009, BIN: 00000
26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 000 100
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 10
34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 010
FC = 8, CC = 15181, BIN: 000000100
```

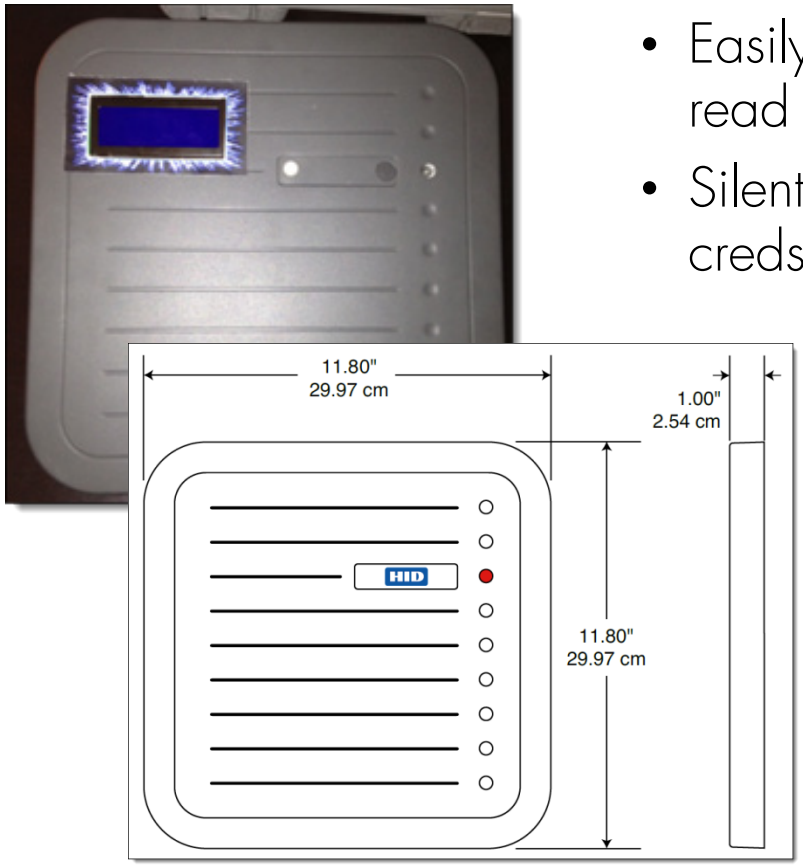


BISHOP FOX

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

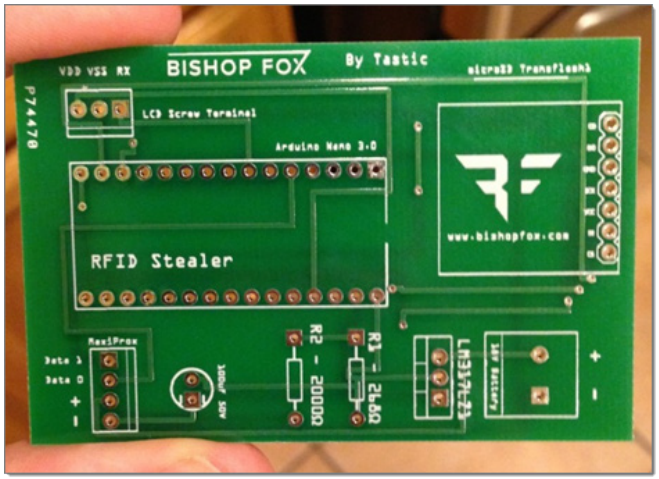
Tastic RFID Thief

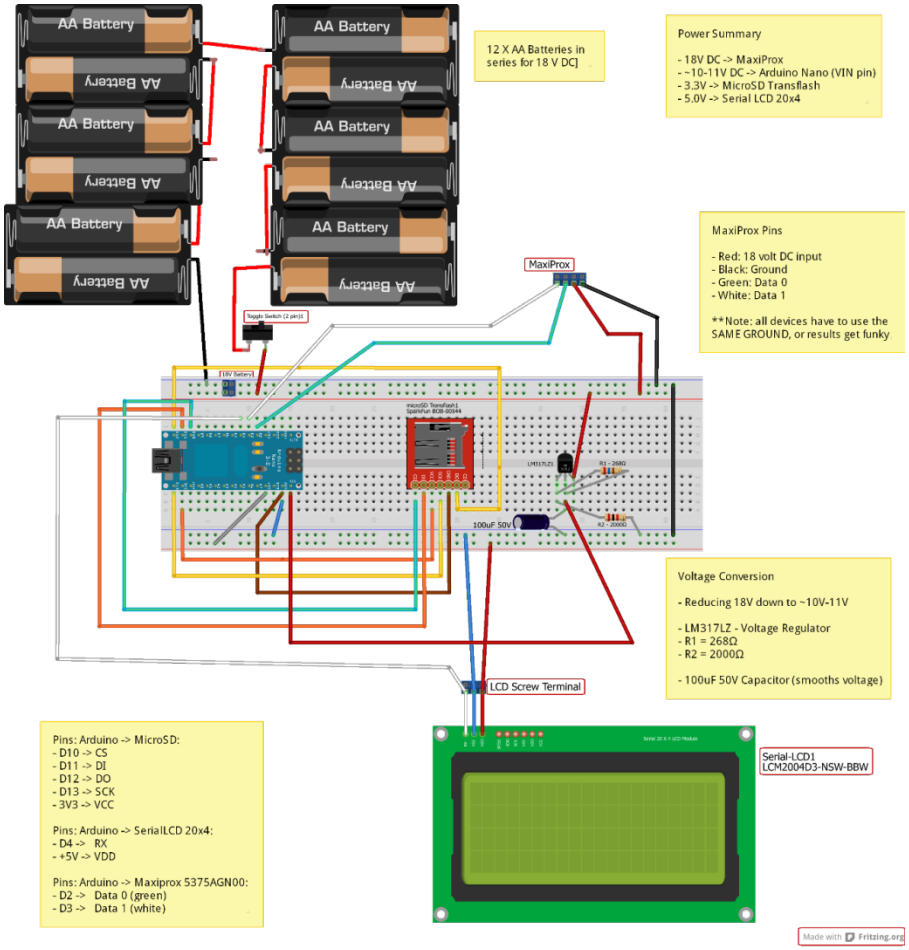
LONG RANGE RFID STEALER

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



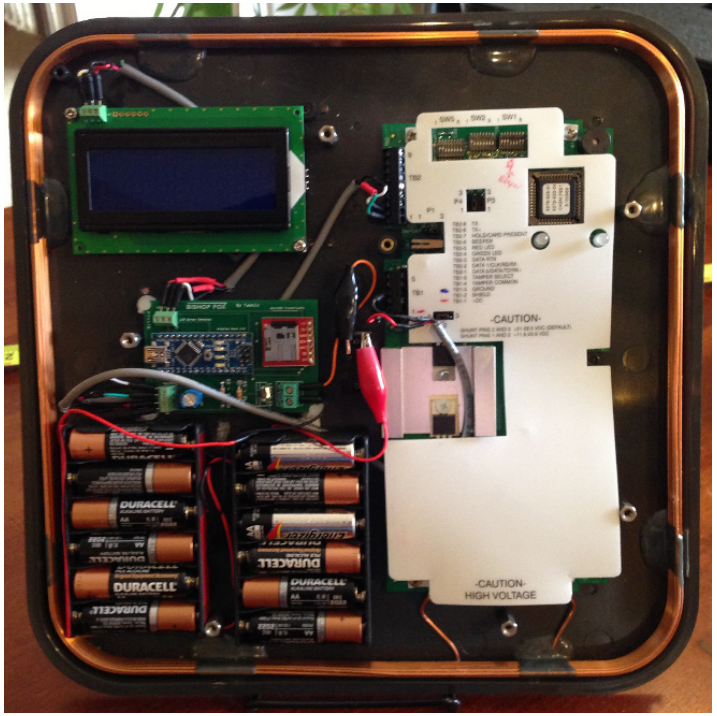


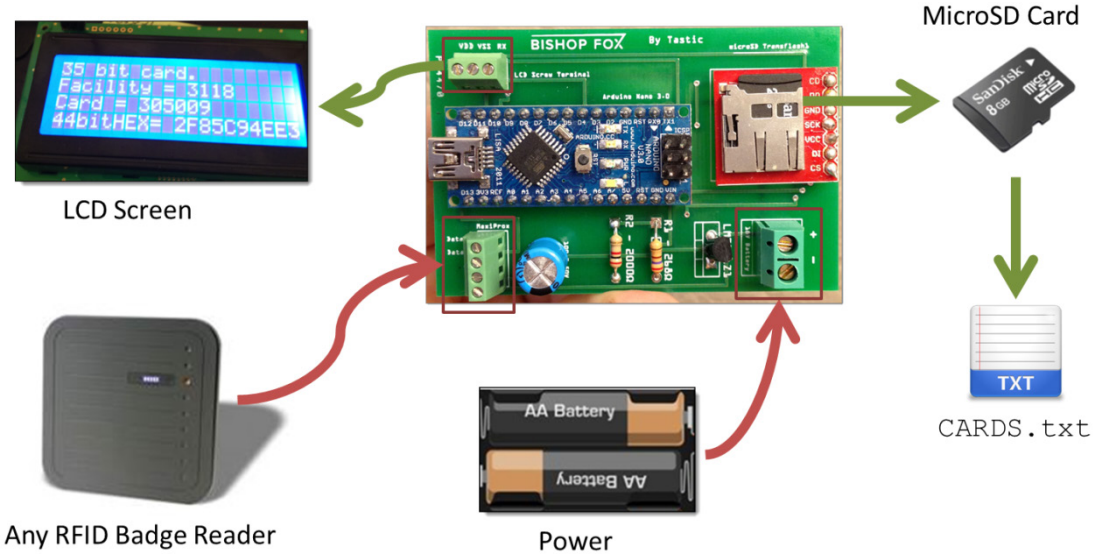
BISHOP FOX

Custom PCB

TASTIC RFID THIEF

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





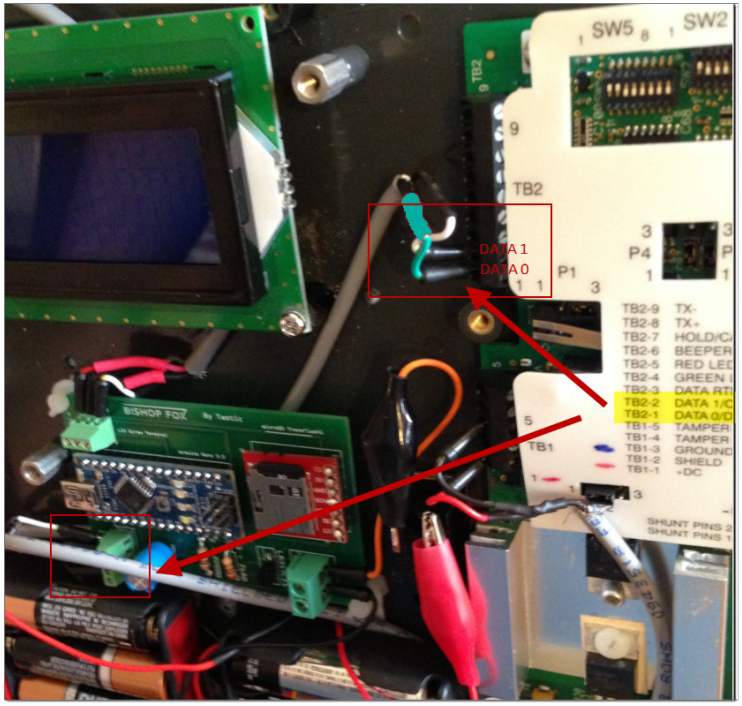
Wiegand Input

TASTIC RFID THIEF

Wiegand

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

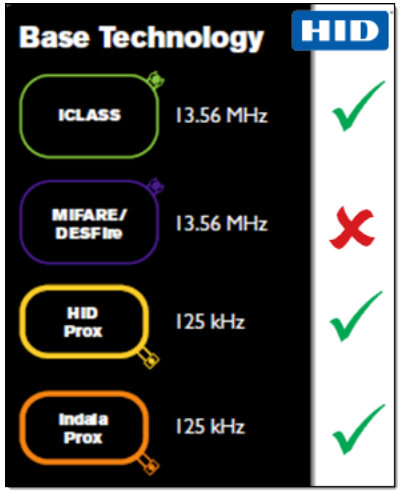
- Outputs a badge binary number by sending electrical pulses for '0' and '1' on wires Data 0 and Data 1
- Wiegand Interface consists of 3 lines: "Data 0", "Data 1", "Data Return" (Ground)
- To send a '0'-bit, a pulse is sent on DATA 0 (Green)
- To send a '1'-bit, a pulse is sent on DATA 1 (White)
- Every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



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

Commercial Readers

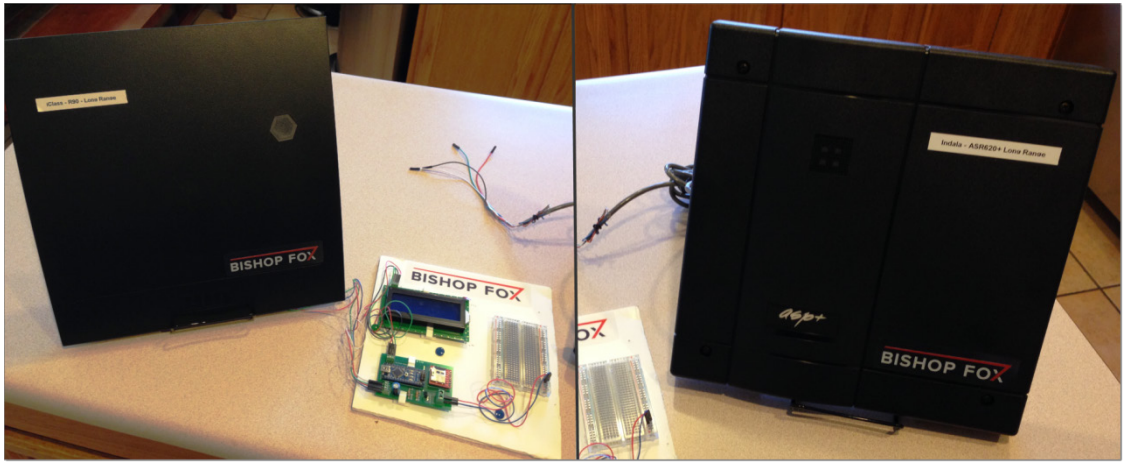
TASTIC RFID THIEF



Long-range commercial RFID readers to weaponize:

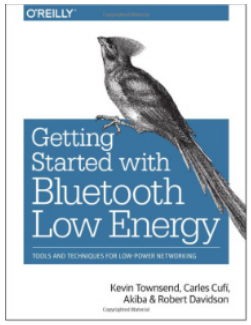
RFID Product Family	Frequency	Long Range Reader	URL
HID Prox	Low Frequency	HID MaxiProx 5375	https://www.hidglobal.com/products/readers/hid-proximity/5375
Indala Prox	Low Frequency	Indala Long-Range Reader 620	http://www.hidglobal.com/products/readers/indala/620
iCLASS	High Frequency	iCLASS - R90 Long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

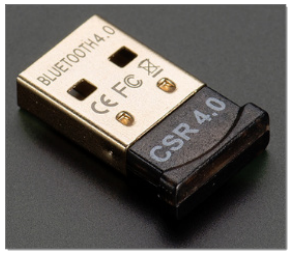
3 out of 4 HID RFID product families covered



Bluetooth – Other

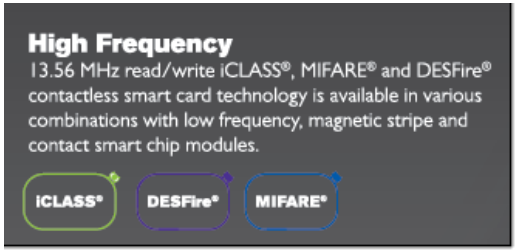
- Bluetooth Modules:
  - SparkFun BLE Mate 2
  - Bluetooth Mate Gold - Sparkfun
  - Bluetooth Module Breakout - Roving Networks (RN-41)
  - Bluetooth Modem - BlueSMiRF Silver (RN-42)
  - Bluetooth Bee for Arduino - Seeedstudio
  - Bluetooth Bee Standalone with built-in Arduino
  - KEDSUM Arduino Wireless 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')





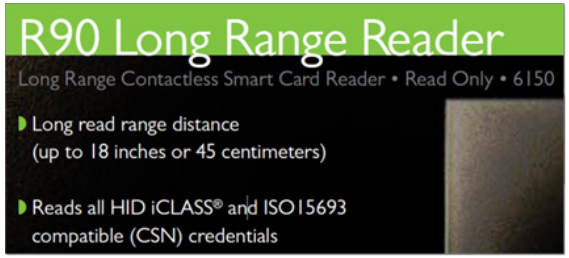
Commercial Readers

TASTIC RFID THIEF



~$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".

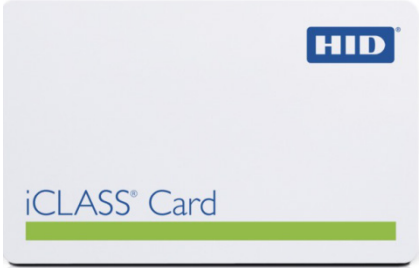


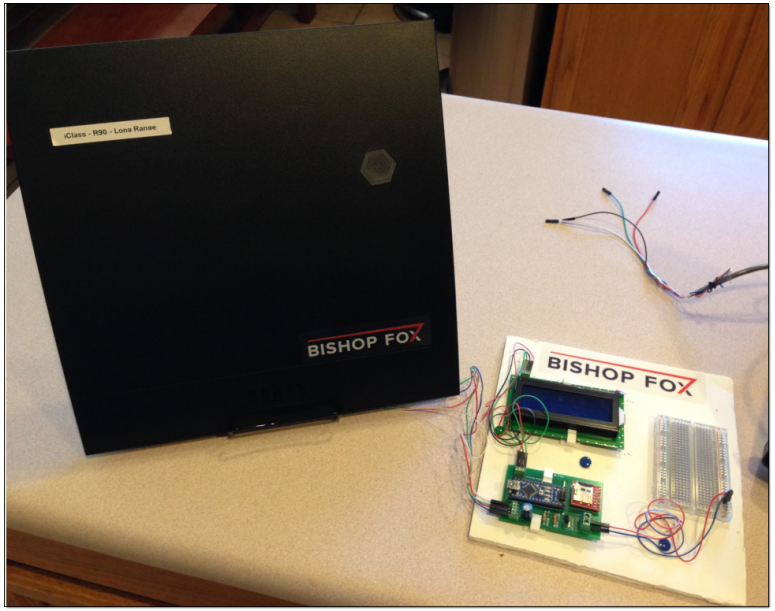
iCLASS Security Levels

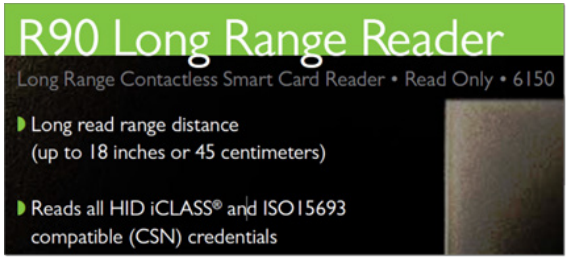
- **Standard Security**: two keys are shared across all HID readers world-wide. Swiping any standard security card in front of a standard security reader results in "beep-n-blink" of the reader. Cards are provided by HID and have a unique combination of a card ID (not UID) and a facility ID.
- **High 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.

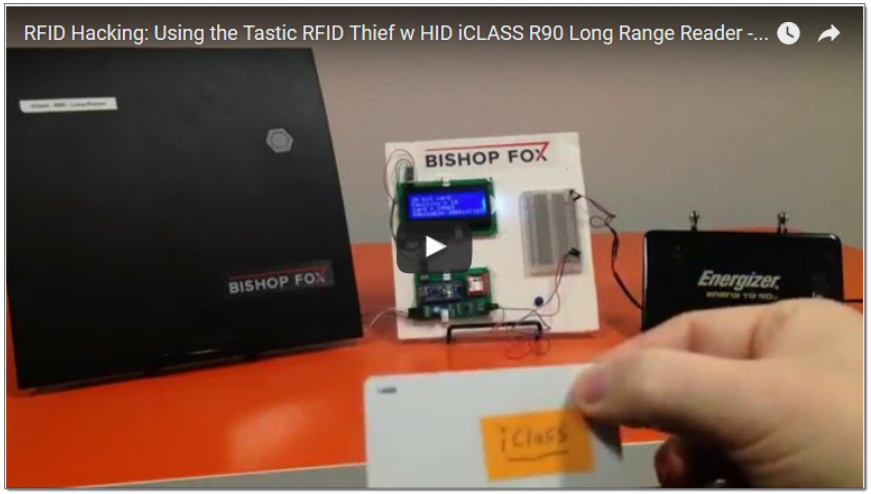
Tastic RFID Thief

LONG RANGE RFID STEALER



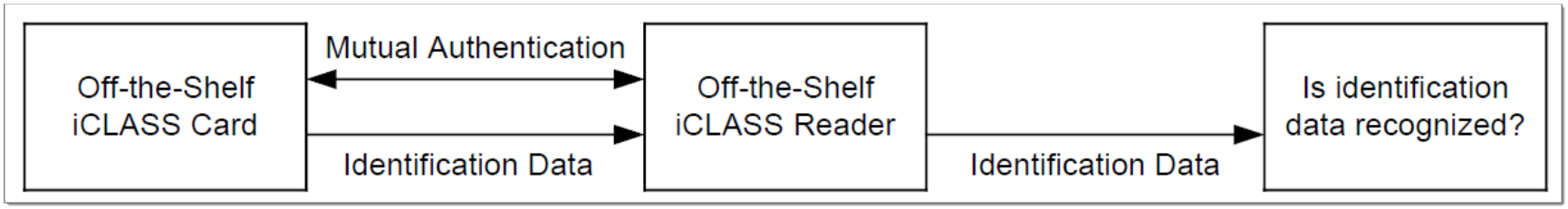


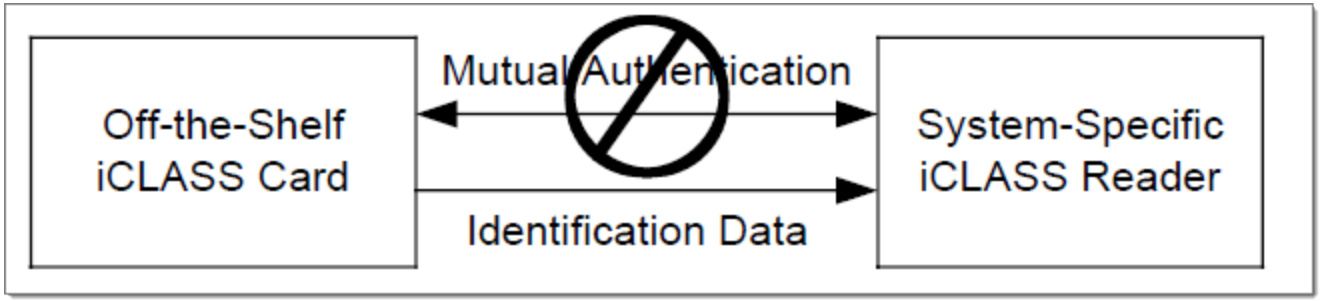




iCLASS

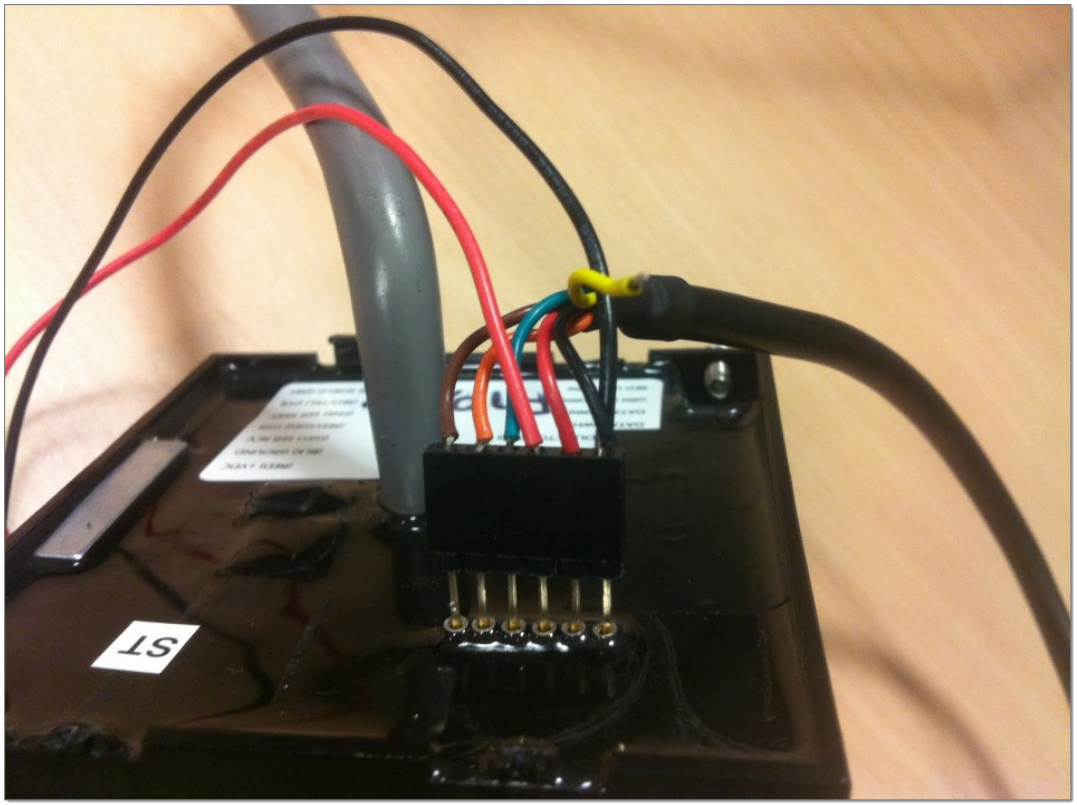
TASTIC RFID THIEF





iCLASS – Dumping Key

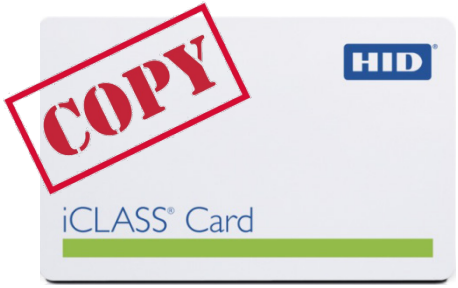
READER ATTACK

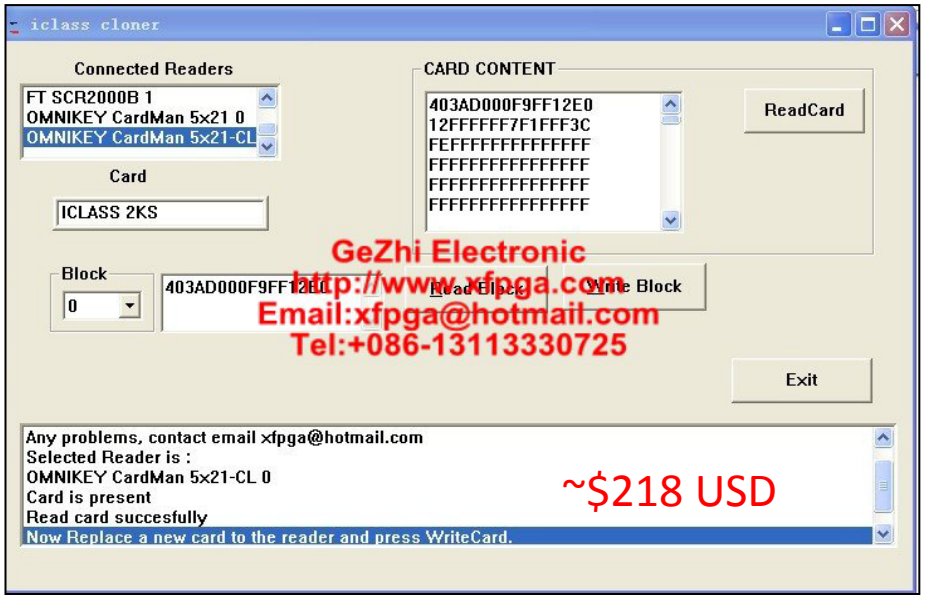


BISHOP FOX

iCLASS Cloner

XFPGA.COM - FROM CHINA

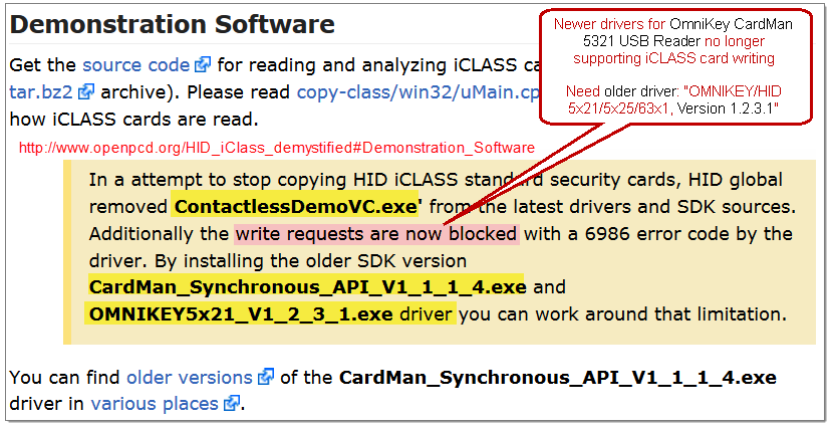




~$218 USD

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

- 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



Demonstration Software

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"

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.

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

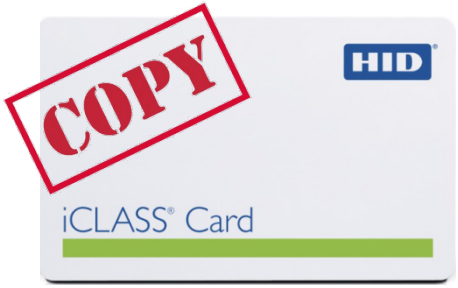
In a attempt to stop copying HID iCLASS standard security cards, HID global removed **ContactlessDemoVC.exe**' from the latest drivers and SDK sources. Additionally the write requests are now blocked with a 6986 error code by the driver. By installing the older SDK version **CardMan_Synchronous_API_V1_1_1_4.exe**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

Write Mifare Key To Reader | Key Nr. | Tr. Option: Plain / Secured | En. Key Nr. 80 | Key (A0A1...)

ATR: 3b8f8001804f0ca0000003060a0018000000007a | UID: 0d757400f7ff12e0 | Card Name: ICLASS 2KS

Old ContactlessDemoVC.exe

Authenticate | Block Nr | Key Number | Read complete

Read | Data Read

Increment | by | Value (4 bytes hex)

Transmit | 5 # byte | 10 # byte | 80B0000600

Refresh Output Screen | Mifare Emulation

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

DESK-Feb2015 ▸ iClass Cloner V3020140831 ▸

New folder

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

Name	Date modified	Type	Size	Date created
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				

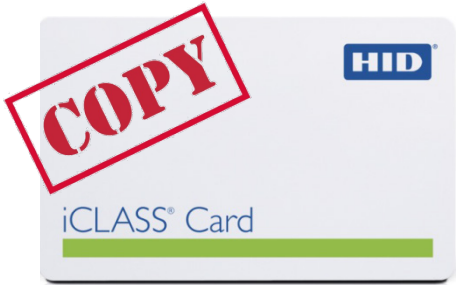
ExeInfo

```
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
```

Show File Info | Copy To Clipboard | Exit

iCLASS Cloner

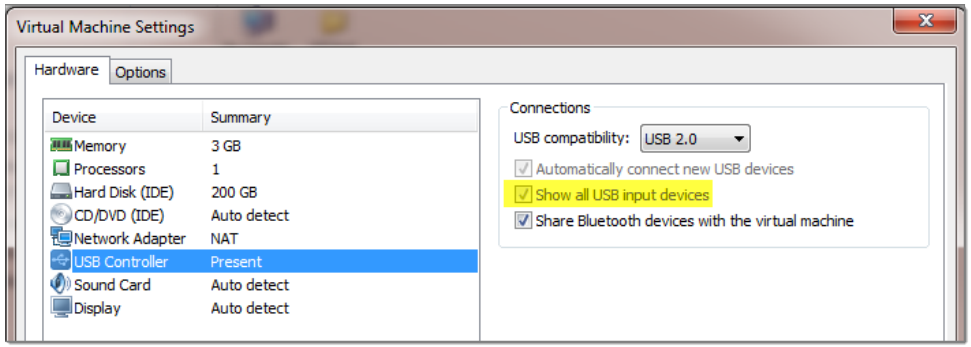
XFPGA.COM - FROM CHINA



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:

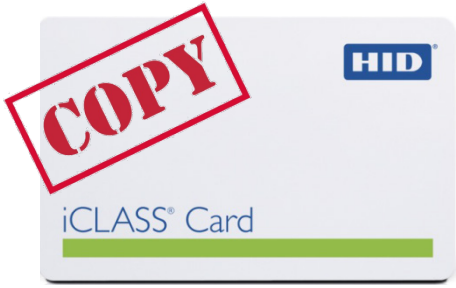


- USB license dongle pass through:

- Omnikey USB pass through:

iCLASS Cloner

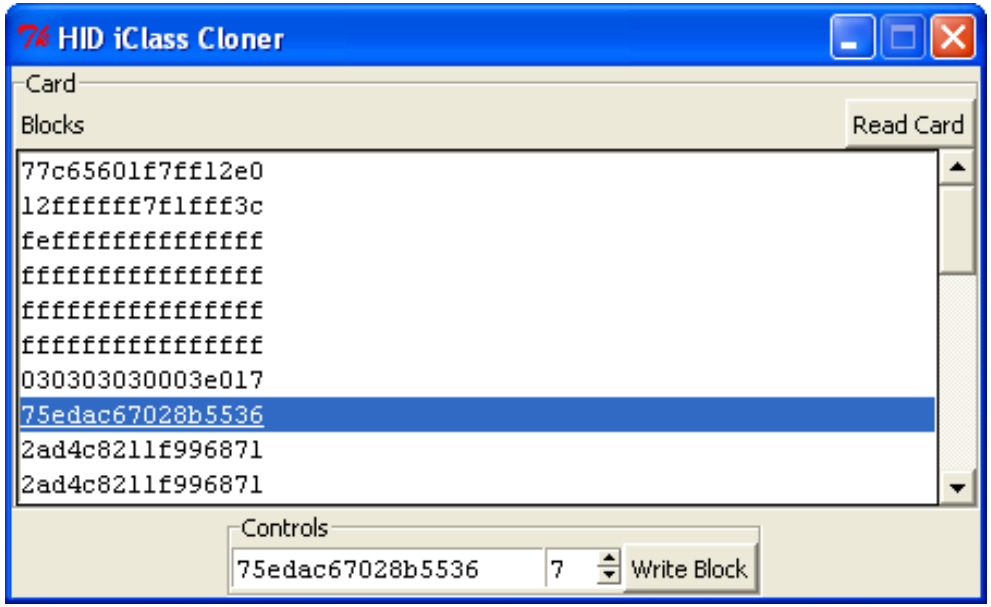
NEW – Bishop Fox – FREE Edition



UPDATE

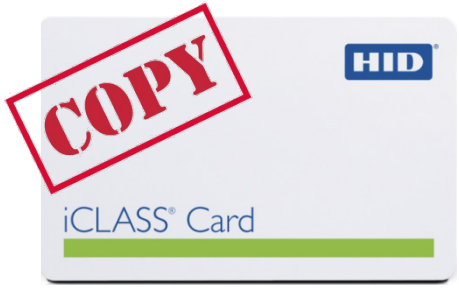
Read / Write to HID iCLASS Cards:

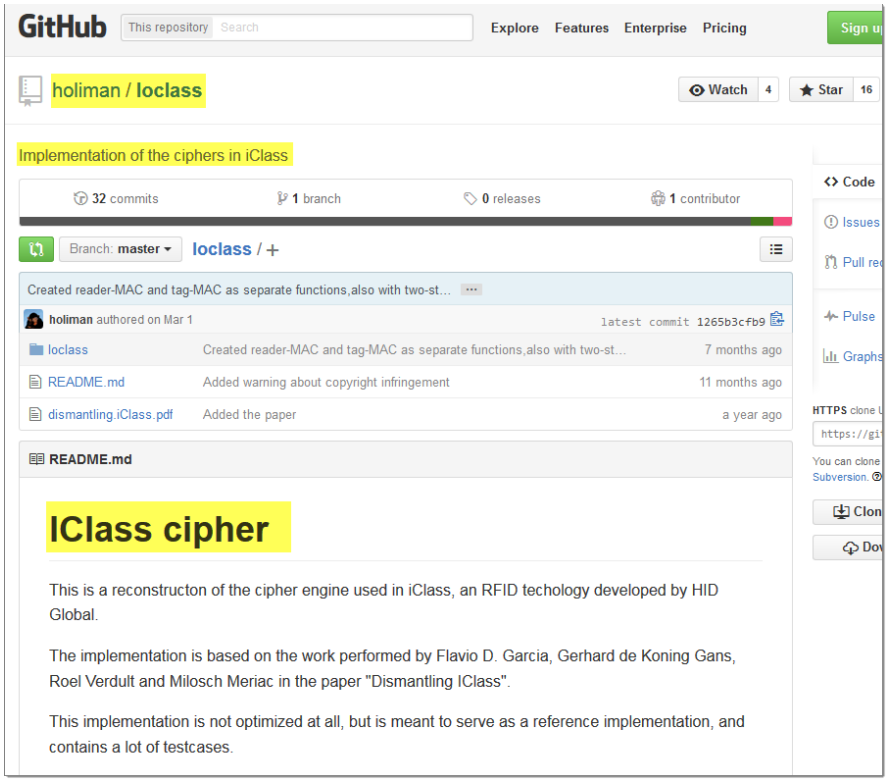
- https://blog.kchung.co/reverse-engineering-hid-iclass-master-keys/
- https://github.com/ColdHeat/iclass

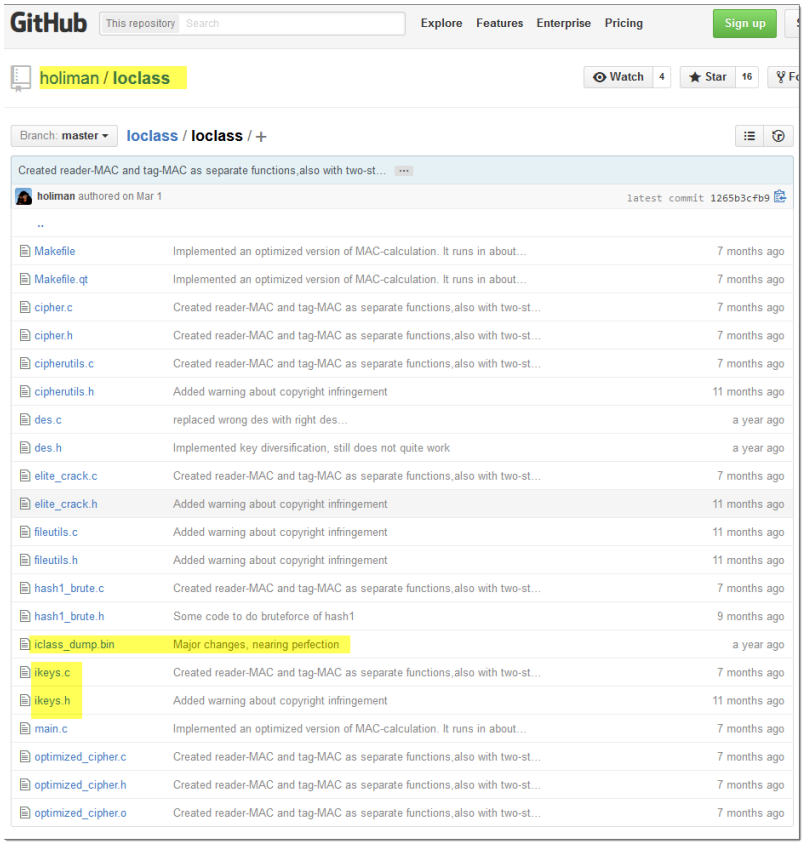


iCLASS Cloning

Ioclass – Implementation of iCLASS Ciphers



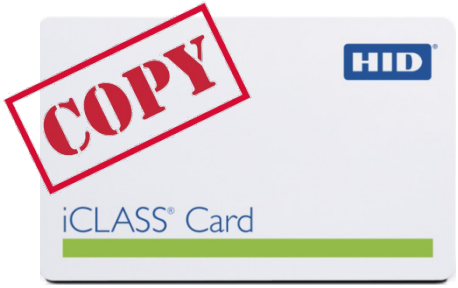




- http://martin.swende.se/blog/Elite-Hacking.html
- https://github.com/holiman/loclass

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

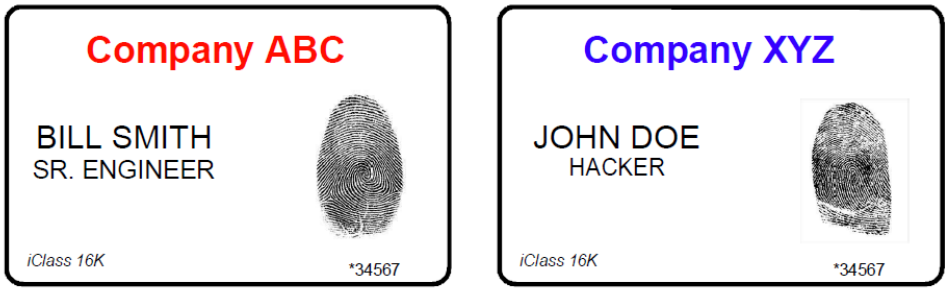
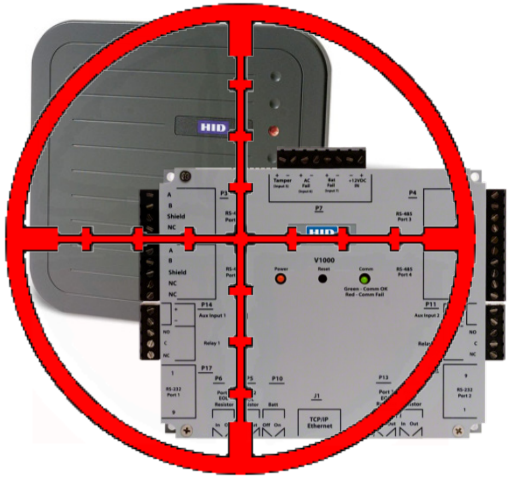


Figure 4. Different cards, yet they are considered identical from the bioCLASS reader and backend controller perspective.

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

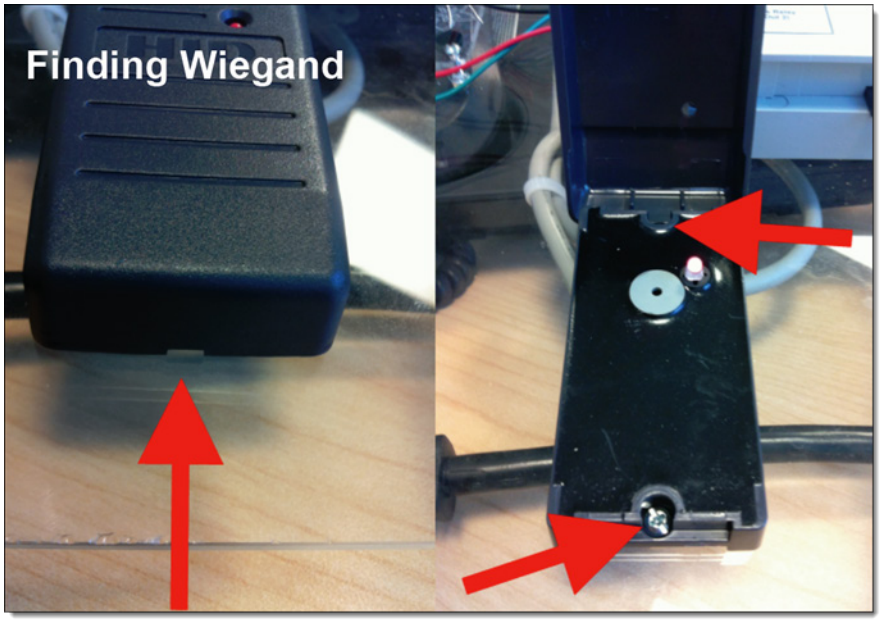


Reader and Controller Attacks

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)

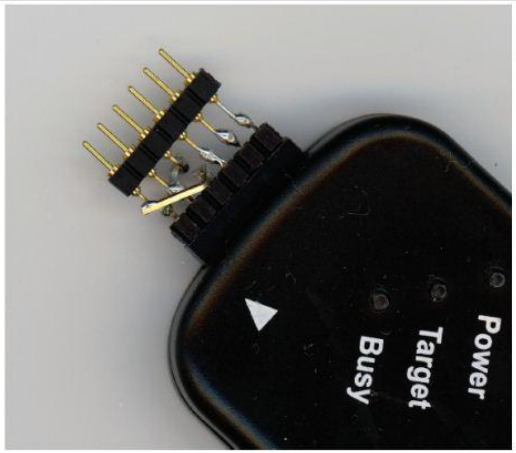
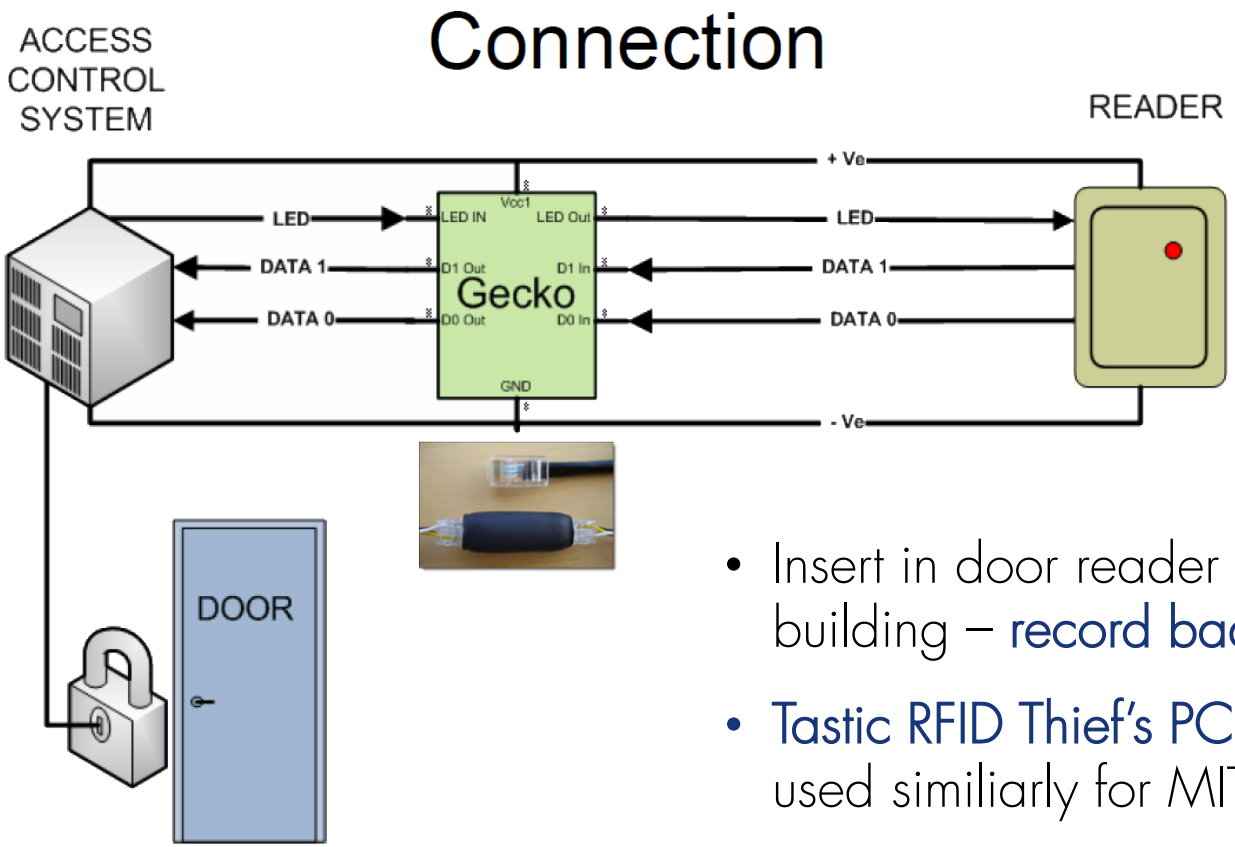


Fig. 3. Programming interface adapter for PICkit2 to switch Pin 1 with Pin 3.

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

Reader Attacks

BLEKEY–MITM ATTACK

threat post

BLEkey

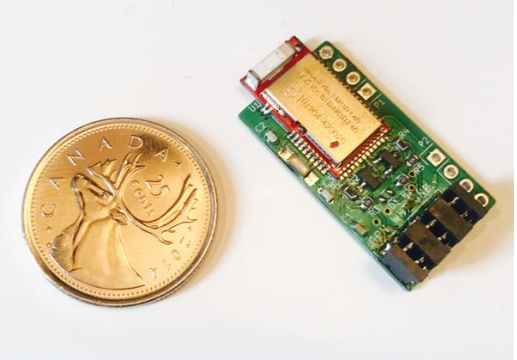
06 Aug 2015

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

BLEKEY DEVICE BREAKS RFID PHYSICAL ACCESS CONTROLS

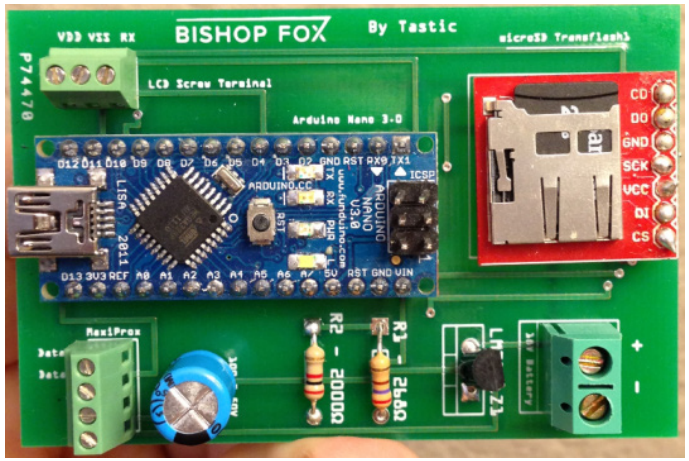
by Michael Mimoso | August 6, 2015 , 4:42 pm

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.

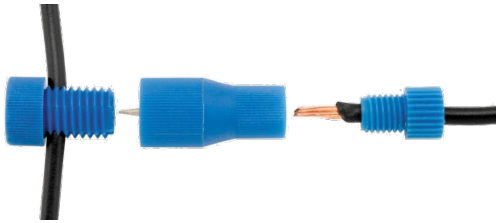


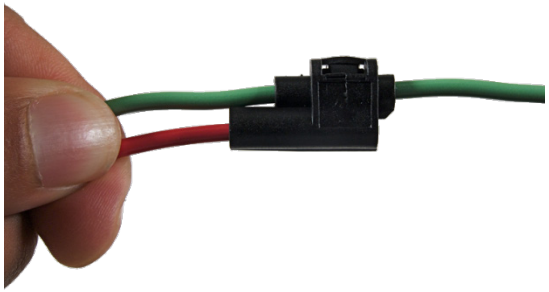
Reader Attacks

TASTIC–MITM ATTACK



+

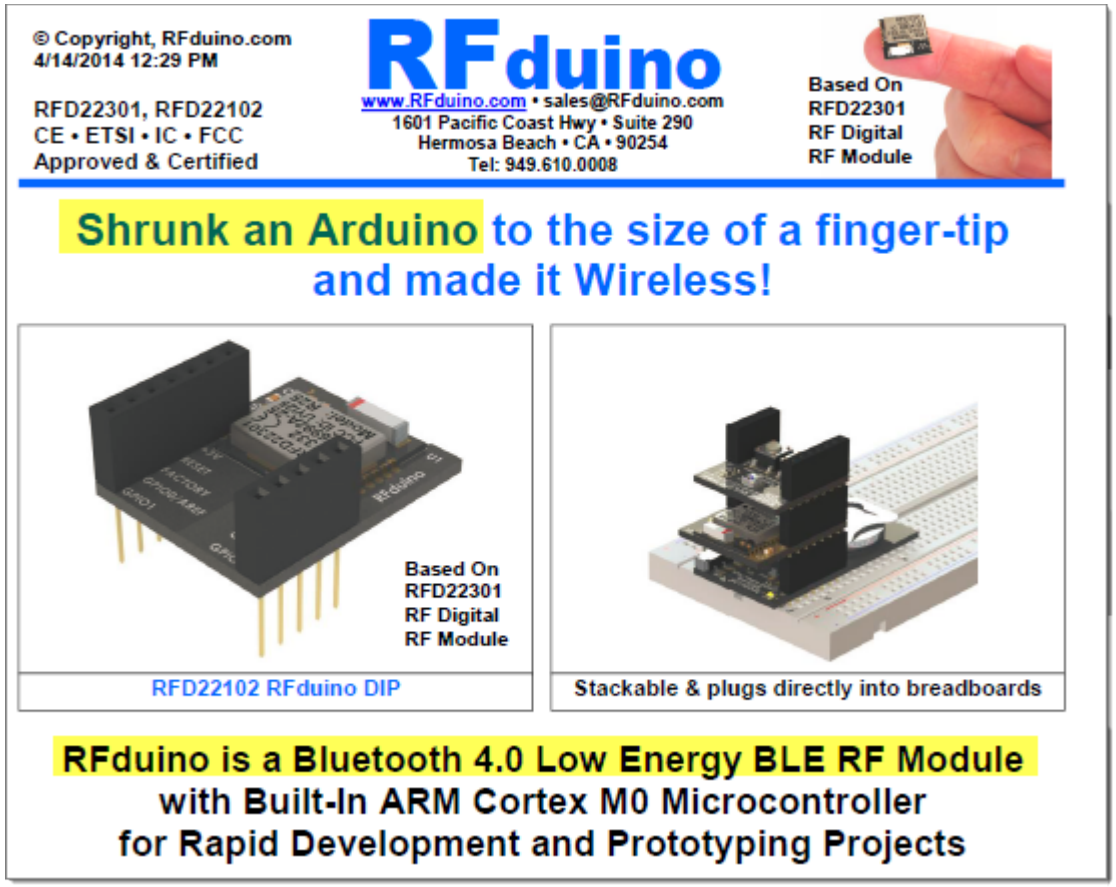




- Insert in door reader of target building – record badge #s
- Tastic RFID Thief's PCB could be used similiarly for MITM attack

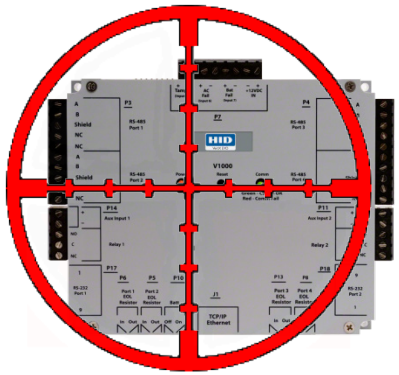
Reader Attacks

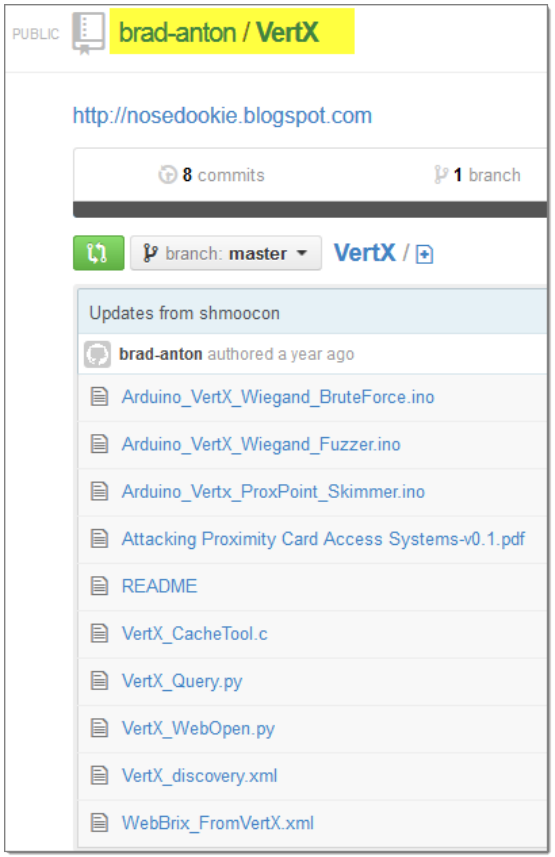
TASTIC–MITM ATTACK

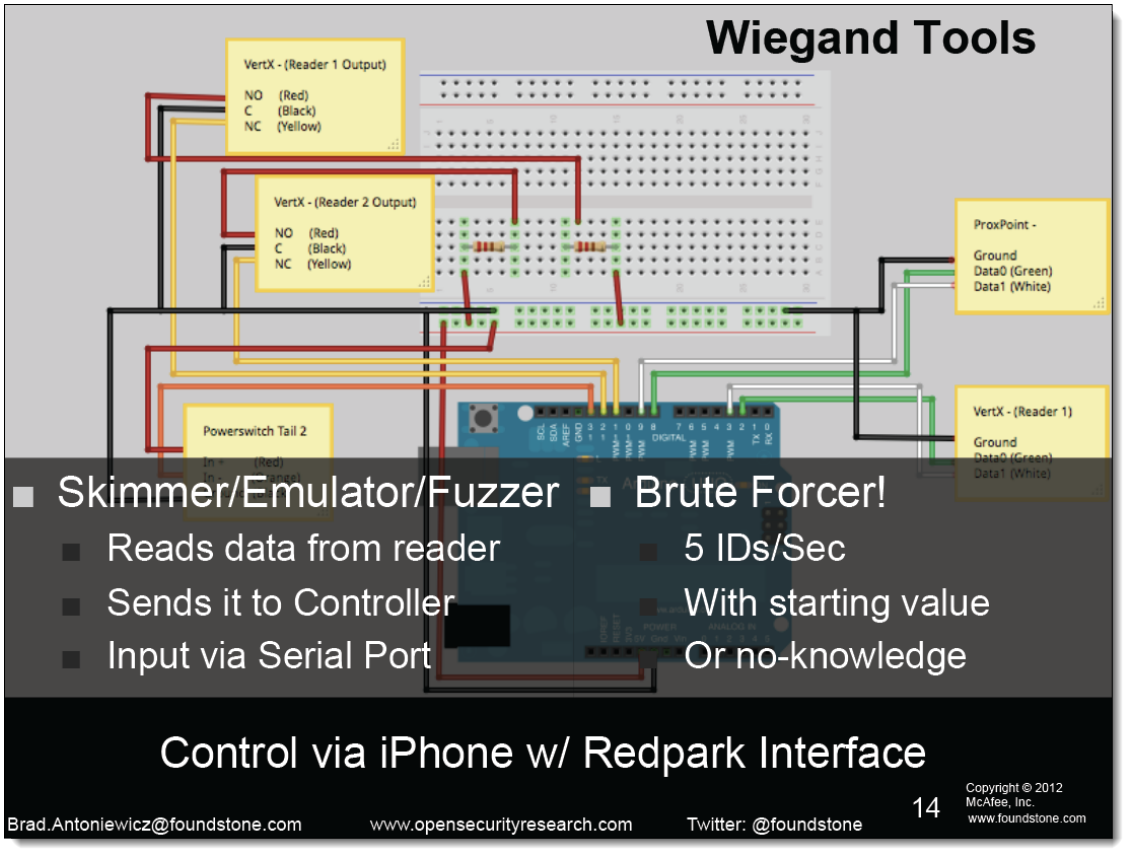


Controller Attacks

JACKED IN

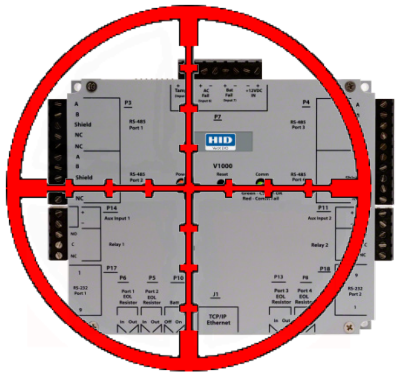






Controller Attacks

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`

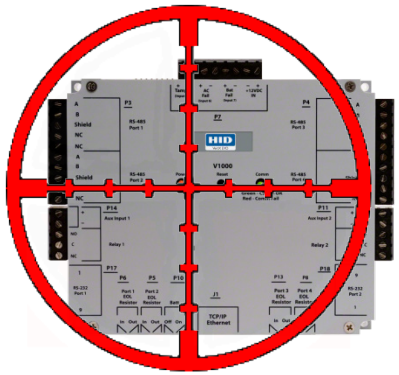
Attacking the VertX Controller Over the Network:

- `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

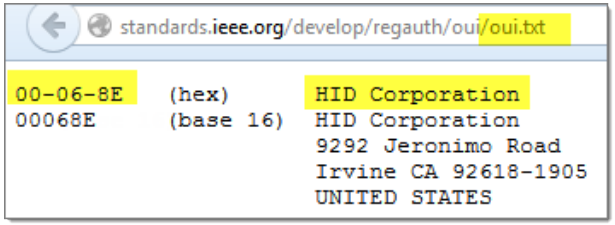
Controller Attacks

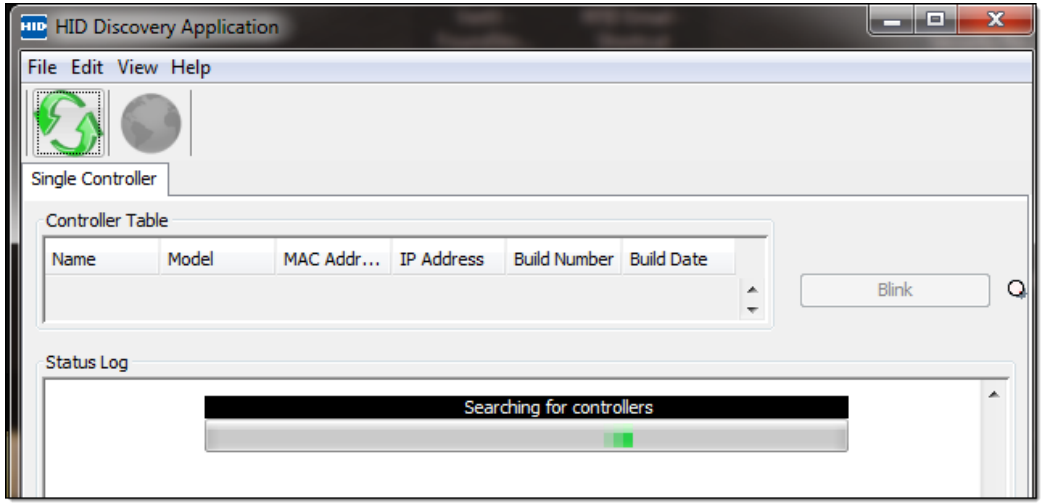
JACKED IN



MAC Address - Targetting HID Controllers Over Network

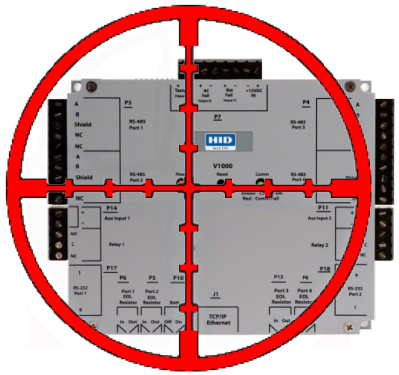
- HID Global – MAC Address OUI: 00:06:8E:*:*:*
- Scan network for MAC Addresses starting with 00:06:8E: directly, or use HID's controller discovery GUI tool:
  - https://www.hidglobal.com/drivers/15654





Controller Attacks

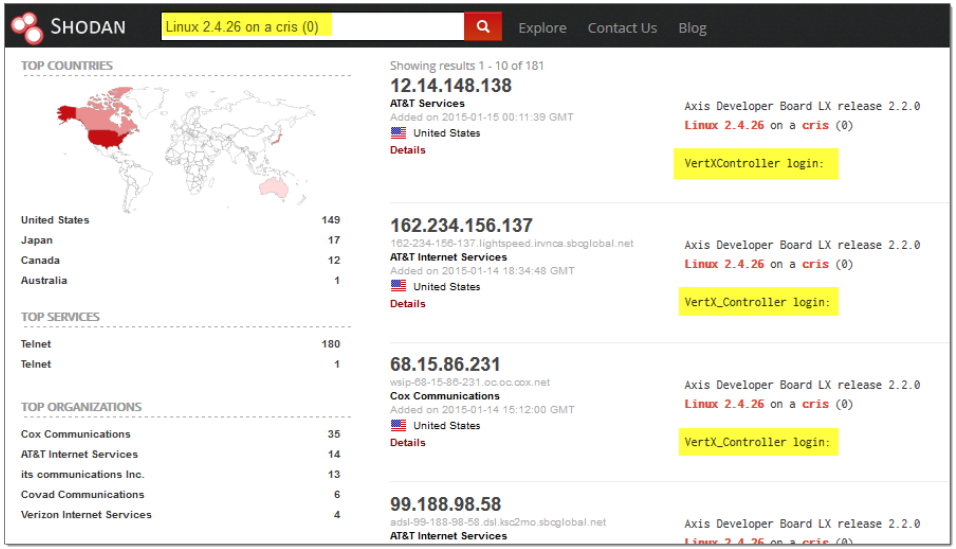
JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

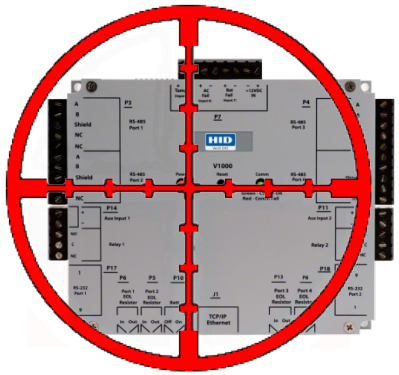
- HID VertX Controller – Default Open Ports:
  - FTP (21), Telnet (23), HTTP (80)
- HID VertX Controller – Connect via FTP / Telnet / HTTP with Default Admin Creds: **`root/pass`**
- Banner grabbing for HID VertX controller discovery
  - Can also find using SHODAN search engine

```
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:
```



Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

Search Diggity

File Options Help

Google | CodeSearch | Bing | LinkFromDomain | DLP | Flash | Malware | PortScan | NotInMyBackyard | BingMalware | Shodan

Simple | Advanced

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

SCAN | Cancel | Settings

API Key: Create [redacted] Hide

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://68.15.8[illegible]31:23/	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[illegible]	-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[illegible]	-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[illegible]	-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

Output | Selected Result

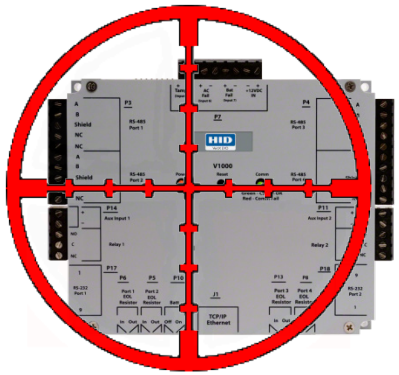
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:

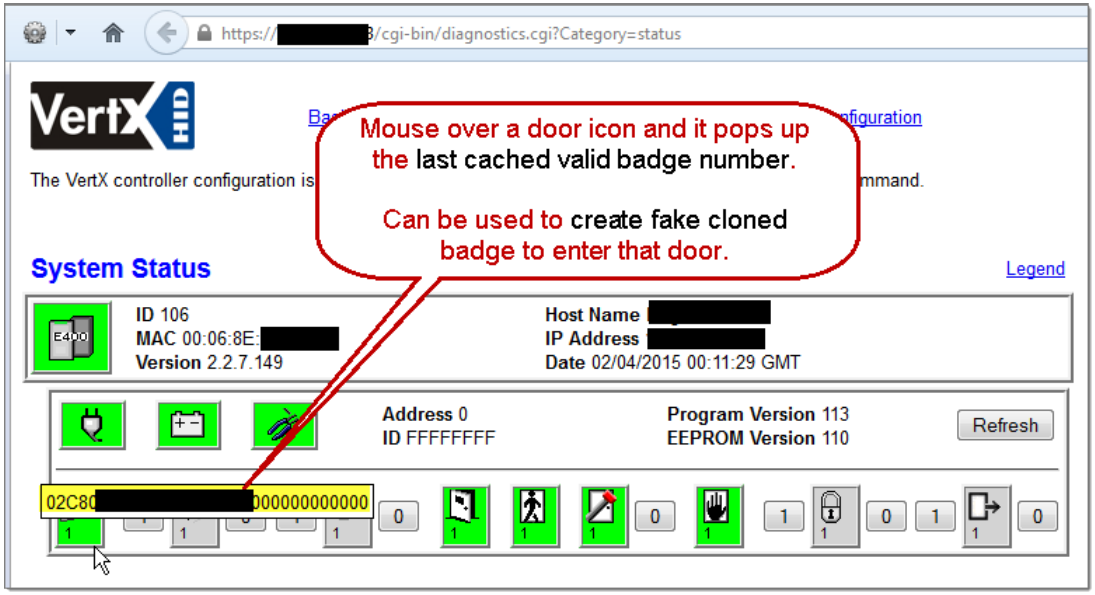
Shodan Status: Ready

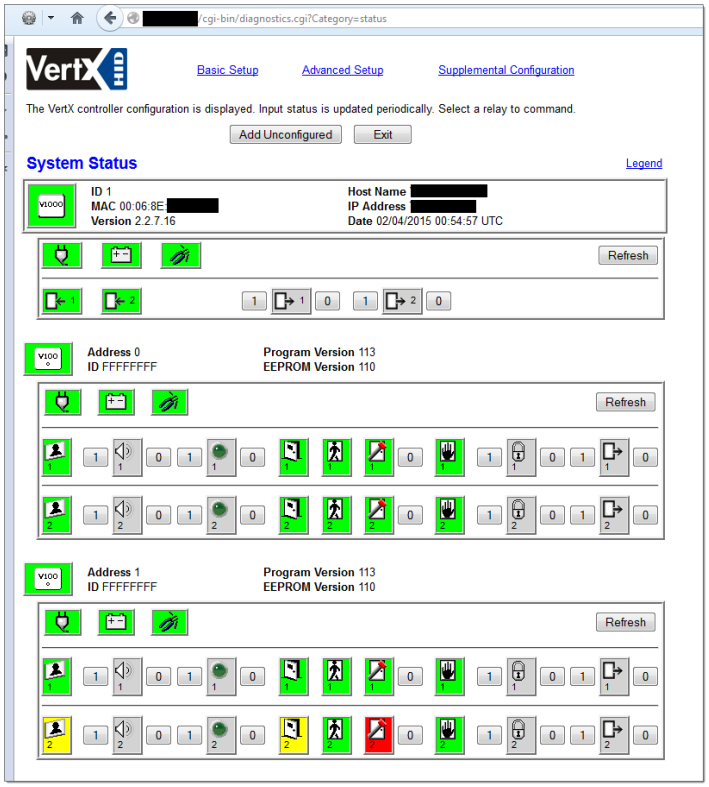
Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network





Controller Attacks

JACKED IN

Mar 2016

TREND MICRO | SIMPLY security

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.

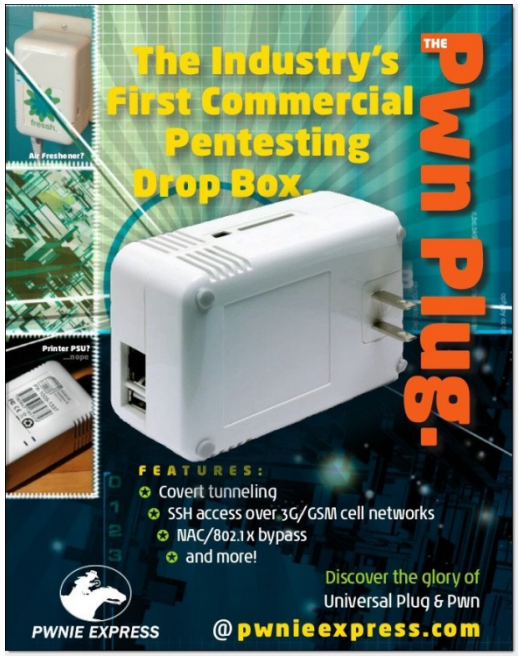
In recent years, these door controllers have been given network interfaces so that they can be managed remotely. It is very handy for pushing out card database updates and schedules, but as with everything else on the network, there is a risk

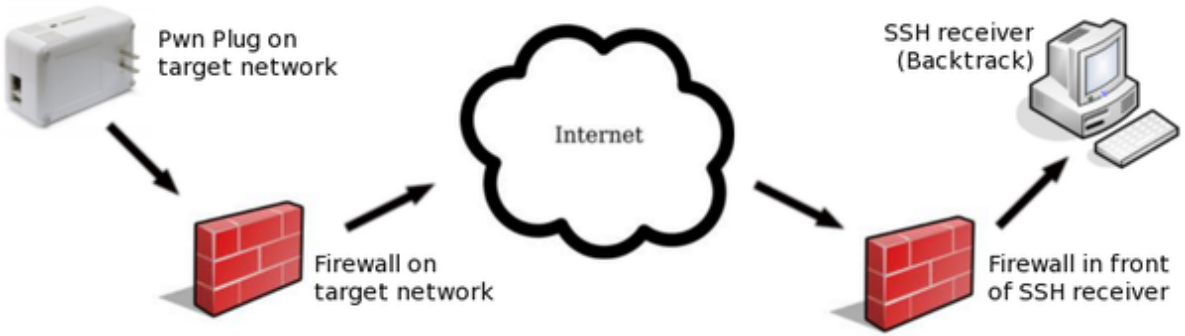
Backdoors and Other Fun

LITTLE DIFFERENCES

Pwn Plug

MAINTAINING ACCESS






```
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

Raspberry Pi

MAINTAINING ACCESS

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

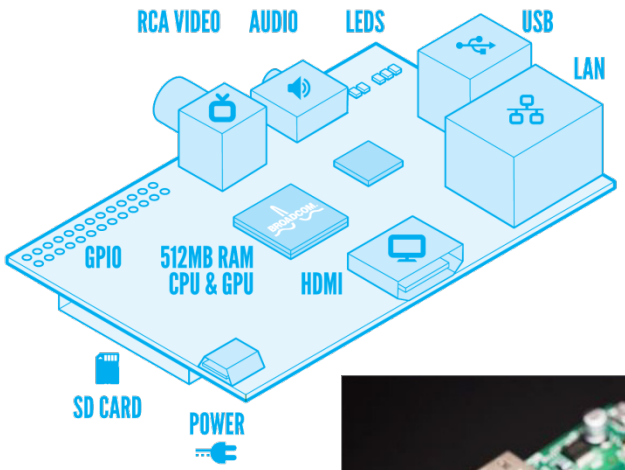
Security Affairs Read, think, share ... Security is everyo

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.

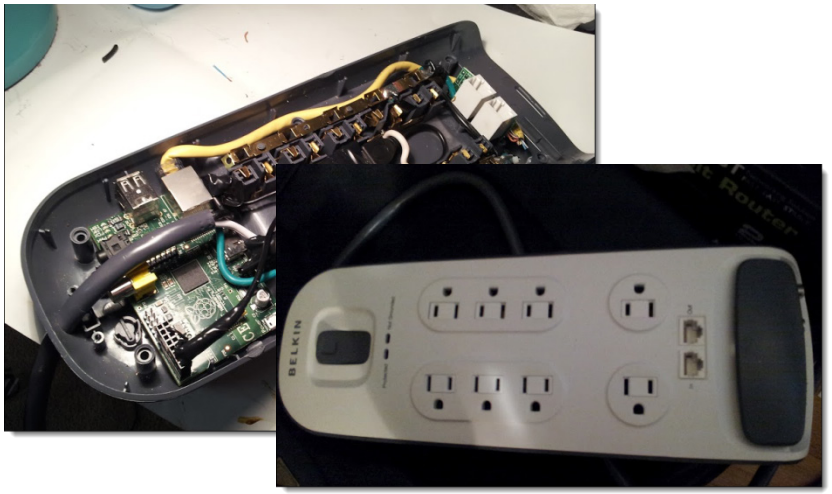
Network security engineer "Richee" published an interesting post on how to use a tiny Raspberry Pi computer to obtain physical access into a corporate network. I decided to publish this post because it gives us a lesson on security perspective, Richee has in fact used the tiny Raspberry Pi hiding it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

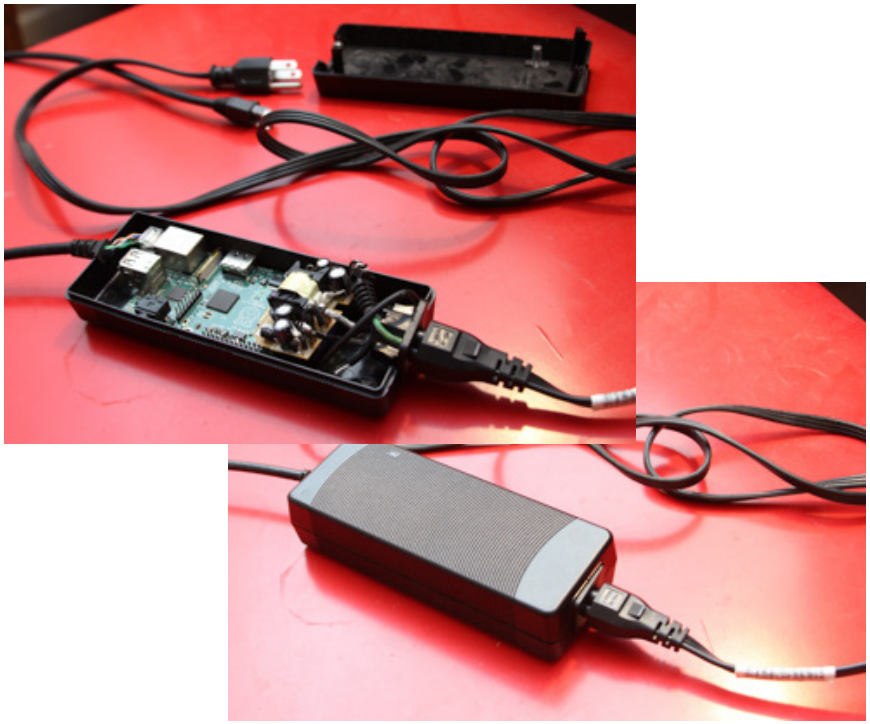


Raspberry Pi

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

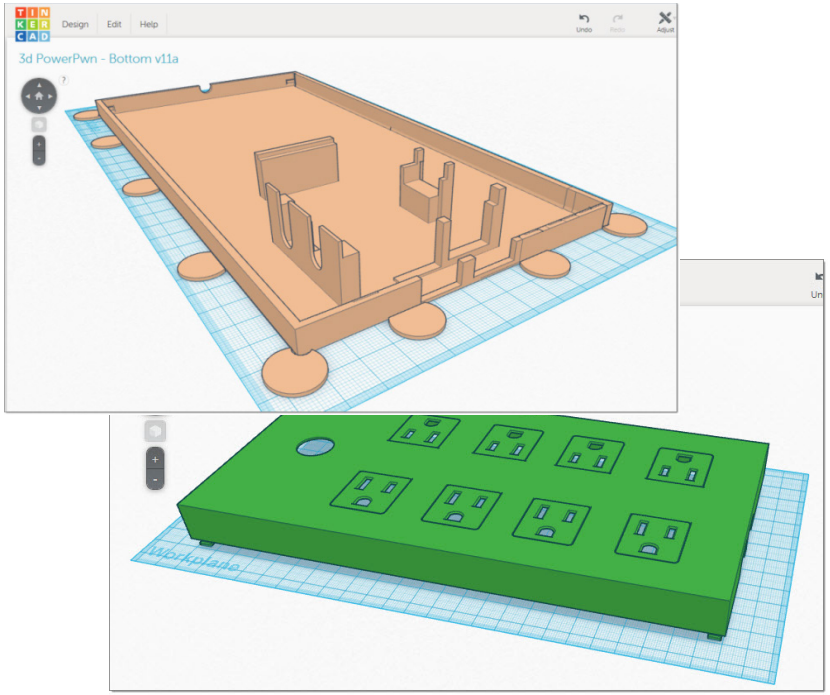




Raspberry Pi

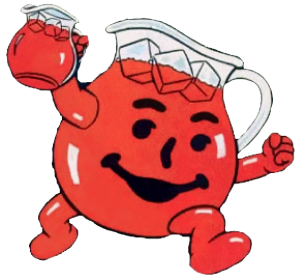
MAINTAINING ACCESS

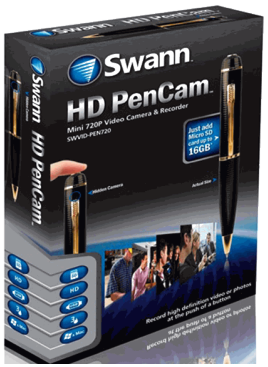
- Raspberry Pi – cheap alternative (~$35) to Pwn Plug/Power Pwn
  - Tastic 3D Case for RaspPi Backdoor Hidden Backdoor Device



Little Extra Touches

GO A LONG WAY

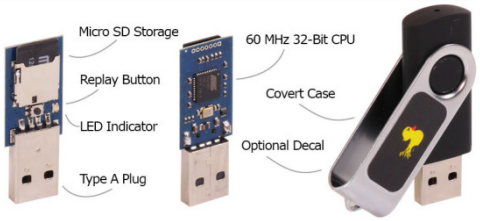




HD PenCam - Mini 720p Video

Lock picks and pick guns

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



USB Rubber Ducky Delux

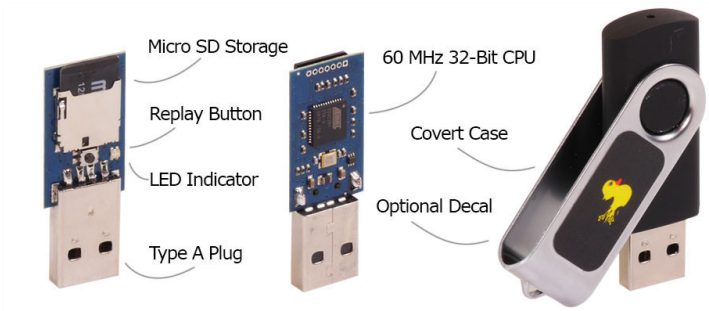
Label Printer and Badge Accessories

Fargo DTC515 Full Color ID Card ID Badge Printer

BISHOP FOX

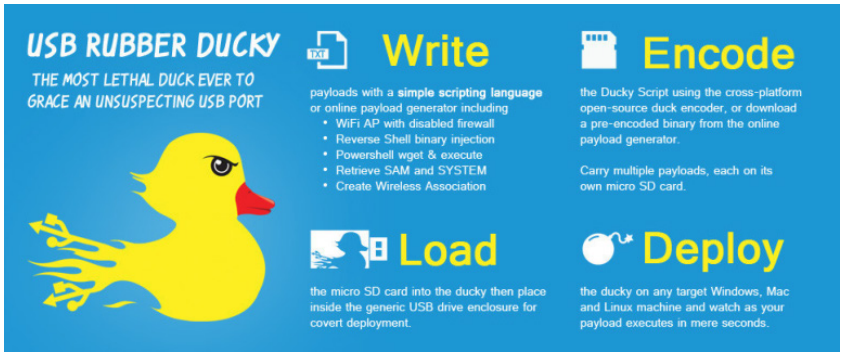
USB Rubber Ducky Delux

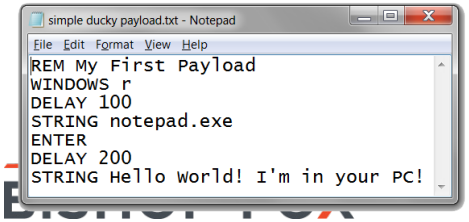
QUICK PHYSICAL OWNAGE

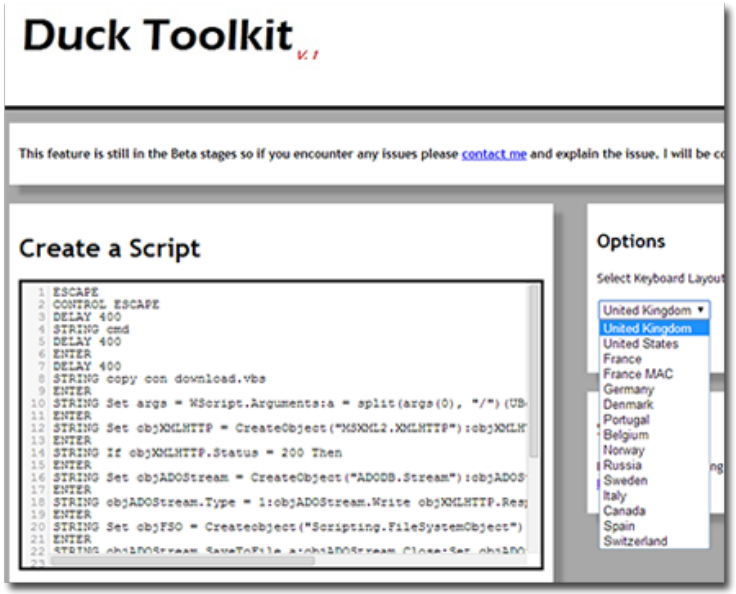


"If it quacks like a keyboard and types like a keyboard, it must be a keyboard."

"Humans use keyboards, and computers trust humans."







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
000000001000000003000000	000000001000000637291901	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)

Credit Card RFID

SKIMMING

Feb 2016

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

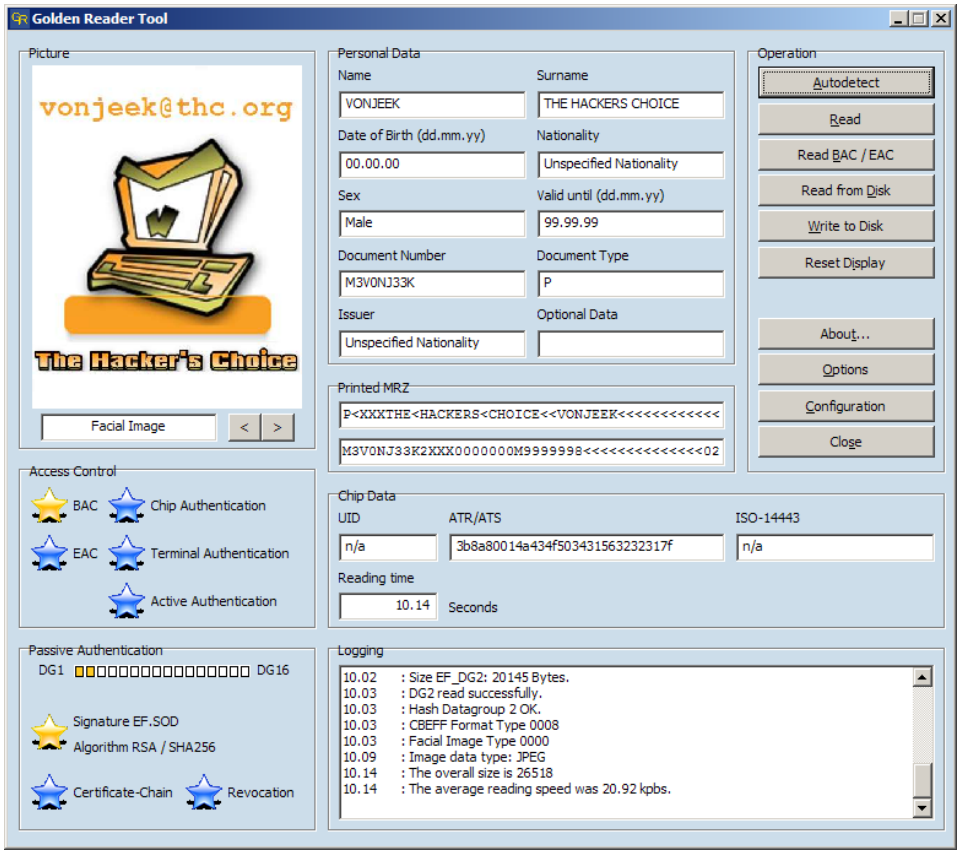
BISHOP FOX

Passports (Book)

R F I D I N I D

Passport Books

RFID



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

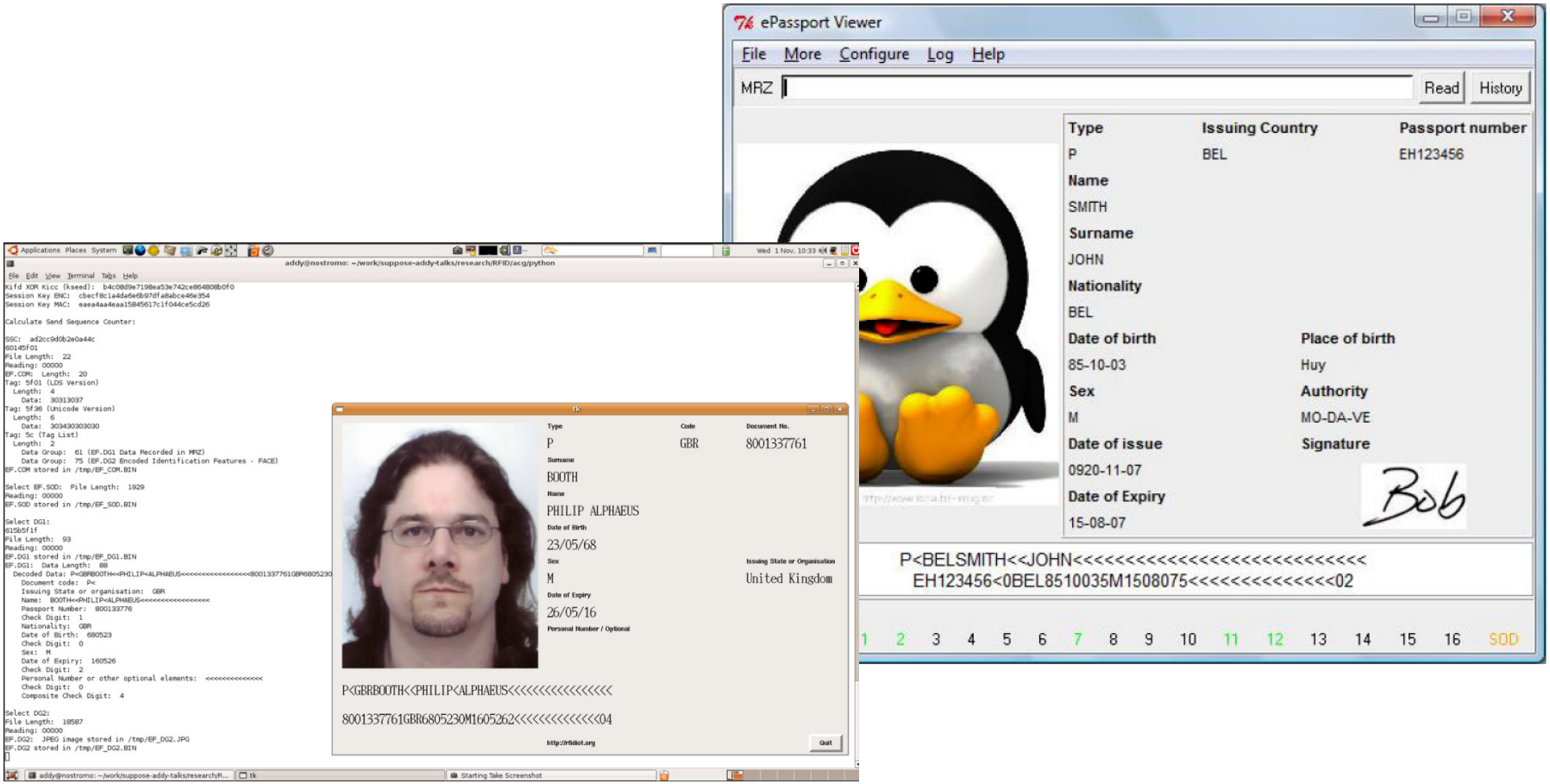
mrpkey.py

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

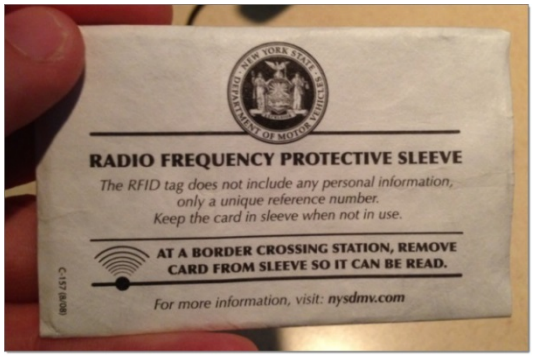


UHF Hacking

ULTRA

Enhanced Licenses

RFID

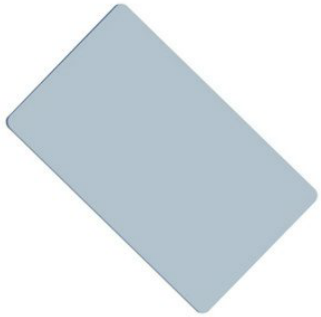


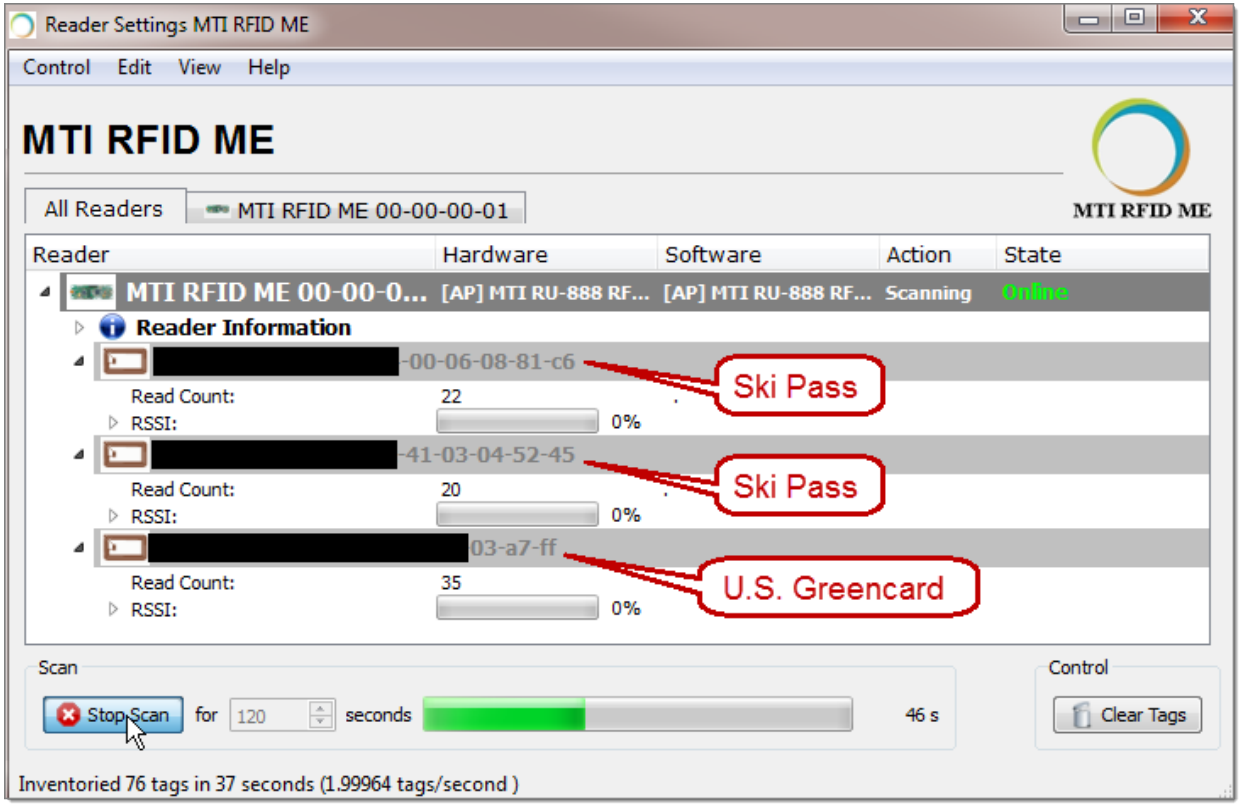
UHF - RFID Gear

ULTRAHIGH FREQUENCY

RFID ME: USB Dongle UHF Reader /Writer

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





BISHOP FOX

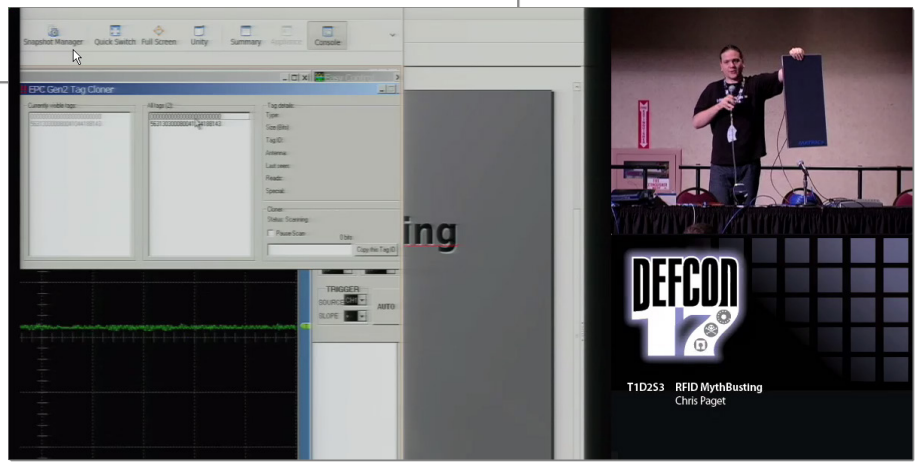
UHF Custom Tools

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

217 feet

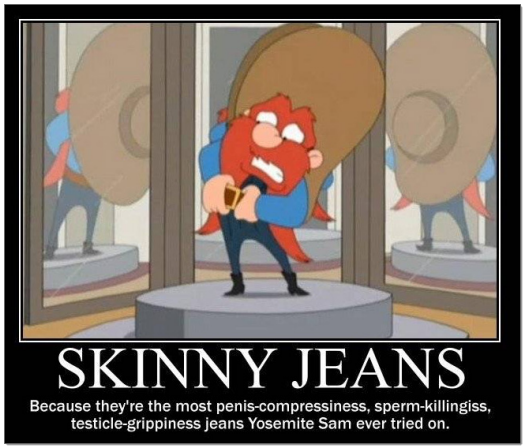


Defenses

AVOID BEING PROBED

Defenses

F L Y G E A R



- 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.

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.

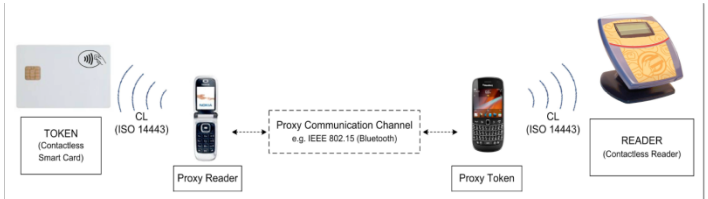
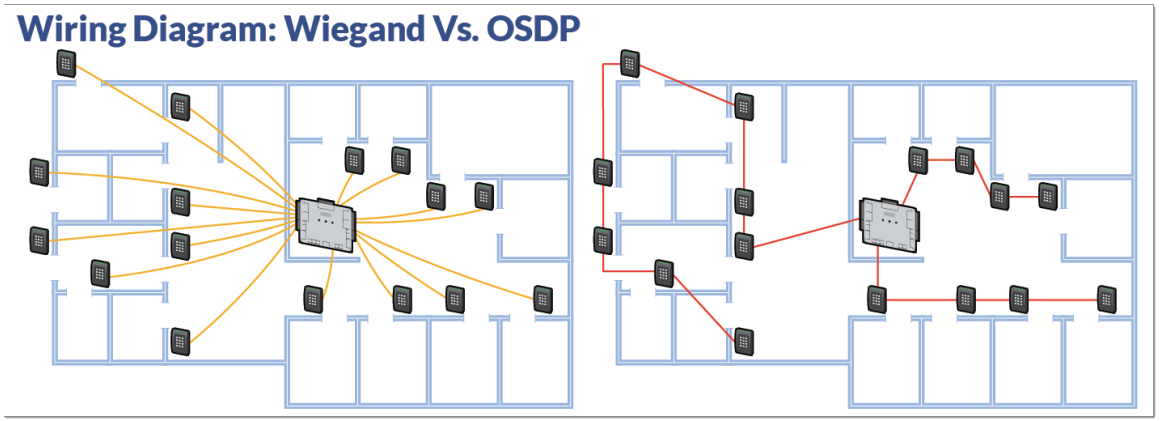
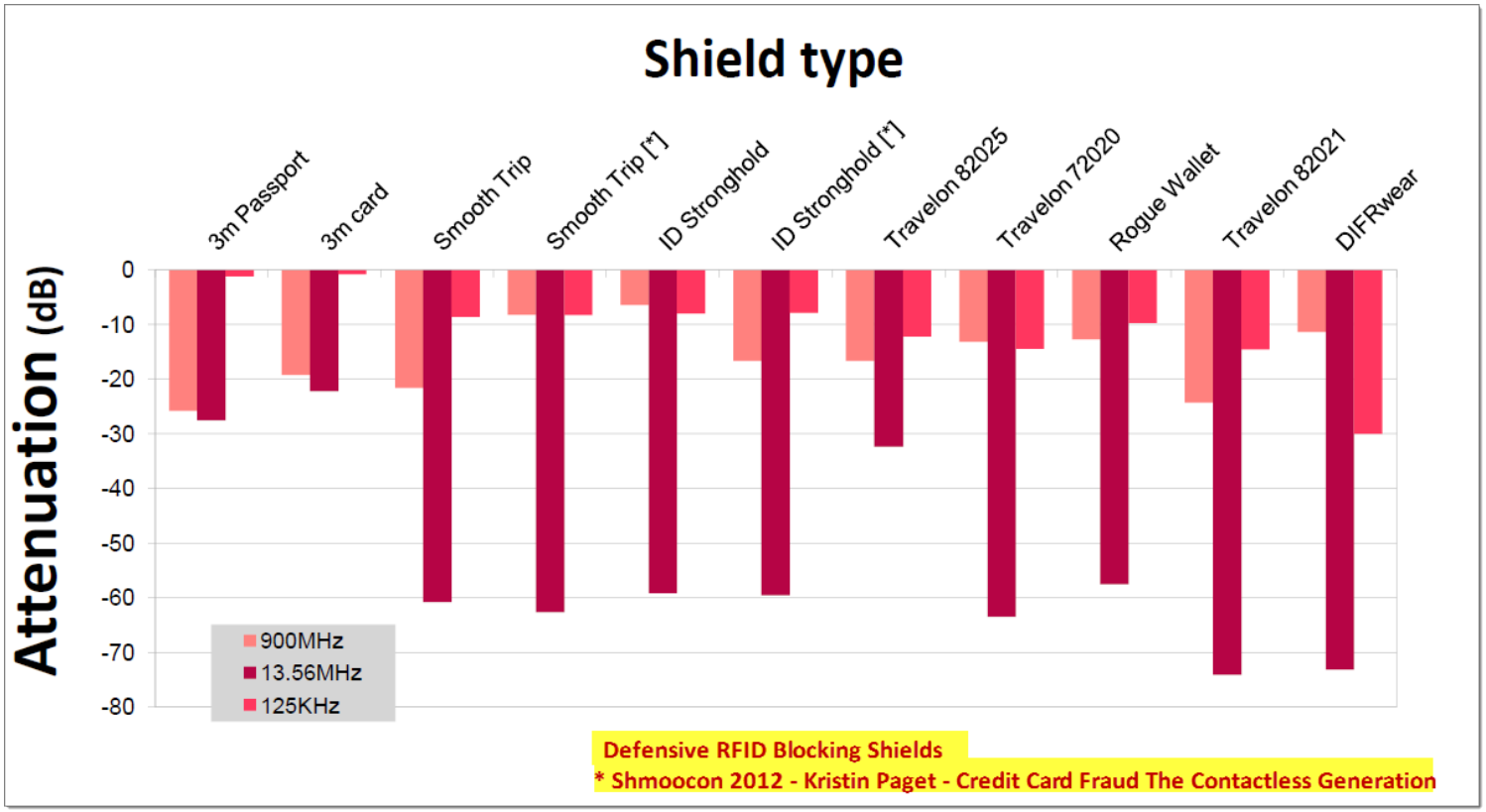


Figure 2: Practical relay setup using only NFC mobile phones.



Defenses (Broken)

SOME DON'T...EXAMPLE...



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/