



# RFID Hacking

Live Free or RFID Hard

03 Aug 2013 – DEF CON 21 (2013) – Las Vegas, NV



Presented by:  
Francis Brown  
Bishop Fox  
[www.bishopfox.com](http://www.bishopfox.com)

# Agenda

## OVERVIEW

- Quick Overview
  - RFID badge basics
- Hacking Tools
  - Primary existing RFID hacking tools
  - Badge stealing, replaying, and cloning
  - Attacking badge readers and controllers directly
  - Planting Pwn Plugs and other backdoors
- Custom Solution
  - Arduino and weaponized commercial RFID readers
- Defenses
  - Protecting badges, readers, controllers, and more





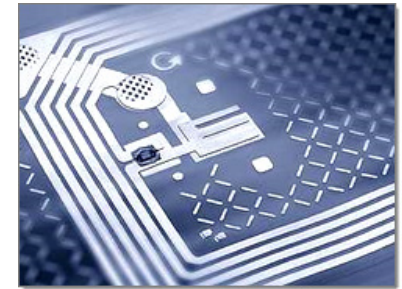
# Introduction/Background

GETTING UP TO SPEED



# Badge Basics

## FREQUENCIES



Name	Frequency	Distance
Low Frequency (LF)	120kHz – 140kHz	<3ft (Commonly under 1.5ft)
High Frequency (HF)	13.56MHz	3-10 ft
Ultra-High-Frequency (UHF)	860-960MHz (Regional)	~30ft



# Legacy 125kHz

STILL KICKIN



- “Legacy 125-kilohertz proximity technology is still in place at around 70% to 80% of all physical access control deployments in the U.S. and it will be a long time” - Stephane Ardiley, HID Global.
- “There is no security, they’ve been hacked, there’s no protection of data, no privacy, everything is in the clear and it’s not resistant to sniffing or common attacks.”

80%

# Opposite of Progress

TALK MOTIVATIONS

HID  
Prox

125 kHz

Indala  
Prox

125 kHz

## So what then?

- If you're using 125KHz Prox, your doors are highly insecure.
- Demo time!

**IOActive™**  
COMPREHENSIVE COMPUTER SECURITY SERVICES

← 2007

2013 →



The Trusted Source for  
Secure Identity  
Solutions

Language

Home > Blog > Making the Leap from Prox to Contactless ID Cards

## Making the Leap from Prox to Contactless ID Cards

Posted: 06/13/13 by Zack Martin

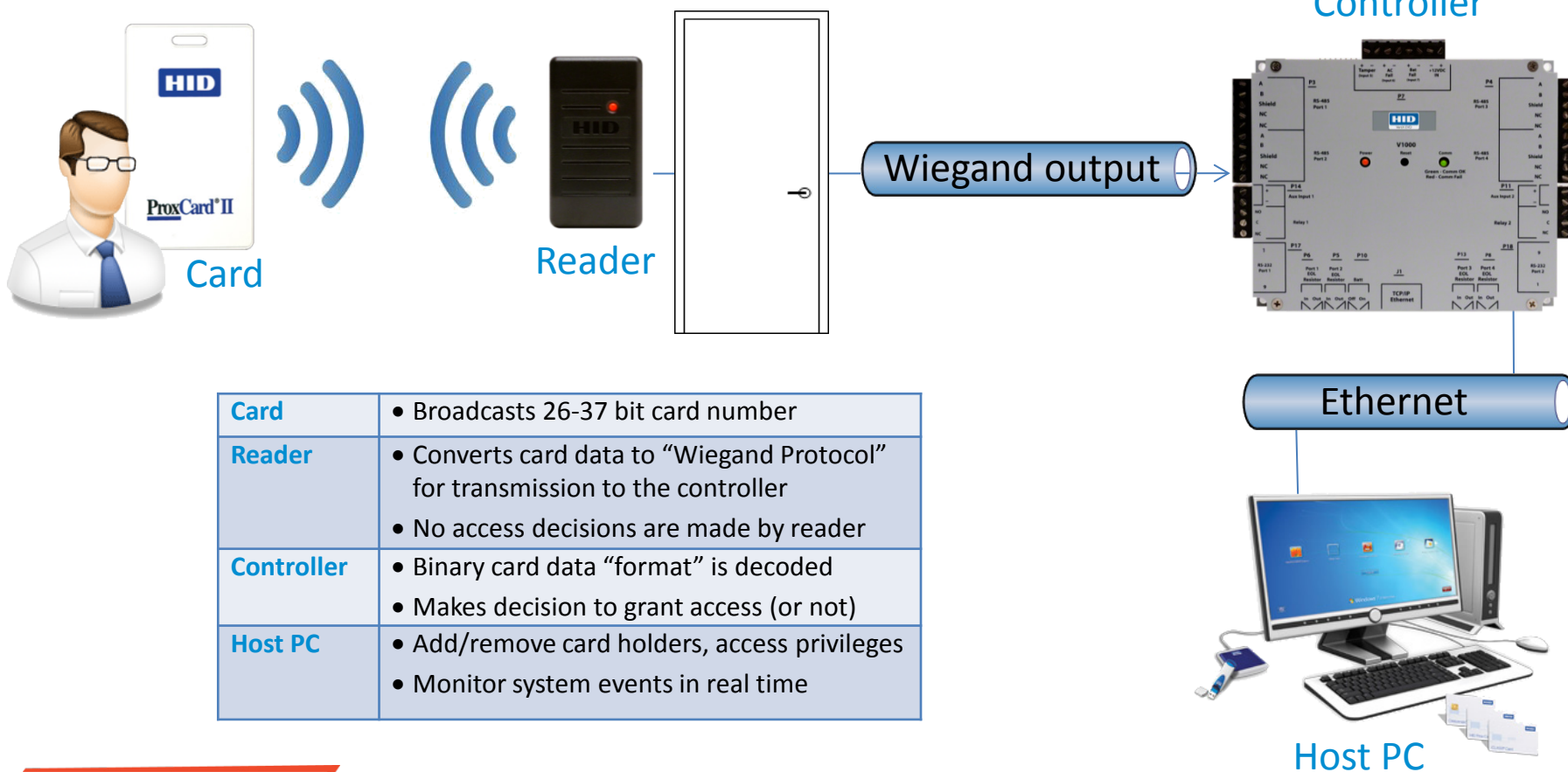
Legacy 125-kilohertz proximity technology is still in place at around 70% to 80% of all physical access control deployments in the U.S. and it will be a long time before that changes, says Stephane Ardiley, product manager at HID Global.

...

Still there are many reasons a migration from older access technologies is inevitable. The biggest is the increase in security. "Proximity cards and mag stripes are basic technologies when it comes to physical access control," Ardiley says. "There is no security, they've been hacked, there's no protection of data, no privacy, everything is in the clear and it's not resistant to sniffing or common attacks."

# How a Card Is Read

## POINTS OF ATTACK



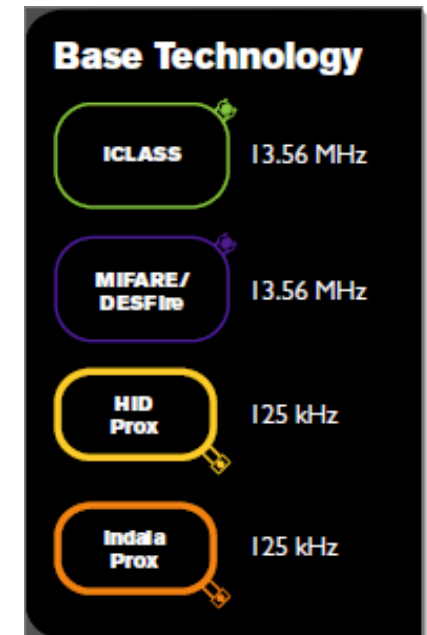
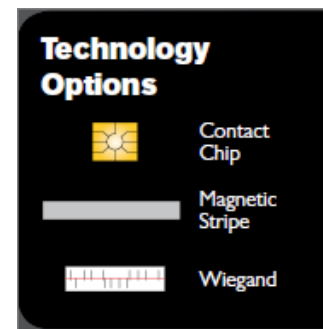
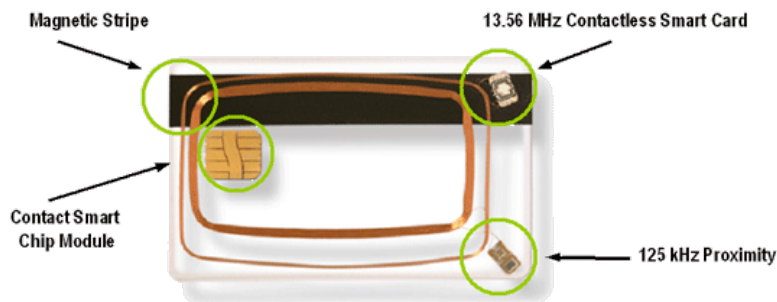
<b>Card</b>	<ul style="list-style-type: none"><li>• Broadcasts 26-37 bit card number</li></ul>
<b>Reader</b>	<ul style="list-style-type: none"><li>• Converts card data to “Wiegand Protocol” for transmission to the controller</li><li>• No access decisions are made by reader</li></ul>
<b>Controller</b>	<ul style="list-style-type: none"><li>• Binary card data “format” is decoded</li><li>• Makes decision to grant access (or not)</li></ul>
<b>Host PC</b>	<ul style="list-style-type: none"><li>• Add/remove card holders, access privileges</li><li>• Monitor system events in real time</li></ul>

# Badge Types

HID PRODUCTS



- The data on any access card is **simply a string of binary numbers** (ones and zeros) of some fixed configuration and length, used to identify the cardholder
- HID makes **different types of cards** capable of carrying this binary data including:
  - Magnetic Stripe
  - Wiegand (swipe)
  - 125 kHz Prox (HID & Indala)
  - MIFARE contactless smart cards
  - iCLASS contactless smart cards
  - \* *Multi-technology cards*





# Badge Types



## HID Technology Card Guide

HID technology cards enable users to seamlessly manage multiple applications and migration projects through a single credential containing diverse technologies.

### 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.



### Low Frequency

Genuine HID™ cards are designed to work with the large installed base of HID Prox and Indala proximity readers.



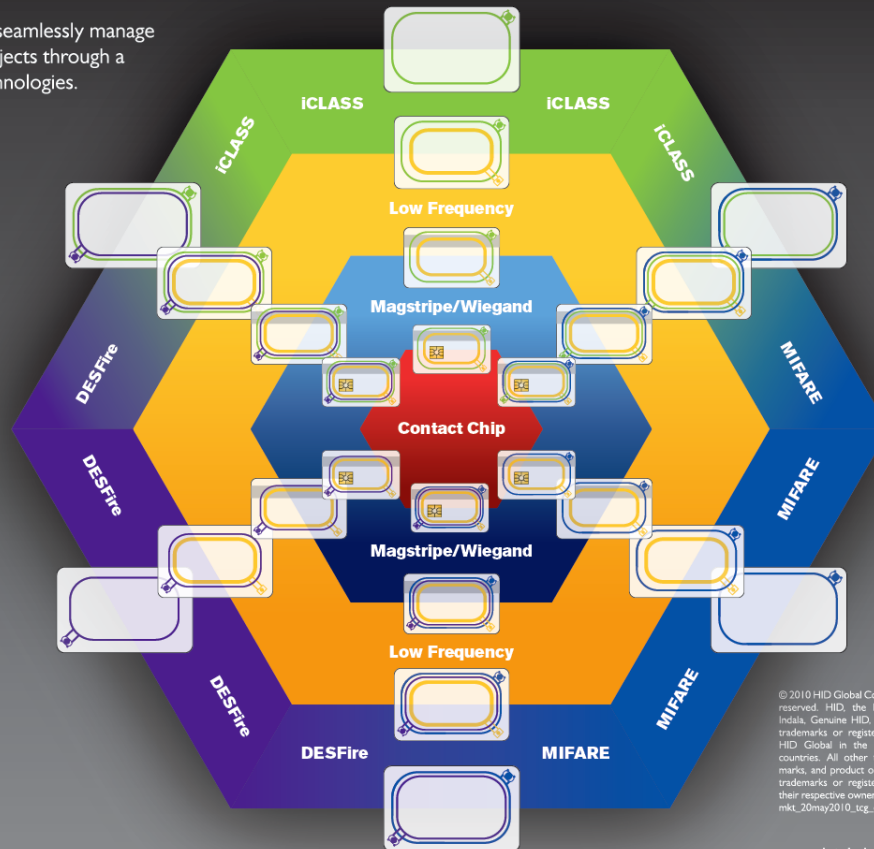
### Magstripe/Wiegand

A magnetic or Wiegand stripe can be added to maintain functionality with legacy access control, time and attendance and vending systems. Wiegand is not available on all combinations, please see the HTOG for details.



### Contact Chip

Crescendo® cards include a wide variety of contactless technologies, paired with an industry standard contact chip, to integrate with physical and logical access control solutions out-of-the-box. HID can also embed a wide range of commercially available contact chips.



© 2010 HID Global Corporation. All rights reserved. HID, the HID logo, iCLASS, Indala, Genuine HID, and Crescendo are trademarks or registered trademarks of HID Global in the U.S. and/or other countries. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.  
mkt\_20may2010\_ttg\_en

hidglobal.com

# Badge Basics





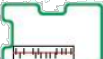

## CARD ELEMENTS



### Card – “Formats” Decoded

- Card ID Number
- Facility Code
- Site Code (occasionally)

#### Legend

-  Contact smart chip module
-  125 kHz proximity antenna and chip
-  13.56 MHz MIFARE contactless smart chip and antenna
-  Magnetic Stripe (1, 2 or 3 track, low or high coercivity, additional options available)
-  125 kHz proximity and Wiegand Code Strip
-  Durable PVC thin card with vertical or horizontal slot punch and high quality printing surface for photo ID and barcode, (ISO 7816 and 7810 compliant)

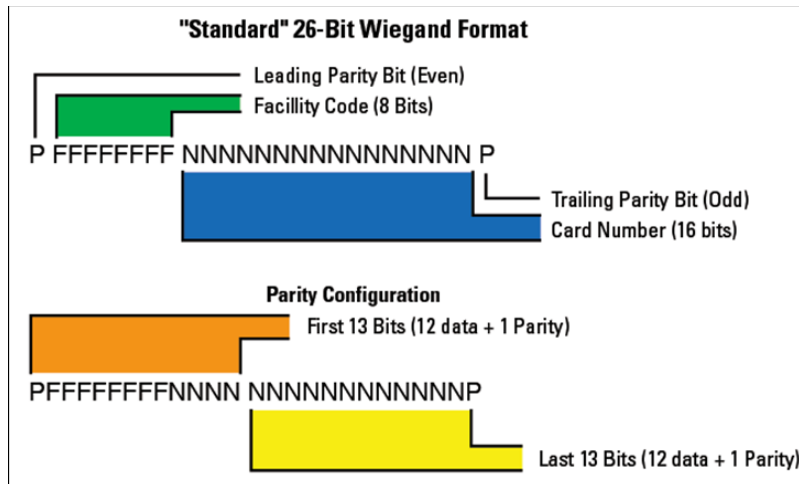
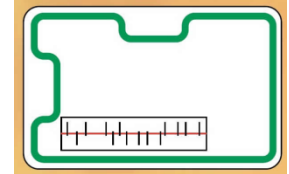


*\*Note: if saw printed card number on badge, could potentially brute force the 1-255 facility code (for Standard 26 bit card)*



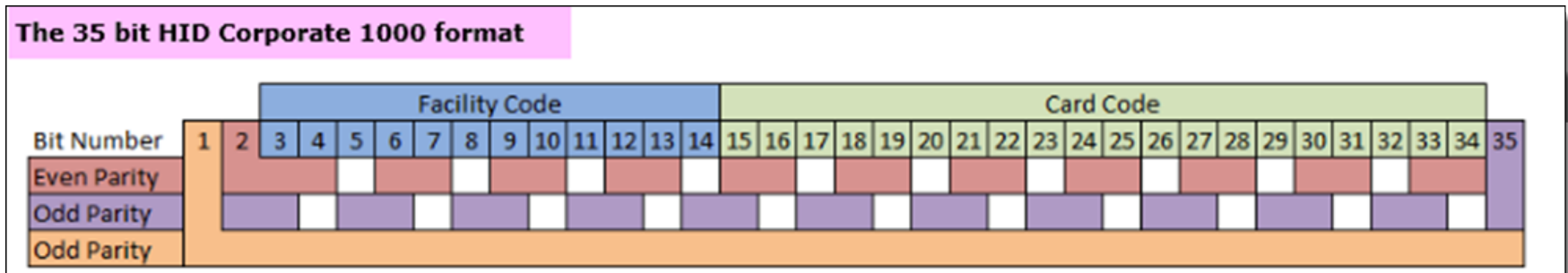
# Badge Formats

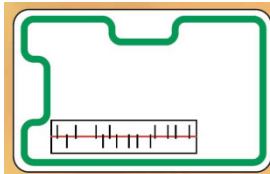
## DATA FORMATS



## HID ProxCard II "Formats"

- 26 – 37 bit cards
- 44 bits actually on card
- 10 hex characters
  - Leading 0 usually dropped





# Badge Formats

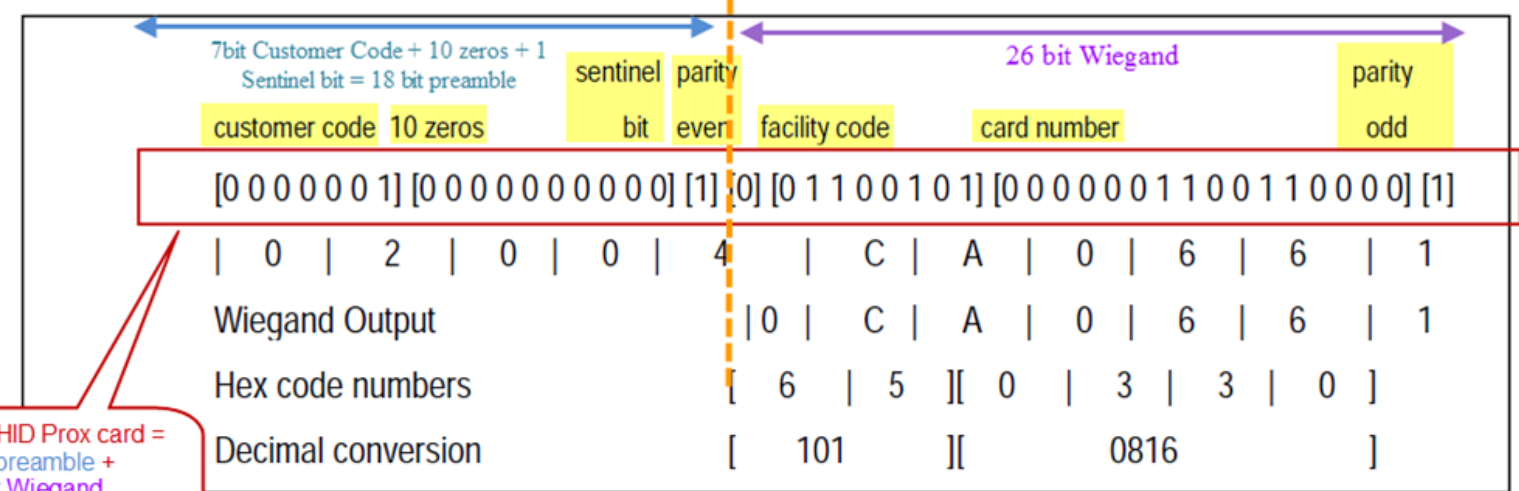
## DATA FORMATS

### 4.1.5 Example Output

The following is an example of an ID card with the number of "816" decimal, which will be output by the MaxiProx reader, the number "02004CA0661" hex.

**Note:** The customer code is never transmitted or displayed.

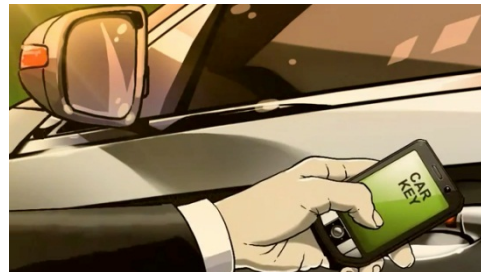
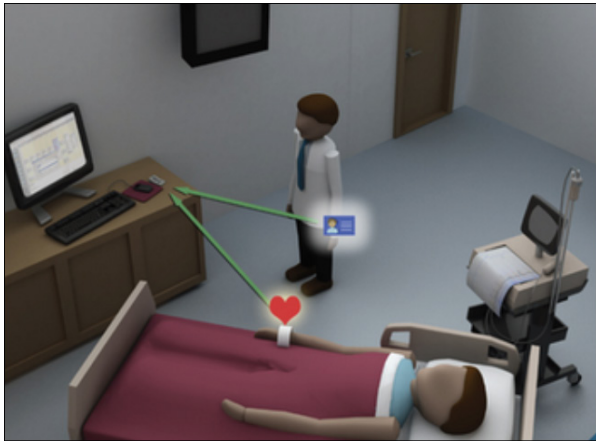
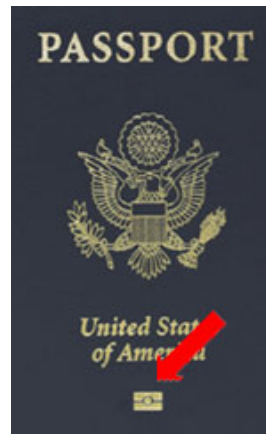
Represented as 10 HEX characters typically (with leading zero dropped)



44 bits on HID Prox card =  
18bit preamble +  
26bit Wiegand

# RFID Other Usage

WHERE ELSE?





# RFID Hacking Tools

PENTEST TOOLKIT

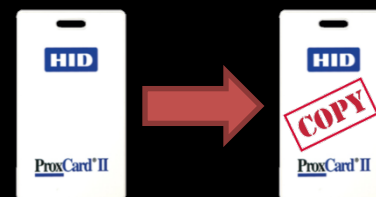
# Methodology

## 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
```



# Proxmark3

proxmark<sup>3</sup>



## RFID HACKING TOOLS

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



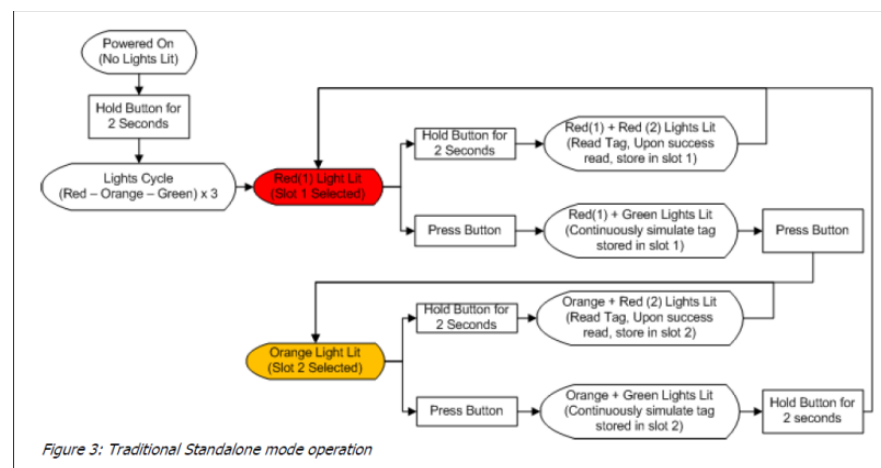
**proxmark<sup>3</sup>** **\$399**

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!**

```
proxmark3> lf hid fskdemod
#db# TAG ID: 98139d7c32 (5432)
#db# TAG ID: 98139d7c32 (5432)
#db# TAG ID: 98139d7c32 (5432)
#db# Stopped
```



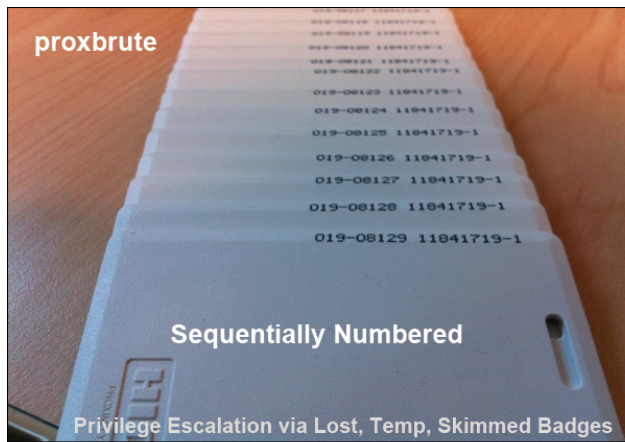
Single button, crazy flow diagram on lone button below

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

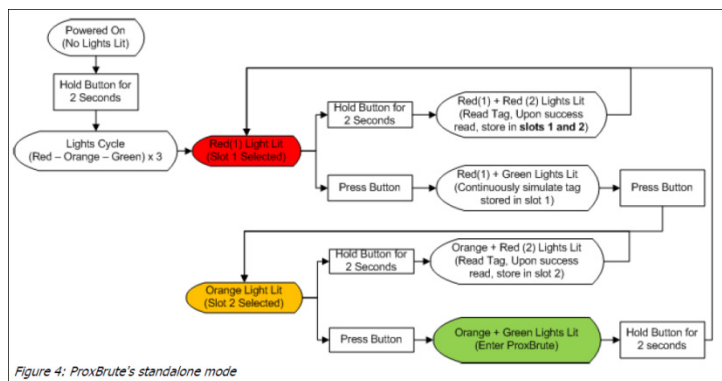


# ProxBruite

## RFID HACKING TOOLS



- Custom firmware for the Proxmark3
- Brute-force higher privileged badges, like data center door



Action	Debug Output
Hold down button for two seconds. Enter standalone mode. Lights cycle colors, then red LED becomes lit (slot 1 selected).	#db# Stand-alone mode! No PC necessary.
(Red lit) Hold down button for two seconds. Enter record mode. Two red LEDs become lit. After successful read, tag is stored in slot 1 and slot 2, and only one red LED is lit.	#db# Starting recording #db# TAG ID: 98139d7c32 (5432) #db# Recorded 98139d7c32 #db# [ProxBruite] In Mode Red, Copying read tag to orange
(Red lit) Press button. Briefly enter play mode.	#db# Playing #db# Red is lit, not entering ProxBruite Mode #db# 98139d7c32 #db# Done playing
	#db# Playing #db# Entering ProxBruite Mode #db# brad a. - foundstone #db# Current Tag: Selected = 1 Facility = 00000098 ID #db# Trying Facility = 00000098 ID 139d7c32 #db# Stopped #db# Trying Facility = 00000098 ID 139d7c31 #db# Stopped #db# Trying Facility = 00000098 ID 139d7c30 #db# Stopped #db# Told to Stop #db# Exiting proxmark3>



# RFIDiot Scripts

RFID HACKING TOOLS

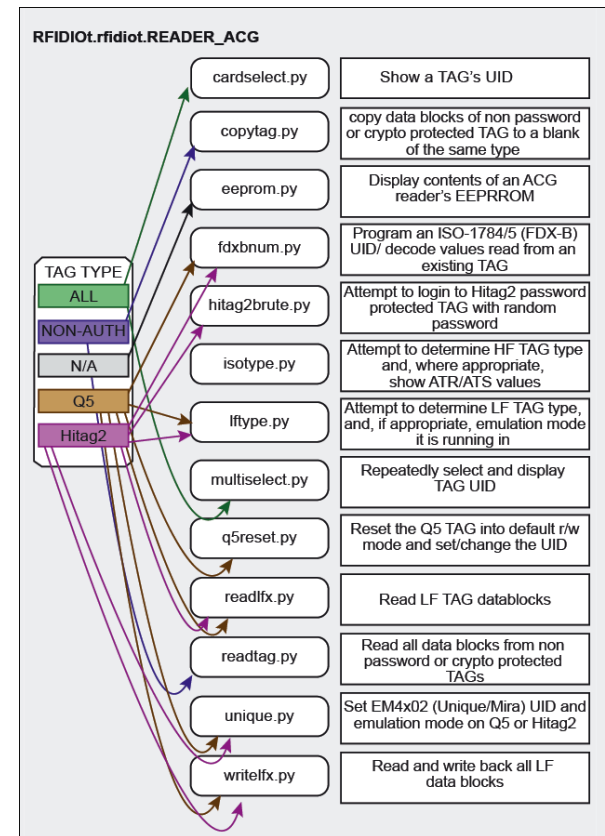


Terminal Output:

```

root@bt:/pentest/rfid/RFIDIOT# ./cardset
PCSC devices:
No: 0 OmniKey_CardMan
root@bt:/pentest/rfid/RFIDIOT#
  
```

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

# RF ID EAS

## RFID HACKING TOOLS

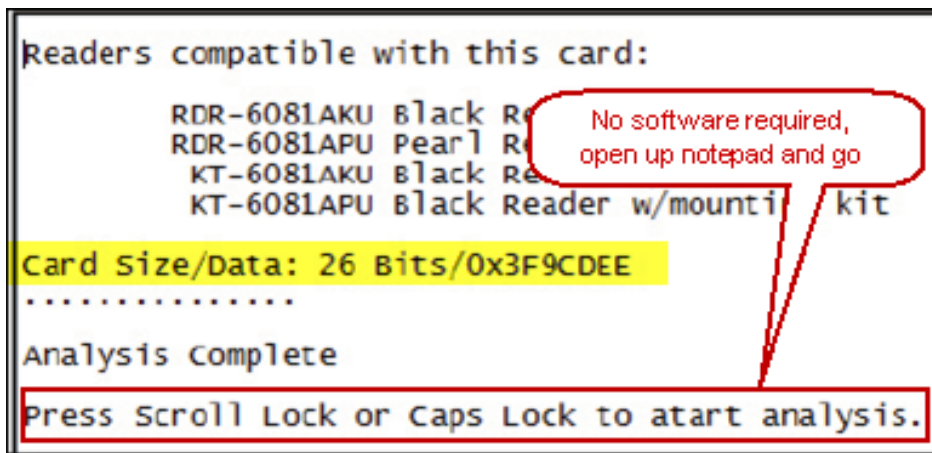
### pcProx® 125 kHz & AIR ID® 13.56 MHz Card Analyzer

\$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



#### 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

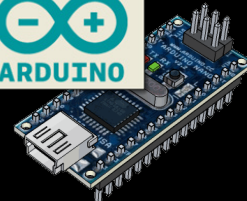
14443A/15693 CSN	*Felica
iCLASS® CSN	MIFARE® CSN
MIFARE® DesFire CSN	*1Sielox
*1XceedID®	

# 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
```



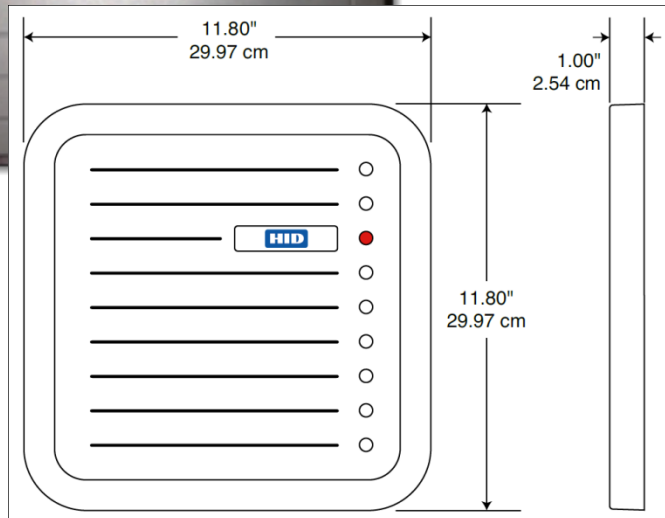


# Tastic RFID Thief



LONG RANGE RFID STEALER

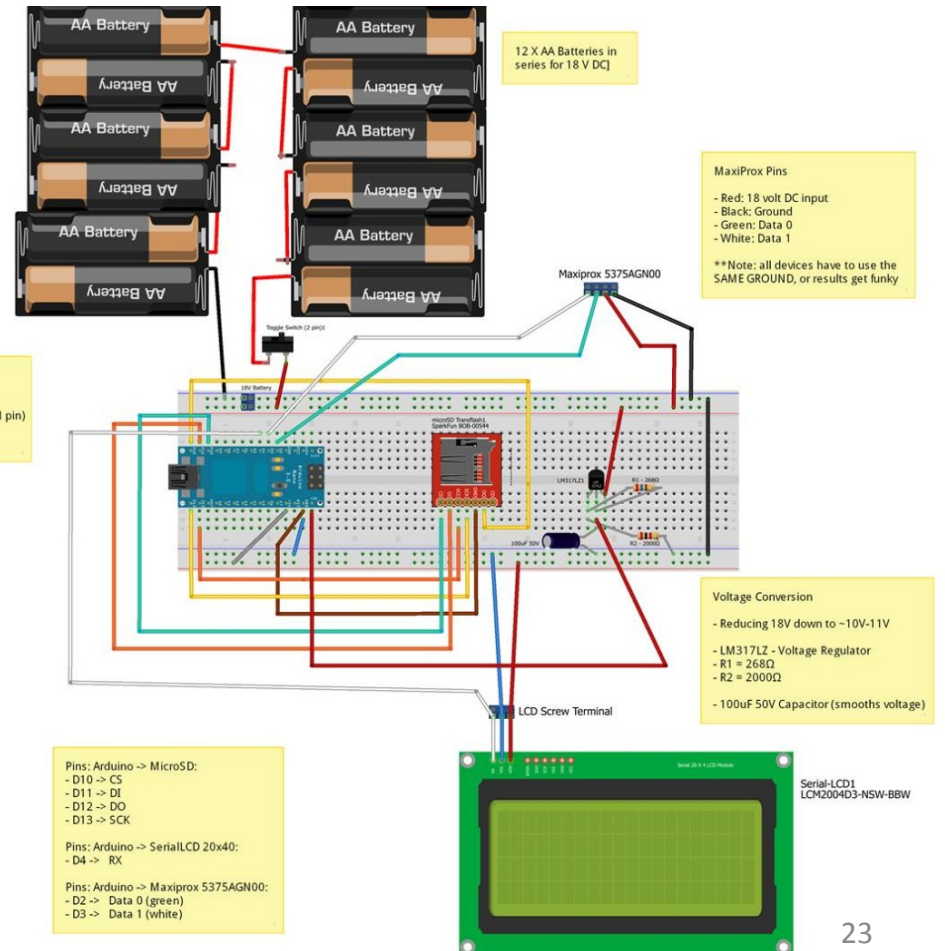
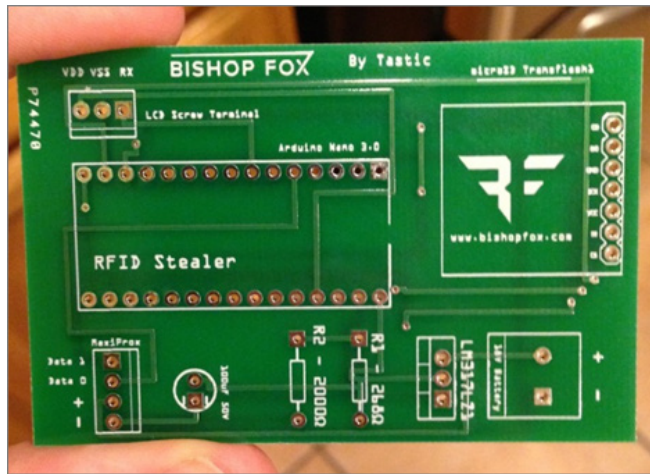
- Easily hide in briefcase or messenger bag, read badges from up to 3 feet away
- Silent powering and stealing of RFID badge creds to be cloned later using T55x7 cards



# Tastic RFID Thief

## LONG RANGE RFID STEALER

- Designed using Fritzing
- Exports to Extended-Gerber
- Order PCB at [www.4pcb.com](http://www.4pcb.com)
  - \$33 for 1 PCB
  - Much cheaper in bulk



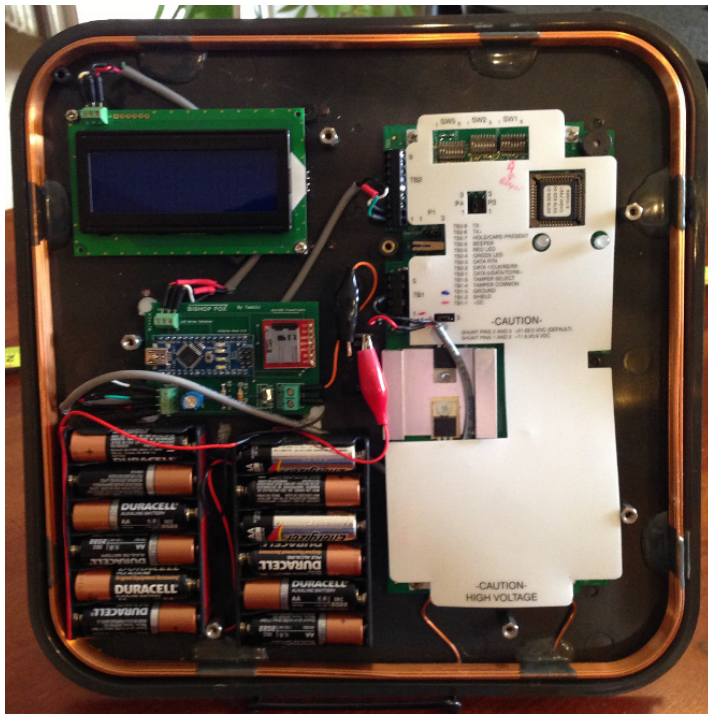


# Custom PCB

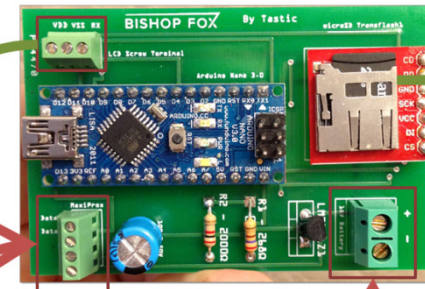


TASTIC RFID THIEF

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



LCD Screen



Any RFID Badge Reader



Power

MicroSD Card

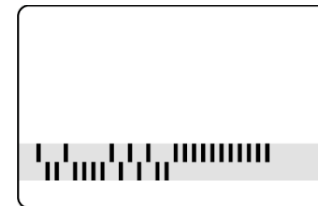


CARDS.txt



# Wiegand Input

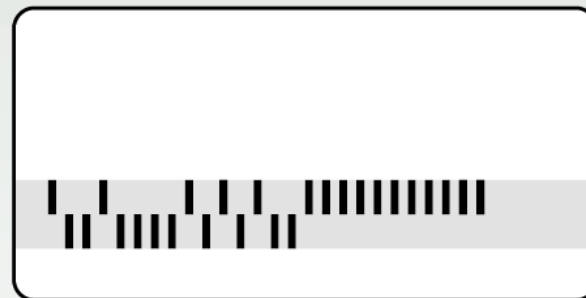
TASTIC RFID THIEF



Custom PCB – reads from Wiegand output of reader

## The Wiegand interface is still widely used

- ▶ The Wiegand interface has 3 wires:
  - ▶ GND
  - ▶ DATA0
  - ▶ DATA1
- ▶ To send a '0'-bit, a pulse is sent on DATA0
- ▶ To send a '1'-bit, a pulse is sent on DATA1
- ▶ Very widely used, especially in the U.S.
- ▶ Even to this day every HID reader has a Wiegand output





# Commercial Readers

TASTIC RFID THIEF

**Low Frequency**  
 Genuine HID™ cards are designed to work with the large installed base of HID Prox and Indala proximity readers.

HID Prox    Indala®



- HID MaxiProx 5375AGN00

<b>**Read Range</b>	ProxCard® II card - up to 24" (60.9 cm) ISOProx® II card - up to 20" (50.8 cm) DuoProx® II Card - up to 20" (50.8 cm) Smart ISOProx® II - up to 20" (50.8 cm) Smart DuoProx® II Card - up to 20" (50.8 cm) HID Proximity & MIFARE® Card - up to 20" (50.8 cm) ProxCard® Plus card - up to 13" (33 cm) ProxKey® II key fob - up to 17" (43.2 cm) MicroProx® Tag - up to 15" (38 cm) ProxPass® Active Vehicle Tag - up to 6' (1.8 m)
---------------------	---



- Indala Long-Range Reader 620



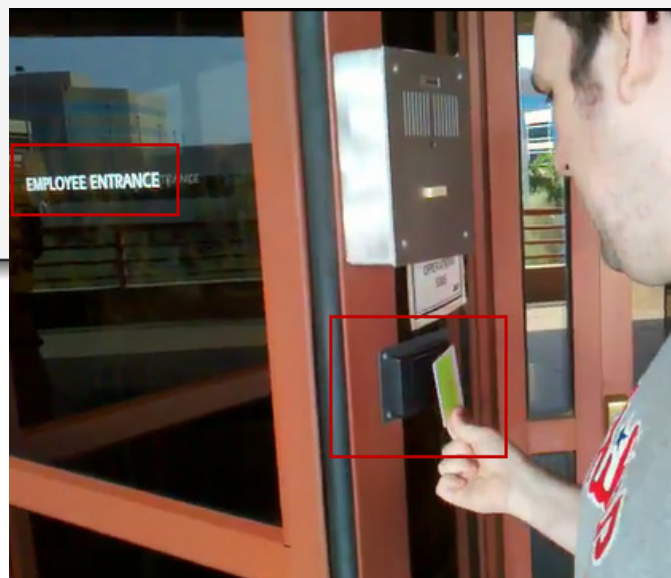
# Indala Cloning

EXAMPLE IN PRACTICE



```
proxmark3> lf indalademod
Expecting a bit less than 312 raw bits
Recovered 311 raw bits
worst metric (0=best..7=worst): 6 at pos 20
UID=0000000000000000000000000000000010011110010101100000100010100010101 (4f2b04515)
Occurrences: 4 (expected 4)
proxmark3>
```

```
proxmark3> lf indalacclone 4f2b04515
Cloning 64bit tag with UID 4f2b04515
#db# DONE
proxmark3>
```

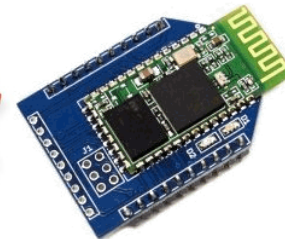
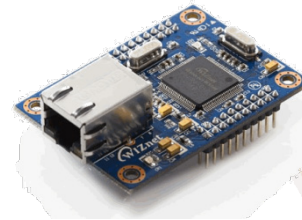
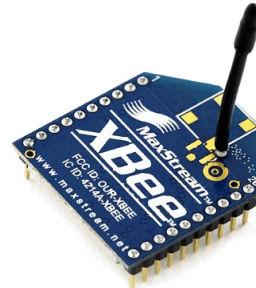
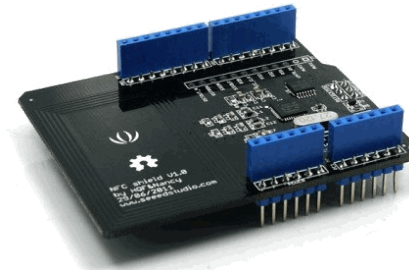




# Tastic Solution: Add-ons

MODULES TO POTENTIALLY ADD

- Arduino NFC Shield
- Arduino BlueTooth Modules
- Arduino WiFly Shield (802.11b/g)
- Arduino GSM/GPRS shields (SMS messaging)
- WIZnet Embedded Web Server Module
- Xbee 2.4GHz Module (802.15.4 Zigbee)
- Parallax GPS Module PMB-648 SiRF
- Arduino Ethernet Shield
- Redpark - Serial-to-iPad/iPhone Cable





# Forward Channel Attacks

EAVESDROPPING RFID



# Droppin' Eaves

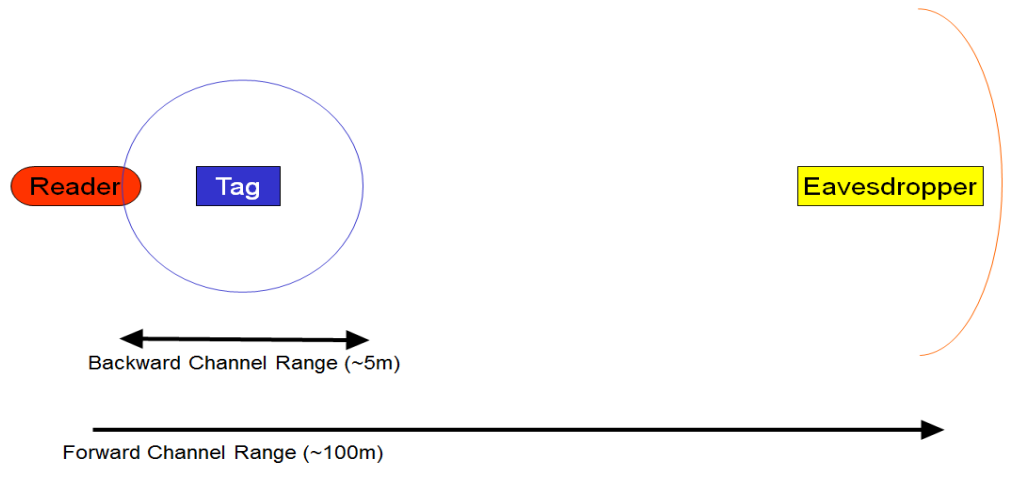
## BADGE BROADCASTS



- Card is powered by 125 kilohertz sine wave.
- Card responds with AM broadcast of bits.
- Broadcast can be received with modified AM radio or oscilloscope.



## Asymmetric Channels



# Cloner 2.0 by Paget

## EAVESDROPPING ATTACK

- Chris Paget talked of his tool **reaching 10 feet** for this type of attack
- Tool **never actually released**, unfortunately
- **Unaware of any public tools** that exist for this attack currently

**Cloner 2.0**

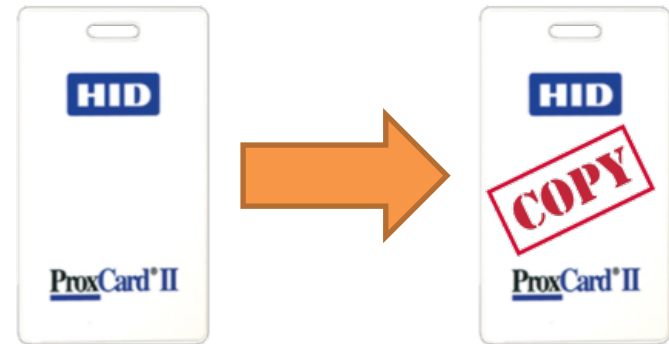
- In development
- Massively improved capabilities
  - Passive mode
    - Let someone else power the card, sniff at a distance
    - Aiming for 10 feet
    - Drop it in a bush, come back the next day
- Blackhat 2008?

Callouts:

- Paget's tool unfortunately was never released
- Eavesdropping attack proposed

IOActive™  
COMPREHENSIVE COMPUTER SECURITY SERVICES

IOActive, Inc. © 2007



# RFID Card Cloning

CARD PROGRAMMING

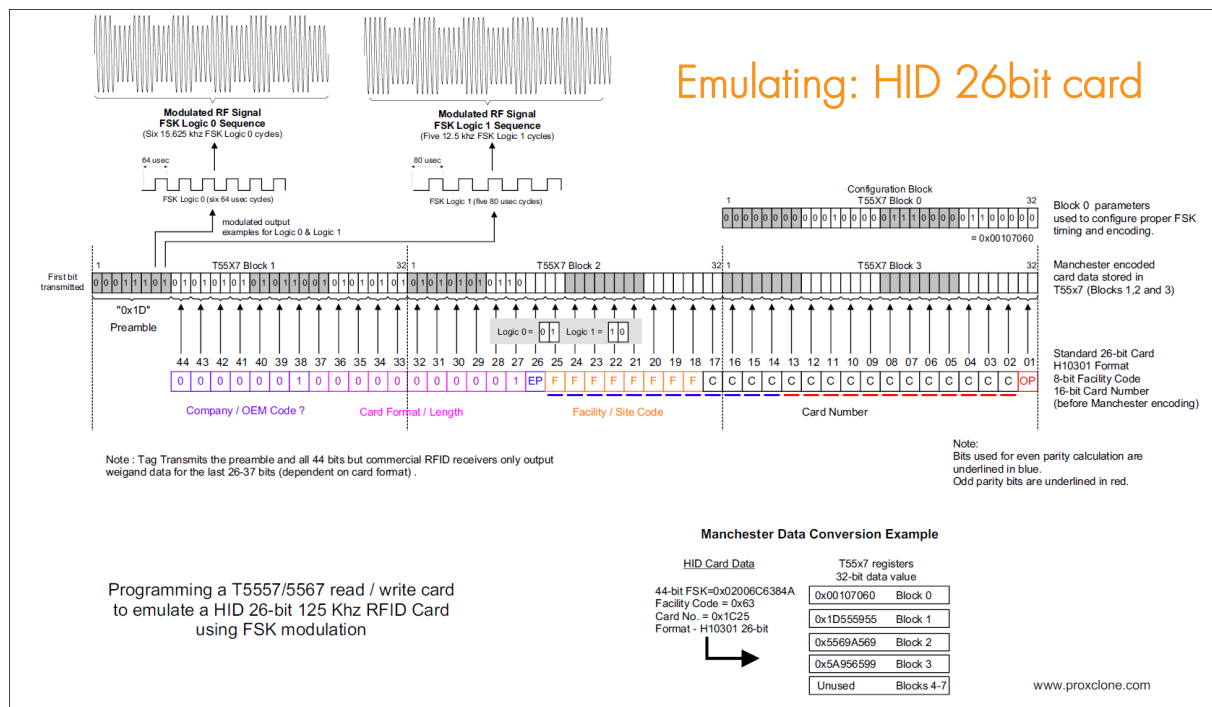


# Programmable Cards



Simulate data *and behavior* of any badge type

- T55x7 Cards
- Q5 cards (T5555)



# Programmable Cards



## Cloning to T55x7 Card using Proxmark3

- HID Prox Cloning – example:

```
lf hid clone <HEX>  
lf hid clone 20068d83d5
```

- Indala Prox Cloning – example:

```
lf indalaclose <HEX>  
lf indalaclose 4f2b04795
```



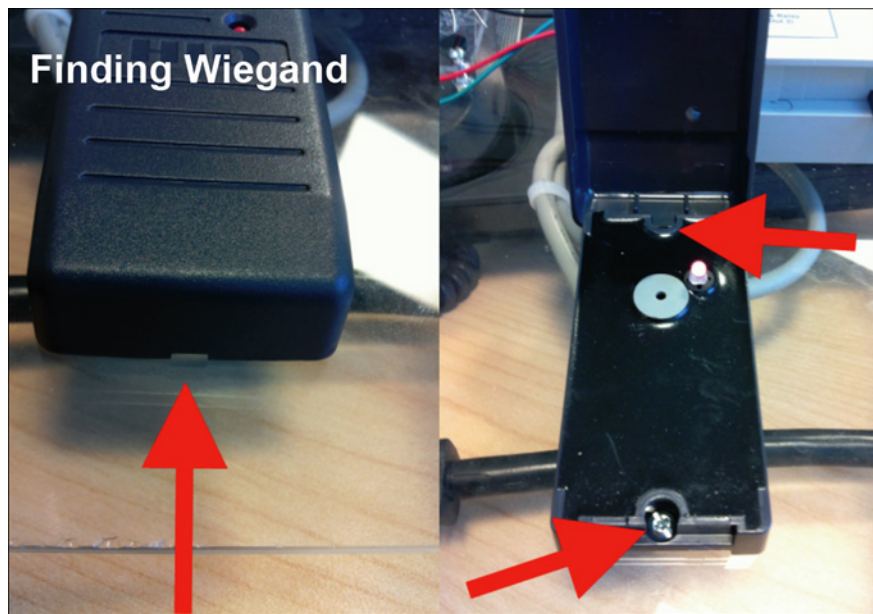


# Reader and Controller Attacks

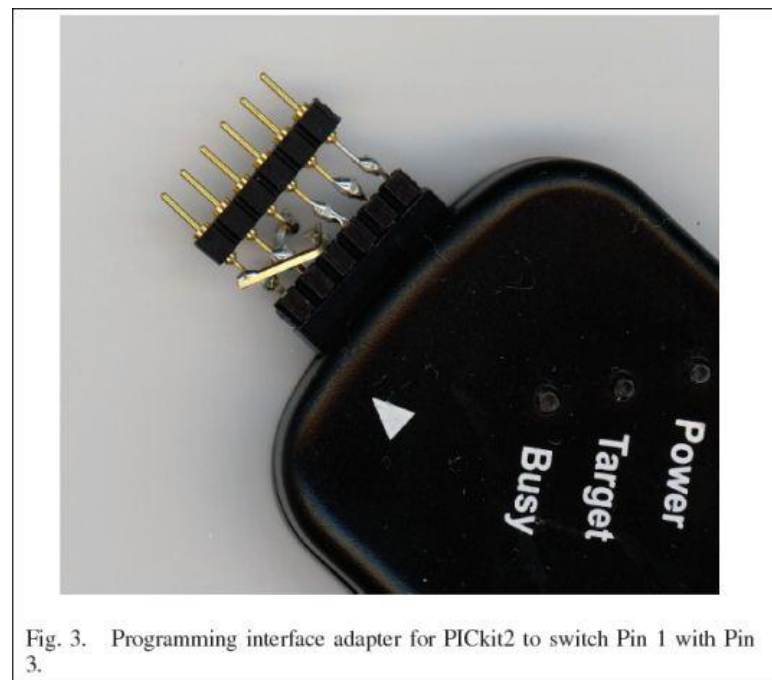
DIRECT APPROACH

# Reader Attacks

JACKED IN

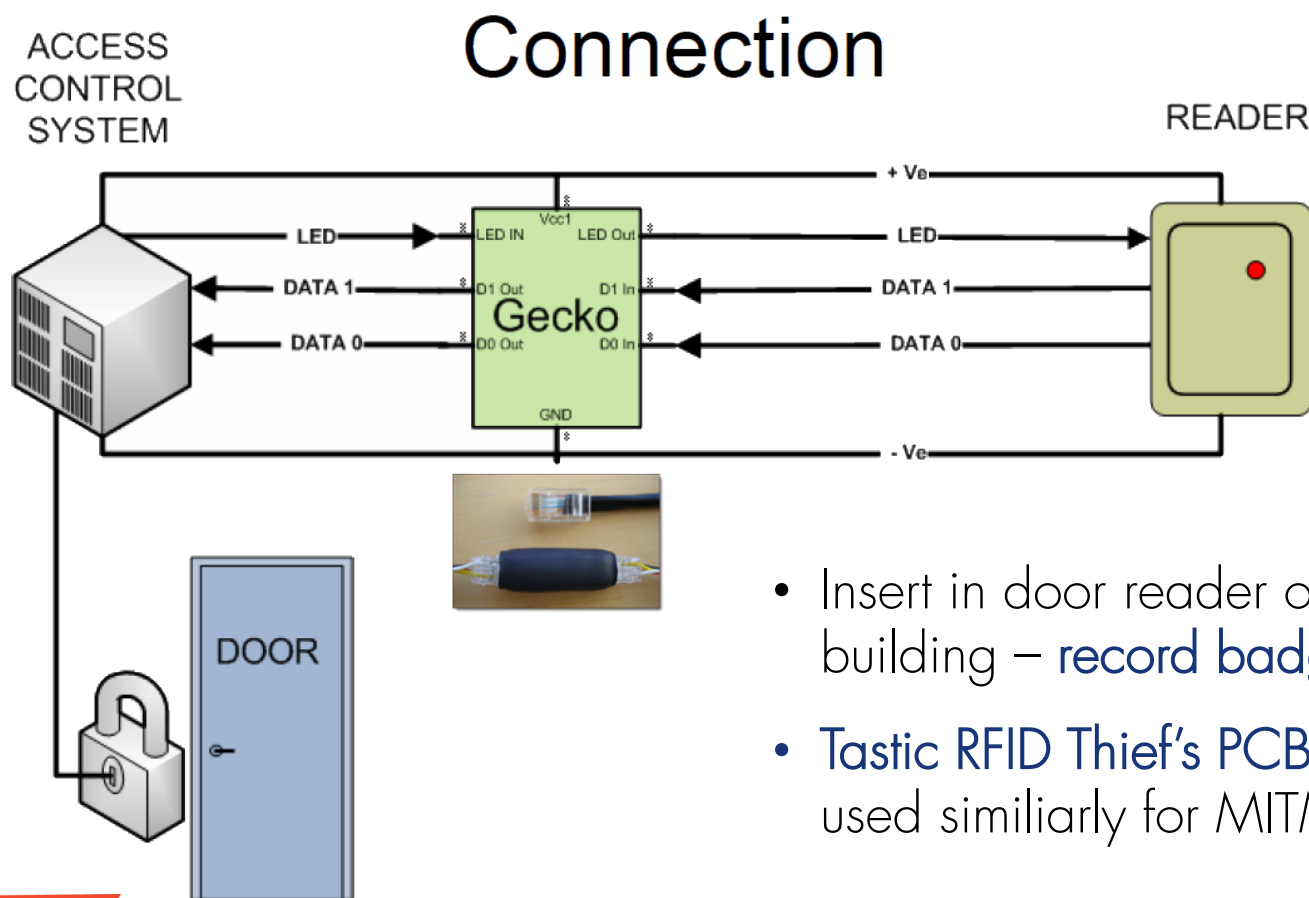


- Dump private keys, valid badge info, and more in few seconds



# Reader Attacks

## GECKO-MITM ATTACK



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

# 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

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



# Backdoors and Other Fun

LITTLE DIFFERENCES



**PWNIE  
EXPRESS**

# Pwn Plug

## MAINTAINING ACCESS

**The Industry's First Commercial Pentesting Drop Box.**

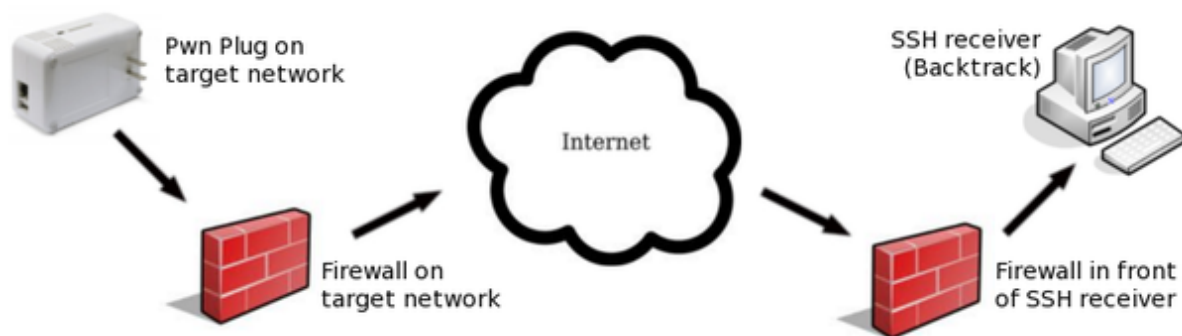
**THE Pwn Plug.**

**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
```





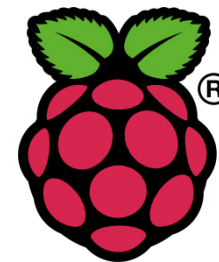
# Pwn Plug

## MAINTAINING ACCESS



- Pwn Plug Elite: \$995.00
- Power Pwn: \$1,495.00





# 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

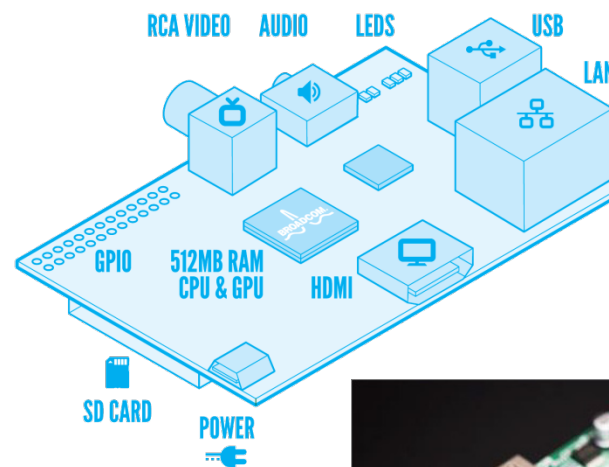
by paganinip on June 22nd, 2013



**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

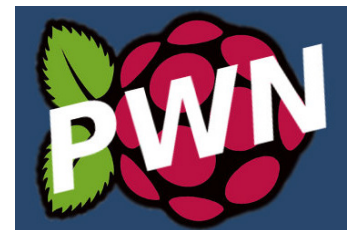
how to use a tiny Raspberry Pi computer to obtain physical access into a corporate network. I decided to publish this post because it gives us a lesson on security perspective, Richee has in fact used the tiny Raspberry Pi hiding it in an ordinary laptop power brick, an object very common in any office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



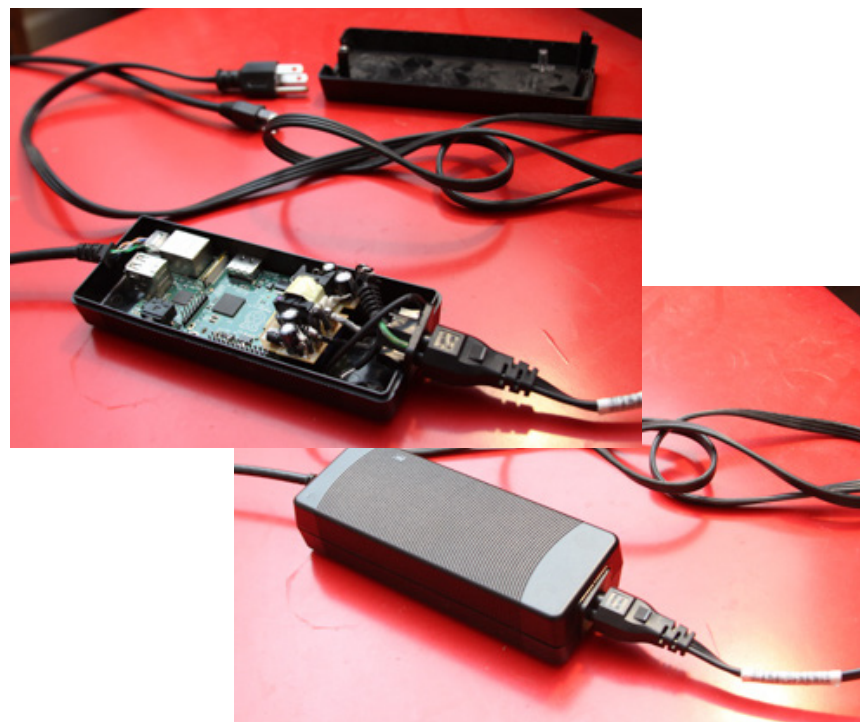


# Raspberry Pi

## 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



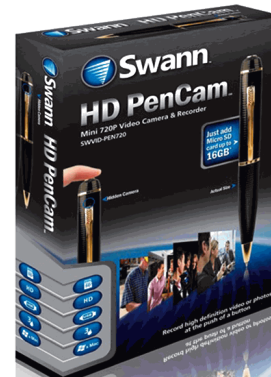


# Little Extra Touches

GO A LONG WAY



- Fake polo shirts for target company
  - Get logo from target website
- Fargo DTC515 Full Color ID Card ID Badge Printer
  - ~\$500 on Amazon
- Badge accessories
- HD PenCam - Mini 720p Video Camera
- Lock pick gun/set





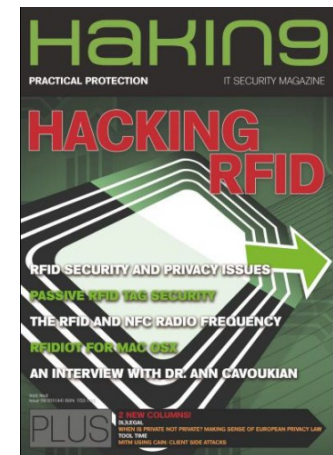
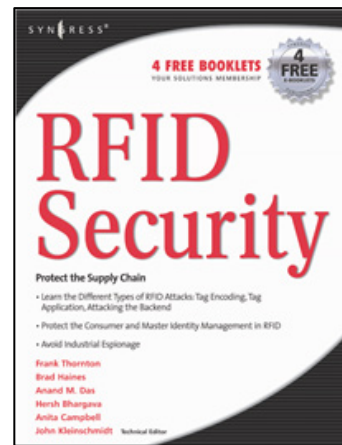
# Defenses

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

# RFID Security Resources

SLIM PICKINS...

- RFID Security by Syngress
  - Not updated **since July 2005**
- NIST SP 800-98 – Securing RFID
  - Not updated **since April 2007**
- Hackin9 Magazine – Aug 2011
  - RFID Hacking, **pretty decent**



**NIST**  
National Institute of  
Standards and Technology  
Technology Administration  
U.S. Department of Commerce

Special Publication 800-98

## Guidelines for Securing Radio Frequency Identification (RFID) Systems



# 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.



# 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 (Broken)



SOME DON'T...EXAMPLE...

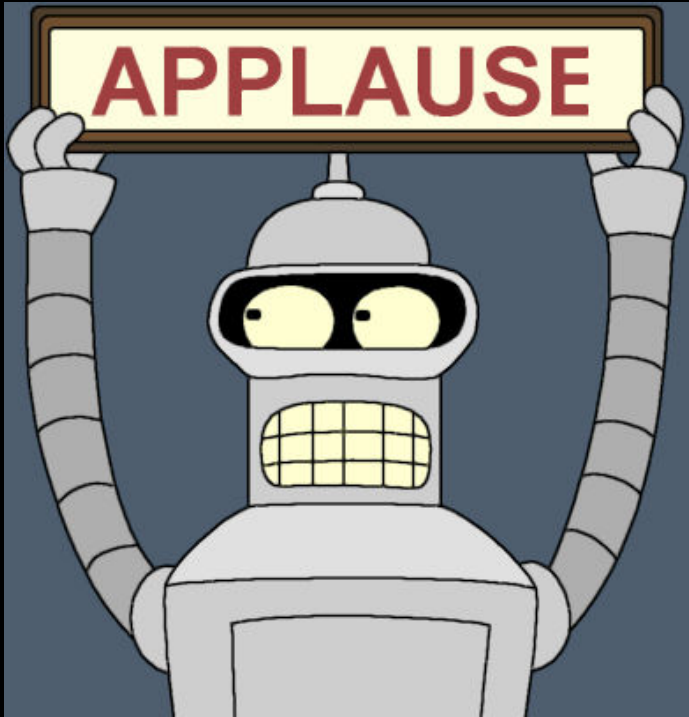
## USA - Green Card Sleeve

- Since May 11, 2010, new Green Cards contain an RFID chip
- Tested Carl's "*protective sleeve*", doesn't block anything.
- False sense of security

**FAILED**



# Thank You



Bishop Fox – see for more info:

<http://www.bishopfox.com/resources/tools/rfid-hacking/>