ALL YOUR BADGES ARE BELONG TO US

DEFCON 22

Eric Smith & Joshua Perrymon

LARES

AGENDA

- INTRO
- WHAT IS RED TEAMING
- TRADITIONAL ATTACKS/TECHNIQUES
- RFID OVERVIEW
- ADVANCED ATTACKS
- REMEDIATION/RISK MITIGATION

ABOUT: LARES CORP

- Minimum of 15 years InfoSec Experience per consultant (90+ combined)
- Penetration Testing Execution Standard Core Members (PTES)
- Publications
  - Aggressive Network Self Defense
  - Contributing writer to COBIT
  - Contributing writer to ISO17799, and one of less than 1000 certified auditors of the ISO17799 (international standards for security best practices)
  - Authors of multiple national / international security awareness training programs
  - Blogs/Podcasts/Media/Conferences

ABOUT: LARES PRESENTERS

- TedX
- InfraGard
- Defcon
- BlackHat
- OWASP
- SANS
- BruCon
- SOURCE
- ToorCon
- ISACA/ISSA
- ShmooCon
- PHNeutral
- Dark Reading
- Security B-Sides
- ChicagoCon
- NotaCon
- White Hat World
- Sec-T
- Troopers
- CSI
- HackCon
- Derbycon
- DakotaCon
- ShakaCon

ABOUT: ERIC SMITH

Over 15 years IT/IS experience

- Red Team Testing/Physical Security Assessments
- Social Engineering
- Penetration Testing
- Risk Assessments

Qualifications

- B.Sc. Information Security/CISSP, CISA, CCSA, CCNA

Work Experience:

- Senior Partner/Principal Security Consultant – Lares Consulting
- Senior Partner/Principal Security Consultant – Layer 8 Labs
- Senior Security Consultant – Alternative Technology
- Application Security Analyst – Equifax, Inc.
- Senior Security Consultant – International Network Services
- Security Engineer – GE Power Systems
- Security Analyst - Bellsouth

ABOUT: JOSH PERRYMON

Over 15 years IT/IS experience

- Risk Assessments
- Red Team Testing/Physical Security Assessments
- Social Engineering
- Vulnerability Assessments & Penetration Testing
- Application Assessments
- Wireless Security Assessments

Qualifications

- CEH, OPST, OPSA, OSSTMM Trainer

Work Experience:

- Senior Adversarial Engineer– Lares
- Senior Partner – Layer 8 Labs
- Advanced Insider Threat/Intel – Bank of America
- Red Team Leader– Bank of America
- CEO– PacketFocus
- Sr. Consultant – BE&K
- Sr. Consultant - EBSCO

TRUE STORY


WHAT YOU LOVE
HAPPY BUT POOR
JUST A DREAM
#WIN
WHAT YOU'RE GOOD AT
RICH BUT BORED
WHAT PAYS WELL

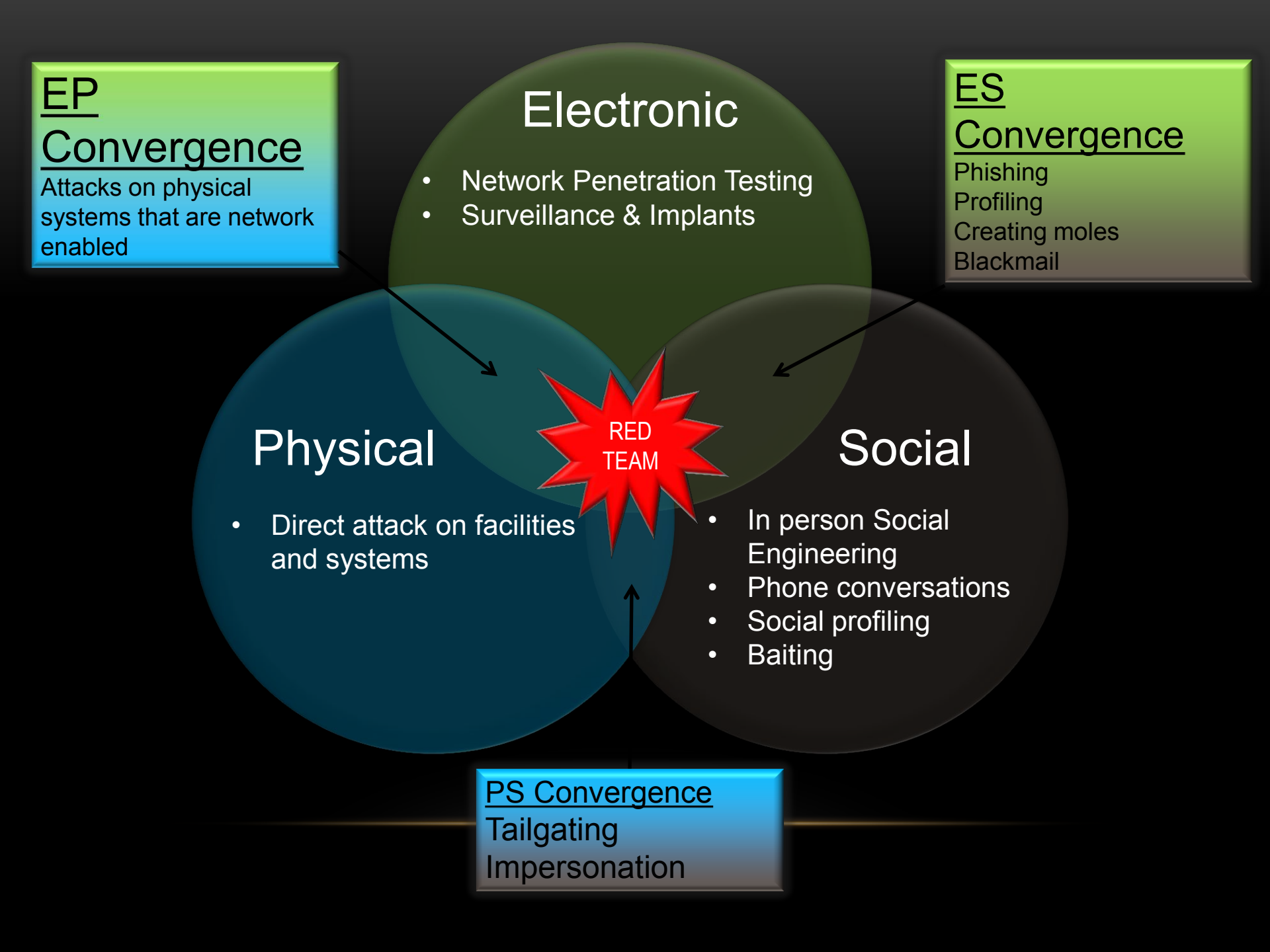
WHAT IS RED TEAMING

The term originated within the military to describe a team whose purpose is to penetrate security of "friendly" installations, and thus test their security measures. The members are professionals who install evidence of their success, e.g. leave cardboard signs saying "bomb" in critical defense installations, hand-lettered notes saying that “your codebooks have been stolen" (they usually have not been) inside safes, etc. Sometimes, after a successful penetration, a high-ranking security person will show up later for a "security review," and "find" the evidence. Afterward, the term became popular in the computer industry, where the security of computer systems is often tested by tiger teams.

How do you know you can put up a fight if you have never taken a punch?

REASONS TO CONDUCT

- Real world test to see how you will hold up against a highly skilled, motivated and funded attacker
- The only type of testing that will cover a fully converged attack surface
- Impact assessment is IMMEDIATE and built to show a maximum damage event
- This IS the FULL DR test of an InfoSec Program


EP Convergence
Attacks on physical systems that are network enabled
Electronic
Network Penetration Testing
Surveillance & Implants
ES Convergence
Phishing
Profiling
Creating moles
Blackmail
Physical
Direct attack on facilities and systems
RED TEAM
Social
In person Social Engineering
Phone conversations
Social profiling
Baiting
PS Convergence
Tailgating
Impersonation

TRADITIONAL ATTACKS & TECHNIQUES

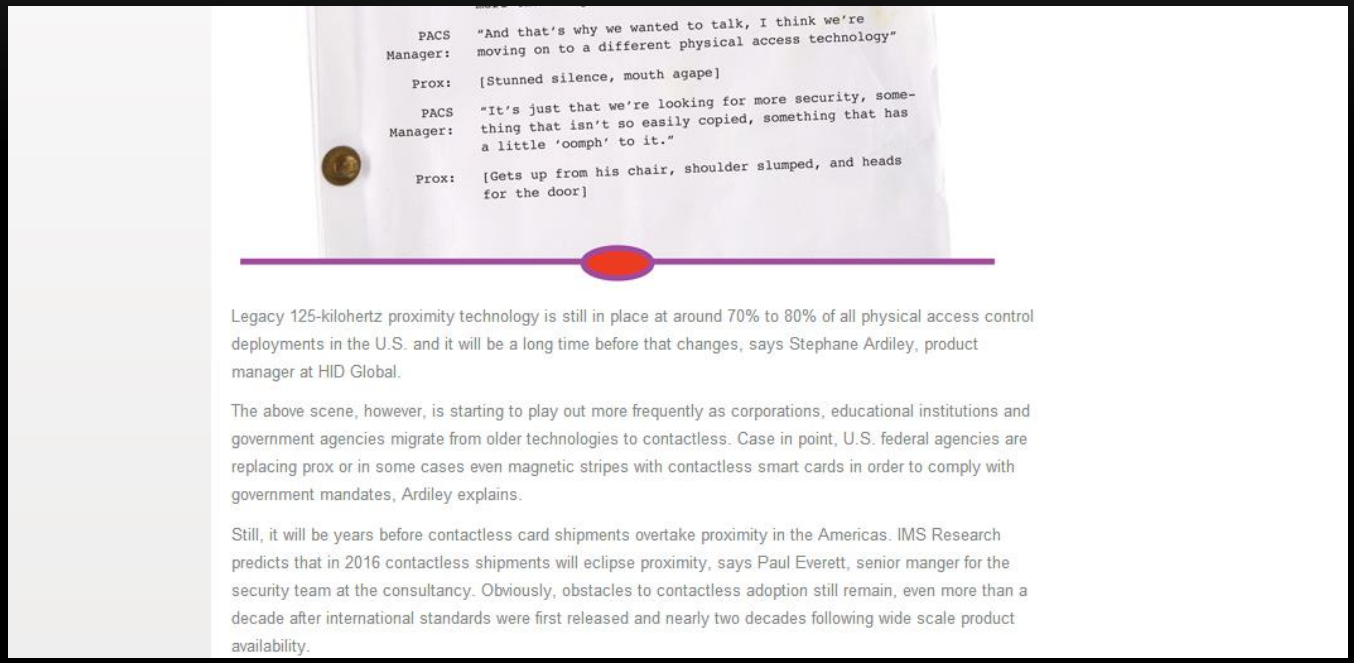
- Tailgating
- Lock Picking
- Shimming
- Key Bumping
- Under Door Hooks (K22)
- Lock Bypass
- Elevator Keys

RFID OVERVIEW

RFID TAG FREQUENCIES

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

WHO USES IT?



PACS Manager: "And that's why we wanted to talk, I think we're moving on to a different physical access technology"

Prox: [Stunned silence, mouth agape]

PACS Manager: "It's just that we're looking for more security, something that isn't so easily copied, something that has a little 'oomph' to it."

Prox: [Gets up from his chair, shoulder slumped, and heads for the door]

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.

The above scene, however, is starting to play out more frequently as corporations, educational institutions and government agencies migrate from older technologies to contactless. Case in point, U.S. federal agencies are replacing prox or in some cases even magnetic stripes with contactless smart cards in order to comply with government mandates, Ardiley explains.

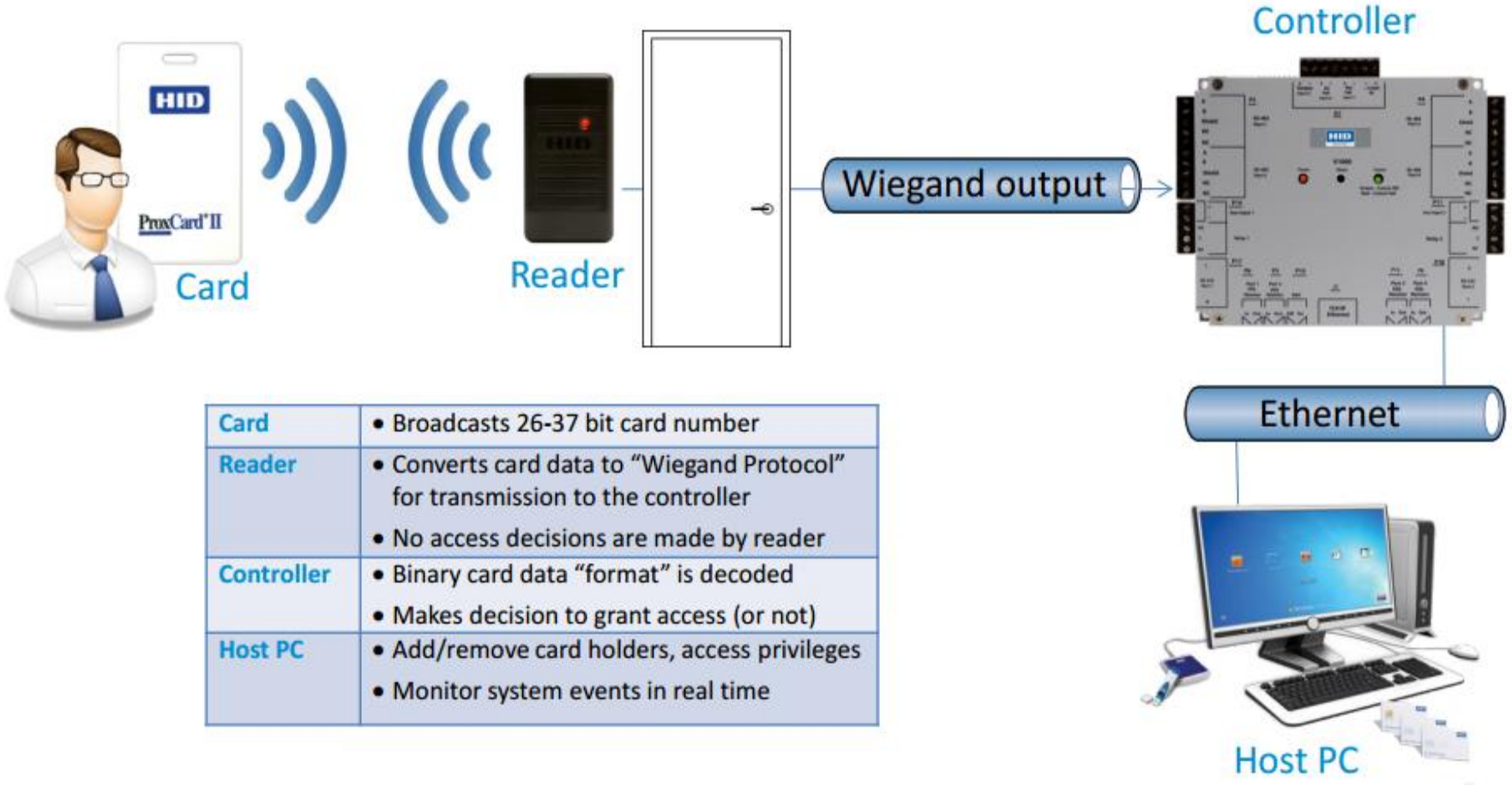
Still, it will be years before contactless card shipments overtake proximity in the Americas. IMS Research predicts that in 2016 contactless shipments will eclipse proximity, says Paul Everett, senior manger for the security team at the consultancy. Obviously, obstacles to contactless adoption still remain, even more than a decade after international standards were first released and nearly two decades following wide scale product availability.

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.

WHO IS VULNERABLE?

- Government facilities (contractors too)
- Medical Facilities
- Financial Institutions
- Nuclear facilities
- Power/Water Facilities
- Education
- List is endless….

UNDERSTANDING BADGE SYSTEMS



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

MULTI-TECHNOLOGY CARD GUIDE

PROXIMITY CARD

Works with existing HID proximity readers. Add new applications to your proximity card with a contact smart chip module.

ISOProx II (1386)	DuoProx II (1336)	Smart ISOProx II (1397)	Smart DuoProx II (1398)
			
1. 125 kHz Proximity	1. 125 kHz Proximity with Magnetic Stripe	1. 125 kHz Proximity 2. Contact Smart Chip (optional)	1. 125 kHz Proximity with Magnetic Stripe 2. Contact Smart Chip (optional)

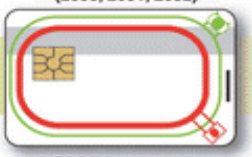
iCLASS BY HID

Features 13.56 MHz *iCLASS* read/write contactless smart card technology in various combinations with magnetic stripe and contact smart chip module.

iCLASS Card (2000, 2001, 2002)	*iCLASS* Card (2000, 2001, 2002)	*iCLASS* embeddable (2010, 2011, 2012)	*iCLASS* embeddable (2010, 2011, 2012)
			
1. 13.56 MHz *iCLASS* contactless smart chip and antenna	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. Magnetic Stripe (optional)	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. Contact Smart Chip (optional)	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. Magnetic Stripe (optional) 3. Contact Smart Chip (optional)

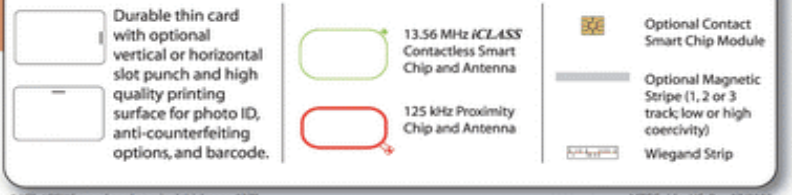
MULTI-TECHNOLOGY CARDS

- Seamlessly upgrade from existing magnetic stripe, HID proximity and/or Wiegand readers and cards to a contactless smart card system.
- Implement multiple applications requiring diverse technologies with a single credential.

iCLASS Prox (2020, 2021, 2022)	*iCLASS* Prox (2020, 2021, 2022)	*iCLASS* Prox embeddable (2030, 2031, 2032)	*iCLASS* Prox embeddable (2030, 2031, 2032)
			
1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. 125 kHz Proximity	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. 125 kHz Proximity 3. Magnetic Stripe (optional)	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. 125 kHz Proximity 3. Contact Smart Chip (optional)	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. 125 kHz Proximity 3. Magnetic Stripe (optional) 4. Contact Smart Chip (optional)

iCLASS Wiegand* (2040, 2041, 2042)	*iCLASS* Wiegand* (2040, 2041, 2042)
	
1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. Wiegand Strip	1. 13.56 MHz *iCLASS* contactless smart chip and antenna 2. Wiegand Strip 3. Magnetic Stripe (optional)

Technology Card Components



* *iCLASS* Wiegand card nominal thickness .033"

MTCGuide_US Rev 07/2005

HID

RFID OVERVIEW – READ RANGES

iCLASS® 13.56 MHz Contactless – Credentials









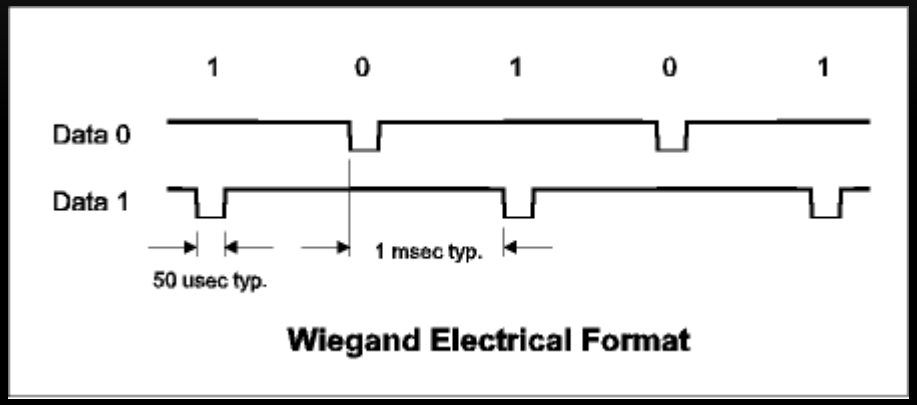




	iCLASS Clamshell	iCLASS Card	iCLASS Composite Card	iCLASS Card Embeddable	iCLASS Card Embeddable Composite	iCLASS Prox	iCLASS Prox Composite	iCLASS Prox Embeddable	iCLASS Prox Embeddable Composite	iCLASS Wiegand	iCLASS Wiegand Composite	iCLASS Key	iCLASS Tag
Base Part Number	2080	200X	210X	201X	211X	202X	212X	203X	213X	204X	214X	205X	206X
Read Range: *													
R10/RW100	Up to 2.5" (6.3 cm)	Up to 3.25" (8.2 cm)								Up to 3.0" (7.6 cm)		1.5" (3.8 cm)	
R30/RW300	Up to 3.0" (7.6 cm)	Up to 4.0" (10.1 cm)								Up to 3.00" (7.6 cm)		2.0" (5.0 cm)	
R40/RW400	Up to 4.5" (10.2 cm)	Up to 4.25" (10.8 cm)								Up to 4.5" (11.4 cm)		2.0" (5.0 cm)	
RK40/RK400	Up to 4.0" (8.9 cm)	Up to 3.5" (8.9 cm)								Up to 2.5" (6.3 cm)		2.0" (5.0 cm)	
Memory Size/ Application Areas	2k bits with 2 areas	2k bits with 2 application areas; 16k bits with 2 application areas (16k/2); 16k bits with 16 application areas (16k/16); 32k bits (16k/2+16k/1); 32k bits (16k/16+16k/1)											
HID Proximity 125 kHz	No					Yes				No			
Contact Smart Chip Module Embeddable	No			Yes		No		Yes		No			
Wiegand Strip	No									Yes	No		
Magnetic Stripe	No	Optional										No	
Printable **	Yes											No	
Slot Punch	Vertical Included	Vertical Optional								Horizontal or Vertical Optional		Key Ring Hole	No
Visual Security Options	N/A	Yes										N/A	
Warranty	Lifetime												

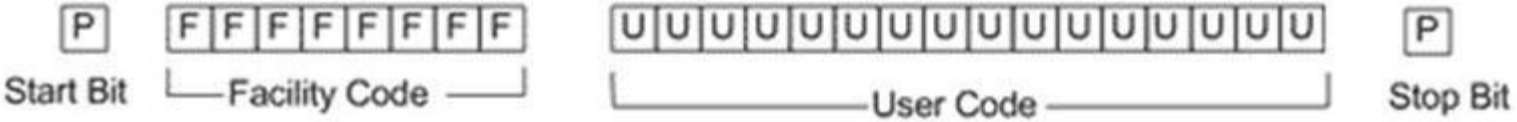
* Dependant upon installation conditions. ** Some types of printing processes can take these credentials out of ISO compliance for thickness. Consult factory for more information.

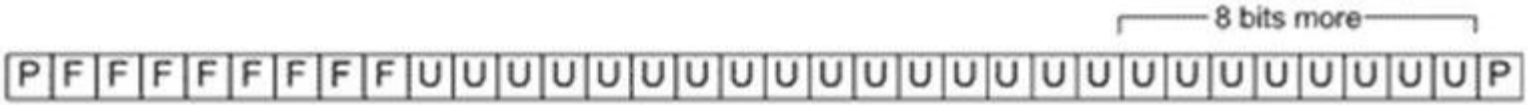
RFID OVERVIEW – WIEGAND PROTOCOL



Wiegand Electrical Format

26 BITS WIEGAND





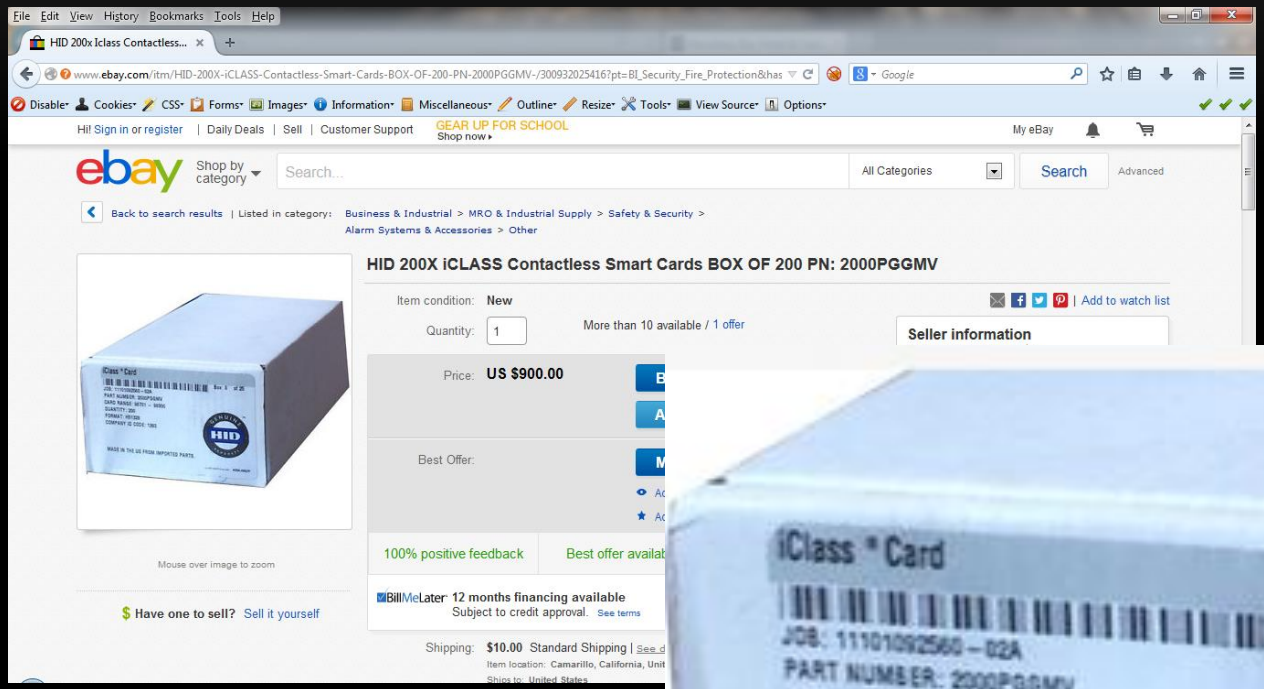
34 BITS WIEGAND

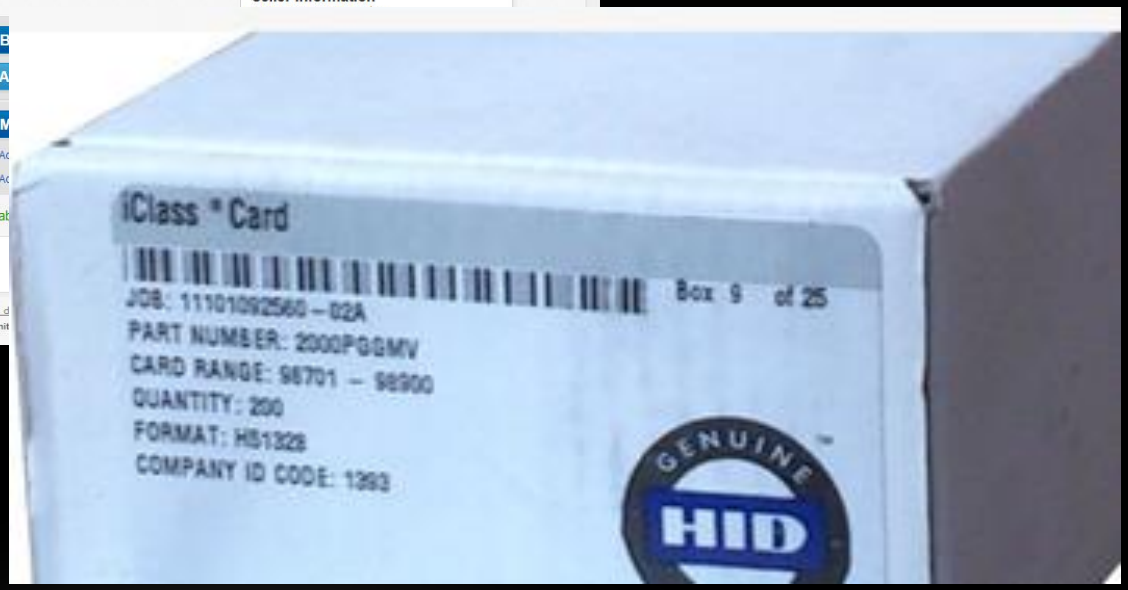
Internet FTW

FACILITY Code & Access Card #

Not so private.

EBAY FTW


HID 200x Iclass Contactless...
www.ebay.com/itm/HID-200X-iCLASS-Contactless-Smart-Cards-BOX-OF-200-PN-2000PGGMV-/300932025416?pt=BI_Security_Fire_Protection&has
Hi! Sign in or register | Daily Deals | Sell | Customer Support
GEAR UP FOR SCHOOL
Shop now
My eBay
ebay
Shop by category
Search...
All Categories
Search
Advanced
Back to search results | Listed in category: Business & Industrial > MRO & Industrial Supply > Safety & Security > Alarm Systems & Accessories > Other
HID 200X iCLASS Contactless Smart Cards BOX OF 200 PN: 2000PGGMV
Item condition: New
Add to watch list
Quantity: 1
More than 10 available / 1 offer
Seller information
Price: US $900.00
Best Offer:
100% positive feedback
Best offer availab
Mouse over image to zoom
$ Have one to sell? Sell it yourself
BillMeLater 12 months financing available
Subject to credit approval. See terms
Shipping: $10.00 Standard Shipping | See d
Item location: Camarillo, California, Unit
Ships to: United States


iClass ® Card
Box 9 of 25
JOB: 11101092560 – 02A
PART NUMBER: 2000PGGMV
CARD RANGE: 98701 – 98900
QUANTITY: 200
FORMAT: H51328
COMPANY ID CODE: 1383
GENUINE
HID

RESELLER SERVICES

Identify HID/Indala card programming specs service

Name: **Identify HID/Indala card programming specs service**

Price: USD$25.00

part : HID-Indala-IDcard

Description

If you need to know the format, facility code or serial number of your HID or Indala proximity cards, please take a working card sample and provide us with the XXXXXXXX-X number printed near the card's corner (see example photo of an HID ProxCard II).

We will use this info to check the HID database and locate the format and facility code for you. For security reasons, we will provide this info only to card owners, belonging to established companies or institutions.

Company e-mail addresses only- no free email (Yahoo!, Hotmail, Gmail...) requests.

Payment will be reimbursed as a USD$25 coupon to use towards your HID or Indala card purchase in our store.

0 Tweet Like 0

Product Reviews

RFID HACKING

CLONING/REPLAY – LOW FREQUENCY (PROX II)

DEMO
Low Freq Clone/Replay
Proxmark III

PRIV ESCALATION - PROX BRUTE

McAfee
An Intel Company

Business Home | About Us | Purchase

Search Go

Threat Center | Products & Solutions | Services | Support | Partners | Community

Business Home ▸ Products & Solutions ▸ Product Downloads & Trials ▸ Free Tools

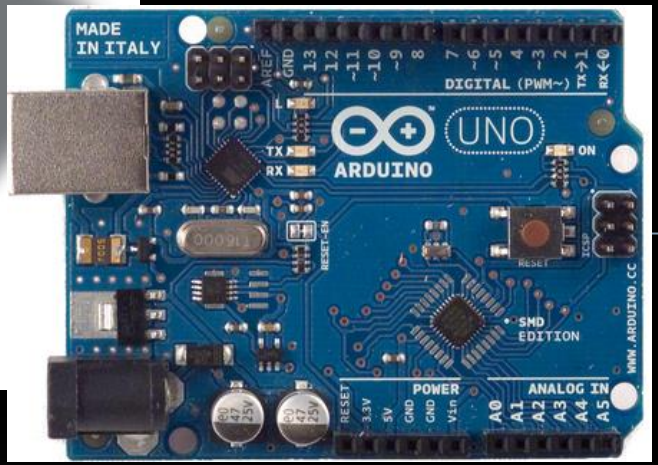
+1 Like Tweet Share

Proxbrute v0.3

ProxBrute is a custom firmware written for the proxmark3. It extends the currently available firmware (revision 465) to support brute force attacks against proximity card access control systems. This version of ProxBrute requires the knowledge of a [once] valid tag value to vertically or horizontally escalate the tag's privileges.

Download this tool now

LONG RANGE READING – LOW FREQUENCY

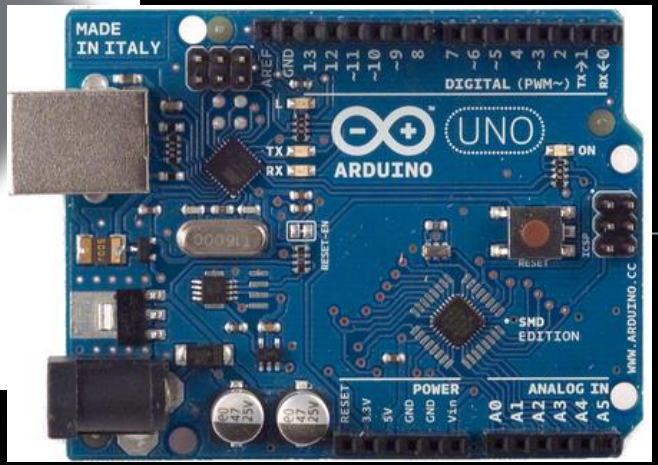


Long Range Tastic Reader (Low Frequency)

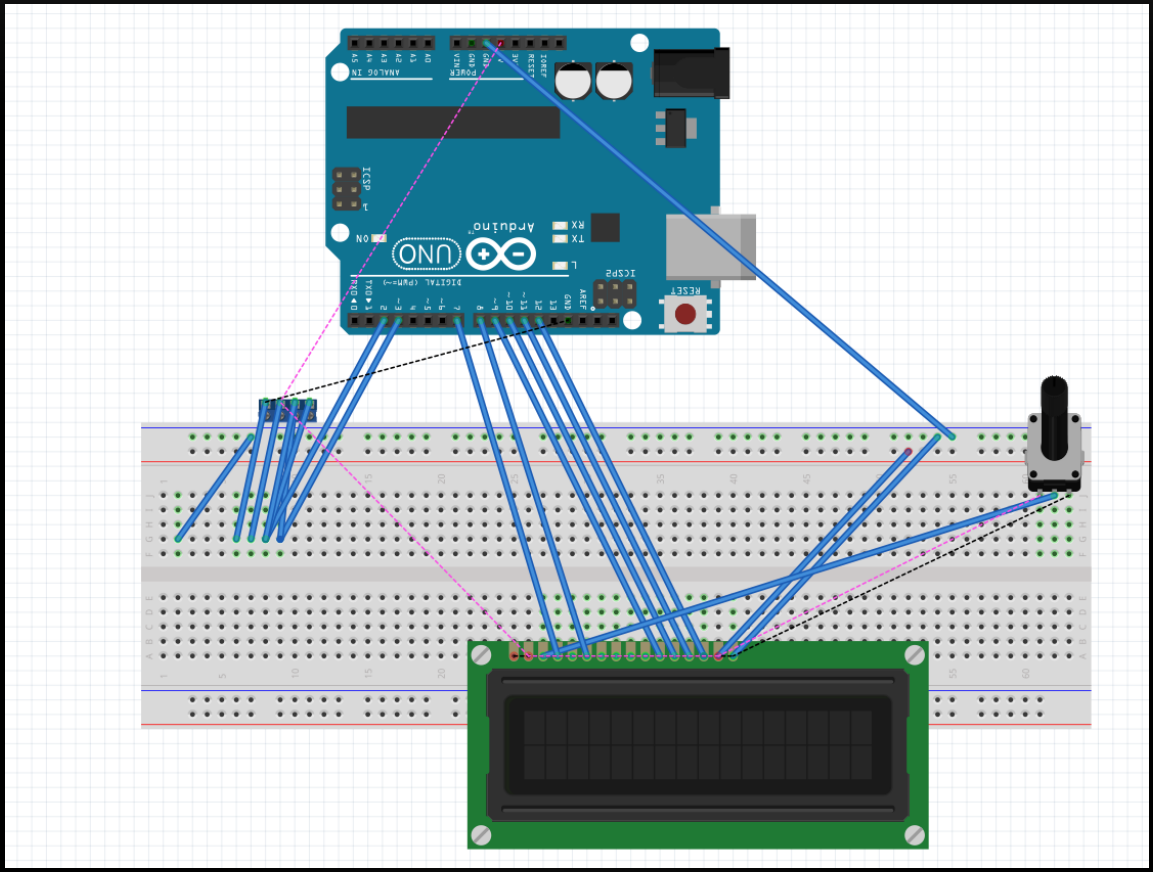
BISHOP FOX

ADVANCED RFID ATTACKS

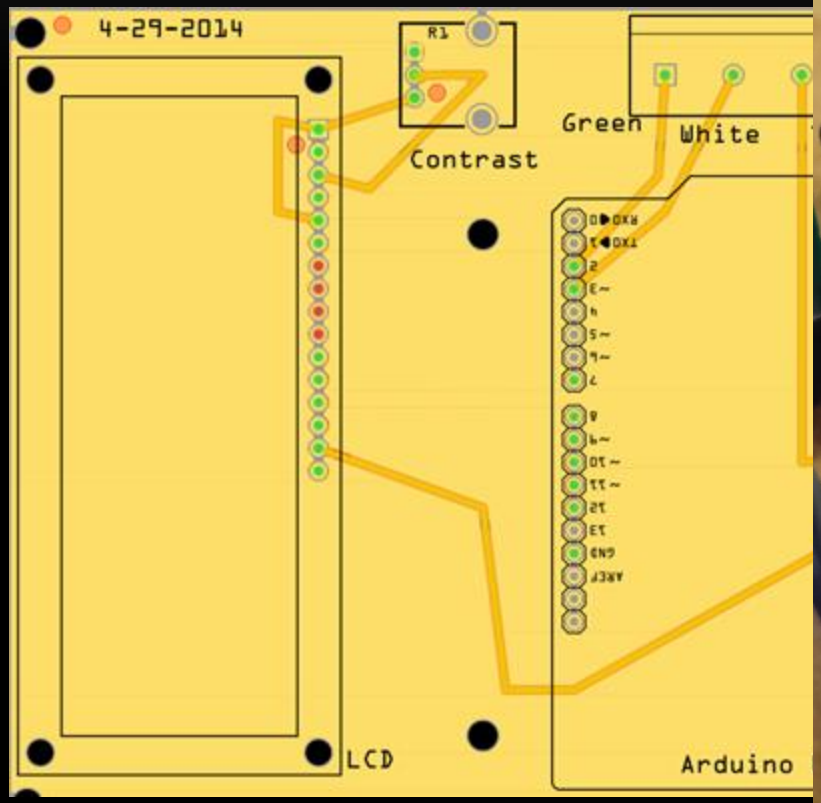
LONG RANGE READING – HIGH FREQUENCY (ICLASS)



ARDUINO WITH LCD, MOBILE READER



MOBILE READER PCB BUILD

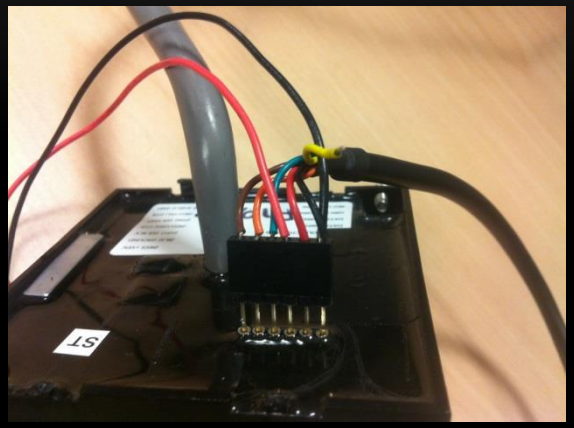


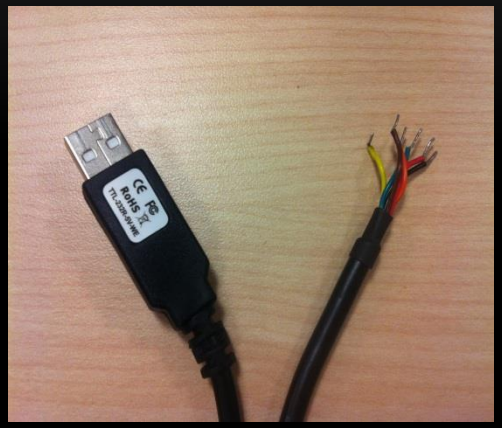
DEMO
Long Range Read – High Frequency

ICLASS VULNERABILITY (PUBLIC)

- Heart of Darkness - exploring the uncharted backwaters of HID iCLASS security
  - Milosch Meriac, meriac@OpenPCD.de
- 27TH CHAOS COMMUNICATION CONGRESS IN BERLIN, DECEMBER 2010
- Firmware was dumped and encryption keys for Standard Security were compromised.

ICLASS CARD CLONING





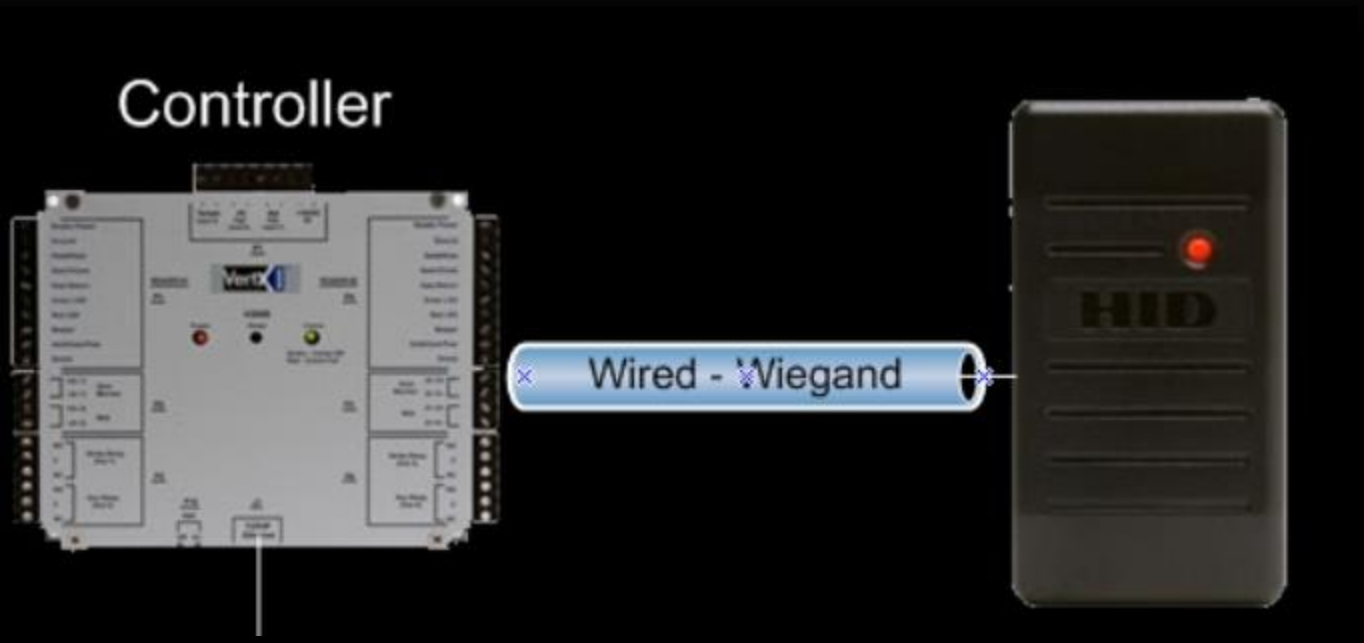
DEMO
IClass Cloning

ICLASS PRIVILEGE ESCALATION

- **Block 7 – Contains encrypted format of facility code and access card number**
- **Use compromised keys and calculate new block 7 for Weigand data string**
- **Write block 7 to clone card**
- **Badge in!**
- **Work in progress:**
  - **iClass brute**

DEMO
IClass Priv Esc

GECKO WIEGAND CAPTURE



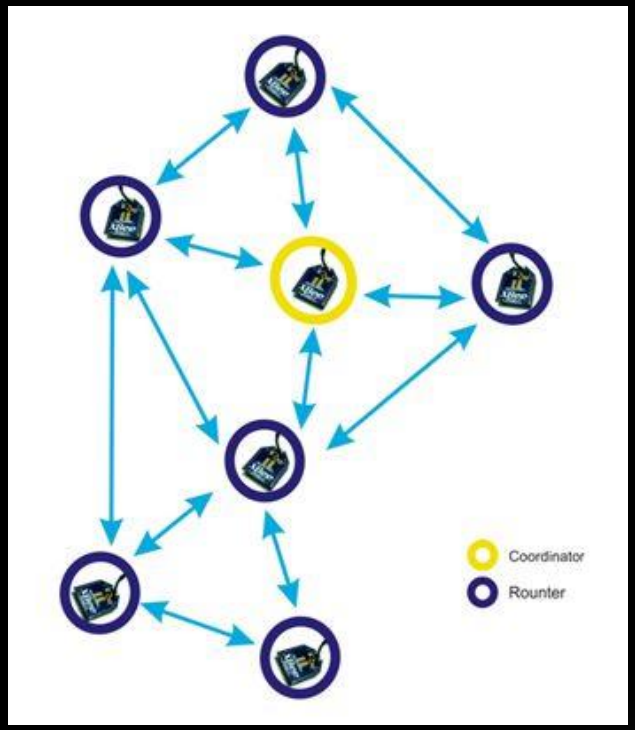
BLENDED ATTACK – PRIVILEGE ESCALATION

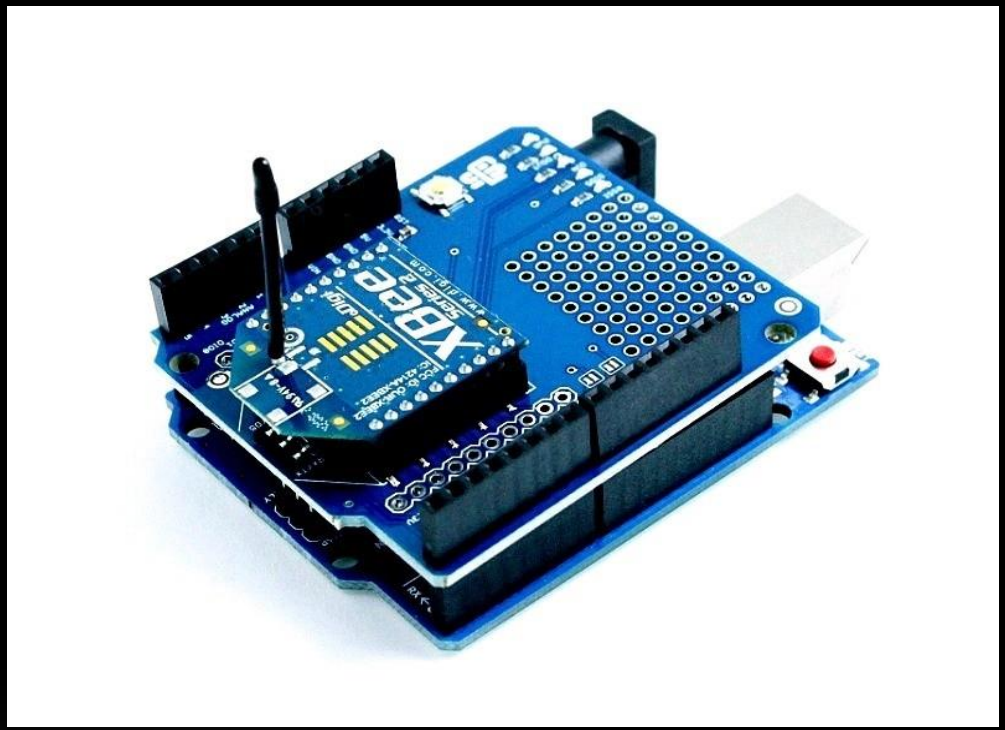
- Information leak from badge system
- Remote compromise of access controls
- Monitor activity
- Identify system faults
- Profiling
- Access rights modification

UNDER DEVELOPMENT – BIO AND PIN ATTACKS

UNDER DEVELOPMENT – MESH NETWORK

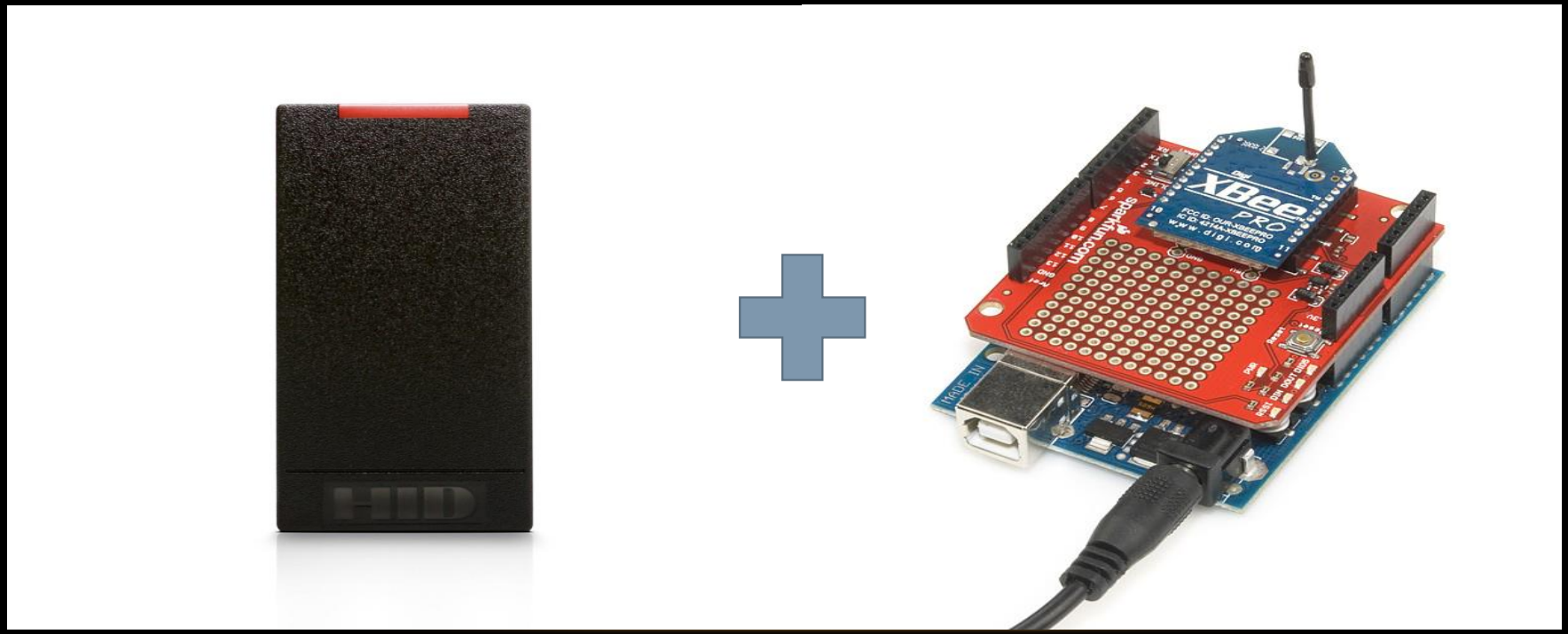
- Real Time Mesh Network – collaboration of multiple Red Team members and field hardware





UNDER DEVELOPMENT – BACKDOORED READER

- Backdoored reader with Audrino
  - Captures Wiegand data and transmits over Zigbee or wifi to other Red Team member's hardware device in the field



RISK MITIGATION

REMEDIATION/RISK MITIGATION

- Standard RFID asset protection/best practices
- Protection strategies of badge systems (physical and electronic)
  - Protection against blended threads/Red Team targeted attacks
- Custom card formats and Time To Reverse (TTR)
- Protect badge systems with VLANs, 2-factor authentication or isolation
- Training – Staff and Guards
- Log Monitoring – IPS?

QUESTIONS?

Eric Smith
esmith@lares.com
@infosecmafia

Josh Perrymon
jperrymon@lares.com
@packetfocus

http://www.lares.com

Code: https://github.com/LaresConsulting