Physical Penetration Testing

Sponsored by IBM Cyber Engineer Chris DeRobertis

By Chris Danyluk, Nicholas Regan, Daniel MacCarthy, and Jacob Shapiro

Overview

We attempted to discover a new method to teach Cybersecurity analysts about physical penetration testing. We started by taking an assessment of our knowledge and then completing 11 challenges, before retaking the same assessment again. This ensured that information discovered during the pen test was retained.

01 Hacker Mindset

Facility Recon

- Sign location: **Bartow, City of Oaks and Azaleas**
- Location: **Polk County, Florida**
- Shop decal *Sara Fl*
  - Further investigation indicated location to be in **Bartow, Florida**
- Target Found: **Florida Department of Citrus**

Car Hacking

- Reverse image search to find **2020 Honda Breeze**
- CVE Association:
  - **CVE-2021-46145**
  - **CVE-2022-27254**
- Rolling PWN attack
- Software-Defined Radio
- Flipper Zero

02 Amazon OSINT

Facility Recon

- Main points of entry:
  - **All Trucks**
  - **Visitors and Associates**
- Pictures of inside and outside of building
- Contact Information
- Security Door Found
- Employee Uniform
- Shodan map of Hikvision Camera usage.

03 Amazon Recon

Points of Entry

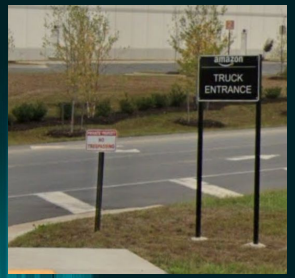
- **Delivery Truck**
- **Water Runoff**

Social Engineering

- Wear clothes similar to employees
- Learn common lingo/expressions
- Wear Earbuds to stay in contact with team
- Obtain Access Code

Telephone Entry

- Brand name: Linear
- Default Access Code: 123456
- Default key found on amazon for $17.99
- Follow congested foot traffic to avoids suspicion







04 OSINT Keypad Lock

Trilogy DI2700

- Reverse image search provided us the name of the lock
- Allows for 5 digit code input
  - 10^5 = 100,000 possible combinations
- Factory Default code = **12345**
- Fingerprint erosion on buttons 14789
  - 5! = 120 possible combinations
- Successful combination: **14789**

Lishi Tool

- Multi-functional lock picking tool
  - Pick the lock while measuring teeth length
  - After lock is picked, key can be made for future use
- Simple to use!

05 RFID Cloning

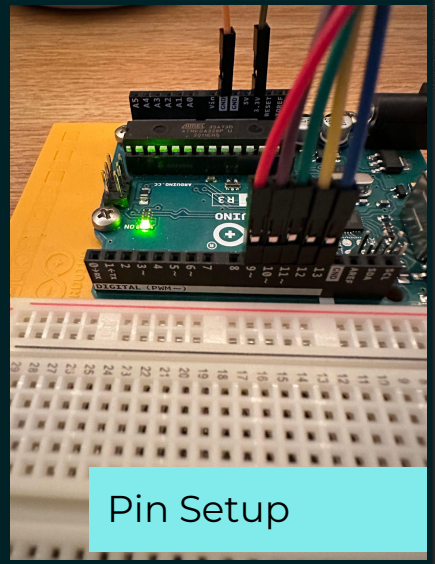
Program and Findings

- Utilized RC522 attachment
- Code pulled from Github Repository found
- Key card scanners emit 13.56Mhz Frequency
- Encrypted hex dumps
- UID is a key factor

```
0  D9 A3 BE 20  E4 08 04 00  62 63 64 65  66 67 68 69  [ 0 0 0 ]
```

```
35  /* Set your new UID here! */
36  #define NEW_UID {0xDE, 0xAD, 0xBE, 0xEF}
```

UID & Change UID



Pin Setup

```
Card UID: EA AC C9 3F
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15      63  PCD_Authenticate() failed: Timeout in communication.
  14      59  PCD_Authenticate() failed: Timeout in communication.
  13      55  PCD_Authenticate() failed: Timeout in communication.
  12      51  PCD_Authenticate() failed: Timeout in communication.
  11      47  PCD_Authenticate() failed: Timeout in communication.
  10      43  PCD_Authenticate() failed: Timeout in communication.
   9      39  PCD_Authenticate() failed: Timeout in communication.
   8      35  PCD_Authenticate() failed: Timeout in communication.
   7      31  PCD_Authenticate() failed: Timeout in communication.
   6      27  PCD_Authenticate() failed: Timeout in communication.
   5      23  PCD_Authenticate() failed: Timeout in communication.
   4      19  PCD_Authenticate() failed: Timeout in communication.
   3      15  PCD_Authenticate() failed: Timeout in communication.
   2      11  PCD_Authenticate() failed: Timeout in communication.
   1       7  PCD_Authenticate() failed: Timeout in communication.
   0       3  PCD_Authenticate() failed: Timeout in communication.
```

Hilton Keycard

Hex Dump

```
Firmware Version: 0x88 = (clone)
Scan PICC to see UID, SAK, type, and data blocks...
Card UID: D9 A3 BE 20
Card SAK: 08
PICC type: MIFARE 1KB
Sector Block   0  1  2  3   4  5  6  7   8  9 10 11  12 13 14 15  AccessBits
  15      63  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          62  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          61  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          60  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  14      59  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          58  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          57  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          56  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  13      55  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          54  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          53  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          52  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  12      51  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          50  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          49  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          48  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  11      47  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          46  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          45  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          44  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
  10      43  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          42  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          41  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          40  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   9      39  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          38  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          37  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          36  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   8      35  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          34  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          33  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          32  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   7      31  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          30  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          29  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          28  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   6      27  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          26  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          25  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          24  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   5      23  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          22  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          21  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          20  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   4      19  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          18  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          17  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          16  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   3      15  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          14  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          13  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
          12  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   2      11  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
          10  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
           9  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
           8  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   1       7  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
           6  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
           5  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
           4  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
   0       3  00 00 00 00  00 00 FF 07  80 69 FF FF  FF FF FF FF  [ 0 0 1 ]
           2  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
           1  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00  [ 0 0 0 ]
           0  D9 A3 BE 20  E4 08 04 00  62 63 64 65  66 67 68 69  [ 0 0 0 ]
```

06 Elevator Access

Security Terms

- Independent Service Mode
- Sabbath Mode
- Security Mode
- Riot Mode
- Code Blue
- Fire Service

Otis Elevator

- 10 possibly viable keys
  - Keys can be found on ElevatorKeys.com
- Keys separated by region

06 Continued

ESPkey

- Debugging tool and implantable logic analyzer
- Installation instruction can found here
- Stores unique credential bitstreams that is replayable
- Wiegand protocol is vital

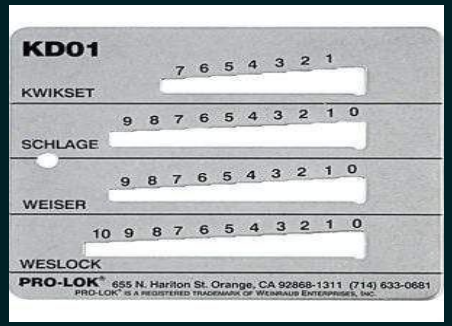
Infamous 2642 key

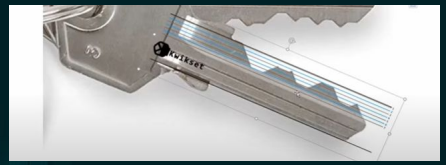
- Required by the construction codes to be in elevators in the State of New York
- Override the elevator to take us anywhere we want to go
- Key can be found here.

07 Key Bitting

Identify

Measure





Copy

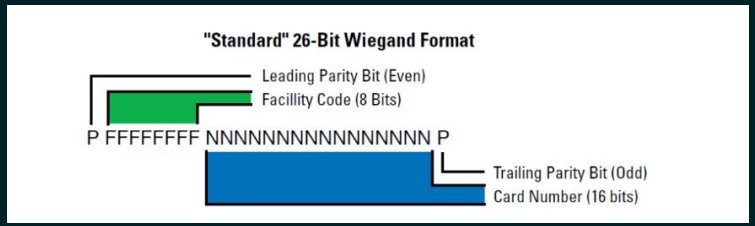
08 Cloning via Proxmark

Proxmark

- Can clone RFID cards by scanning or providing proper info
- Can Broadcast RFID card info
- Binary to Decimal
- Facility Code - 12
- Card Number - 61744

Wiegand Protocol

- Use of the Wiegand Wire in the real world
- Wiegand Wires change polarity near magnetic fields
- When measured, creates a bitstream used for credentials



09 Keypad Safe

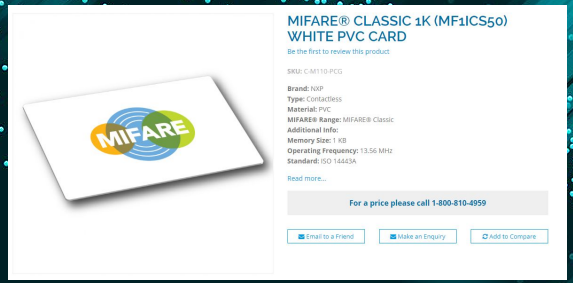
Mechanical Lock

- TL-15
  - 1 inch steel walls and a 1.5 inch steel door
  - 15 minute break in time
- TRTL
  - Protection against oxy-fuel and gas cutting techniques.
  - 30 minute break in time
- TXTL
  - Withstand explosives leaving them to be the most secure safes on the market

Opening Safe

- Default access code: 999999
- Identify potential structural weaknesses; loose nails, bent hinges, etc
- Cause Physical damage via dropping safe to dislodge locking mechanism

10 RFID Blanks



Frequencies

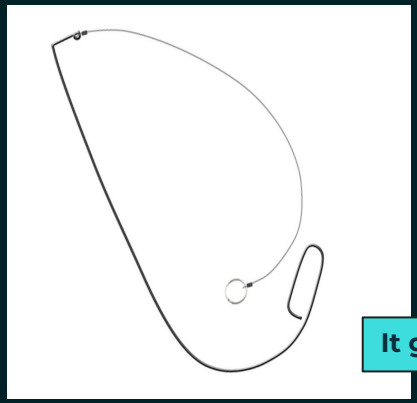
- LF - Low
  - 30 KHz to 300 KHz
  - Range: Centimeters/inches
- HF - High
  - 3MHz to 30 MHz
  - Range: 3 feet omnidirectional
- UHF - Ultra High
  - 300MHz and 3GHz
  - Range: 40 Feet
  - Susceptible to radio interference

MIFARE

- Examples:
  - Staff ID cards, Access control management, and Special access cards
- Card Frequency Options
  - 125kHz, 13.56MHZ, 902-928 MHz, 2.45 GHz, Mechanical, and Touch Plate
- Format Options
  - AWID, DK Prox, HID, IDTeck, and SecuraKey

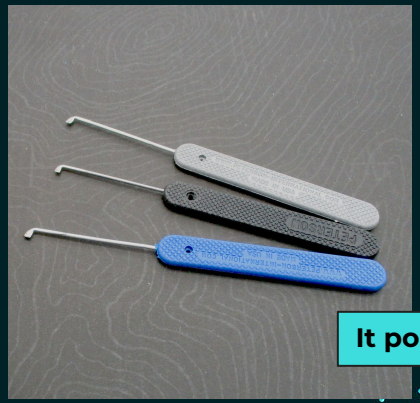
11 Lock Forcing

UDT



It goes under

The Peterson Tool



It pops open

12 Learning Statistics

Before/After Assessment Comparison

Questions?

Thank you!

We truly hope you learned something new and enjoyed!