RFID Tag Replication
Remote Replication of HID Access Cards

Matthew Abazis, Elijah Swift

November 12 2018

Introduction to Passive RFID

Receiver System

- Provide induction power to tag
- Wirelessly read tag ID
- Check tag ID against Database
- Preform tasks, dependent on tag ID

Tag

- Normally small, simple, and cheap
- Powered by induction
- Static ID code
- No on-tag processing

Uses for Passive RFID

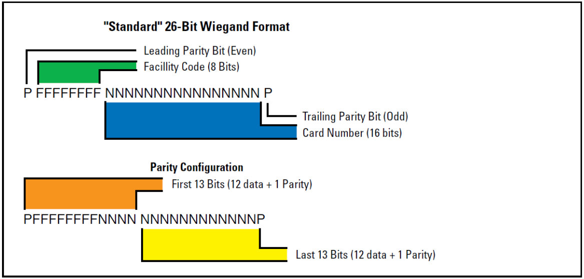
RFID can used anywhere an identification scheme is present

- Inventory Management
- Traffic Tolls
- Animal Tracking
- Access Control

RFID at Binghamton University

HID brand RFID tags are used for access control all around campus

- Easy to implement
- Easy to use
- Even easier to exploit


"Standard" 26-Bit Wiegand Format
Leading Parity Bit (Even)
Facillity Code (8 Bits)
P FFFFFFFF NNNNNNNNNNNNNNNN P
Trailing Parity Bit (Odd)
Card Number (16 bits)
Parity Configuration
First 13 Bits (12 data + 1 Parity)
PFFFFFFFFNNNN NNNNNNNNNNNNP
Last 13 Bits (12 data + 1 Parity)

Wiegrand Card Format

Exploiting RFID

Overview

- Intercepting RFID Tags
  - How do we put ourselves in a position to capture tag IDs
- Reading RFID Tags
  - How do we actually read and process the information once we are in position to capture it
- Replicating RFID Tags
  - How do we replay the information once we process it

Exploiting RFID

Intercepting RFID Tags

Potential Ideas

- Briefcase pass-by
- Scanner over scanner
- Long-range scanner
- Lifting RFID cards off targets

(a) Briefcase (b) Skimmer (c) Long-range

Different methods of card interception

Exploiting RFID

Reading RFID Tags

- Equipment for long/moderate range scanners is expensive
- Purchased multiple third-party scanners, which did not properly support the HID card format
- Current reader is in transit, but supports proper HID card formats
- Will amplify antenna signal to read cards from a distance

HID Card Reader

Exploiting RFID
Writing RFID Tags

The current plan

- Purchase HID card writer
- Write replicas of intercepted HID cards
- Use replicas to impersonate owners of intercepted HID cards

HID Card Writer

HID Beyond Binghamton University

- HID used everywhere
- Protocol for HID tags are fairly uniform, and universally compatible
- Simple technique could be used to get key card access to almost anywhere that uses RFID authentication

Conculding Points

- RFID system
  - Tag with a static ID
  - Readers power tag and forward data
  - Central authentication server
- The attack
  - Amplify antenna power
  - Read card data
  - Write card data
- HID is industry standard, but still very vulnerable
  - Could provide extra security by requiring keypad entry of a unique PIN
  - Could provide extra security by writing a new ID to a tag after each time it is read

References

- 1 https://www.hidglobal.com/sites/default/files/hid-understanding_card_data_formats-wp-en.pdf
- 2(a) https://www.bishopffox.com/resources/tools/rfid-hacking/attack-tools/
- 2(b) https://mediaassets.wxyz.com/photo/2016/10/01/Skimmer1_1475340147161_47211627_ver1.0_640_480.jpg
- 2(c) https://vertassets.blob.core.windows.net/image/d7a097e8/d7a097e8-c248-41b0-9079-2d4535b4e8cc/madonna.jpg
- 7 http://proxmark3-gezhitech.blogspot.com/2013/05/125khz-rfid-honeywell-hid-em4100-card.html
- 8 http://1.bp.blogspot.com/-09vMX5HYHVM/UYdbAx44cVI/AAAAAAAAAKs/xUP7lgTb-9Y/s1600/cloner+with+hid+keyfob.jpg