BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session: 09 (Hardware Hacking)

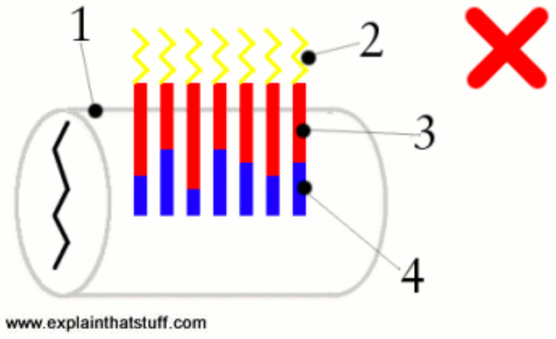
Agenda

- Lock Bumping
- Magnetic Card Cloning
- EVM & RFID Cards
- ATA Hard & USB Disk
- Reverse Engineering Hardware
- Default Configuration
- Router Compromises
- Smartphone Hacking – Beacon Swarm
- Evil Twin Attack
- Man-In-The-Middle

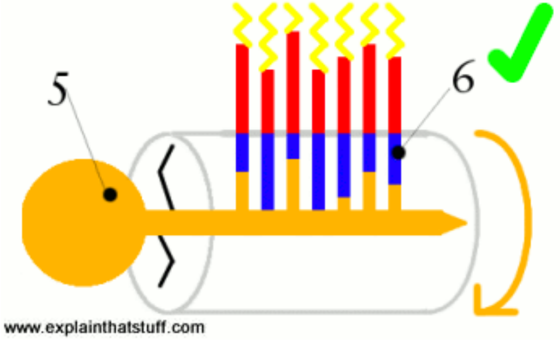
Hardware Hacking

Lock Bumping

- Locks secure an asset by using a series of pins that restrict the mechanism from turning.
- Standard locks have two sets of pins: driver pins and key pins.
- Driver pins are suspended by springs and push down on key pins.
- The key pushes the key pins against the driver pins to align a clear path for the mechanism.
- Once the pins have been aligned, the mechanism is clear and allows the lock to be turned.



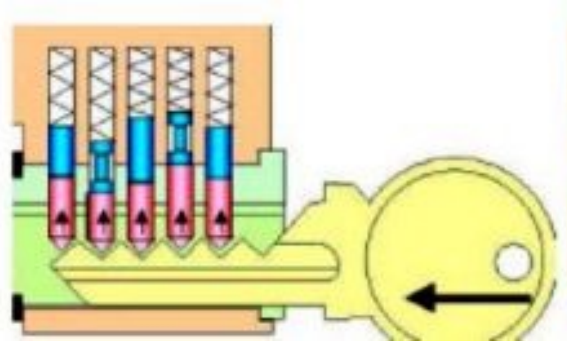
www.explainthatstuff.com

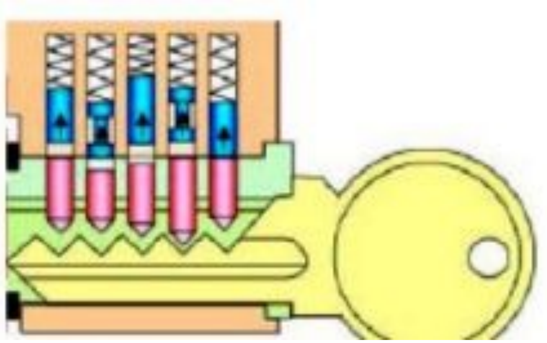


www.explainthatstuff.com

Lock Bumping …

- A specially constructed key (bump key) has teeth that sit below the key pins.
- When a bump key is inserted into any standard lock and then struck (“bumped”), each of the tips on the bump key transfers the force to the key pins causing them to “bump” into place temporarily for just a fraction of a second.
- With good practice, this window of alignment is enough to allow the lock to turn.
- Bumped locks have no evidence of tampering
- A trained person can bump a lock faster than someone with the real key can open it.

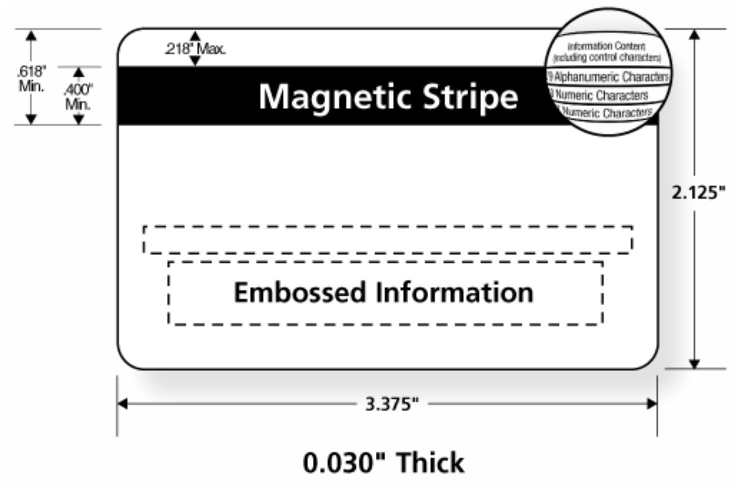


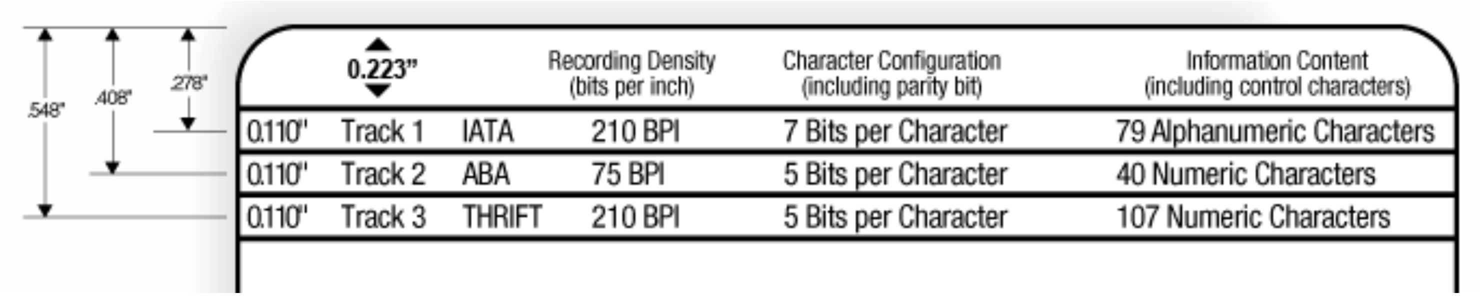


Magnetic Card Cloning

- Most of magstripe cards use ISO standards 7810, 7811, and 7813.
  - 7810: Physical characteristics
  - 7811(1,2,3,6): Embossing, Magnetic stripe, location of embossed chars
  - 7813: Financial transaction cards
- A card has three data tracks referred to as tracks 1, 2, and 3.
- Most magstripe cards have no security measures to protect the data stored on the card and encode the data on the card.
- Several tools are available to clone, alter, and update magstripe card data.
- Tools have a Reader & Writer and Magnetic-Stripe Card Explorer software.

Magnetic Card Cloning …

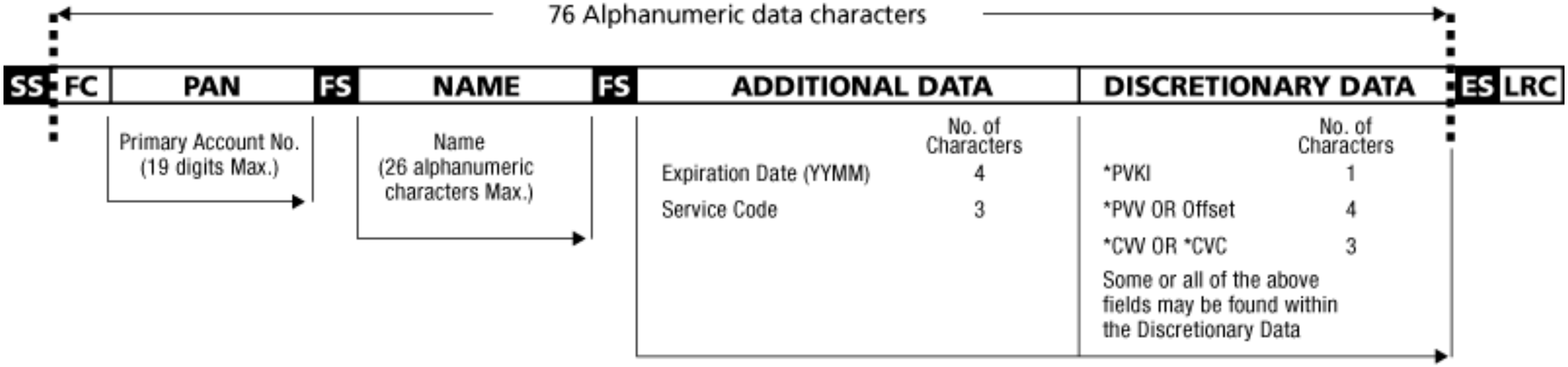




0.223"			Recording Density (bits per inch)	Character Configuration (including parity bit)	Information Content (including control characters)
0.110"	Track 1	IATA	210 BPI	7 Bits per Character	79 Alphanumeric Characters
0.110"	Track 2	ABA	75 BPI	5 Bits per Character	40 Numeric Characters
0.110"	Track 3	THRIFT	210 BPI	5 Bits per Character	107 Numeric Characters

Magnetic Card Cloning …

Track 1:



76 Alphanumeric data characters

SS	FC	PAN	FS	NAME	FS	ADDITIONAL DATA	DISCRETIONARY DATA	ES	LRC

Primary Account No. (19 digits Max.)

Name (26 alphanumeric characters Max.)

	No. of Characters
Expiration Date (YYMM)	4
Service Code	3

	No. of Characters
*PVKI	1
*PVV OR Offset	4
*CVV OR *CVC	3

Some or all of the above fields may be found within the Discretionary Data

Shaded area identifies control characters

SS	Start Sentinel	%
FS	Field Separator	^
ES	End Sentinel	?

FC	Format Code
LRC	Longitudinal Redundancy Check Character

*(PVKI) PIN Verification Key Indicator

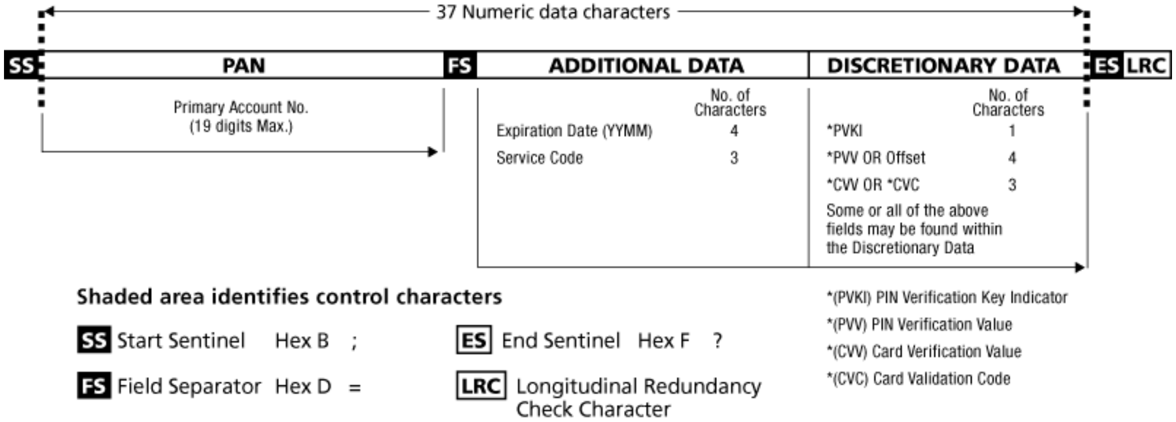
*(PVV) PIN Verification Value

*(CVV) Card Verification Value

*(CVC) Card Validation Code

Magnetic Card Cloning …

Track 2:



37 Numeric data characters

SS | PAN | FS | ADDITIONAL DATA | DISCRETIONARY DATA | ES | LRC

Primary Account No. (19 digits Max.)

	No. of Characters
Expiration Date (YYMM)	4
Service Code	3

	No. of Characters
*PVKI	1
*PVV OR Offset	4
*CVV OR *CVC	3

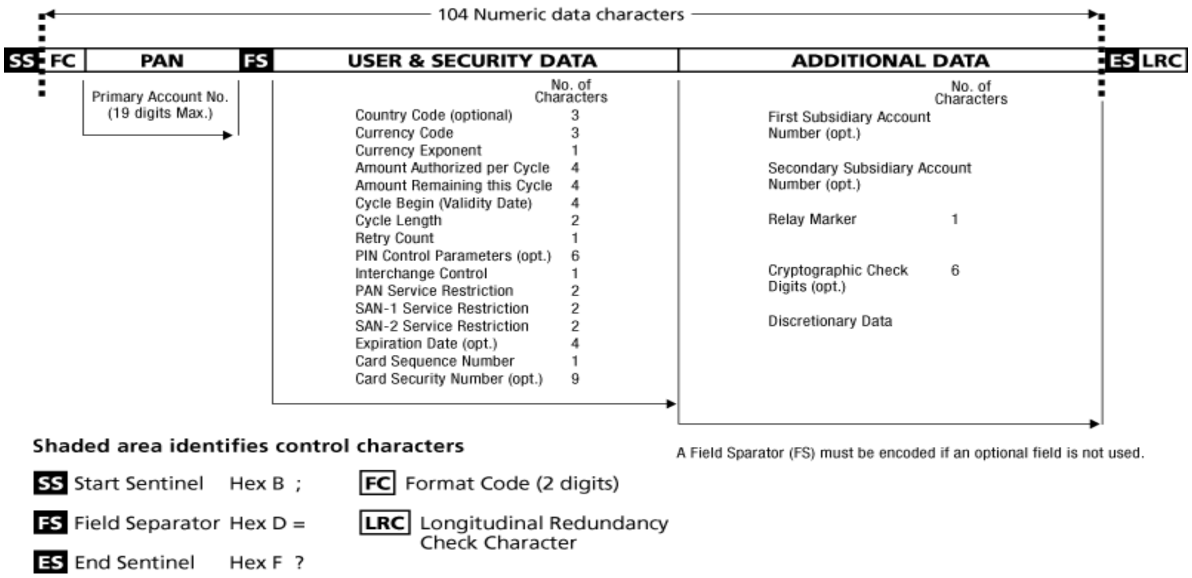
Some or all of the above fields may be found within the Discretionary Data

Shaded area identifies control characters

SS	Start Sentinel	Hex B	;
FS	Field Separator	Hex D	=
ES	End Sentinel	Hex F	?
LRC	Longitudinal Redundancy Check Character		

*(PVKI) PIN Verification Key Indicator
*(PVV) PIN Verification Value
*(CVV) Card Verification Value
*(CVC) Card Validation Code

Track 3:



104 Numeric data characters

SS | FC | PAN | FS | USER & SECURITY DATA | ADDITIONAL DATA | ES | LRC

Primary Account No. (19 digits Max.)

	No. of Characters
Country Code (optional)	3
Currency Code	3
Currency Exponent	1
Amount Authorized per Cycle	4
Amount Remaining this Cycle	4
Cycle Begin (Validity Date)	4
Cycle Length	2
Retry Count	1
PIN Control Parameters (opt.)	6
Interchange Control	1
PAN Service Restriction	2
SAN-1 Service Restriction	2
SAN-2 Service Restriction	2
Expiration Date (opt.)	4
Card Sequence Number	1
Card Security Number (opt.)	9

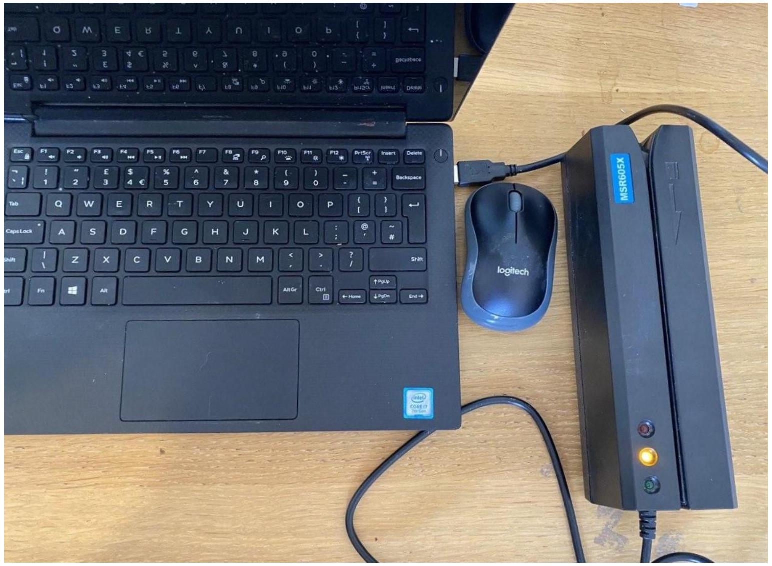
	No. of Characters
First Subsidiary Account Number (opt.)	
Secondary Subsidiary Account Number (opt.)	
Relay Marker	1
Cryptographic Check Digits (opt.)	6
Discretionary Data	

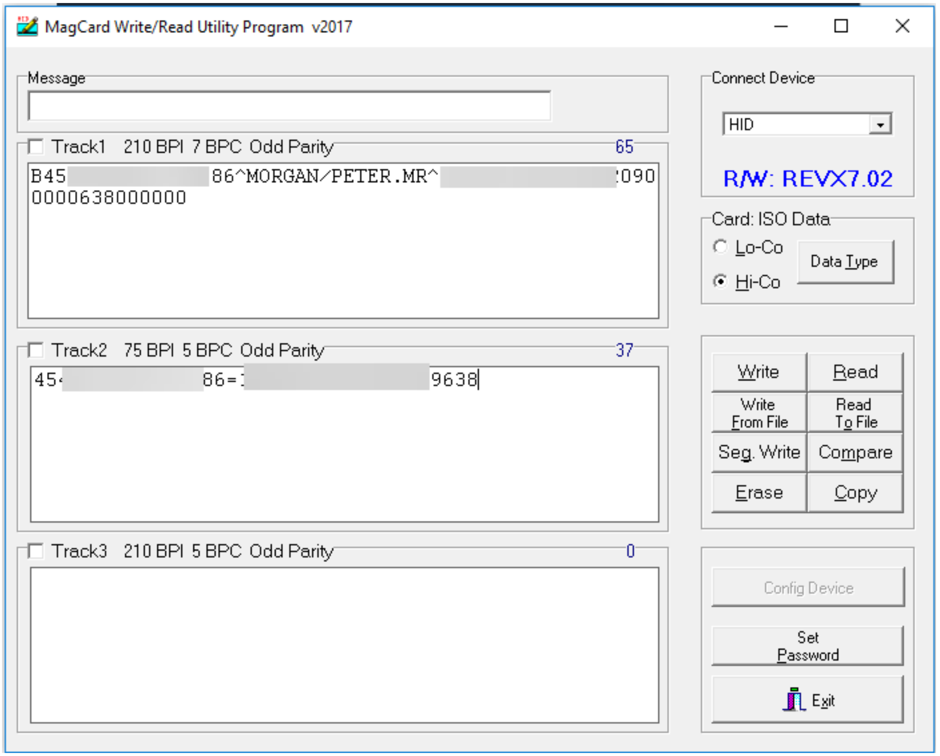
Shaded area identifies control characters

SS	Start Sentinel	Hex B	;
FS	Field Separator	Hex D	=
ES	End Sentinel	Hex F	?
FC	Format Code (2 digits)		
LRC	Longitudinal Redundancy Check Character		

A Field Sparator (FS) must be encoded if an optional field is not used.

Magnetic Card Cloning …





MagCard Write/Read Utility Program v2017

Message

□ Track1 210 BPI 7 BPC Odd Parity 65

```
B45[redacted]86^MORGAN/PETER.MR^[redacted]090
0000638000000
```

□ Track2 75 BPI 5 BPC Odd Parity 37

```
45[redacted]86=[redacted]9638
```

□ Track3 210 BPI 5 BPC Odd Parity 0

Connect Device: HID

R/W: REVX7.02

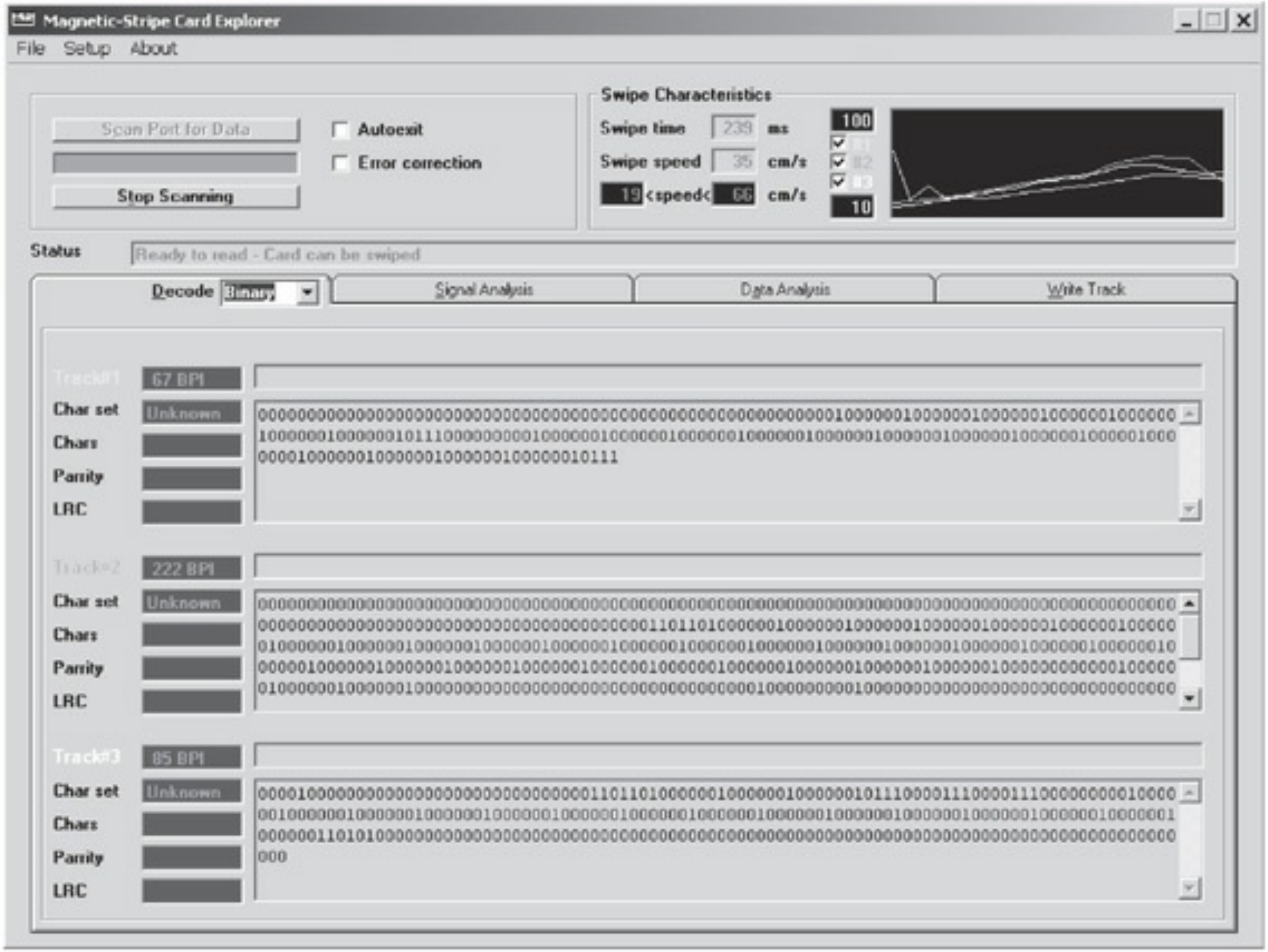
Card: ISO Data

○ Lo-Co

● Hi-Co

- MSR605 is a magnetic card reader and writer that plugs into a computer via USB and comes with pre-packaged software for Windows.
- Required to set it into "read" mode and swipe a credit or debit card to capture card details

Magnetic Card Cloning …



Magnetic-Stripe Card Explorer

☐ Autoexit

☐ Error correction

Swipe Characteristics

Swipe time 239 ms

Swipe speed 35 cm/s

19 <speed< 66 cm/s

100

☑ T1

☑ T2

☑ T3

10

Status: Ready to read - Card can be swiped

Decode: Binary

Track#1: 67 BPI

Char set: Unknown

Chars

Parity

LRC

```
00000000000000000000000000000000000000000000000000000000000010000001000000100000010000001000000
10000001000000101110000000001000000100000010000001000000100000010000001000000100000010000001000
0000100000010000001000000100000010111
```

Track#2: 222 BPI

Char set: Unknown

Chars

Parity

LRC

```
00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000000000000000000000000000000000000000110110100000010000001000000100000010000001000000100000
01000000100000010000001000000100000010000001000000010000001000000100000010000001000000100000010
00000100000010000001000000100000010000001000000010000001000000100000010000001000000000000100000
01000000100000010000000000000000000000000000000000001000000000100000000000000000000000000000000
```

Track#3: 85 BPI

Char set: Unknown

Chars

Parity

LRC

```
00001000000000000000000000000000001101101000000010000001000000101110000111000011100000000010000
00100000010000001000000100000010000001000000100000010000001000000100000010000001000000100000001
00000011010100000000000000000000000000000000000000000000000000000000000000000000000000000000000
000
```

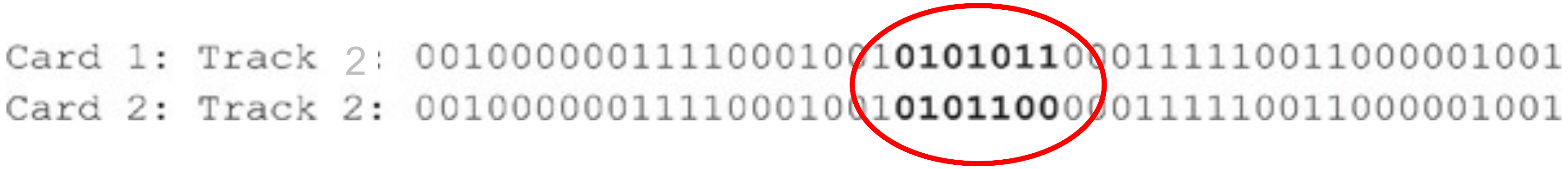
Data on card may include:

- Id Number
- Serial Number
- Social Security Number
- Name & Address
- Account Balance
- Others.

- Data is often in a custom format and needs to be decoded to human-readable form.

Magnetic Card Cloning …

- A quick analysis of the data is enough to predict how to create a cloned card.
- Many access cards simply contain an ID or other sequential number.
- Brute-forcing card values can be a quick way to gain access to a system or bypass a panel.
- Simplest option to analyse the card data on the three tracks is to read multiple cards of the same type.
- Once the data has been acquired, use a ‘diff’ tool to do a visual inspection of the data find contextual data.

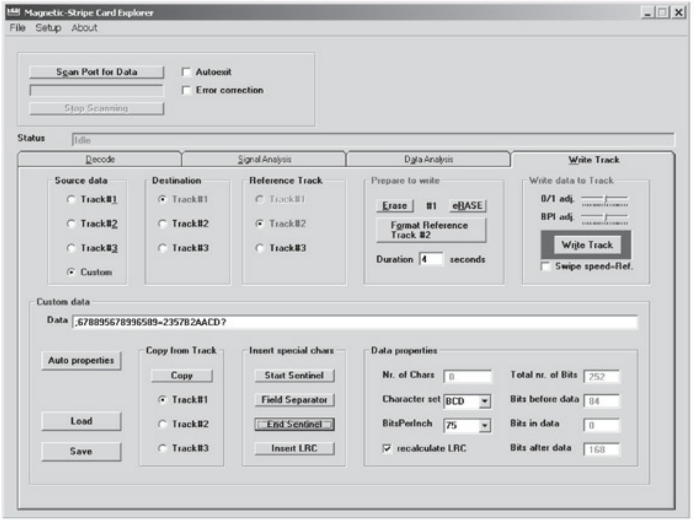


```
Card 1: Track 2: 0010000000111100010010101011000111110011000001001
Card 2: Track 2: 0010000000111100010010101100000111110011000001001
```

Magnetic Card Cloning …

Writing data back to a card:

- Choose the track to write the data to.
- A track may include checksum data to verify that the data on the card is valid or the card wasn't damaged.
- If there is a checksum, determine what checksum is being used and recalculate a new one before the card can be used.
- Sometimes a card contains a checksum but it's not actually used by the reader



Magnetic-Stripe Card Explorer

□ Autoexit
□ Error correction

Status: Idle

Source data: ○ Track#1 ○ Track#2 ○ Track#3 ● Custom

Destination: ● Track#1 ○ Track#2 ○ Track#3

Reference Track: ○ Track#1 ● Track#2 ○ Track#3

Duration: 4 seconds

□ Swipe speed=Ref.

Custom data

Data: ;678895678996589=235782AACD?

Copy from Track: ● Track#1 ○ Track#2 ○ Track#3

Data properties

Nr. of Chars: 0

Character set: BCD

BitsPerInch: 75

☑ recalculate LRC

Total nr. of Bits: 252

Bits before data: 84

Bits in data: 0

Bits after data: 168

EMV Cards

- EMV = Europay, Mastercard and Visa, commonly referred to cards with chips
- EMV standard is a security technology used worldwide for all payments done with credit, debit, and prepaid EMV smart cards
- EMVs are chip & signature (mainly US) or chip & PIN (most of the world)
- EMV cards are similar in data structures to Magstripe cards
- EMV cards track 1 and track 2 data is almost same
- PIN number provision makes it much more secure

EMV Cards: Pre-Play Attack

- An EMV payment card authenticates itself with a MAC of transaction data
  - Uses a freshly generated Unpredictable Number (UN).
  - If you can predict it, you can record everything you need from momentary access to a chip card to play it back and impersonate the card at a future date.
- Many ATMs and point-of-sale terminals have defective or simple random number generators (often simple counters)
- EMV specification encourages this by requiring that only four successive values of a terminal’s “unpredictable number” have to be different for it to pass conformance testing.
- A hacker with transient access to a payment card (a programmer of a terminal in a Mafia-owned shop) can harvest authentication codes to create a “clone” of the card to be used later in ATMs and elsewhere.
- This is called a “pre-play” attack.

RFID Cards

- RFID card systems operate on one of two different spectrums: 135 kHz or 13.56 MHz.
- RFID cards are normally unprotected and can be cloned easily.
- RFID cards have started to employ custom cryptography and other security measures to improve security.
- RFID card use proprietary protocol.
  - Hardware tools are available to read and imitate common RFID cards.
  - An advanced version of an RFID reader/writer is the proxmark3 device.
    - Proxmark3 has an on-board FPGA built in to allow for the decoding of different RFID protocols. This tool requires skills and is costly.
  - Universal Software Radio Peripheral (USRP) is another option to intercept and decode RFID traffic
    - USRP can send and receive raw signals on the common RFID frequencies allowing it to intercept and imitate cards.

ATA Hard Disk Password Hacking

- ATA (Advance Technology Attachment) security requires that user types a password before a hard disk can be accessed by the BIOS.
- ATA does not encrypt or protect the contents of the drive.
- Multiple bypass products and services exist for specific drives but the most common and easiest is simply to hot-swap the drive into a system with ATA security disabled.
- Hot-swap work steps:
  - Boot the computer with unblocked hard drive and open BIOS menu that allows to reset ATA password
  - Carefully remove the unlocked drive from the computer and insert the locked drive.
  - Set the hard-disk password using the BIOS interface.
  - Drive will accept the new password.
- Hot swapping is risky and may damage the drive, the drive's file system or the computer.
- Requires high degree of precaution for use of this technique.

Hot Swapping

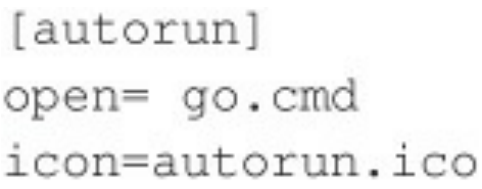
- A hot swap is the replacement of a hard drive, CD-ROM drive, power supply, or other device with a similar device while the computer system using it, remains in operation.
- Replacement can be because of a device failure or, for storage devices, to substitute other data.
- Hot swapping works by providing a rack or enclosure for the device that provides an appearance to the computer's bus or I/O controller that the device is still there while it is removed and replaced with another device.
- A hot swap arrangement is sometimes provided where multiple devices are shared on a local area network.

Hacking USB Drives

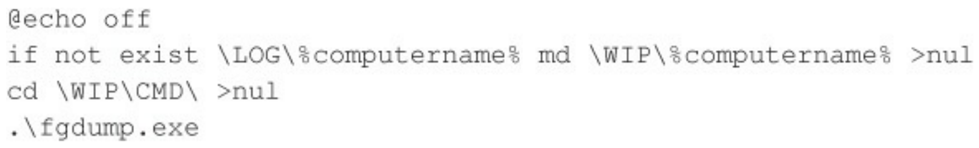
- USB drives normally use U3 standard
  - It has a secondary partition included with USB flash drives.
  - U3 partition is read only and partition menu is configured to auto execute when the USB stick is inserted into a computer
  - U3 hacking takes advantage of the autorun feature built into Windows.
- When inserted into a computer, the USB flash drive is enumerated and two separate devices are mounted:
  - U3 partition
  - Regular flash storage partition.
- U3 partition immediately runs whatever program is configured in the autorun.ini file on the partition.
- Each manufacturer provides a tool to replace the U3 partition with a custom ISO file for branding or deleting the partition.

Hacking USB Drives …

- U3 partition can be overwritten using the manufacturer's tool to include a malicious program.
- Most common attacks are to read the password hashes from the local Windows password file or install a Trojan for remote access.
- Password file can be e-mailed to the attacker or stored on the flash drive for offline cracking later using tools like **fgdump**.
- Steps to build a USB drive based malicious program:



```
[autorun]
open= go.cmd
icon=autorun.ico
```



```
@echo off
if not exist \LOG\%computername% md \WIP\%computername% >nul
cd \WIP\CMD\ >nul
.\fgdump.exe
```

- Copy the scripts and utilities to U3CUSTOM folder provided by devices manufacturer or use a tool like Universal_Customizer

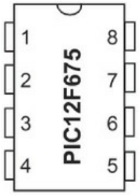
Hacking USB Drives …

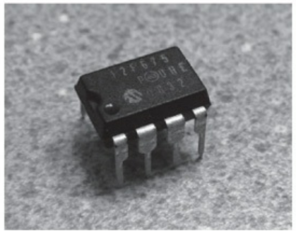
- ISOCreate.cmd included with Universal_Customizer can package up the autorun program, executables, and scripts in the U3CUSTOM directory into an ISO to be written to the U3 device.
- Final step is to write the ISO to the USB drive with the Universal_Customizer.exe.
- U3 stick is now armed and ready for use.
- Any computer that has autorun enabled will launch the fgdump.exe program and record the password hashes.

- Refer link: https://www.raymond.cc/blog/hack-u3-usb-smart-drive-to-become-ultimate-hack-tool/

Reverse Engineering Hardware

- Map the device
  - Remove the coverings of the device
  - May be glued shut (use heatgun) or hermetically shut (destroy external housing gently)
  - May use special security screws – find details about such components
- Remove physical protections
  - Use suitable chemicals
  - Can use x-ray imaging as well – non-invasive
- Identify ICs used
  - Get detailed datasheet of ICs from internet
- Get details of Microcontrollers, EPROMs etc
- Identify external interfaces (HDMI, USB, Audio Jack etc)
- Trace connection between various components





Reverse Engineering Hardware …

- Sniffing bus data
  - Use logic analyzer to sniff or monitor data between various components
  - Attach a basic client device to sniff data from wireless interface
    - Identify FCC Id of interface and use FCC website to get details
    - Find out radio frequencies used by interface
- Firmware reverse engineering
  - Get firmware files from manufacturer website
  - Use hex editor to find details like default passwords, administrative ports, debug interfaces etc
- EEPROM programmers
- Microcontroller programming
- JTAG (Joint Testing Action Group)

Default Configurations

- Every device that requires a user login comes with the chicken & egg problem of how to communicate the initial default device password to the user.
- Most devices have standard passwords or insecure security settings.
- These passwords are available publicly on internet (Ex:Phenoelit default password list http://www.phenoelit.org/dpl/dpl.html)
- Embedded routers often share default passwords across entire product lines.
- Number of routers with remote administration and default password is very high are serious security risk.
- An attacker can log in to the router easily and change the settings to redirect the users to a malicious DNS and other services.

Default Configurations …

- Many cell phones are shipped with Bluetooth default discovery mode ON, allowing any attacker to discover and connect with the device.
- One inexpensive off-the-shelf tool to help with Bluetooth hardware hacking is Ubertooth (ubertooth.sourceforge.net).

Router Hacking

- Router hacking allows a cyber criminal to take control of a targeted router without its owner’s consent.
- Hackers conduct automated scans of routers to identify hardware that is vulnerable to an attack.
- Extract configuration files enabling them to control or manipulate any devices that connect to your network, as well as the Internet connection.
- Attacks on routers focus on those with Simple Network Management Protocol (SNMP) that is exposed to the Internet.
  - A default setting normally established during the setup of a network.
  - Many organisations leave SNMP OPEN after the setup process is complete creating risk of compromise.

How does Router Hacking Work?

- Using the default login credentials:
  - Easiest way to hack a router (If you’ve never changed your router’s admin password, anyone can simply log in with default credentials)
- Exploiting a firmware vulnerability:
  - Firmware is the built-in software that tells a hardware device, such as router, how it should work.
  - A hacker can leverage a router’s firmware has a vulnerability, to access router’s administrative settings.
  - Regularly check and install router manufacturer’s website for firmware updates.
- Cracking your password:
  - Hackers can guess or brute-force a router’s password
  - Simpler passwords are very easy to crack
  - Always create a strong password for routers.

Uses of Router Hacking

- Eavesdropping
- Monitor HTTP connections
- Interfere with HTTP connections
- Install router malware
- Detect and attack devices on network
- Redirect internet traffic
- Use internet connection
- Add router to botnet

How to know a Router is Hacked?

- Altered DNS settings
- Admin password not working
- Slow internet
- Strange software or malware on your devices
- Unrecognised devices on your network

Correction Actions for a Hacked Router

- Disconnect router from internet and other devices
- Perform factory reset
- Change admin password
- Create a new SSID and password for Wi-FI
- Create a guest network
- Update firmware regularly

Preventive Actions Router Hacking

- Create a new admin id and password
- Disable remote access settings
- Monitor wi-Fi network traffic
- Opt for WPA3 – implements AES encryption
- Disable WPS
- Change default SSID name
- Update router firmware regularly
- Setup router firewall

Steps to Hack a Router

- Select an IP range say. **XXX.XXX.30.0 to XXX.XXX.30.255**
- Scan for routers (preferably home)
- When finished scan, find IP addresses which has open ports such as http port(80), ftp port(21) and telnet port(23).
- Access these addresses thru web browser because http port is opened
  - Find whether the web page is router log in page.
  - Error message - TD-8817 indicates "default username and password"
- Try to access the IP address using default logins.
  - Default username and passwords are not same for every routers.
- With default credential, log in to the router administration page

Smartphone Hacking with Beacon Swarm

- Smartphones keep looking for networks in vicinity on constant basis by broadcasting
  - Normally broadcast using a fake MAC id
  - Once a connection is found, it connects using the real MAC id
- Smartphones connect automatically to previously connected networks
- One can setup fake networks (SSID) to lure a phone to connect to it
- Once connected, the fake network effectively becomes the MITM
- Hardware required to create a fake network swarm
  - NodeMCU or ESP8266 device
  - Micro USB cable
- Steps
  - **Setup Arduino IDE:** to build and upload scripts for micro-controller devices
  - Download and install: http://arduino.esp8266.com/stable/package_esp8266com_index.json
  - Configure Arduino for NodeMCU boards – connect NodeMCU to computer
  - Download and install Spacehuhn's Becaon Spammer project from GITHUB - git clone https://github.com/spacehuhn/esp8266_beaconSpam.git

Smartphone Hacking with Beacon Swarm

- Steps
  - Open Beacon spammer file in Arduino IDE
  - Prepare and sort list of Open SSIDs – collect SSID list/details thru War Drive
    - "JWMarriott_GUEST\n"
    - "McDonalds Free WiFi\n"
    - ”Starbucks WiFi\n"
  - Drop these SSID names into Beacon Spammer script
  - Configure Beacon Spammer and push to NodeMCU
  - Open Wireshark, set channel and filter
  - Search for probe and authentication requests
  - Filter search by MAC id being broadcasted by fake beacon – normally first 3 MAC octet

  - Ref reading: https://null-byte.wonderhowto.com/how-to/use-esp8266-beacon-spammer-track-smartphone-users-0187599/

  - **What can be done to prevent such attack?**

Evil Twin Attack

- Evil Twin attack takes advantage of the fact that most computers and phones will only 'see' the name of SSID of a wireless network as part of connection process.
- A hacker can take advantage of this vulnerability by setting up an Access Point with same name.
- This will trick a user into connecting if the network has the same name, same password, and same encryption.
- How does the hacker get password?
- It uses Advanced Social Engineering
  - Create a captive portal style phishing page similar to the login/password page of the network
  - Screen is similar to original one with T&C, other data and password entry fields
  - Can use **Airgeddon** or **Aircrack-ng** tools
  - Flood the actual trusted network with de-authentication requests so that the user is not able to connect and comes to join via the twin (but fake) name network
  - Upon connecting to phishing page, user will be asked for password with an plausible explanation (router has updated and requires password etc)

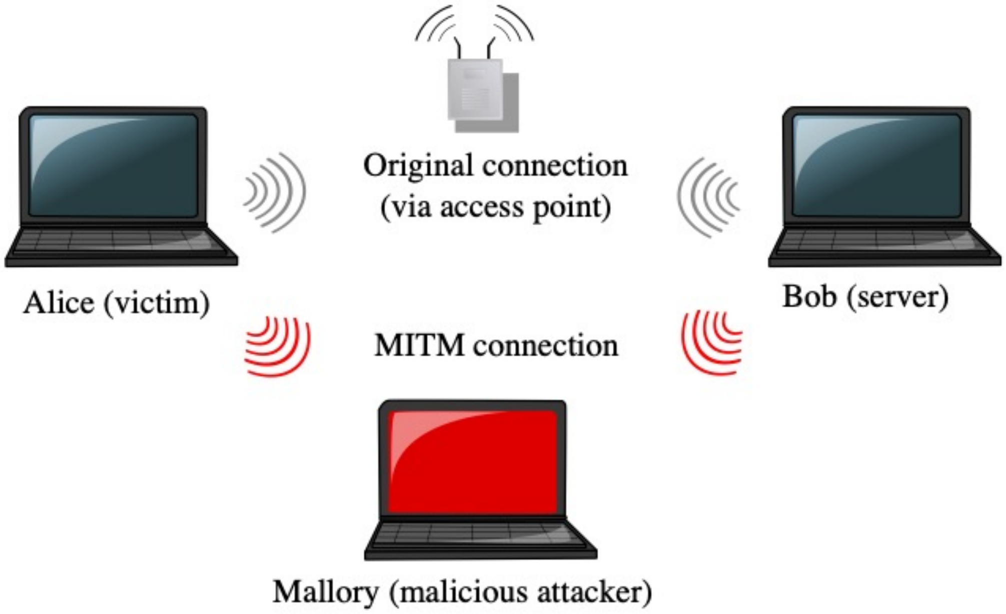
Evil Twin Attack…

- It uses Advanced Social Engineering
  - Use a previously captured password handshake from the actual network to validate the password entered by the user
  - If users enters wrong password, display appropriate message
  - Once user enters correct password, the network is hacked
  - This is known as **technology assisted Social Engineering**
- Steps
  - Requirements: Airgeddon, Kali Linux, Wireless adapter
  - Install and configure Airgeddon
  - Select a target
  - Gather handshake
  - Setup phishing page
  - Capture network credentials

- Ref: https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/

Man In The Middle Attack

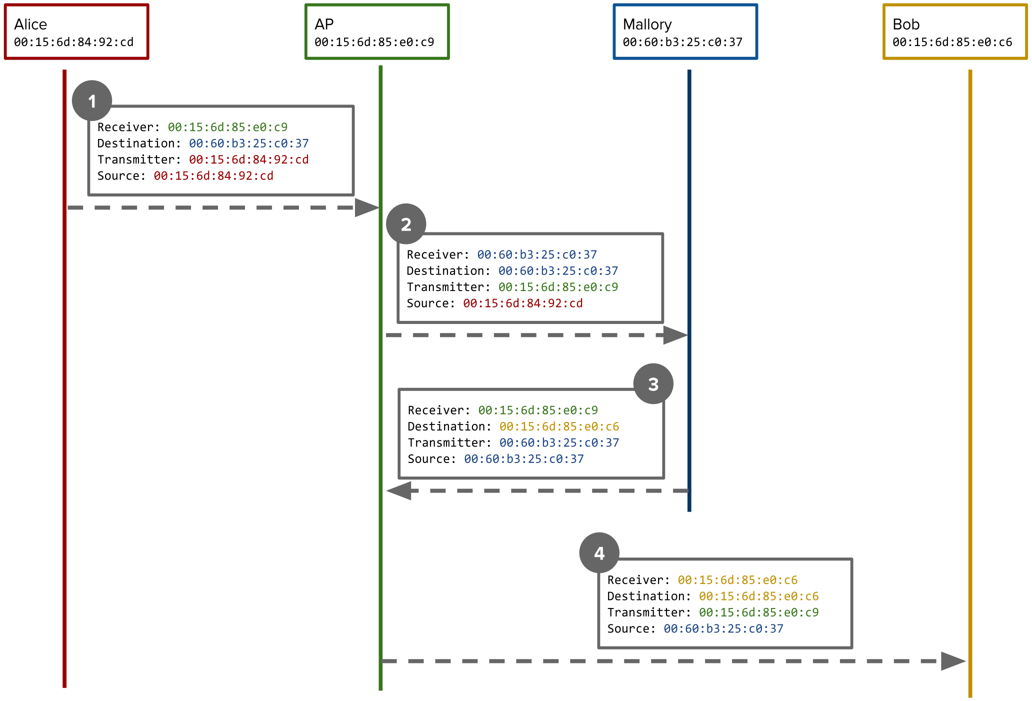
- Man In The middle (MITM) attack is one where the attacker (Mallory) secretly captures and relays communication between two parties who believe they are directly communicating with each other (Alice and Bob).
- One of the technique used for MITM is ARP spoofing or ARP poisoning.



- Alice and Bob are connected to a WiFi hotspot.
- They will use ARP requests and replies to find out the physical address (MAC address) to which to direct their traffic.
- Attacker (Mallory) will send a false ARP messages to Alice, giving its own MAC address as the physical address for Bob; and similar ARP messages to Bob, giving its own MAC address as the physical address for Alice.

Man In The Middle Attack

- When Alice and Bob communicate, they will treat Mallory as the destination for all of their traffic, and send their entire communication through her.
- Mallory will forward the traffic, so that neither side is aware that she is intercepting it.
- A packet from Alice to Bob will be transmitted over the air four times, with different addresses in the Layer 2 header each time
- Ref: https://youtu.be/GVu91EISH_M



Alice
00:15:6d:84:92:cd

AP
00:15:6d:85:e0:c9

Mallory
00:60:b3:25:c0:37

Bob
00:15:6d:85:e0:c6

1

```
Receiver: 00:15:6d:85:e0:c9
Destination: 00:60:b3:25:c0:37
Transmitter: 00:15:6d:84:92:cd
Source: 00:15:6d:84:92:cd
```

2

```
Receiver: 00:60:b3:25:c0:37
Destination: 00:60:b3:25:c0:37
Transmitter: 00:15:6d:85:e0:c9
Source: 00:15:6d:84:92:cd
```

3

```
Receiver: 00:15:6d:85:e0:c9
Destination: 00:15:6d:85:e0:c6
Transmitter: 00:60:b3:25:c0:37
Source: 00:60:b3:25:c0:37
```

4

```
Receiver: 00:15:6d:85:e0:c6
Destination: 00:15:6d:85:e0:c6
Transmitter: 00:15:6d:85:e0:c9
Source: 00:60:b3:25:c0:37
```

Best Practices to Prevent Wi-Fi Hacks

- Purge networks not required in the preferred network list
- Use VPN to keep local traffic encrypted
- Disable auto-connect when joining networks
- Never use hidden networks
- Disable WPS functionality on routers
- Never re-use password for Wi-Fi
- Isolate clients to their own sub-net

- Ref: https://www.varonis.com/blog/7-wi-fi-security-tips-avoid-being-easy-prey-for-hackers/

Demo

1. **10 important changes to Kali Linux after installation**
   https://www.youtube.com/watch?v=8VL0K0rFgxw

2. **Lazy script for wi-fi hacking**
   https://www.youtube.com/watch?v=PUQ1bMtft-o

3. **Find information about phone number using OSINT tools**
   https://www.youtube.com/watch?v=WW6myutKBYk

4. **Hunt down Social Media accounts by username using Sherlock**
   https://www.youtube.com/watch?v=HrqYGTK8-bo

5. **Track and connect to Smartphone with a Beacon Swarm**
   https://www.youtube.com/watch?v=o95Or-Z_Ybk

6. **Top 10 browser extension for hackers and OSINT researchers**
   https://www.youtube.com/watch?v=F3tJUNHbwnA

Thank You