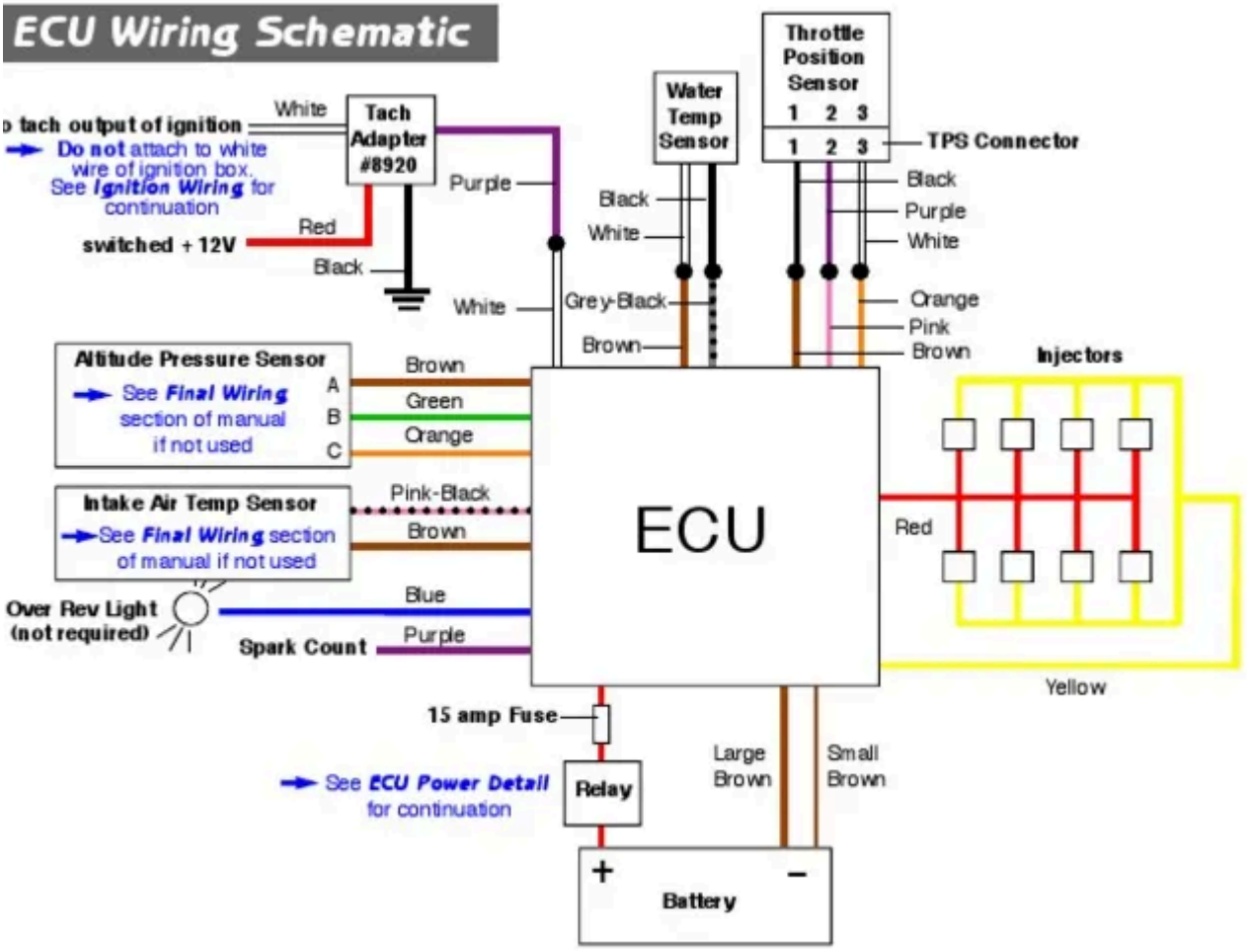
How to Hack a Car - Explanation

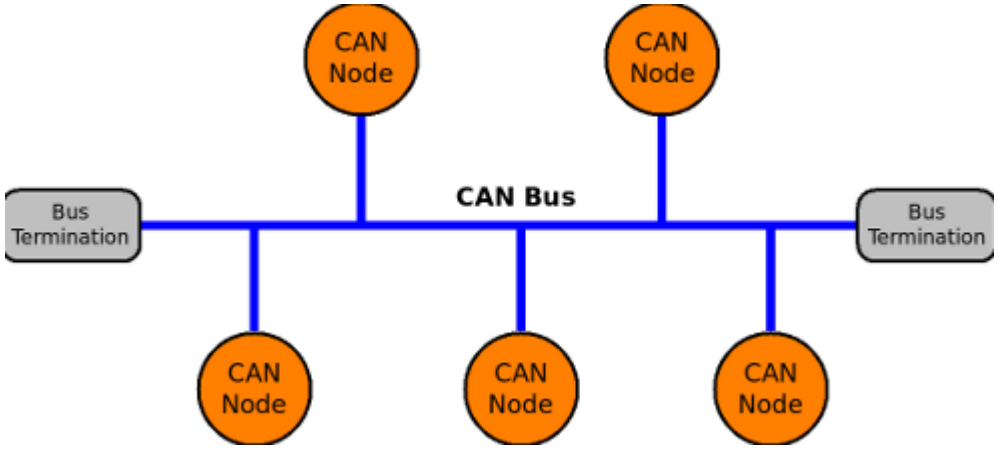
Peace be upon you I explained some time ago on YouTube how to hack a car If you don't want to watch it come here sit down and listen to me

Okay to hack a car you first need to fully understand how it works

There is something called an ECU which is basically the car's brain It is made up of several small computers that control the car's engine



The ECU is connected to something called the CAN bus. Simply put, instead of having many wires and cables, the CAN bus simplifies all of that into just two wires. The gist of CAN bus is that it's a network that transmits data.



Good? Good. Now we know how the car operates.

If I manage to hack the car and get access to the ECU, I can control the car-for example, the windshield wipers or the car doors-and I can do many things depending on the type of hack.

There are many ways to hack a car, but some of the most common

methods are: Hacking through USB

Hacking through a network

Hacking through Bluetooth

Hacking through two devices .

How to Hack a Car - Explanation

Okay, hacking through USB: Some cars have a USB port, usually to charge your phone or update the system.

If the system is poorly designed or has a security vulnerability, a malicious USB device could implant harmful commands inside the system.

To hack the car through USB, the port must be connected to the car's display system, not directly to

the engine.

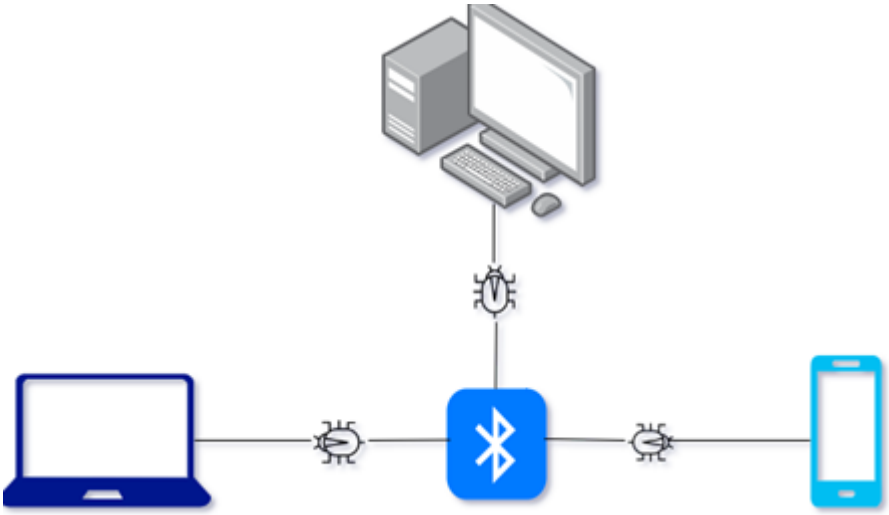
How to Hack a Car - Explanation

But if both systems are connected through the CAN bus network without isolation, the vulnerability can spread to other systems.

If the hack succeeds, what happens?

The hacker can control the brakes, control the speed, or manipulate the display

screen. Now, regarding Bluetooth: There are Bluetooth vulnerabilities.



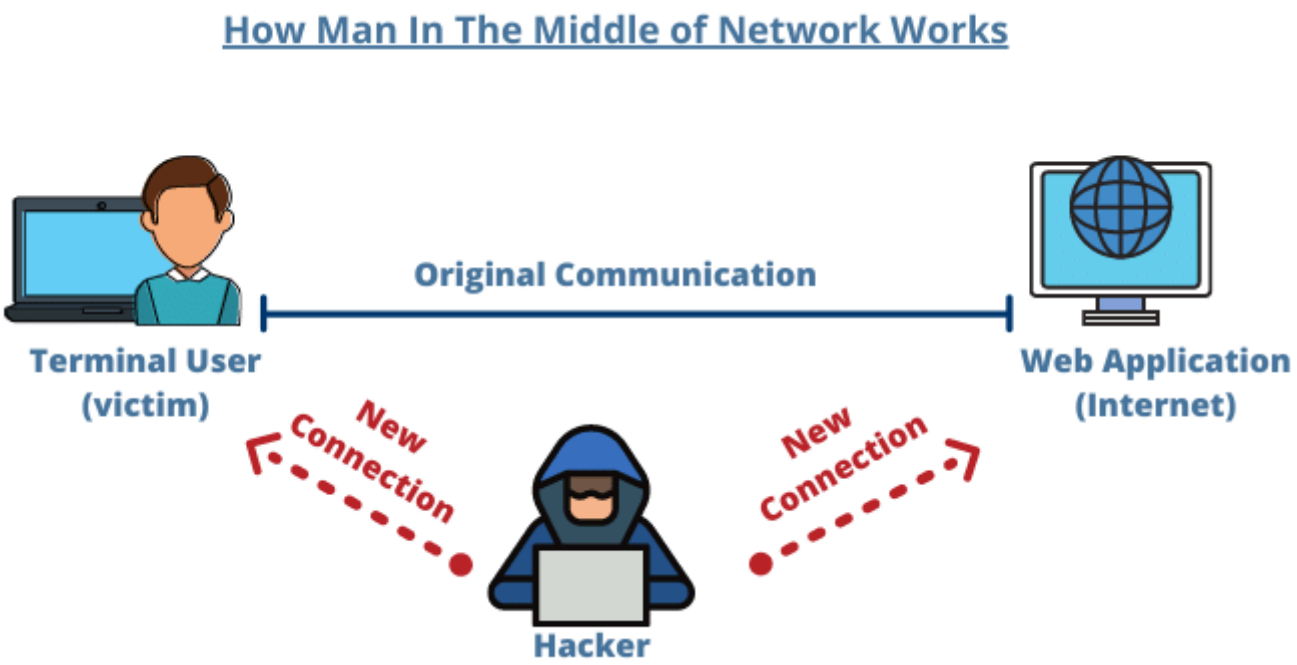
This means discovering a weakness in the Bluetooth system that allows the hacker to control the car
For example, the hacker can perform a Bluesnarfing attack which lets them steal information from the connected device via Bluetooth without the user noticing

Or they can perform a Bluebugging attack which allows the hacker to control the car — for instance making calls, sending voice commands, and more
If the hacker manages to hack the car via Bluetooth what could they do?
They might control the volume level or disable some systems .

How to Hack a Car - Explanation

Okay, hacking through a network
If the car has a private network the hacker might find vulnerabilities there
If there are flaws in the protocols or software the car's network can be hacked

One common attack is called Man-in-the-Middle MITM



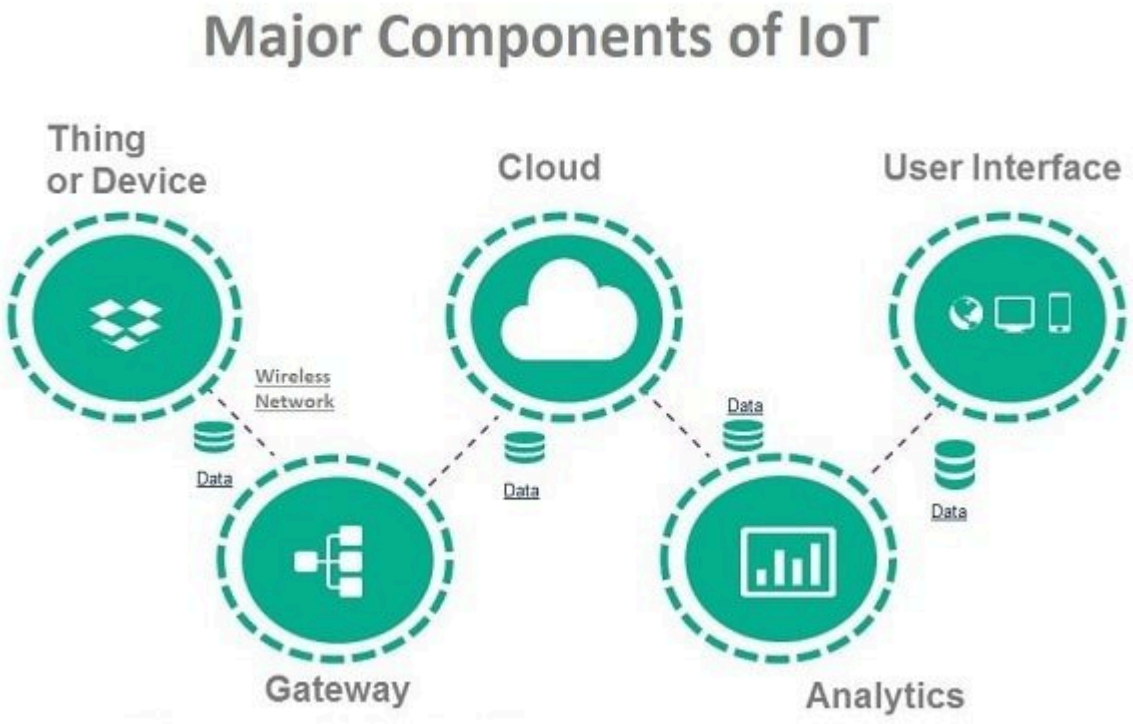
The idea is that you connect to Wi-Fi and through that Wi-Fi the hacker performs a middleman attack
Simply put the hacker intercepts communication between the car and cloud services or apps and can change data or steal confidential car information

There are many methods

So what happens if the hacker manages to hack the network?
They can control systems like brakes or steering
They can disable the engine
They can manipulate the car's settings .

How to Hack a Car - Explanation

What is IoT ?



IoT means the Internet of Things It simply means that ordinary devices like cars refrigerators or electrical devices are connected to the internet and communicate with each other

How does IoT work in smart car systems?
Modern cars today are not just a means of transportation They have become smart devices connected to the internet through systems called IoT

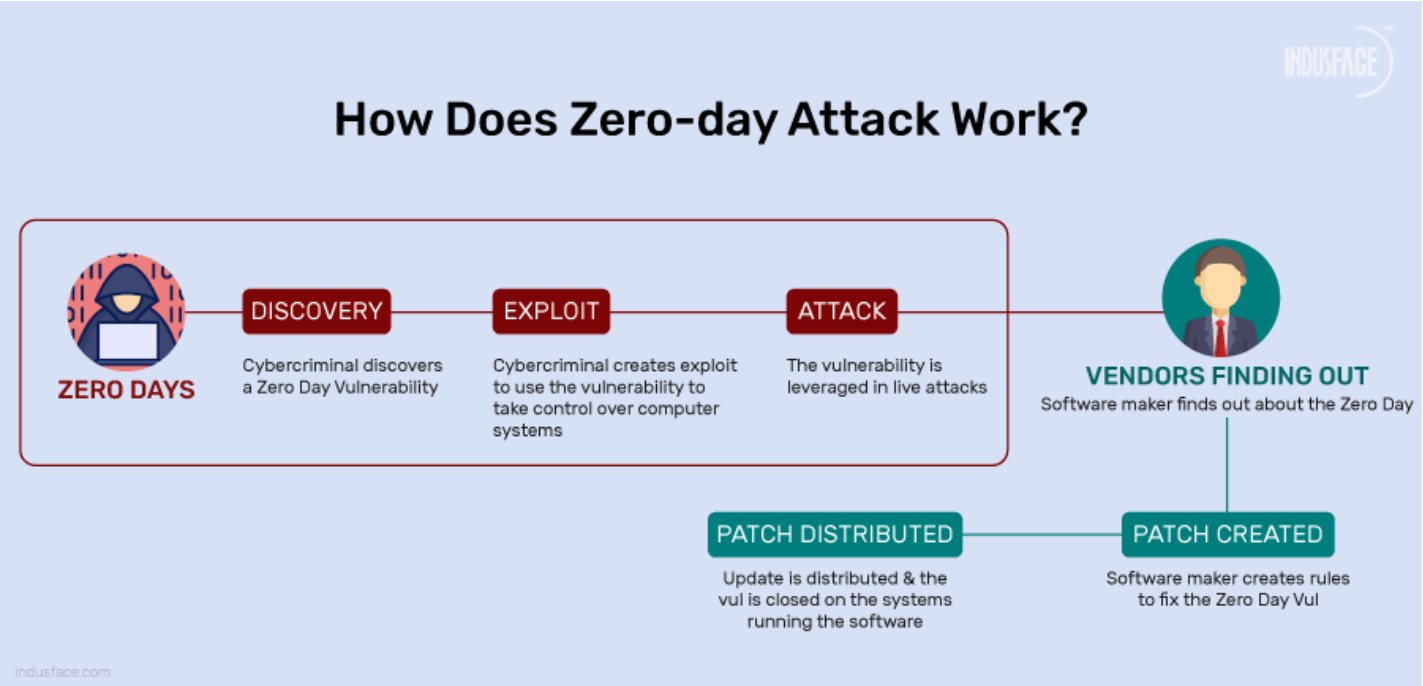
These systems allow the car to control remotely such as unlocking the car or starting the engine through a mobile app Receive updates over the air OTA which means updating the car's software and systems without visiting a service center through the internet and provide location services and monitoring so you can track the car's location engine status and fuel level via the internet

How do hackers attack IoT systems in cars?
Hackers try to find vulnerabilities in the IoT devices inside the car One important method they use is Reverse Engineering which means hackers try to break down the car's system or software step by step to understand how it works and discover vulnerabilities or weaknesses .

Page5

How to Hack a Car - Explanation

What is a Zero Day vulnerability?



Zero Day vulnerabilities are security flaws unknown to car manufacturers or software developers. These flaws have not been discovered or fixed yet and hackers can exploit them before anyone becomes aware.

How do Zero Day vulnerabilities appear in cars?

Modern cars use complex software and connected systems like IoT. This complexity sometimes causes hidden bugs or security holes that remain undiscovered. These are called Zero Day vulnerabilities.

How do hackers find Zero Day vulnerabilities?

Hackers use techniques such as reverse engineering or fuzz testing to analyze the car's software. They search for weaknesses that can be exploited before manufacturers find out about them.

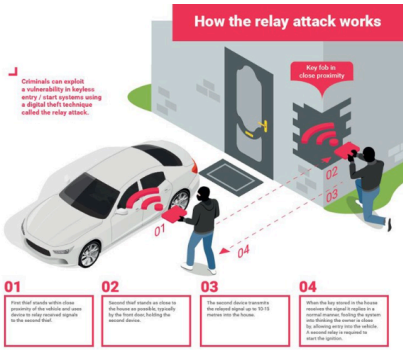
What is the impact of Zero Day attacks on cars?

If these vulnerabilities are exploited successfully, hackers can cause dangerous situations such as disabling safety features or remotely controlling the car. This makes Zero Day vulnerabilities a serious threat to car security.

Page6

How to Hack a Car - Explanation

How Is Relay Attack



Relay Attack - How Hackers Hack a Car Using Relay Devices

Relay Attack - How Hackers Hack a Car Using Relay Devices

Peace be upon you. I will explain how hackers use a relay attack to hack a car. If you don’t want to watch a video, just come here, sit down, and listen carefully.

Okay, first, to understand the relay attack, you need to know how smart keys work. Modern cars use smart keys that send radio signals to the car to unlock doors or start the engine without a physical key.

The smart key sends a radio signal over a very short distance to the car. This signal tells the car to unlock or start the engine.

The hacker uses two devices.

Device 1 is placed close to the smart key, for example inside the owner’s house or in their pocket.

Device 2 is placed near the car.

Device 1 receives the radio signal from the smart key and retransmits it to Device 2, which is near the car.

The car receives the signal from Device 2 and thinks the real smart key is right next to it.

As a result, the car unlocks the doors or starts the engine as if the smart key was present.This attack bypasses the short-range limit of the smart key by extending the signal over a longer distance using the two relay devices.

What happens if the hacker successfully performs this attack?

If the hacker successfully performs the relay attack, they can unlock the car doors without the owner's permission, start the car engine remotely, and steal the car or drive it away without needing the physical key.

This type of attack exploits the smart key's short-range communication by extending its signal, effectively tricking the car into believing the real key is nearby. This makes this attack a serious security threat for modern cars with keyless entry systems .

With best regards