PT Report

"CySDR"

Executive Summary

This report presents the findings of a recent penetration testing engagement that focused on the use of Software Defined Radio (SDR) to assess the security of the new smart city. The testing revealed two vulnerabilities that could be exploited by an attacker to compromise the security of residents and the city premises.

The first finding - The city security cameras are susceptible to attacks. An attacker can use this vulnerability to disrupt the camera's signal and prevent it from detecting non authorized personal. This could allow unauthorized access to the premises or enable concealing other malicious activities.

The second finding – The city vehicles are vulnerable to attacks. An attacker can gain unauthorized access to the vehicle by manipulation of radio signals. This enables an attacker to gain non permitted access to the city vehicles.

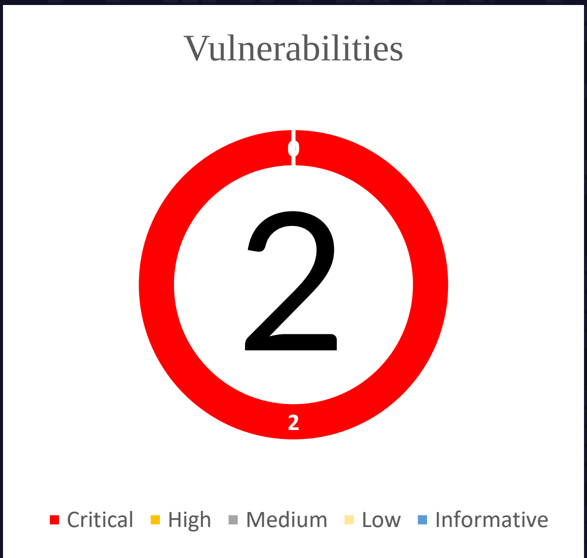
• Conclusions

Our professional team perspective, is that the overall security level of the system for a smart 24/7 connected city based on wireless device communication and flawless connectivity is **Low**.

The smart city was found to be deficient in enforcing security measures which are rudimentary for a smart 24/7 online city, a simple SDR device was the only tool needed to circumvent the camera security or taking control over the local vehicles, the main exploitations vectors are as follows:

- Jamming a Security Camera
- Taking control over a vehicle

The exploitation of these vulnerabilities requires **low to zero** technical knowledge



Finding Details

VULN-001 Jamming a security camera – SDR device frequency jam (**Critical**)

Description

Jamming a security camera describes the ability of non-authorized elements to use an SDR (Software Defined Radio) device in order to analyse the frequency the security camera uses and then process to jam it, rendering the camera inoperable for a while.

This vulnerability can be exploited by non-authorized elements to pass through the city grounds undetected or be able to enter sensitive supposed to be monitored areas, unsupervised.

Details

During the audit of the smart city devices and security implementations, our tester discovered that an SDR device can be used to bypass the security cameras deployed in the city.

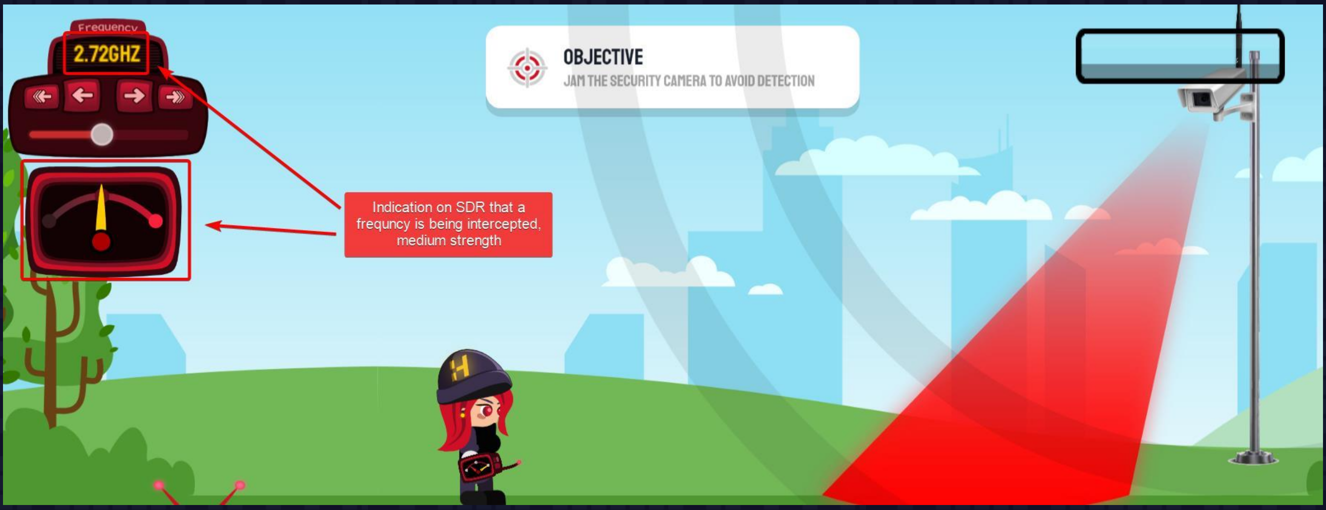
The enabler of this bypass is the SDR device - a simple electronic device, much like a remote control, easy to operate and requires no tech knowledge. The SDR has a few buttons through which the user can identify the frequency a device uses and then use the SDR to jam the identified frequency, rendering the security camera inoperable, in this case the jamming lasts ~7 seconds.

An attacker or non-authorized element can exploit this signal jamming capability to render any security camera inoperable and go through any checkpoint undetected or gain entry to any sensitive or restricted areas.

Evidence

This vulnerability was identified during our tester city tour, using the SDR device, the tester has identified a signal from the security camera, and was able to carry out the attack by standing in the vicinity of the security camera.

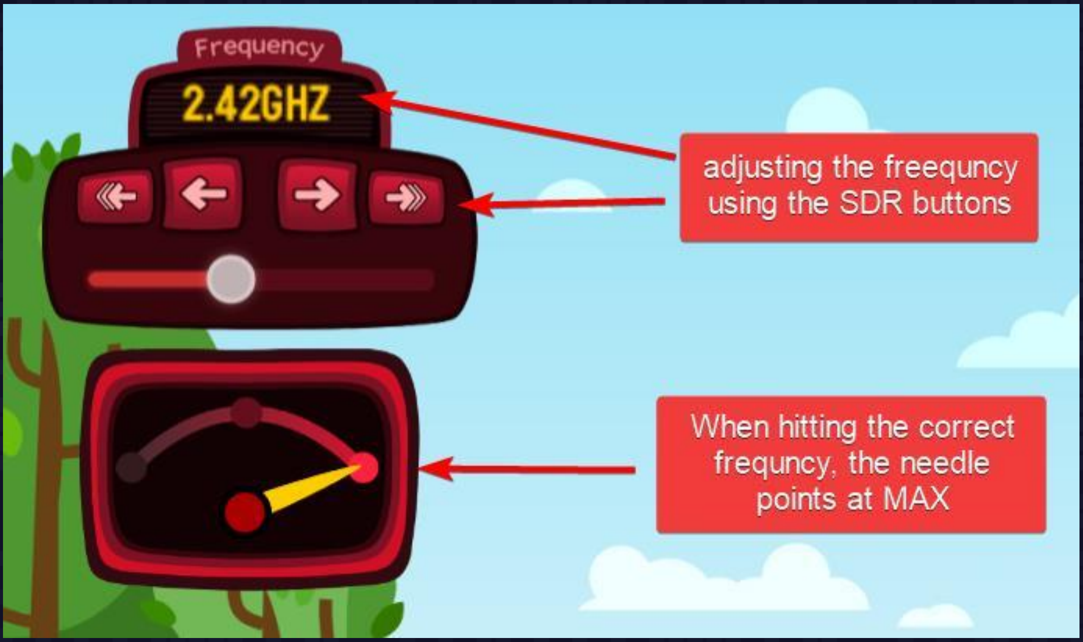
During our tester patrol through the city, he has positioned himself near the security camera and was able to sense the camera frequency, the SDR device defaults to 2.72 GHZ and the indicator came to life showing a signal is identified but not at full strength



Indication on SDR that a frequncy is being intercepted, medium strength

Figure 1: the SDR device indicates it identified a frequency

Amall adjustment were made to match the frequency of 2.42, the device indicates it has hit the specific frequency indicated by the needle hitting “max” range

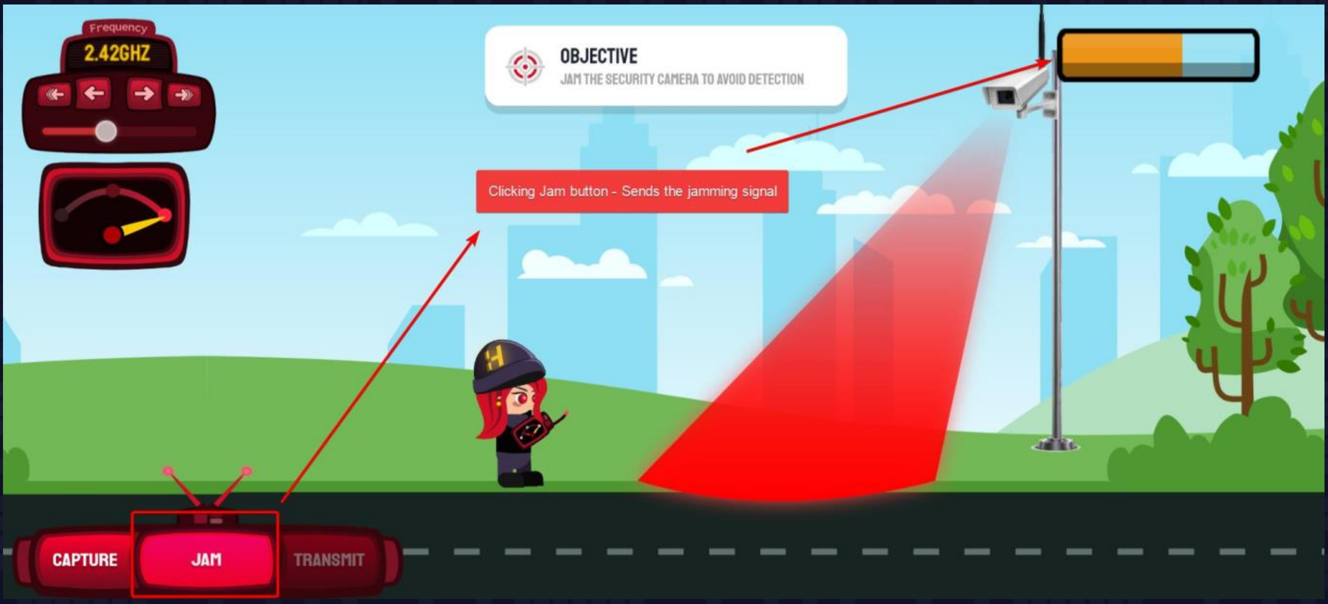


adjusting the freequncy using the SDR buttons

When hitting the correct frequncy, the needle points at MAX

Figure 2: the SDR device has been adjusted to the matching frequency, needle is at full strength

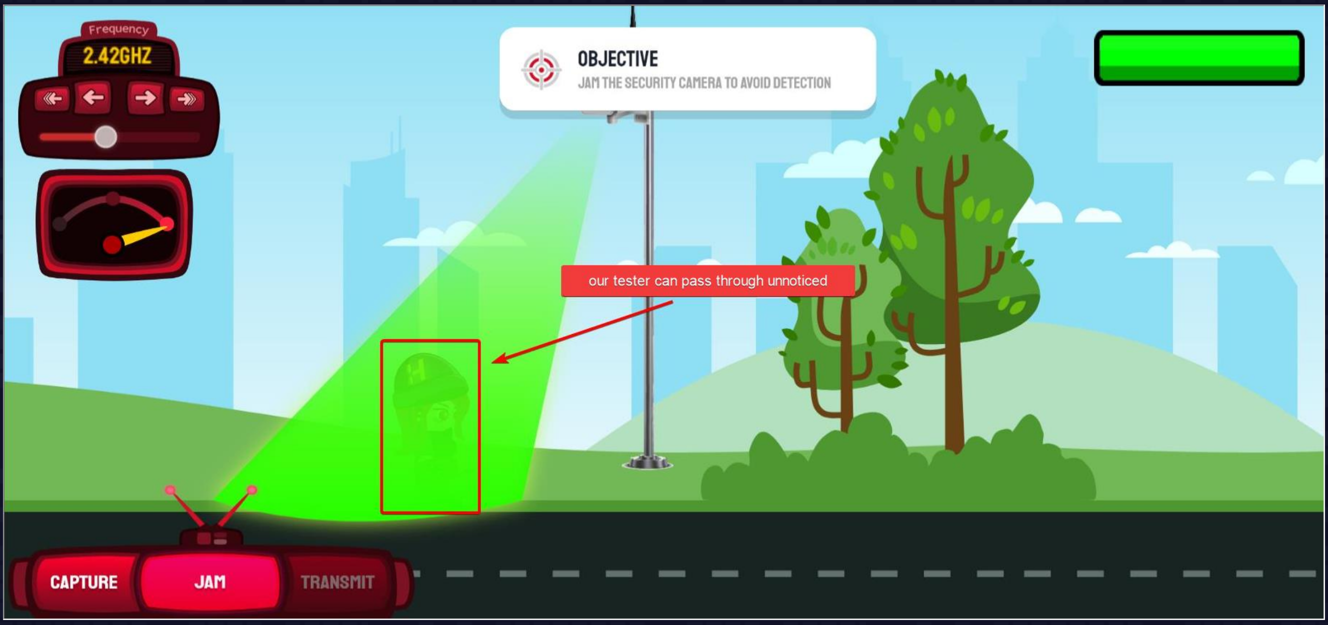
Once the frequency is locked in, the tester clicks the “jam” button and the jamming signal is broadcasted



Clicking Jam button - Sends the jamming signal

FIGURE 3: THE JAMMING SIGNAL IS BEING BROADCASTED

Camera is jammed, our tester can pass unnoticed and without any authorization limitations



our tester can pass through unnoticed

FIGURE 4: TESTER PASSES THROUGH THE SECURITY CAMERA, CAMERA IS JAMMED

Remediation Options

- Anti Jamming Algorithms - It is recommended to use cameras which employ Anti-Jamming algorithms and technology aimed to detect and mitigate jamming attempts.
- Frequency Hopping Spread Spectrum (FHSS) - In the same sense it is recommended to use Frequency Hopping Spread Spectrum (FHSS), allowing the cameras and receivers to change frequencies often, based on a pattern known to both and make it difficult for SDR devices to jam them.
- Supplementary wired connections – it is recommended to add wired connections as backup to the camera feed in case of signal disruption (where possible).
- Directional Antennas – It is recommended to use directional antennas as these can focus the transmission in a specific direction, reducing the likelihood of interference from jamming devices.
- Jamming Detection Systems – it is recommended to incorporate jamming detection systems which will be able to alert the security personal in real time if any jamming attempts are in progress.

VULN-002 Taking control over a vehicle – SDR relay attack (Critical)

Description

SDR relay attack describes the ability of non-authorized elements to use an SDR (Software Defined Radio) device in order to analyse the signal of the car remote control, capture it into the SDR device and then send the same signal to the vehicle, allowing full access to the vehicle.

This vulnerability can be exploited by non-authorized elements to gain control of any vehicle which uses this technology, this can lead to property theft be it personal belongings from within the vehicle or even theft of the vehicle itself.

Details

During the audit of the smart city devices and security implementations, our tester discovered that an SDR device can use it's "relay attack" to hack into Vehicles – A relay attack is where the device captures, saves and sends that same saved signal back to the target device to gain access or control over it, in this case, gaining access to the city vehicles.

The enabler of this bypass is the SDR device - a simple electronic device, much like a remote control, easy to operate and requires no tech knowledge. The SDR has a few buttons through which the user can identify the frequency a device uses and then use the SDR to capture that frequency, save it into the SDR device, and then send that same signal, opening the vehicle doors and giving full access to the vehicle.

An attacker or non-authorized element can exploit this signal relay capability to gain unauthorized access to any vehicle and be in position to exploit the vehicle or its contents however the attacker pleases.

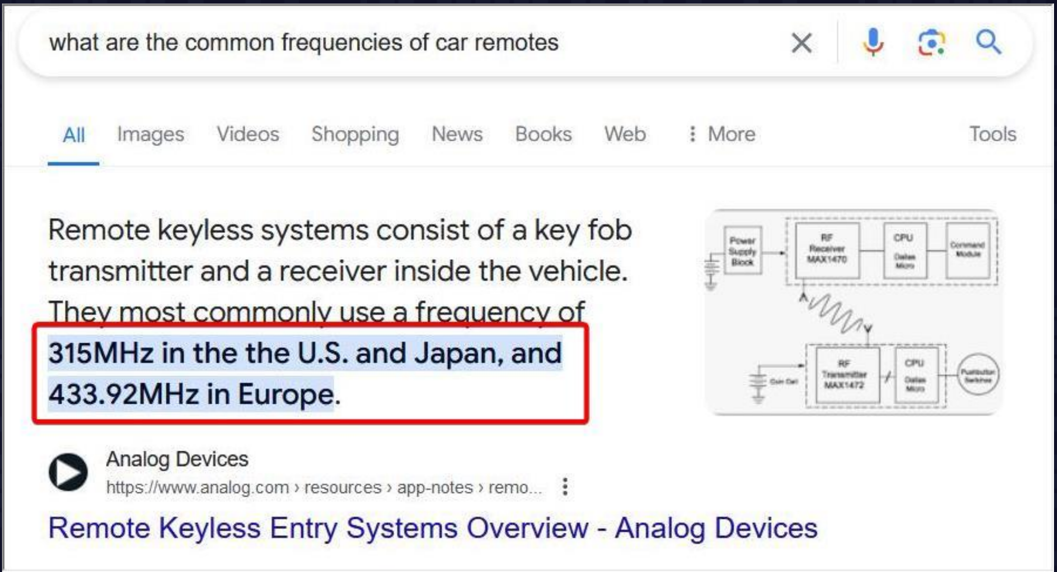
Note

Due to the sensitive nature of such a test, at no time did our tester access the interior of the vehicle. We just verified the relay attack allowed access to the vehicle as if the tester is in the possession of the remote control.

Evidence

This vulnerability was identified during our tester city tour, he positioned himself near a city vehicle, checked online for common frequencies to be tested and had set the SDR to frequency of 433 MHZ. Once the user interaction with the vehicle has started, the signal was verified to fit the 433 MHZ range and saved on the SDR. When the user left, our tester proceeded to send the saved signal through the SDR device resulting in gaining access to the Vehicle.

During our tester patrol through the city, he has positioned himself near one of the city's vehicles and ran a search online for commonly used frequencies that car remote controls use.



what are the common frequencies of car remotes

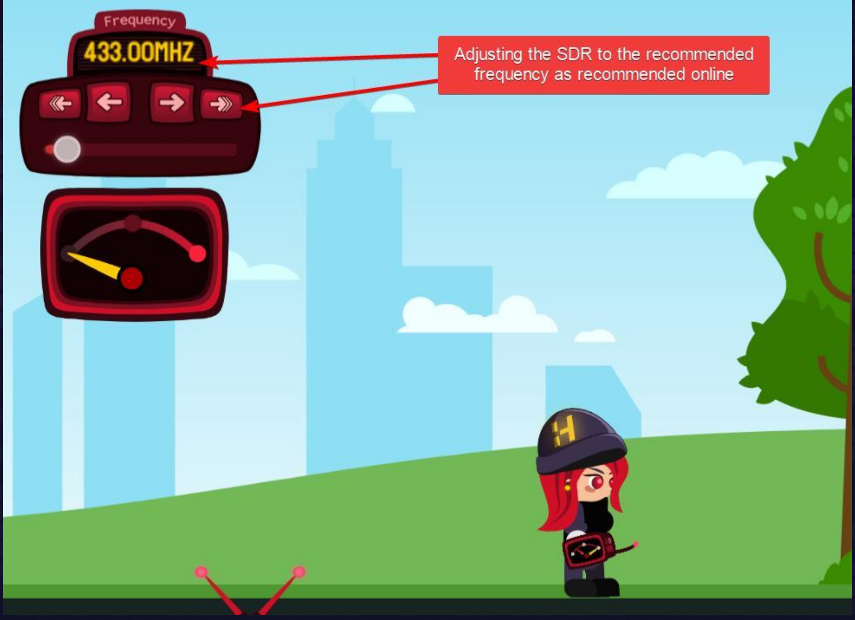
Remote keyless systems consist of a key fob transmitter and a receiver inside the vehicle. They most commonly use a frequency of 315MHz in the the U.S. and Japan, and 433.92MHz in Europe.

Analog Devices
https://www.analog.com › resources › app-notes › remo...

Remote Keyless Entry Systems Overview - Analog Devices

FIGURE 5: FREQUENCIES ARE EASILY SEARCHABLE ON THE WORLD WIDE WEB

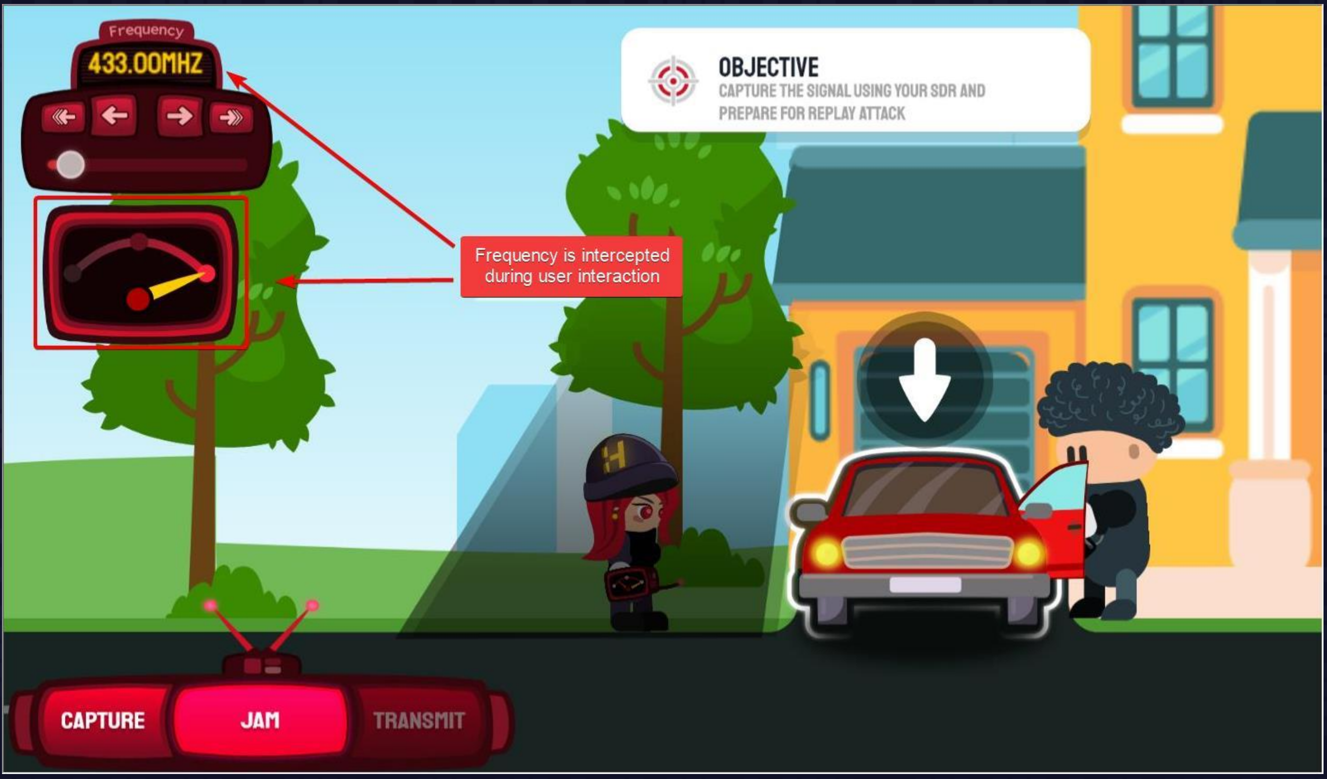
Using the SDR buttons our tester has adjusted the SDR device to the frequency of 433 MHZ as suggested online.



Adjusting the SDR to the recommended frequency as recommended online

FIGURE 6: THE SDR DEVICE HAS BEEN CONFIGURED TO BE SET ON 433 MHZ FREQUENCY AS SUGGESTED ONLINE

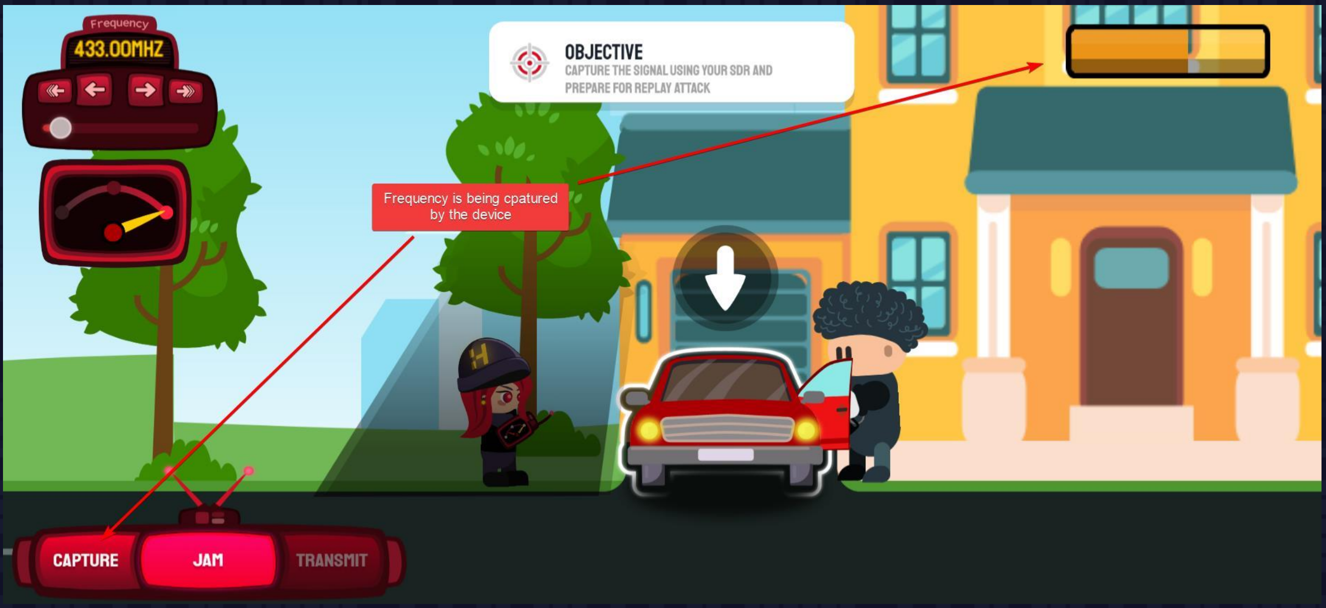
As the user arrives and interacts with the vehicle using the remote, the SDR indicates we have the right frequency, signal strength is optimal, 433 MHZ is indeed the correct frequency


Frequency
433.00MHZ
OBJECTIVE
CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK
CAPTURE
JAM
TRANSMIT

Frequency is intercepted during user interaction

FIGURE 7: USER INTERACTS WITH THE VEHICLE AND SDR IS AT MAX SIGNAL STRENGTH

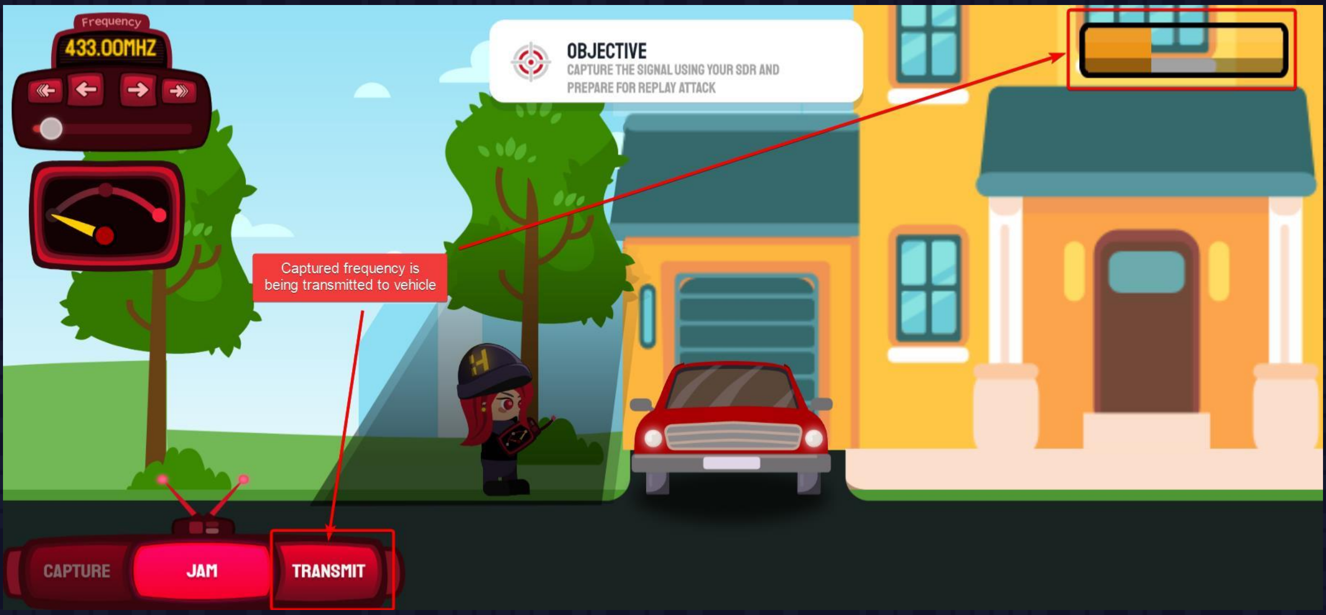
Clicking the capture button, we can save the remote controller signal for use in the next step, the “relay attack”


Frequency
433.00MHZ
OBJECTIVE
CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK
CAPTURE
JAM
TRANSMIT

Frequency is being cpatured by the device

FIGURE 8: THE SDR DEVICE IS CAPTURING AND SAVING THE REMOTE CONTROLLER SIGNAL

Now that the user has left, we can proceed to carry the "relay attack", clicking on transmit the SDR sends the saved signal to the vehicle

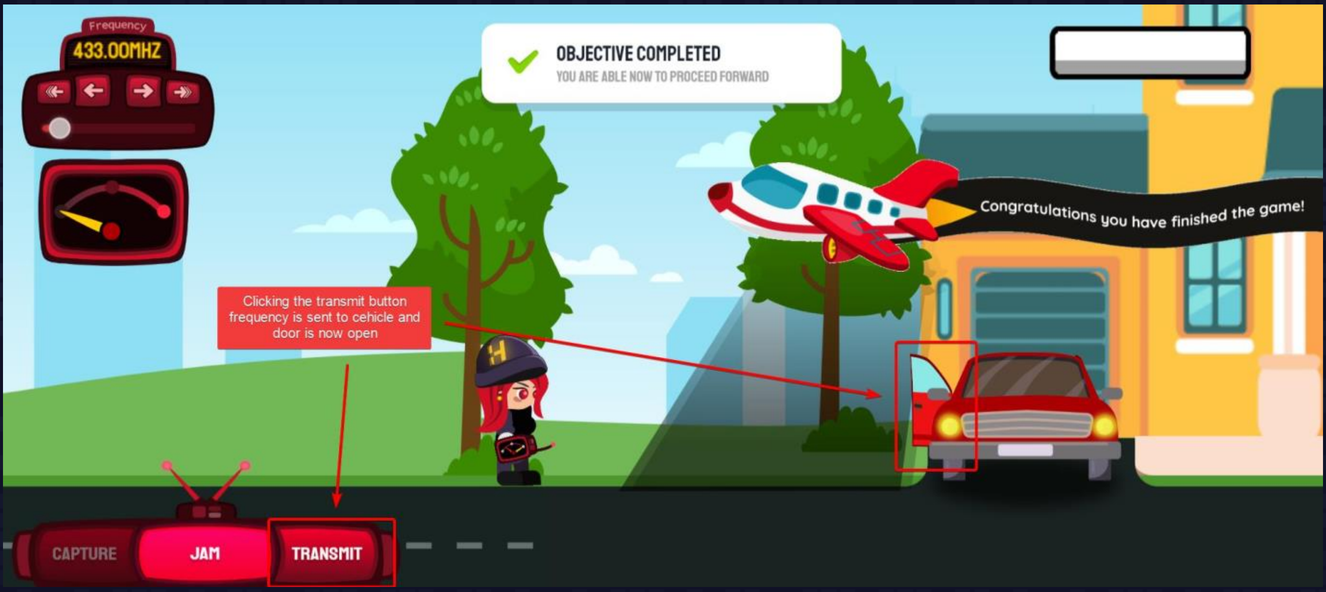


OBJECTIVE
CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

Captured frequency is being transmitted to vehicle

FIGURE 9: THE SAVED REMOTE CONTROLLER SIGNAL IS BEING BROADCASTED

Vehicle door opens and we now have full control over it



OBJECTIVE COMPLETED
YOU ARE ABLE NOW TO PROCEED FORWARD

Congratulations you have finished the game!

Clicking the transmit button frequency is sent to cehicle and door is now open

FIGURE 10: THE VEHICLE DOOR IS OPEN, TESTER GAINED FULL ACCESS TO IT

Remediation Options

- Frequency Hopping Spread Spectrum – It is recommended to Integrate FHSS technology in remote controller and vehicles. FHSS allows for rapid changes in frequencies during communication, making it difficult for attackers to capture and relay the signal effectively.
- Two-Factor Authentication (2FA) – It is recommended to Implement two-factor authentication for secure vehicle access. For instance, after the remote control is detected or used, the user might need to enter a PIN or use a biometric method like a fingerprint or face recognition to unlock and start the vehicle.
- Advanced Encryption Protocols – It is recommended that encryption would be employed on any communication between the vehicle and the remote. Strong encryption makes it more challenging for attackers to intercept and relay signals successfully.