PT REPORT

CySDR

EXECUTIVE SUMMARY

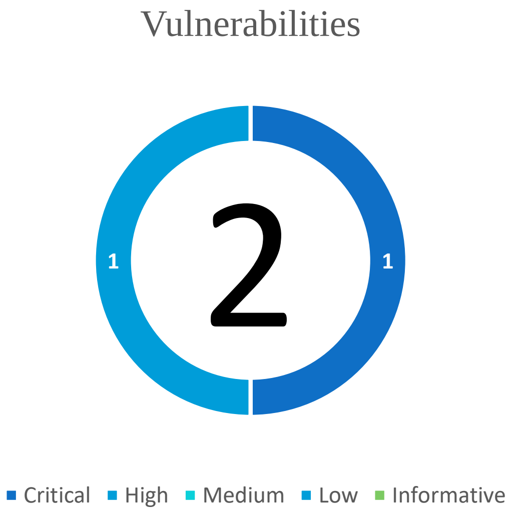
In our security assessment, we discovered two key wireless vulnerabilities in the smart devices. First, we were able to jam a Wi-Fi camera by disrupting its signal at 2.42 GHz, using Software Defined Radio (SDR) technology and proving how easily its feed could be compromised. The second vulnerability involved intercepting and replicating key fob signals for keyless car entry. We intercepted and mimicked the signal of a car key fob between 433-434 MHz frequencies, demonstrating a method to unlock and potentially start the car without physical access to the key. These findings underscore the urgent need for stronger security in wireless communications to protect against potential breaches in smart-city environments.

CONCLUSIONS

Our analysis leads us to conclude that the current state of security for the examined wireless systems is inadequate, with an overall assessment of 'Low'. The vulnerabilities found were:

- Unauthorized Wi-Fi Service Interruption via Signal Jamming Vulnerability
- Key Fob Relay Attack Vulnerability

Both vulnerabilities could be exploited with relatively basic technical knowledge, highlighting the need for immediate security improvements to mitigate the risk of disruption and unauthorized access to essential city services and private vehicles.



CONCLUSIONS

VULN-001 Unauthorized Wi-Fi Service Interruption via Signal Jamming (CRITICAL)

Description

This vulnerability is exploited by interrupting a Wi-Fi network's operations using a signal-jamming technique at the 2.42 GHz frequency range. Performed with readily accessible SDR tools, this attack can create a Denial-of-Service (DoS) condition, severely impacting smart-city services dependent on wireless communications. The criticality of this vulnerability lies in its capacity to cause significant disruptions with relatively low technical effort, posing a serious security threat to public and private sectors reliant on Wi-Fi connectivity.

Details

The investigation revealed a critical vulnerability in the wireless network’s ability to resist unauthorized interference. An attacker, with just a basic understanding of Software Defined Radio (SDR) technology, could disrupt Wi-Fi connectivity by transmitting at the network's operational frequency, 2.42 GHz. This was achieved by directly targeting the frequency used by the Wi-Fi cameras, causing a Denial-of-Service (DoS) situation where the camera's signals were effectively drowned out by the interference. This method bypasses the need for network authentication, rendering the Wi-Fi camera inoperative and blind to legitimate users. If exploited, this could allow for unmonitored activities within its field of view and compromise the safety and security of the environment under surveillance.

Note

During the security assessment, we adhered to the guidelines provided and did not permanently disable any Wi-Fi cameras. This vulnerability has been classified as Critical due to its potential to indiscriminately disrupt wireless services, which could lead to broader security breaches within the smart-city network. The impact of such a vulnerability is far-reaching, as it could compromise any dependent system utilizing Wi-Fi, from public surveillance to essential urban services. A successful attack could result in significant downtime and undermine public trust in the reliability and security of smart-city infrastructures.

PT REPORT

To discover this vulnerability, we need to stand as closest as we can without being detected by The Security Camera.

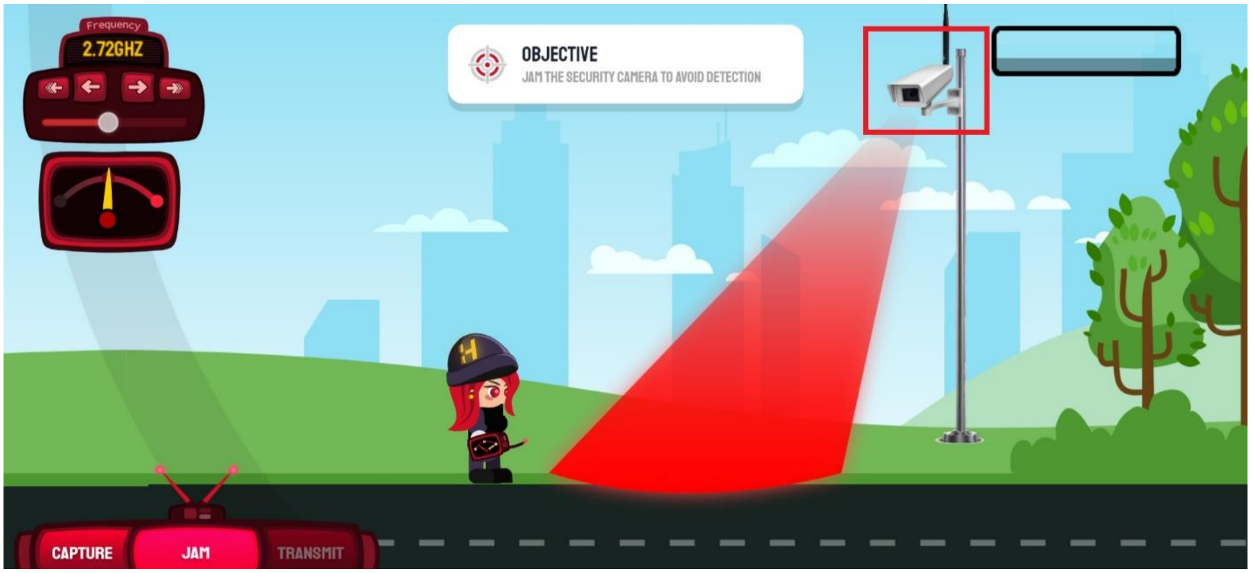


FIGURE 1: CAMERA IS ACTIVE AT THIS MOMENT.

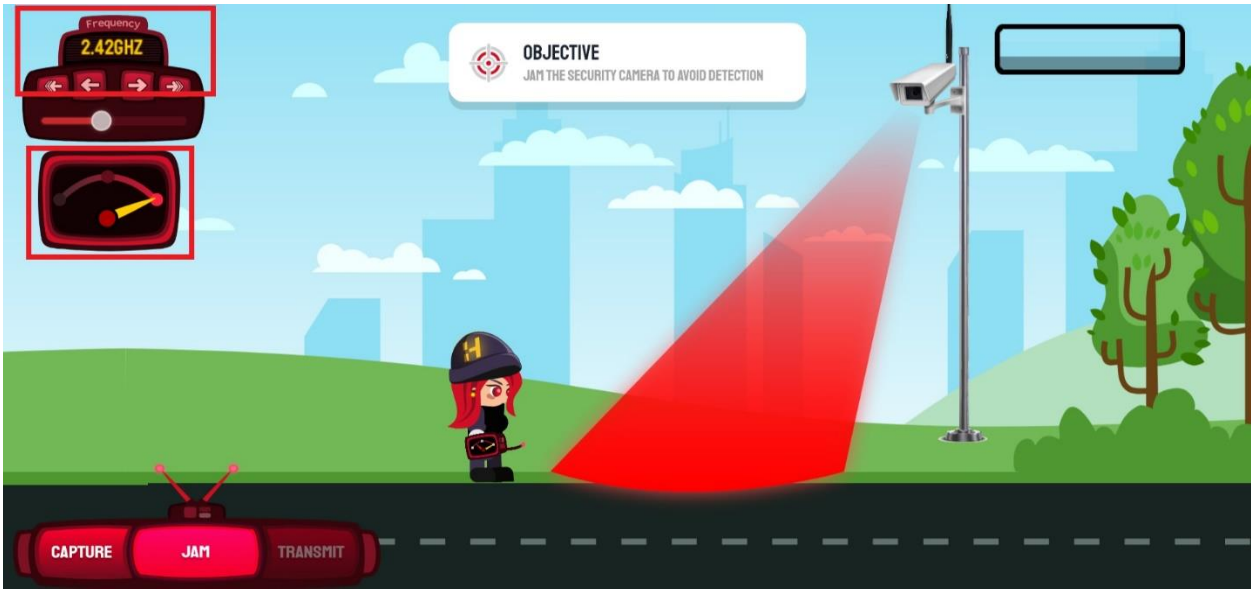


FIGURE 2: STEP 1 SETTING THE SDR TO THE CORRECT FREQUENCY OF 2.42GHZ

PT REPORT

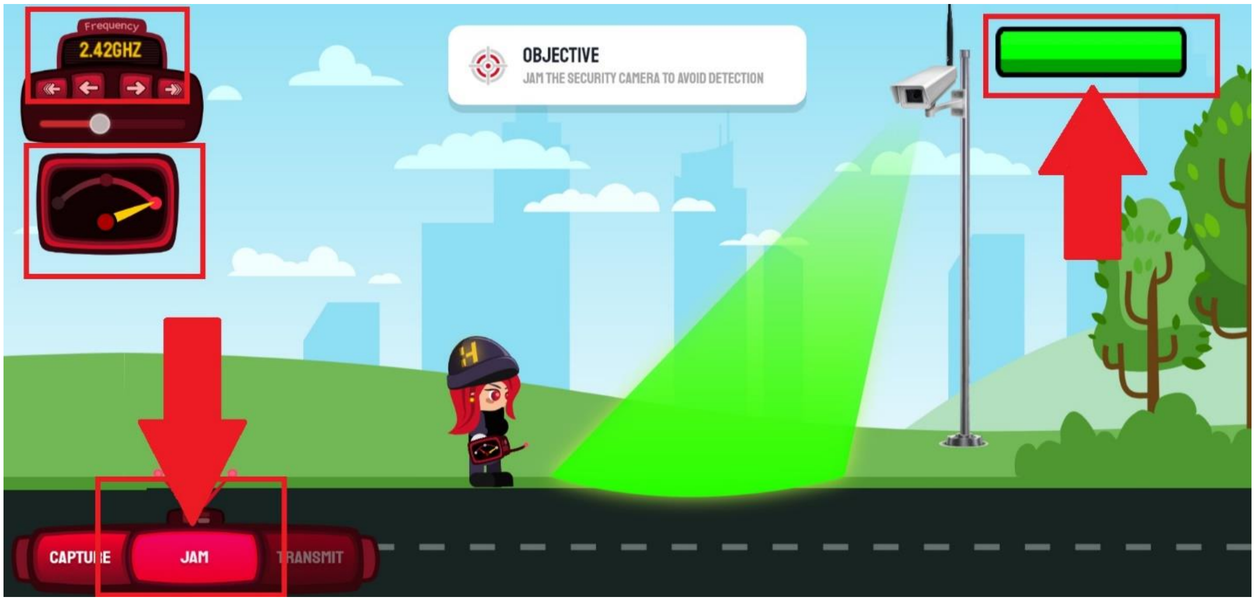


FIGURE 3: STEP 2 JAMMING THE SECURITY CAMERA WITH THE RIGHT FREQUENCY

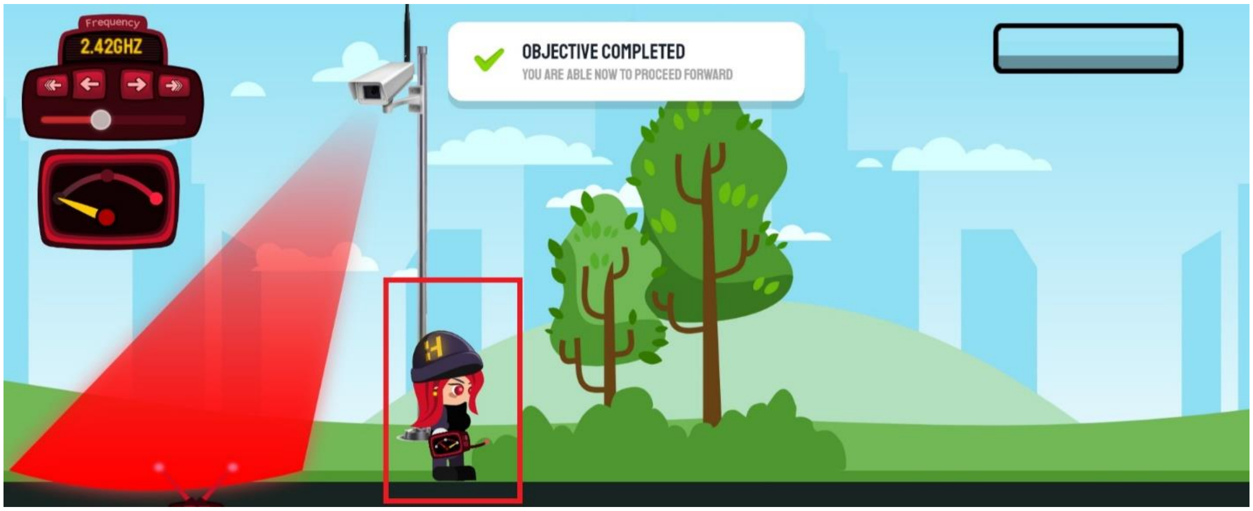


FIGURE 4: MANAGED TO GO THROUGH UNDETECTED.

Remediation Options

- Establish a wireless intrusion prevention system (WIPS) that actively monitors the airspace for unauthorized devices and signals, providing real-time alerts and automatic countermeasures against potential jamming attempts.

- Implement robust frequency hopping or spread spectrum techniques to minimize the risk of RF jamming interference. These methods make it more difficult for an attacker to disrupt the signal as they would need to jam a broader range of frequencies.

- Conduct regular security audits to monitor for signs of RF jamming and establish protocols for rapid response and mitigation in the event of an attack to reduce downtime.

- Train staff in the recognition of and response to cyber incidents, including RF interference, and conduct regular simulations to ensure preparedness for real-world attack scenarios.

CONCLUSIONS

VULN-002 Key Fob Relay Attack Vulnerability (HIGH)

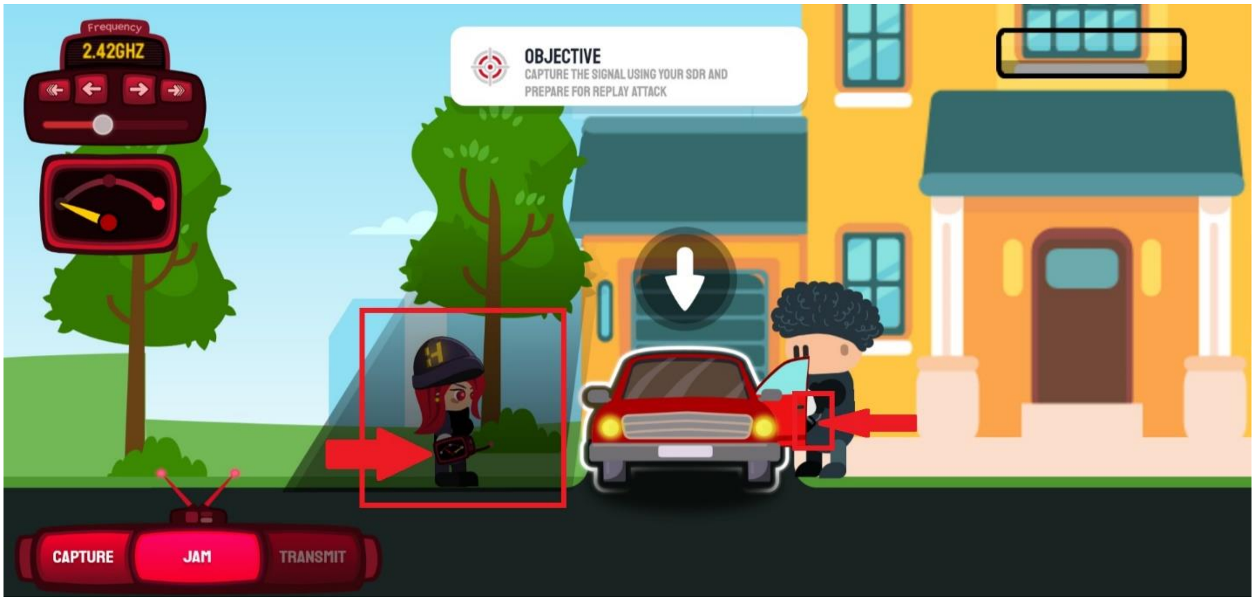
Description

The Key Fob Relay Attack vulnerability pertains to the exploitation of the keyless entry system of vehicles. Attackers can amplify or relay the signal from a car's key fob to unlock and start the vehicle without physical possession of the key. This breach is possible due to the lack of sufficient encryption and authentication between the key fob and the vehicle's electronic control unit. The vulnerability is exacerbated by the key fobs continuously broadcasting signals that can be captured by unauthorized devices, making vehicles susceptible to theft and unauthorized use.

Details

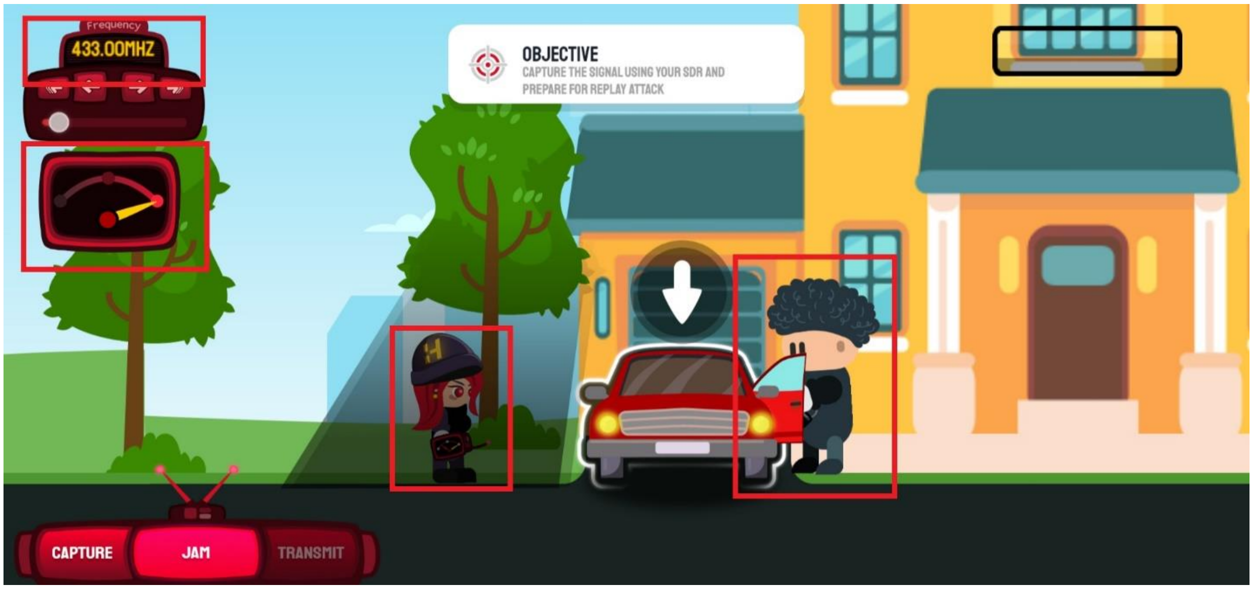
In our testing, it was observed that the signal between the vehicle's key fob and its corresponding receiver lacks robust encryption, making it vulnerable to relay attacks. By utilizing a signal amplification device, an attacker can extend the range of the key fob's signal, allowing them to unlock and start the car from a distance, bypassing any need for direct contact with the key fob. This vulnerability is critical as it allows for unauthorized access to the vehicle without triggering traditional alarms or needing to overcome physical barriers.

PT REPORT



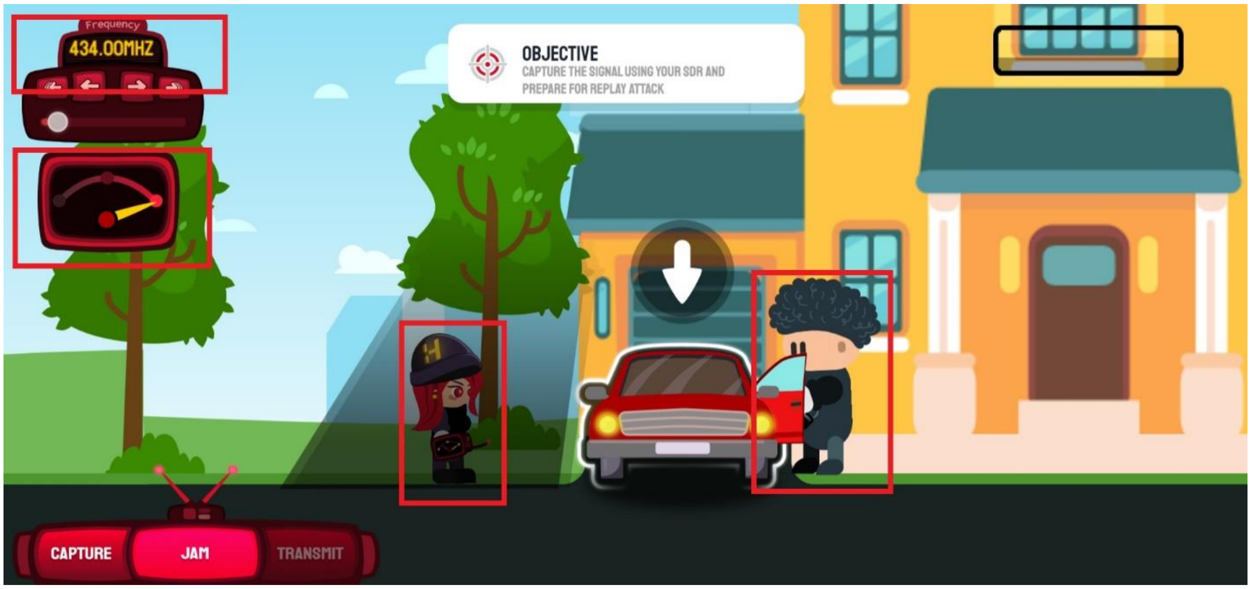
OBJECTIVE
CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

FIGURE 1: FOR OPTIMAL CAPTURE OF THE VEHICLE'S KEY SIGNAL ACTIVATION, IT IS RECOMMENDED TO SECURE A PROXIMATE AND CONCEALED POSITION.



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

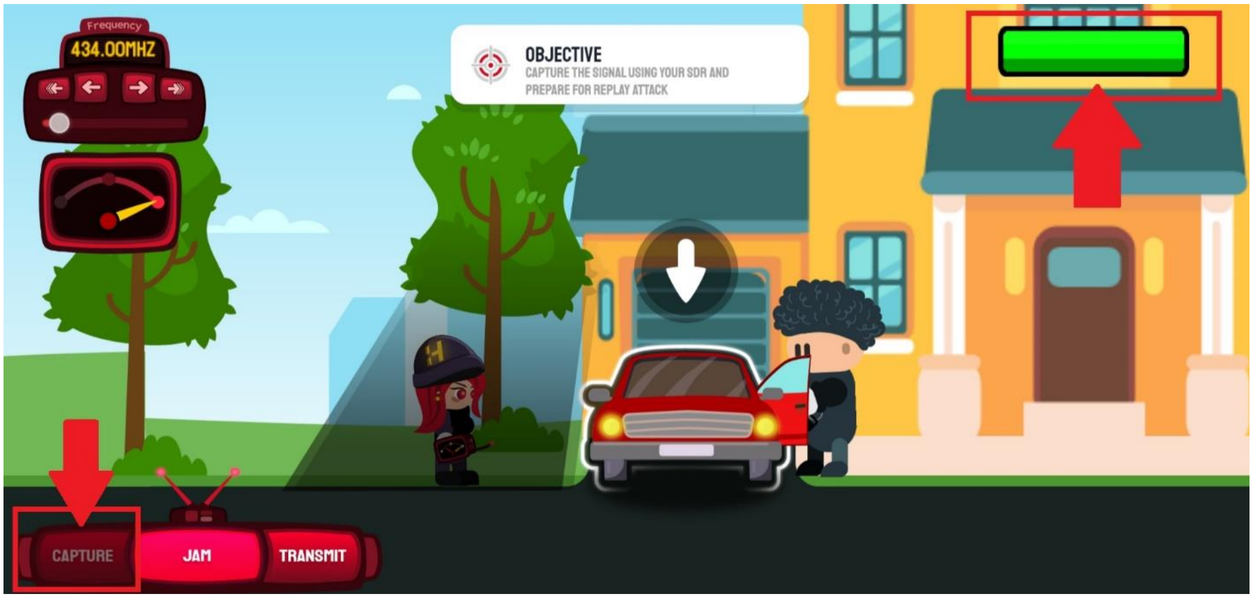
FIGURE 2: SUCCESSFULLY INTERCEPTED A SIGNAL AT 433MHZ.



OBJECTIVE

CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

FIGURE 3: ADDITIONALLY, MAINTAINED POSSESSION OF A SIGNAL AT 434MHZ AS WELL.

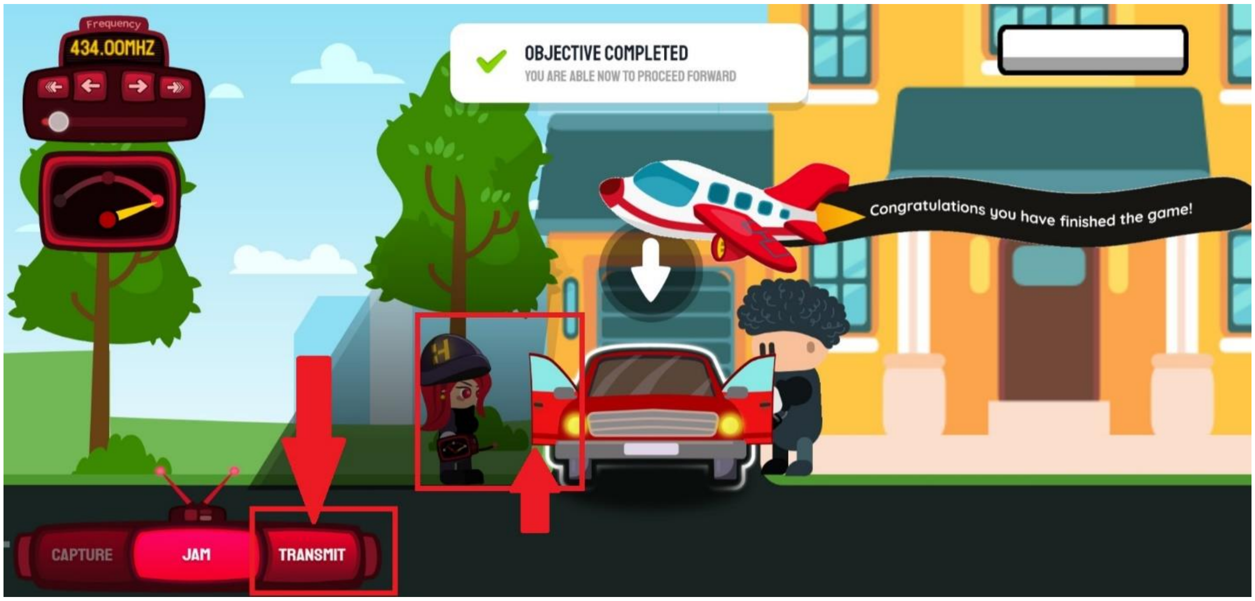


OBJECTIVE

CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

FIGURE 4: SIGNAL SUCCESSFULLY INTERCEPTED!

PT REPORT

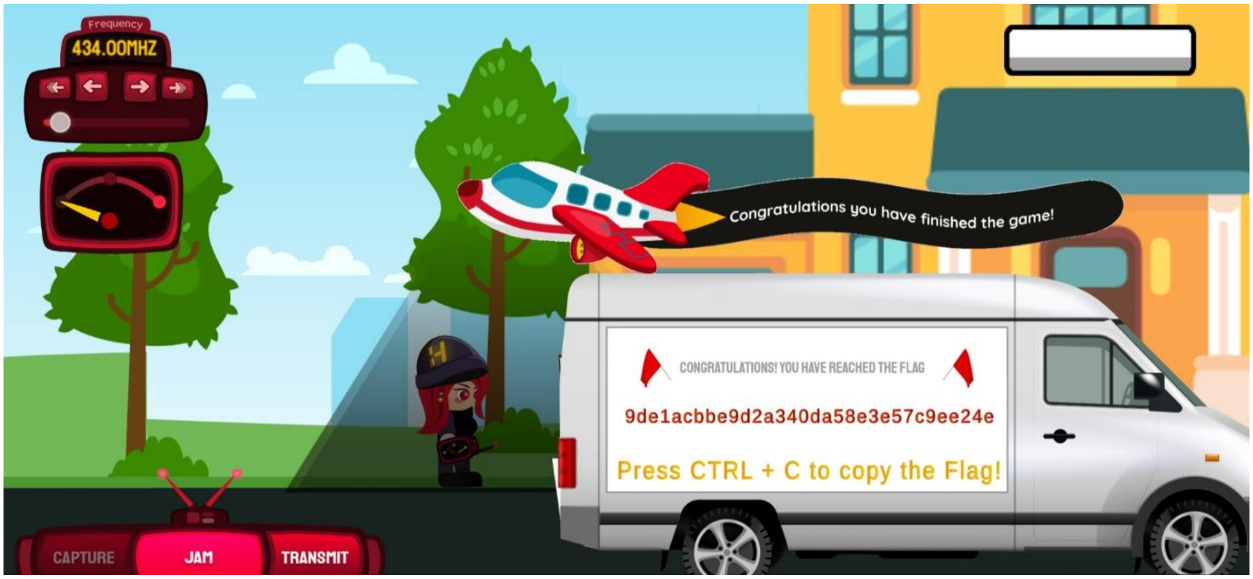


OBJECTIVE COMPLETED

YOU ARE ABLE NOW TO PROCEED FORWARD

Congratulations you have finished the game!

FIGURE 5: SUBSEQUENTLY, TRANSMISSION RESULTED IN THE VEHICLE'S DOOR UNLOCKING WITH EASE.



Congratulations you have finished the game!

CONGRATULATIONS! YOU HAVE REACHED THE FLAG

9de1acbbe9d2a340da58e3e57c9ee24e

Press CTRL + C to copy the Flag!

FIGURE 5: SUCCESSFULLY COMPLETED THE SIMULATION.

PT REPORT

Remediation Options

- Parking area: It is important to secure the parking areas in the city, make sure they are well lit, the view is clear and there are no hiding spots and there are security cameras surrounding the area

- Educate Owners on Key Fob Security: Provide vehicle owners with information on how to secure their key fobs, such as using Faraday pouches to block signals when not in use and the importance of disabling keyless entry features when they are not necessary.

- Update the Vehicle's Software: Regularly updating the software of a car, just like you would with your smartphone or computer, is essential to protect against potential vulnerabilities.

GOOD LUCK!