PT Report

“CySDR"

Executive Summary

Summary

During the test, I was able to exploit frequency vulnerabilities in a simulated environment. By identifying the frequencies associated with an IP camera and a car, I managed to bypass the camera’s security and gain access to the car. This test highlights risks associated with wireless frequencies in IoT environments, emphasizing the need for secure signal management.

Conclusions

From my professional perspective, the overall security level of the system remains **Low**, as the identified vulnerabilities could be exploited with minimal technical knowledge.

The main exploitation vectors were based on the following:

- **Unsecured Frequency Control**: Vulnerability in camera and car frequencies.
- **Lack of Signal Encryption:** Susceptibility to jamming or spoofing attacks.
- Both of them are critical depends on the content

Finding Details

VULN-001: RF Signal Jamming – IP Camera Bypass (Critical)

Description

RF Signal Jamming is a technique used to disrupt the communication signals of wireless devices, making them inoperable by overwhelming them with noise or interference at their operating frequency. Many wireless systems, such as IP cameras and other IoT devices, operate on common, unencrypted frequencies, making them susceptible to signal jamming if proper safeguards like encryption or frequency hopping are not implemented.

Details

In the game scenario, the IP camera operated on a fixed, unencrypted frequency of 2.42 GHz, which made it vulnerable to RF Signal Jamming. I exploited this vulnerability through the following steps:

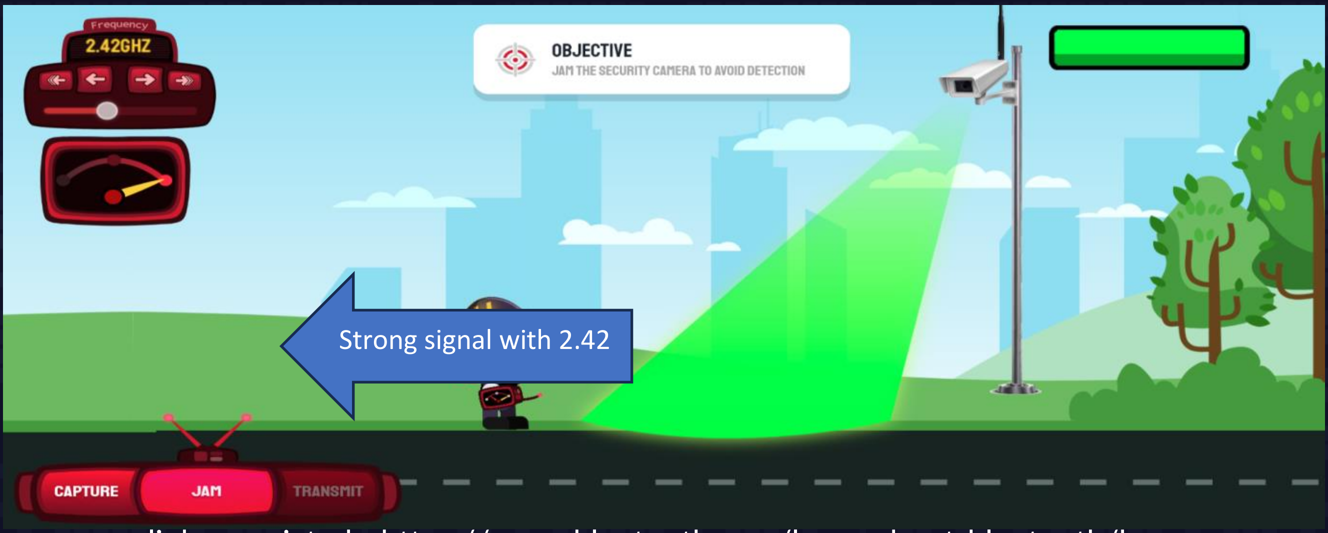
1. **Frequency Identification:** Through online research, I discovered that many IP cameras commonly use the 2.4 GHz range for communication. I tested this in the game and confirmed the camera was operating at 2.42 GHz.
2. **Exploitation Process:**
   - As I navigated toward the camera's location, I switched my frequency to 2.42 GHz.
   - I activated a "jam" function, which disrupted the camera's ability to detect me.
   - By jamming the camera's signal, I successfully passed its line of sight undetected.

This demonstrates the risks associated with using publicly known frequencies without encryption or interference protection.

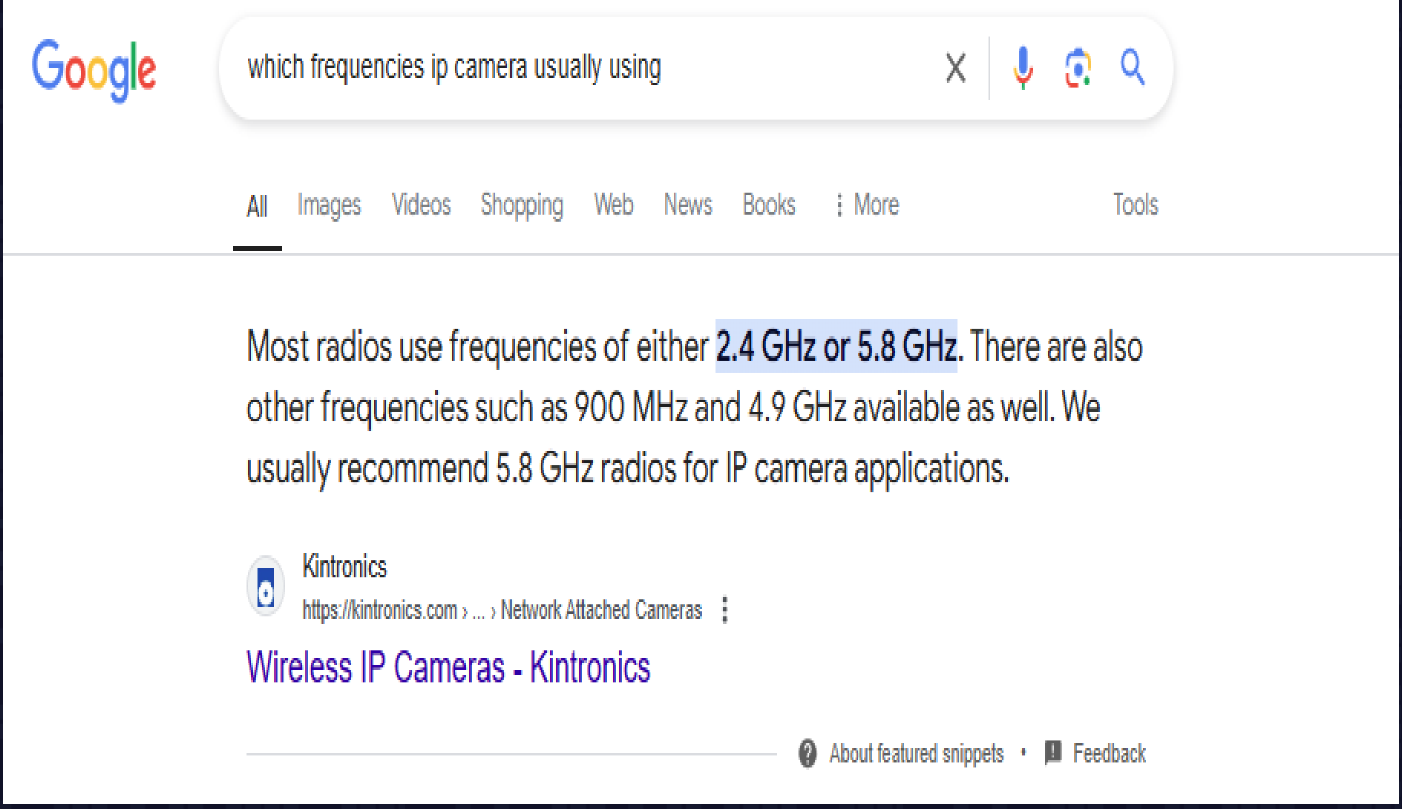
Evidence

Screenshots taken during the game show the camera bypass in action, with the frequency adjustment and jamming method clearly depicted.

This is the moment I managed to jam with the 2.42 GHz frequency.



link associated - https://www.bluetooth.com/learn-about-bluetooth/key-attributes/range/#:~:text=Bluetooth%C2%AE%20technology%20uses%20the,balance%20between%20range%20and%20throughput.



which frequencies ip camera usually using

Most radios use frequencies of either 2.4 GHz or 5.8 GHz. There are also other frequencies such as 900 MHz and 4.9 GHz available as well. We usually recommend 5.8 GHz radios for IP camera applications.

Kintronics
https://kintronics.com › ... › Network Attached Cameras

Wireless IP Cameras - Kintronics

Screenshot of the frequency search online

Impact

Unsecured camera frequencies allow attackers to disrupt or jam surveillance systems. In real-world scenarios, this could enable unauthorized access to restricted areas by disabling or bypassing monitoring systems.

Remediation

To mitigate RF signal jamming vulnerabilities, we recommend the following:

1. Frequency Obfuscation and Hopping: Implement frequency-hopping spread spectrum (FHSS) technology to make it difficult to jam or predict the frequency.
2. Encryption of RF Signals: Use encryption for signal transmissions to prevent unauthorized jamming or interference.
3. Jamming Detection and Alerts: Install sensors that detect jamming attempts, triggering alerts if interference is detected.

• Finding Details

VULN-002: Key Fob Replay Attack(Car) – Unauthorized Vehicle Access (High)

Description

Replay Attacks exploit unencrypted wireless signals used by access control devices. In these attacks, intercepted signals are retransmitted, allowing unauthorized access if the system lacks secure mechanisms like rolling codes or encryption to prevent signal reuse.

Details

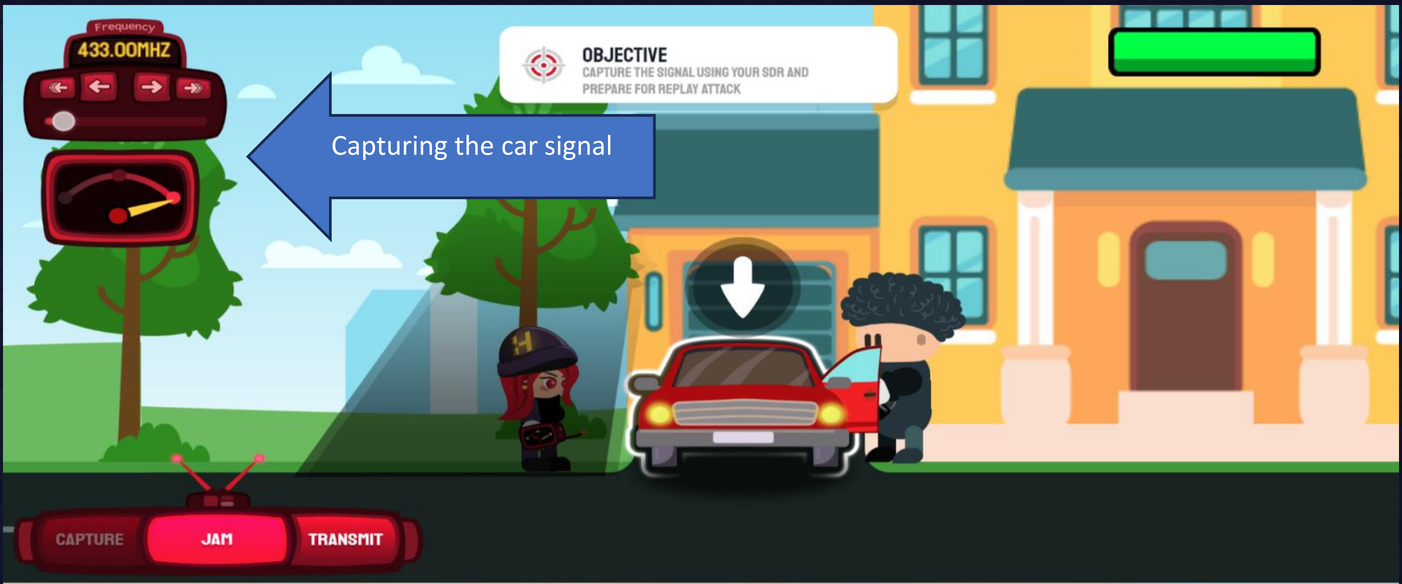
In this scenario, the car operated on a 433 MHz frequency for access control, rendering it vulnerable to replay attacks. The following steps were executed to exploit this vulnerability:

1. **Frequency Identification:** Research revealed that 433 MHz is commonly used for car key fob access and remote control signals.
2. **Exploitation Process:**
   - After bypassing the IP camera, I encountered a car blocking the next path.
   - The device was set to the 433 MHz frequency, where I waited for the car owner to approach.
   - Upon the owner using their key fob to unlock the car, I captured the unencrypted signal.
   - I then replayed the captured signal to gain unauthorized access to the car and proceed through the game.

The use of an unencrypted signal enabled me to intercept and reuse the frequency transmission, bypassing the car's security mechanisms.

Evidence

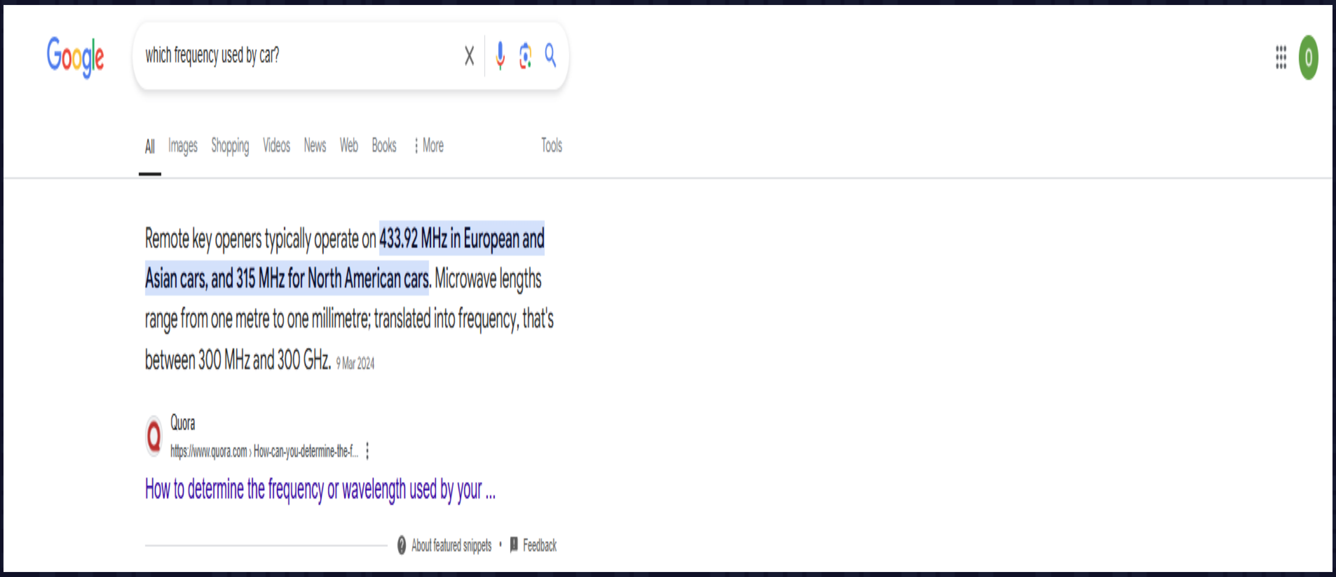
Screenshots from the game show successful access to the vehicle using the captured 433 MHz signal and the flag obtained after pressing "transmit."



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

Link to the source that shows the relevant frequency - https://www.quora.com/How-can-you-determine-the-frequency-or-wavelength-used-by-your-cars-key-fob-and-other-electronic-devices-without-specifications#:~:text=Remote%20key%20openers%20typically%20operate,300%20MHz%20and%20300%20GHz.

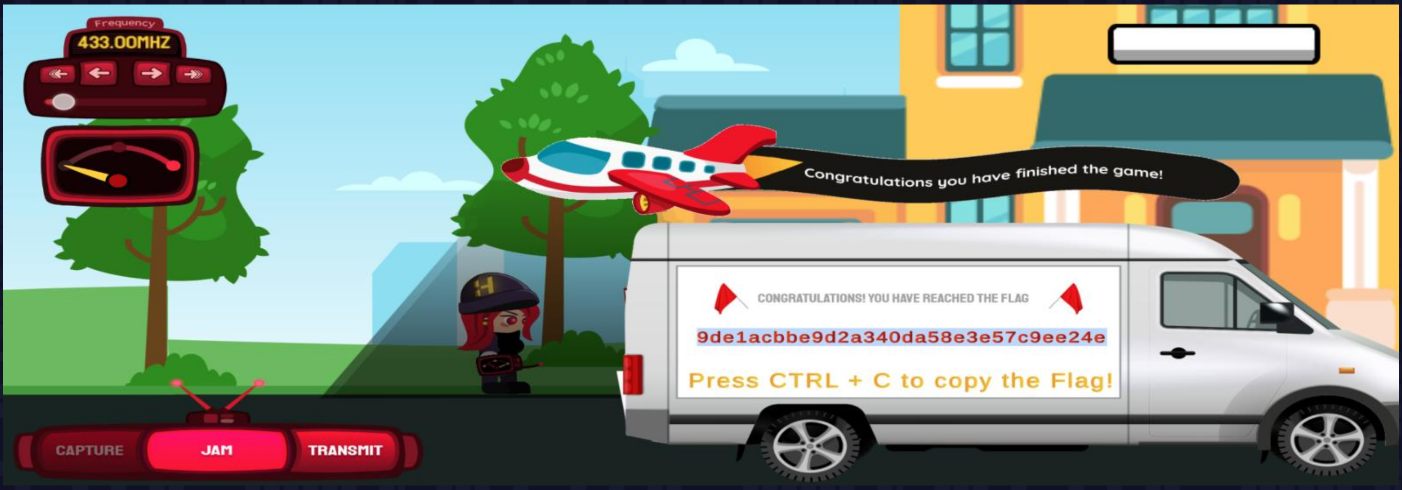
Screen shot of the source I looked over the net



Remote key openers typically operate on 433.92 MHz in European and Asian cars, and 315 MHz for North American cars. Microwave lengths range from one metre to one millimetre; translated into frequency, that's between 300 MHz and 300 GHz. 9 Mar 2024

Quora
https://www.quora.com › How-can-you-determine-the-f...

How to determine the frequency or wavelength used by your ...



CONGRATULATIONS! YOU HAVE REACHED THE FLAG

9de1acbbe9d2a340da58e3e57c9ee24e

Press CTRL + C to copy the Flag!

Impact

The absence of signal encryption facilitated an effective replay attack, leading to unauthorized vehicle access. In real-world applications, this vulnerability could result in vehicle theft or unauthorized entry into restricted areas.

Remediation

To prevent replay attacks on frequency-based access systems, the following measures are recommended:

1. Implement Rolling Code or Challenge-Response Mechanisms: Use rolling code technology or challenge-response protocols to prevent captured signals from being reused.
2. Encrypt Signal Transmissions: Encrypt the signal used for access control to prevent interception and unauthorized replay.
3. Monitor for Suspicious Signal Activity: Employ systems to detect and alert on repeated or unusual signal activity on sensitive frequencies.

Written by omri kogot