PT REPORT

CySDR

EXECUTIVE SUMMARY

Redioelctric simulation challenge.

a IOT expert team successfully intercept and manipulate trasmited data from wireless camera and from car remote key that works on standard redio frequencies.

The team baypass ip camera and capture the frequency of the car remote key by using a jammer device to disrupt wireless signals.

The camera use common frequency of 2.4 GHz unencrypted transmission.

The remot car key capture by using signal replay recording data transmission on 434 MHz.

CONCLUSIONS

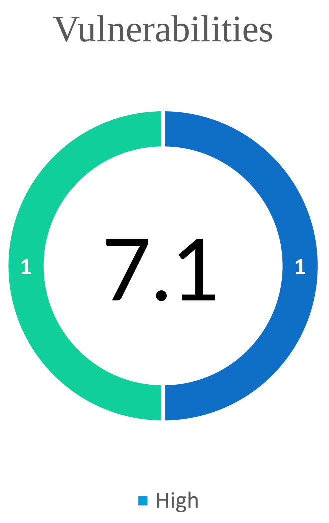
The security level of the system remaind low .

The tested environment was a weak encryption make it easier fot unauthorized to intercept the information.

The main exploitation vectors is a common operating frequencies, unencrypted transmission, using standard protocols.

This vulnerability requires low level technical knowledge.

PT REPORT



CONCLUSIONS

VULN-001 Unencrypted wireless communication (HIGH)

Description

Disrupt or disable wireless can be use for legitimate purposes like low inforcment, military operations, and ilegal activites like unauthorized interception and interapting the public safety communication, or invating privacy.

Details

The team use a jammer device that disrupt wireless communication signals .the jammer emitat radio frequency (RF) signals of the targeted camera and can overpowering or blocking the original signals.

The team exploit the wireless camera using common wellknown frequencies, whit unencrypted transmission and using standard protocols.

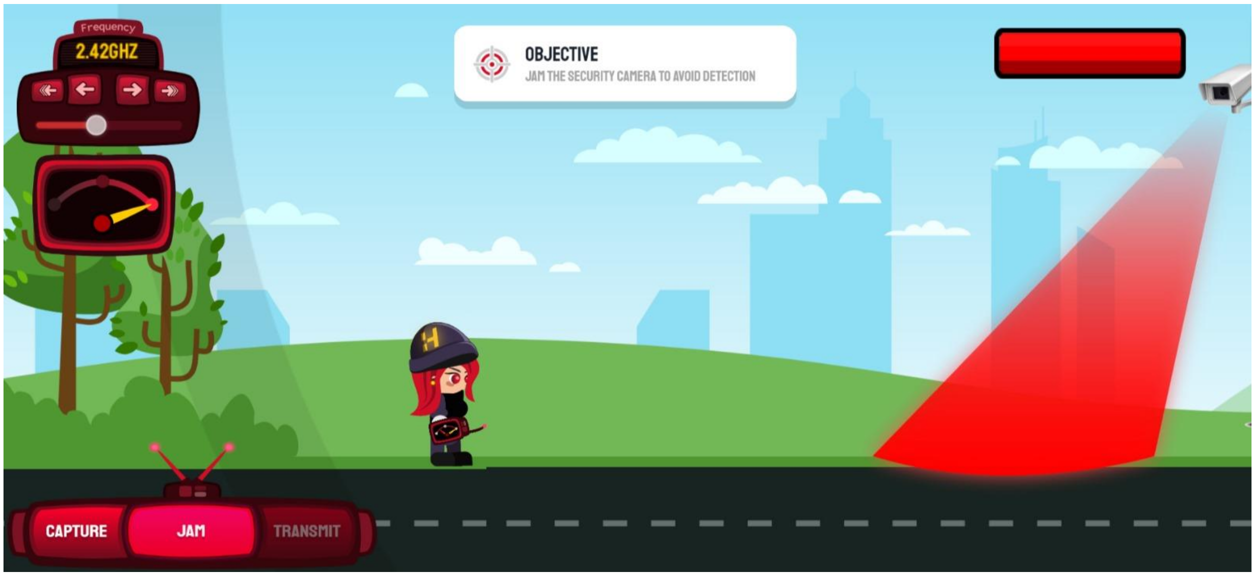
Wich allows to easily jamm the camera using one of the common frequencies(2.4GHz)

Without improving security the system is predictable and vulnerable.

PT REPORT

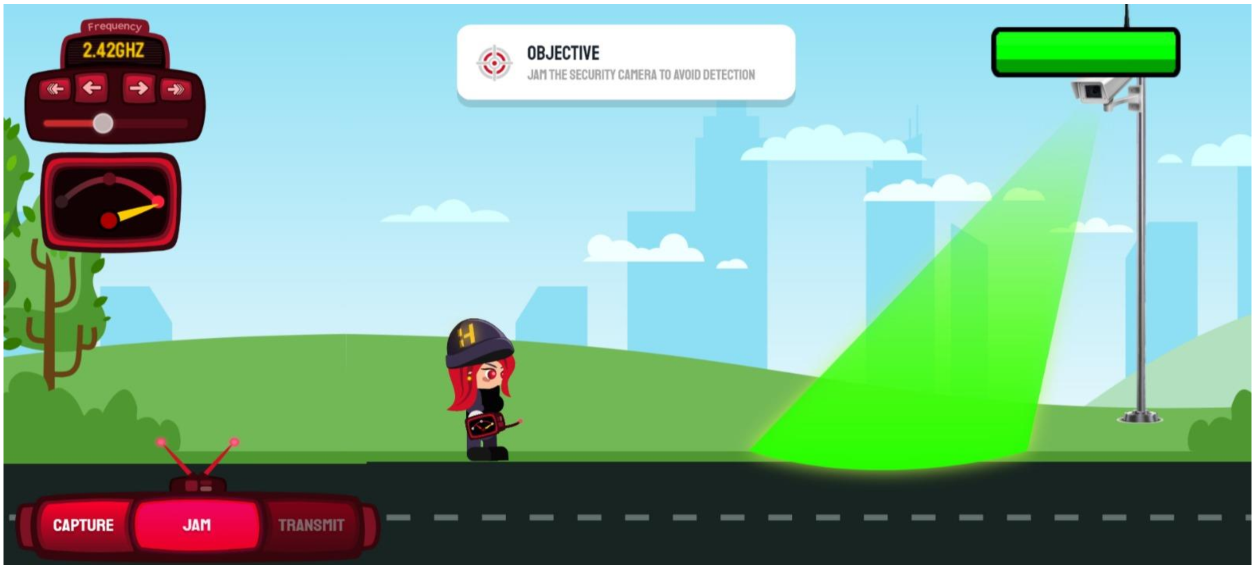
Note

Without improving security the system is predictable and vulnerable.



OBJECTIVE
JAM THE SECURITY CAMERA TO AVOID DETECTION

FIGURE 1: jamming camera whit common frequency (2.4GHz)



OBJECTIVE
JAM THE SECURITY CAMERA TO AVOID DETECTION

FIGURE 2: bypassing the security camera.

--Interception allows unauthorized access to privete videos footag.

--an attacker can be MITM and intercept data and modify it.

--attacker can replace a live feed with recorded video and blind the surveillance system.

--attacker can use the weaknes of the camera to connect to larger network and exploit wite other syber attacks.

Remediation

--it is recommended to improve authentication and encryption mecahnisims so that unauthorized devices cannot connect or interfere.

--it is recommended to update the firmware and soptware.

--it is recommended to perform security audits and penetration testing to find the weak points in the system.

--it is recommended to use FHSS technology to minimize the impact of blockages and interference.

VULN-002 Capture wireless signal for using a replay attack (HIGH)

Description

Capturing a wireless signals can be use by attacker to intercept and records data transmission from the remote control key then replay the signals to tricked the system.

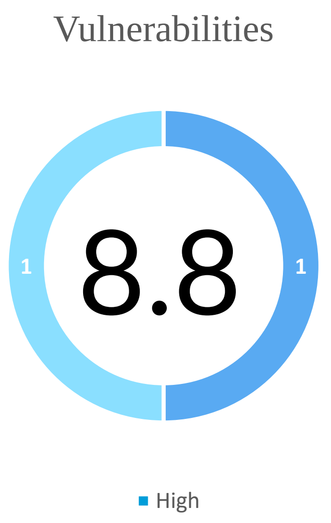
PT REPORT

Details

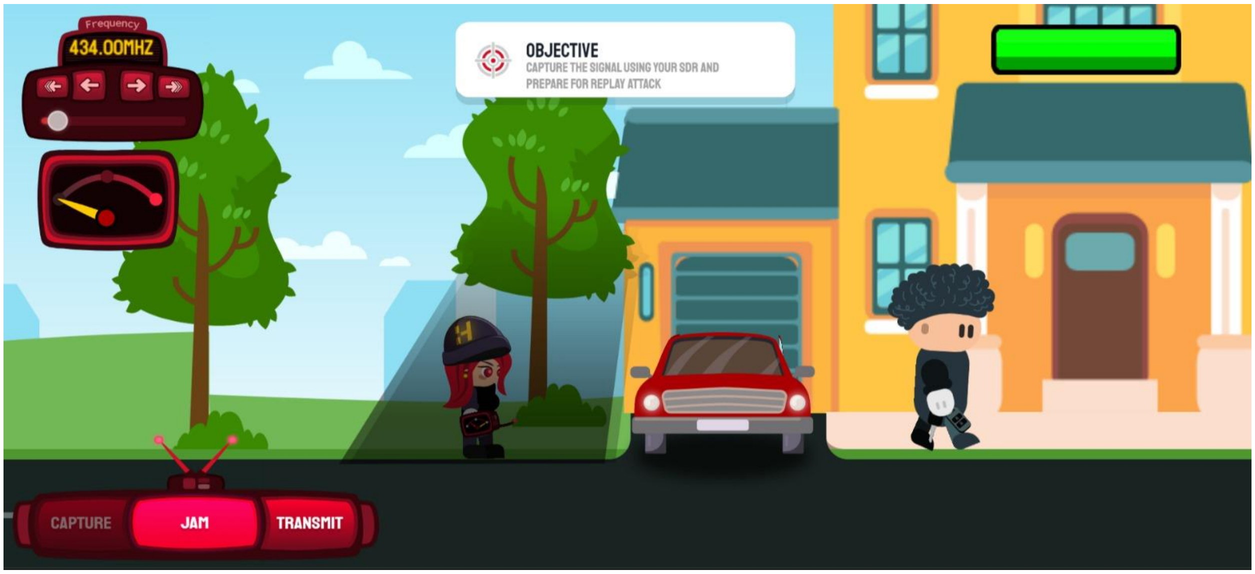
The team was able to captur frequency signals transmitted by the car remote control key. Using SDR to intercept and record the redio frequency signals use for communication.

Replay attack allow attackers to impersonate valid intities by reusing capture data.

The team was able to exploit do to using a common operating frequencies together whit unencypted transmission and using standard protocols. That allow the team to easly capture the signals using a common remote control operating frequencies(4.34MHz).



PT REPORT

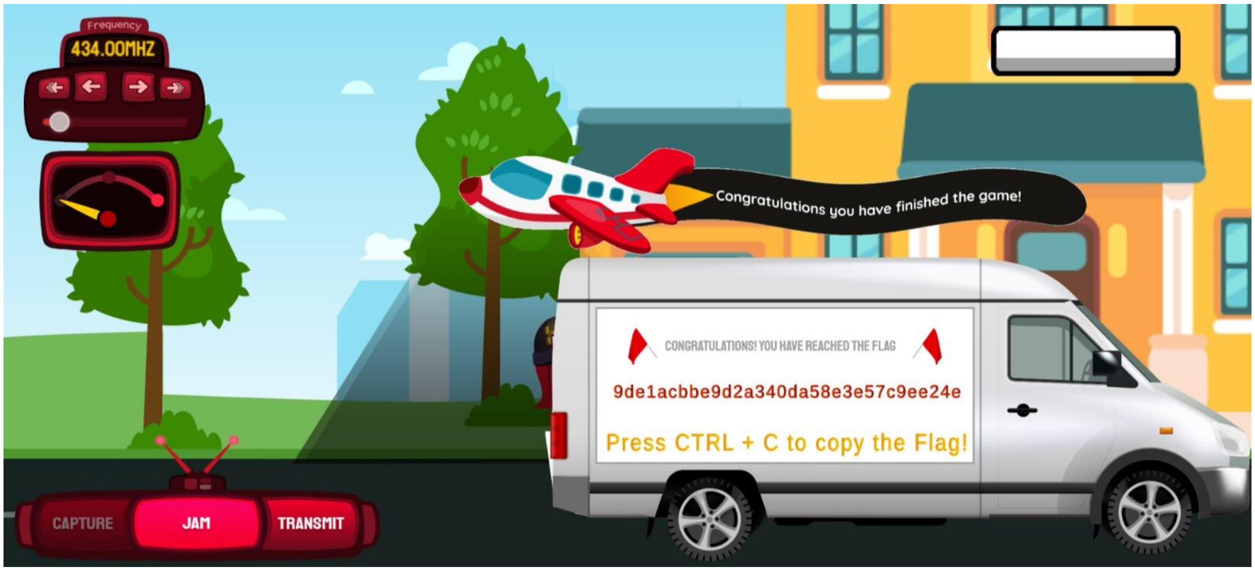


OBJECTIVE

CAPTURE THE SIGNAL USING YOUR SDR AND PREPARE FOR REPLAY ATTACK

FIGURE 3: capture the car remote control signals at 4.34MHz

This involves sending the recorded signals back to the car as if the were originate from a legitimate remote key



Congratulations you have finished the game!

CONGRATULATIONS! YOU HAVE REACHED THE FLAG

9de1acbbe9d2a340da58e3e57c9ee24e

Press CTRL + C to copy the Flag!

FIGURE 4: replay attack using the capture signals.

PT REPORT

Remediation

--it is recommended to implement timestamps and nonces in the communication protocol and include these in each signal transmission.

-- the receiver should reject signals with timestamps that are to old or nonces that was used previously.

-- educate about the importance of security awareness and risks associated whit replay attacks.

GOOD LUCK!