Keyless Entry Hack Project Proposal

Introduction

Embedded systems are largely used in many modern technologies. The security of the embedded systems are currently becoming more and more important. We researched into the specific ECU (Electronic Control Unit) of high end vehicles' passive keyless entry system and found an interesting relay attack specific to this system. We are repeating this relay attack to more modern models of cars to see if the problem still exists.

Problem Statement

Most of car's keyless entry system uses RFID as the near field communication from car to the key. The car emits a 125kHz signal when someone is trying to open the door. If the car key is within the range of 125kHz signal, the key will respond a high frequency signal corresponding to the challenge included in the 125kHz signal received. Then if the car received the correct signal from the key, the door will be opened. The same mechanism can apply to start the engine.

There are two vulnerabilities that can be made use of: 1) The car assumes the the 125kHz signal range is small enough so that if the key can respond then the key is actually presented near the car. 2) The key responded with a signal

in high frequency which can transmit over 50m when there is no obstacles between. The two vulnerabilities make the relay attack possible.

Objective

Our objective for this project is to use an SDR(Software Defined Radio) to detect and collect the 125kHz signal emitted by the car and send the signal to another SDR that near the car's key. After the key received the signal, it will respond with a high frequency signal which we don't need to relay if the car key is within 50 meters from the car. Our main task is to collect and replay the 125kHz signal near the key.

Project Plan

We did a lot of research about types of SDRs which support RFID frequencies and only very few SDRs support frequency in kHz range. We finally decided to use the Proxmark3 SDR which is specifically designed for RFID frequencies and come with a 125kHz and 13 MHz antenna which perfectly met our design specification. The SDR communicate with the computer via a USB port. We need to collect the data from the SDR using our computers and send the data via a WI-FI network to a computer near the key. Using the same interface, after the computer received the signal, we use the other SDR near the key to reproduce the 125kHz signal.

We totally need two SDRs, one for collecting signals near the car and the other for reproducing the signal near the key. Also, two computers with WI-FI capability are needed to drive the SDR and transmit the data.

Timeline

We need approximately 7 weeks to complete this project. Since the main work cannot start until we get the SDR, the timeline needs to be updated, depending on the shipment of SDR. The timeline are as follows:

Week1 (02/04/2018) read documentation and instructions of Proxmark3, tool setup Week2 (02/11/2018) use the SDR to capture the 125 kHz signal Week3 (02/18/2018) midterm status presentation Week4 (02/25/2018) transmit and replay the signal, verify if the time constraint met Week5 (03/04/2018) test the final product on different cars, compare results Week6 (03/11/2018) modification and improvement on the method, re-test, work on the defense mechanism (if possible) Week7 (03/23/2018) final report and presentation

Prior Literature

Mainly two prior documents was researched. One is from ETH Zurich which is named Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, the other one is a powerpoint from Qihoo 360 unicorn team from the Blackhat conference last year.

The ETH's paper gives us a strong theory background about the car's keyless entry system and gave us theoretical support of the possibility of the relay attack. While the Qihoo's project gave us a cheaper possibility to achieve the goal and gave us some detail about the relay timing constraint in order to successfully fool the system. However, both teams' documents used a modulation method to transmit the relayed signal which is fast but need more theoretical skills in RF field. While we are trying to realize the attack using a SDR which is more accessible theoretically. The main obstacle for us is whether we can meet the timing constraint using the SDR to propagate the copied signal.