ISSN 2348 – 9928
IJAICT Volume 4, Issue 11, March 2018 Doi:01.0401/ijaict.2018.03.16 Published on 05 (04) 2018

IDENTIFICATION OF RF SECURITY ANOMALIES IN REMOTE LOCKING OF CARS USING R820T LF PATCHING

Dr. I. Kala
Professor and Head

Ms. P. Devaki
UG Scholar

Mr. J. Francisca Dani
UG Scholar

Mr. K. Giridharan
UG Scholar

Ms. L. Jayasri
UG Scholar

Department of Computer Science and Engineering,
SNS College of Engineering,
Coimbatore, Tamilnadu, India

Abstract – ***The lock system in a Car is accessed only by the authorized persons. It is the means by which the car doors and boot lid are locked and unlocked and the engine is started. The Car-lock system is operated with a remote control. Remote controls are used in increasing frequency of small cars; interchange the functions of a common key to all purposes. A RF signal transmitter sends a signal and a coded order instruction to a RF signal receiver inside the car, which routinely controls a number of functions. Wireless remote controls send on radio frequencies and have a range of 100m about. In this paper, we present vulnerabilities in Remote key entry schemes used by many of the Car manufacturers. This we present using the RTL-SDR which is the Real Time software defined radio that uses the TV tuner dongle depend on the RTL2832U chipset.***

I. INTRODUCTION

The comfort for the devices that we use had changed a lot in our society, Because of the technology development and their impact. [11, 12, 15] The emergence of modern computing allows most of these traditionally hardware based components that is to be implemented into software instead. Hence, the term software defined radio. These permits easy signal processing and thus produce the scanner radios. [13,14,16,18] Nowadays the lock system, especially in cars had been implemented using the key fob and a car transceiver for locking and unlocking, Vulnerability in the key fob system that manufacturer uses for several vehicles, can enable hackers[17,19,20,21] or thieves to clone the key fob to the access the vehicle [1]. This is proved by using the RTL-SDR that uses Tuner Dongle

II. EXISTING SYSTEM

2.1 RKE System

Keyless remotes have a short-range radio transmitter, and must be within a particular range, usually 5–15 meters, of the car to work. When a button is pushed, it sends a signal (coded) by waves to a receiver unit in the car, which locks or unlocks the door. RKEs operate at a frequency of 315 MHz [1] .Earlier systems used infrared instead of radio signals to unlock the vehicle. Some remote keyless fobs also feature a red button which stimulates the car alarm as a basic feature. Keyless ignition does not by default provide better security. Vulnerability had been widely known to be present in many vehicle types but was previously not demonstrated [4].

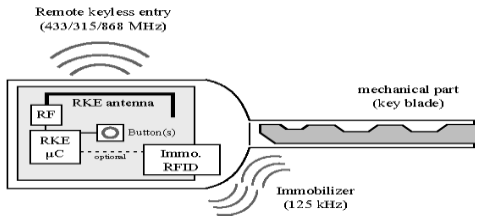


Fig 1.1 RKE System

III. PROPOSED SYSTEM

In our proposed system we are going to enhance the above vulnerability in remote keyless systems. To implement this we use the Dongle -R820T2 SDR and the tuner to tune the frequency ranges of the car. We use SDR# tool to record the frequency of the car remote. The computer connected with the dongle and the car transceiver must be connected to an accurate measurement that is capable of encounter fluctuations from one millisecond to another, in order to generate random numbers [2].

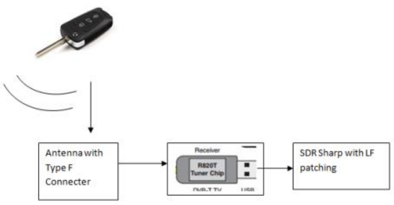


Fig 2: Architecture of the RTL- Dongle

3.1 Mechanism

3.1.1 LF Patching

The common-mode noises coming from the computer are eradicated using the mini-USB socket circuit that has a fuse for protection and filtering networks [3]. The low-noise high-stability 25ppm 200 MHZ crystal oscillator and the LNA are added with Additional noise filtering before applying power.

The Antenna input SMA connector is directly connected to the receiver using an RF relay's normally-closed contacts and the output SMA connector is directly connected to the receiver using an RF that relay's normally-closed contacts and a 50 - ohms micro strip transmission line. This allows for minimum loss when the converter is out of circuit [4]. When the receiver is operated without the converter, no current is drawn and no harm in terms of losses exists. When J1 jumper is placed (or when DC power is applied), the antenna is connected to an m-derived 55 MHZ low-pass filter using the RF relay. Then, another identical relay is used to switch between the LNA.

Then, The IF port of the double-balanced mixer ADE-1ASK is applied with the HF signals. The mixer IF port has chosen because it's frequency response starts at DC, instead of RF port because it starts at 2 MHZ [6]. This makes feasible to use this up-converter for VLF/LF too. As it can be seen on the schematic, with the LNA switched out, there is a DC path from the antenna connector all the way down to the mixer's IF port. With the LNA switched-in, the lower end of the frequency response gets raised to just under 70 KHZ. This is mostly from the transformers ferrite material used (BN-73-202).

3.1.2 Frequency Range:

0Hz
. Direct Sampling Cannot be done
. Tuner is mostly disabled
~13MHz (PLL lower limit - 14MHz)
. Normal tuning, large IF.
. High-side mixing
. Nasty aliasing are seen / attenuation / harmonics
. Near the lower edge of the range
. Lots of noise is seen from the dongle itself near 14.4MHz
.~21MHz (PLL lower limit - 6MHz) <- upstream tuner lower limit
. Normal tuning, regular IF
. High-side mixing
. This behaves much like upstream
.~1844Mhz (PLL upper limit - 6MHz) <- upstream tuner upper limit
. Normal tuning, small IF (getting squashed against the PLL upper bound)
. High-side mixing
~1848MHz (PLL upper limit - 2MHz)
. Tuning with low-side mixing (PLL frequency below tuned frequency)
. Nasty aliasing are seen / attenuation / harmonics
~1864MHz (PLL upper limit + 14MHz) <- that's all, folks
(PLL limits vary by dongle - some go as high as 1885MHz)
This tree is a collection of random tuner hacks which are really exploratory more than anything. They may or may not work for you.

3.1.3 Internals of the Dongle

* The R820T tuner has a tunable PLL that can generate frequencies between 27MHz and 1850MHz. The exact range varies from dongle to dongle.
* The tuner mixes the incoming RF signal with this PLL output. These shifts the RF signal down to a frequency that is the difference between the PL frequency and the RF signal's frequency.
* The tuner sends this intermediate frequency (IF) signal to the RTL2838U
* The RTL2838U does a digital down conversion step to generate I/Q samples that are centered on "zero" and digitizes the IF signal. The Down converter can theoretically handle IF signals up to 14.4MHz.

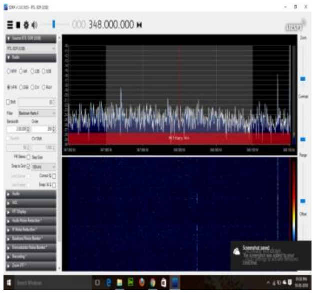
The feeding of information about the actually-tuned frequency back from the R820T(tuner) code to the core code is the main change that allows the core code to adjust to the actual IF in use, rather than requiring a fixed IF. The core code has also been directed how to handle low-side mixing, since the requested frequency is higher than the PLL frequency (e.g. the spectrum inversion changes then)

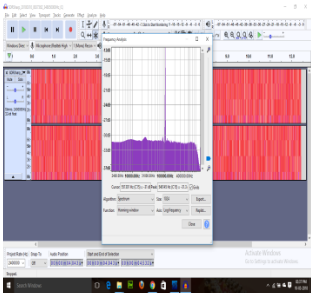
When tuning, the R820T tuner will try to tune to the requested frequency + 6MHz, producing a 6MHz IF [8]. The tuner will try a few things to produce something useful when the PLL cannot handle the frequency.

At the top of the tuning range

* It will tune the highest possibility till it can go normally, then stops there producing a smaller effective IF as the requested frequency gets higher and higher.

* Once the Intermediate Frequency starts getting decreased (below about 1.5MHz), it will alter to low-side mixing and tries to put the PLL frequency under the target frequency.





At the bottom of the range

* It will tune to the lowest possibility till it can go normally, then stops there producing a larger effective IF as the requested frequency gets lower and lower.

* Once the required IF exceeds 14.4MHz, it will switch to a variant of to "no mod direct sampling" mode. This relies on some RF signal leaking through the tuner unchanged, essentially disables the PLL in the tuner entirely. The tuner asserts to be tuned to 0Hz in this mode and the core does all the real tuning. The dongle is almost deaf in this mode; we will have to turn the RF gain WAY UP. The actual PLL limit varies from dongle to dongle, and they're probably temperature related.

The tuner has three sets of tuning limits

A hardcoded '**do not exceed this'** set of limits - see the Initial low or Initial high limits in tuner. These are in place because, especially at the low end of the range, the PLL can get into any state. For example In 25MHz, the PLL claims to be locked OK, but in reality it's actually producing 27MHz, which tighten up the core's calculations of the IF offset needed.

A hardcoded **'known to be OK'** set of limits - see the safe low or safe high limits in tuner. This is a range in which the PLL must work consistently; if the PLL fails to work in this range it is said as a tuning error and tuning fails.

A runtime **"seems to be OK at the moment"** set of limits. This varies from run to run and initially starts at the "do not exceed" limits. Whenever a loss to get PLL lock is seen, the runtime limits are narrowed accordingly and we try again. This allows the tuner to adapt to the particular dongle in use [9].

IV. CONCLUSION AND FUTURE WORK

The proposed method describes the anomalies in the car locking system and the extended future work will be focused on finding the method to overcome the above mentioned anomalies. The method will have the Google authenticating standard as the base

Reference

[1]. Lock It and Still Lose It—On the (In)Security of Automotive Remote Keyless Entry Systems Flavio D. Garcia and David Oswald, University of Birmingham; Timo Kasper, Kasper & Oswald GmbH; Pierre Pavlidès, University of Birmingham

[2]. Abdul Razaque and Syed S. Rizvi, 2017, 'Privacy Preserving Model: A New Scheme for Auditing Cloud Stakeholders', Journal of Cloud Computing: Advances, Systems and Applications, Vol. 6, No. 7.

[3]. Arulmurugan and H. Anandakumar, "Early Detection of Lung Cancer Using Wavelet Feature Descriptor and Feed Forward Back Propagation Neural Networks Classifier," Lecture Notes in Computational Vision and Biomechanics, pp. 103–110, 2018. doi:10.1007/978-3-319-71767-8_9

[4]. Haldorai, A. Ramu, and S. Murugan, "Social Aware Cognitive Radio Networks," Social Network Analytics for Contemporary Business Organizations, pp. 188–202. doi:10.4018/978-1-5225-5097-6.ch010

[5]. Haldorai and A. Ramu, "The Impact of Big Data Analytics and Challenges to Cyber Security," Advances in Information Security, Privacy, and Ethics, pp. 300–314. doi:10.4018/978-1-5225-4100-4.ch016

[6]. Aitar Almeida, Alessandro Fiore, Luca Mainetti, Ruben Mulero, Luigi Patrono and PiercosimoRametta, 2017, 'An IoT Aware Architecture for Collecting and Managing Data Related to Elderly Behavior', Journal of Wireless Communications and Mobile Computing.

[7]. Cetin Sahin and Amr El Abbadi, 2017, 'Data Security and Privacy for Outsourced Data in the Cloud', Proceedings of 20th International Conference on Extending Database Technology.

[8]. Elavarasan, G and Veni, S, 2017, 'Efficient Technique for Privacy Preserving Publishing of Set Valued Data on Cloud', Journal of Advanced Research in Dynamical and Control System, Vol. 5.

[9]. D.Lee,"Keyless cars 'increasingly targeted by thieves using computers'." Internet: www.bbc.com/news/technology-29786320, Oct. 2014 [Apr. 2, 2016].

[10]. A. Moradi and T. Kasper, "A New Remote Keyless Entry System Resistant to Power Analysis Attacks" in ICICS, 2009 c IEEE. doi:10.1109/ICICS.2009.5397727

[11]. [8].A. I. Alrabady and S. M. Mahmud, "Analysis of Attacks Against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs." IEEE Trans. Veh. Technol., vol. 54, no. 1, Jan. 2005.

[12]. L. Vincent and G. Chevret, "Customer identification device, keyless access system for vehicle, vehicle sharing system including such a device and methods using such a device." Patent WO2008044093 A1. Apr, 17, 2008.

[13]. I.Kala , N.Karthikeyan , S.Karthik "Region based AODV Geographic Routing Protocol for Quasi MANET", Asian Journal of Information Technology, ISSN: 1993-5994, December 2016. (Annexure I – Scopus Indexed)

[14]. I.Kala "A Survey on Efficient Routing in VANET", International Journal for Research in Technological Studies, Volume 4,Issue 1,ISSN: 2348-1439,pp 10-13,December 2016.

[15]. I.Kala "Clustering Algorithms in Wireless Sensor networks: A Survey" in the International Journal of Inventions in Computer Science and Engineering", Aug 2015

[16]. I.Kala, N.Karthikeyan , S.Karthik "Pruning Heuristic Vineyard Routing Protocol For MANET" in the International Journal of Applied Engineering Research" PP.30285 – 30287, June 2015.(Annexure II – Scopus Indexed)

[17]. I.Kala,"Efficient Fault Detection Mechanism For Reliable Transmission In Mobile Adhoc Networks" in the International Journal of Applied Engineering Research, ISSN: 0973-4562, Volume 10, Number 41 (2015), pp.30404-30412, June 2015.(ANNEXURE II – Scopus Indexed)

[18]. I.Kala, "Adaptive Position Update For Geographic Routing Based On Mobility Forwarding Node Selection" in the International Journal of Applied Engineering Research, ISSN: 0973-4562, Volume 10, Number 41 (2015), pp.30492-30500, June 2015.(ANNEXURE II – Scopus Indexed)

[19]. I.Kala, N.Karthikeyan , S.Karthik "MR-P Heuristic of Improved Geocast Routing for Mobile Ad Hoc Networks" in the International Journal of Soft Computing, 10: 76-82 , January 2015.(Annexure II – Scopus Indexed)