
Wireless Hacking - SDR

Professor: Ronny Bazan Antequera
Researcher: Patrick Kunza

Table of Contents

Overview.....

2

Introduction.....

3

User Guide.....

5

Testing Plan.....

6

Testing Process.....

9

Future Work.....

10

Suggestions.....

10

Project Contribution.....

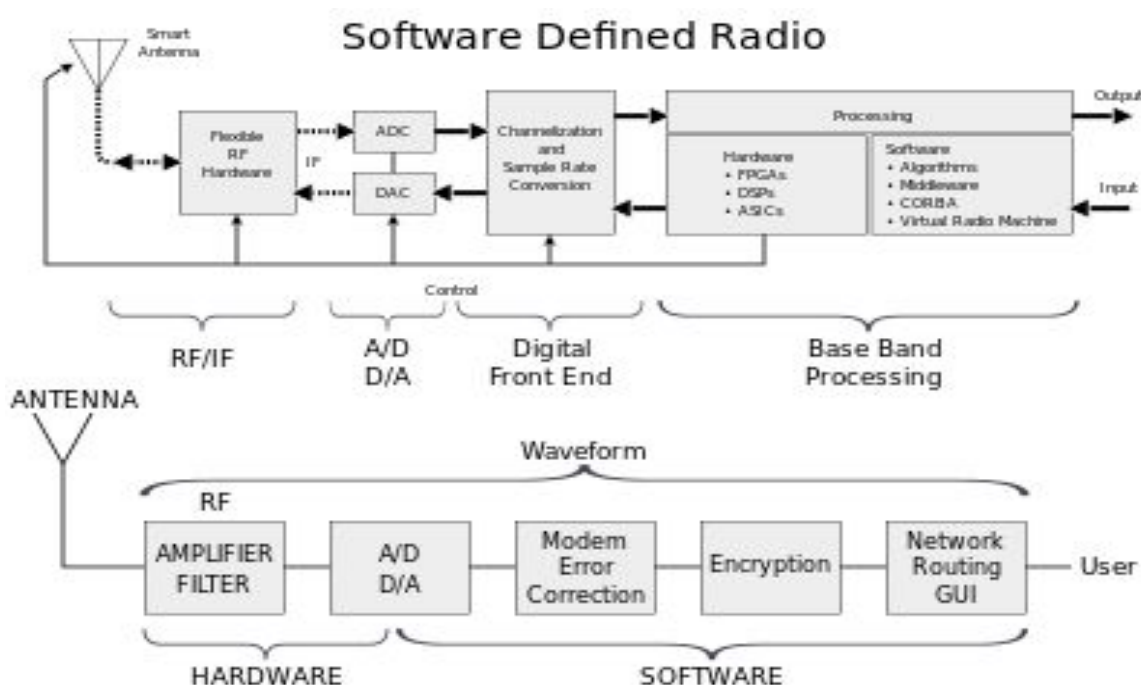
14

Overview

Title:	Wireless Hacking - SDR
Purpose:	To find vulnerabilities within Bluetooth related frequencies and create solutions to patch them.
Materials:	<ol style="list-style-type: none">1. HackRF One2. Pentoo Operating System3. GNU Radio Companion (software)4. GQRX (software)5. SDR Console V2 (software)6. Antenna7. VB Audio Cable8. Intel(R) Core(TM) i7-7700HQ CPU @ 2.80GHz, 2801 Mhz, 4 Core(s), 8 Logical Processor9. Windows Operating System

Introduction

For this project I am researching wireless hacking capabilities within Software Defined Radio (SDR). Software Defined Radio (SDR) is a type of radio in which all of the physical layer functions are software defined. This definition was obtained from the collaboration from the Institution of Electrical and Electronic Engineers (IEEE) and Wireless Innovation Forum. In other words SDR is a type of radio communication system that consists of the traditional components implemented in hardware such as filters, amplifiers and mixers are implemented as software on an embedded system such as a computer, Hackrf One, RTL SDR or other SDR enabled devices.



Within this research project I am looking into vulnerabilities with bluetooth devices. Bluetooth enabled devices is a short-range wireless communication technology that uses radio waves/frequencies to transmit information. There are two forms of Bluetooth, Classic Bluetooth which is used for devices with a high demand for small transistors. The other form of Bluetooth technology is Bluetooth Low Energy (BLE) which is ideal for applications that require small quantities of data occasionally or periodically.



Bluetooth Low Energy (BLE) has a wide range of possibilities and is used in many different fields such as health, fitness, security, home automation and IoT (Internet of Things). In this project I will be researching and testing different vulnerabilities within Bluetooth and BLE enabled devices. After examining vulnerabilities I will work on creating a potential solution that will help patch some of these vulnerabilities.

User Guide

The main goal of looking for exploits within bluetooth enabled devices is to understand better how these systems work and what is capable of being exploited. This research and testing is intended for the use of the IT department in the School of Engineering at the University of Missouri - Columbia.

Users will securely test devices that are legally authorized to test. When testing bluetooth devices with SDR hardware they must only test and practice on personal devices in order to not conduct illegal activity. The user must also test these vulnerabilities in a secure private network in order to guarantee penetration testing will not affect other devices in the neighborhood.



Pledge: I am authorized to only research and to conduct penetration testing on devices that are given to me by the lead professor, Ronny Antequera and or other authorized University of Missouri professors that have been given clearance to assist in research and development.

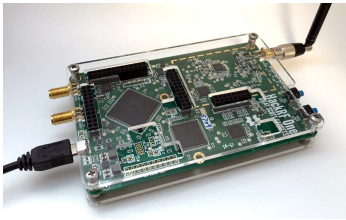
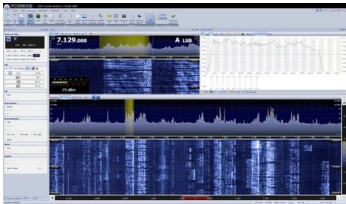
Testing Plan

SDR and Bluetooth Research -

As part of the testing plan, I first conducted research on software defined radio and how bluetooth works in order to understand how to properly manipulate vulnerabilities within bluetooth enabled devices. I read articles and research papers that are similar to my project while also watching instructional and informational videos online.

Hardware Configuration -

Acquiring hardware and software that is appropriate for this study is vital as it will help analyze, capture and record frequency information within testing.

Components	Specifications	
Hackrf One	Frequency Range: 1 MHz to 6 GHz ADC Resolution: 8 Bits Max Bandwidth: 20 MHz TX/RX: TX and RX (Half Duplex)	
SDR Console V2	SDR Analyzer provided by Simon Brown This version is an older kit	

Setting up Hackrf One -

Step 1: Screw in the ANT500 Antenna that came with the Hackrf One

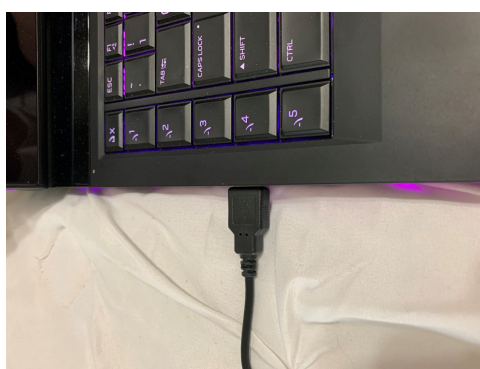


Note: Make sure to attach the antenna to the antenna port and not the CLKIN or CLKOUT coaxial port.

Step 2: Plug in the power USB adapter in the micro USB port of the Hackrf One.

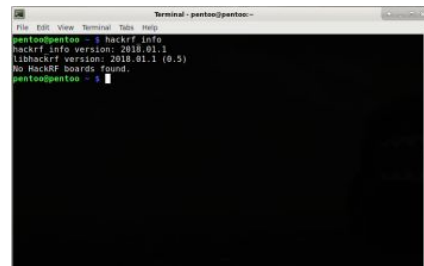
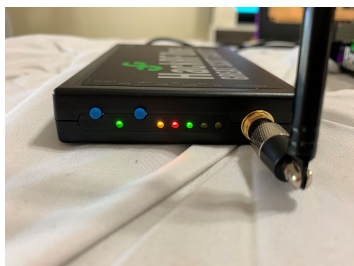


Step 3: Plug the USB end of the power cable into your computer.



Note: When you plug in the Hackrf One make sure that the device is recognized by using the correct USB port and you allow administrative privileges to the device.

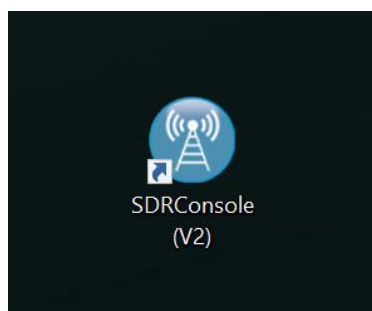
Step 4: Check to see if Hackrf One is running and ready to analyze.



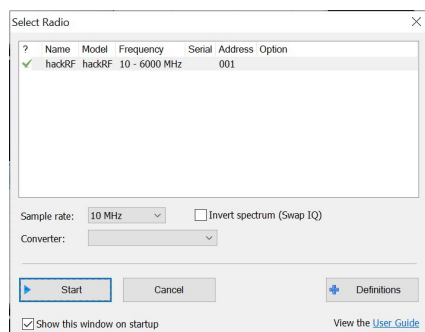
Note: You can check if the Hackrf One is fully operational by logging into Pentoo and running “hackrf_info” in the terminal. It should return if the device is ready or not.

Setting up SDR Console V2 -

Step 1: Run SDR Console V2 as Administration User.



Step 2: Select “hackrf one” as the radio device and then press start.



Testing Process -

After configuring the hardware make sure your own personal network and devices are within a secure and private environment. When beginning to search for signals within a certain frequency make sure to only obtain your test signal. After analyzing and clarifying your own test you may then start recording and manipulating the signal you are transmitting in the test.

Future Work

The development goal for this project was to successfully exploit vulnerabilities within bluetooth enabled devices and patch these vulnerabilities but due to the extensive amount of time dedicated to trial and error I was only able to achieve part of my goal. With that being said I would like to use the rest of this document to put together a future plan in order to prepare and provide researchers with a good base of support to help them to achieve their goals and be successful early on.

Suggestions -

Physical Lab -

Having a physical laboratory for researchers and professors to meet would be beneficial for this project as it would allow time to work with one another and communicate effectively. This would also minimize the potential of illegal activity by restricting the usage of device testing off of the University of Missouri campus.

Research Team -

Having a well developed and connective research team is vital to the progress of this research program. Each researcher should be able to contribute to the project in a wide variety of ways. The more researchers working on this project can add a lot of contribution and speed up the overall process of accomplishing tasks.

Leadership -

Creating a larger research team might make it easier to complete tasks/goals but without good leadership the team will struggle to have direction and might lead to missed deadlines and an increase in testing errors. That is why it is important to have great leadership that can manage and lead the team to success throughout the process of this project. Starting with the level of professors/mentors they should be able to give guidance when it is needed and provide researchers with the material and knowledge needed for this study.

Professor/mentors are important but another key leadership role within this project is the Lead Researcher Position. The Lead Researcher is responsible for guiding the team through daily and monthly objectives as they are the ones to check procedure and documentation to make sure it meets the needs of professor/mentors.

Future Hardware and Testing -

Hardware	Description	Link
1. RTL- SDR Dongle	A very cheap USB dongle that can be used as a computer based radio scanner for receiving live radio signals in your area 500 kHz up to 1.75 GHz	RTL-SDR on Amazon
2. Hackrf One	Software Defined Radio (SDR) peripheral capable of. designing to enable test and development of modern and next generation radio technologies, HackRF One is an open source hardware platform that can be used as a USB peripheral or programmed for stand-alone operation. 1MHz to 6GHz	Hackrf One Device on Amazon

3. Hackrf One with ANT500 & SMA Antenna Adapter Bundle	ANT500 from Great Scott Gadgets is a telescopic antenna designed for operation from 75 MHz to 1 GHz. Its total length is configurable from 20 cm to 88 cm. ANT500 is constructed of stainless steel and features an SMA male connector, rotating shaft, and adjustable elbow. ANT500 is a 50 ohm general purpose antenna.	Hackrf One with Antenna Bundle on Amazon
4. SDR Console V3 (License)	SDR analyzer software that is used for windows and Mac operating systems.	SDR Console V3 Download License
5. PortaPack for Hackrf One	Add a PortaPack to your HackRF One software-defined radio, and leave your laptop behind! The PortaPack attaches to your HackRF and adds a touchscreen LCD, user controls, headphone jack, high-accuracy clock reference, real-time clock, micro SD card slot, and custom aluminum case. When you attach a USB battery, you're ready to explore the radio spectrum wherever you are. The PortaPack firmware runs on the fast ARM processors in your HackRF. No computer is necessary (except for programming firmware). https://github.com/sharebrained/portapack-hackrf/wiki/Assembly	PortaPack for Hackrf One on Amazon
6. Computer	High End processing computer that will be able to easily meet the needs of	Alienware Aurora PC on Amazon

	processing hardware and software. You do not need to necessarily get an Alienware PC but something with similar configuration.	Alienware PC on Amazon
7. USB Battery Pack	Compact size to be your best travel company Real 10000mAh capacity to power your device for days. LCD power display to let you know the power juice timely.	USB Battery Pack on Amazon

Project Contribution



Ronny Bazan Antequera - Professor

IT/CS engineering professor.



Patrick Kunza - Lead Researcher

IT/CS engineering student at the University of Missouri. He has created new tech products that span from application-based software to database creation and configuration. Patrick is also studying cyber security and is an Advanced Cyber Security PLA at the University of Missouri.