International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2019): 7.583

Performing Attacks on Radio Frequency and Embedded based Systems

Preeti Rana

Abstract: ***With the increasing use of embedded devices in our daily life, security threats have also been increasing in a proportional rate. However, ensuring security in the embedded systems has become a great challenge not only for the embedded device experts but also for the manufacturers. The problem especially arises because of the limited hardware and software implementation options for the designers. At the same time, companies are trying to keep the vulnerabilities of the operating system of those embedded devices in secret and they are not relieving any necessary security updates quickly. It has become very urgent to ensure proper security of the embedded systems to save it from any major technological disaster near future. In this paper, I have broadly discussed on how to perform attack on embedded devices, So that you can be aware of embedded devices loopholes. Beside this, I have also discussed about the different causes of security threats so that you can protect the systems from the attackers.***

Keywords: Hardware hacking, Firmware, Rf attacks, Attacking tools both hardware and software

1. Introduction

An embedded system can be defined as a special type of computer system that performs some specific pre-defined programs which is generally used within a larger scale of electrical or mechanical system. Generally, it is started from small MP3 players to largely complex hybrid vehicle systems. Some other examples of frequently used embedded systems in our daily life are keyboard, mouse, ATM, TV, PDA, cell phone, printer, elevator, smoke detector, DVD player, refrigerator, camera, GPS navigator, radio, TV remote, telephone, game controller, monitor, digital image processor, bar code reader, SD card, washing machine, antilock breaking system, blender etc. We use embedded systems especially because of its dependability, efficiency and it meets the real-time constrains. Examples of the embedded system show that it has become a part and parcel of our daily life in term of use. We are very familiar with the term ‘Smart Home’ because of the deployment of smart embedded system in our home. Now-a-days almost all of the embedded systems are connected with the internet. So security threats have become a major issue at present because most of the embedded systems lack security even more than personal computers. One of the reasons for this lack of security is the very limited hardware and software implementation options for the manufacturers of embedded system companies. Again they have to deal with the competitive market price of the other embedded manufacturer companies because they all have to keep the lowest possible price to maintain the customer satisfaction and at the same time they do not conduct any specific security research of their manufactured embedded products. This leads to the security threats for the embedded devices because ensuring advance security techniques for embedded systems means the higher cost of that embedded products. Customers also don’t want to be more expensive usually when buying an embedded device and they are not concerned also about the probable security threats of their products. Lack of security analysis and low-cost market product mentalities of the manufacturer companies lead the hackers the exact environment they are expecting for. Many embedded systems hacking tools are easily available in the internet. Hacking in the PDAs and modems are very common example of embedded systems hacking. Recent development trends of the embedded systems protocol are going to be convergence because of its applications in TCP/IP protocol for the purpose of inter-media interfacing. In this case, using IPv6 will cost much more for the development of the embedded applications at least for the next few years. As a result IPv4 is going to dominate in the applications of embedded systems. This IPv4 is much more challenging for its internal security problems in terms of authentication, integrity and confidentiality.The Internet is as yet developing and online business is on its progress. The immense development of Internet has brought numerous great things like electronic commerce, email, simple access to tremendous stores of reference material and so forth. An ever increasing number of computersget associated with the Internet, wireless devices and networks are blasting. Because of the propel innovation of the Internet, the administration, private industry and the regular computer client have fears of their information or private data being contained by a criminal hacker [1]. These kinds of hackers are called black hat hackers who will covertly take the association's data and transmit it to the open internet. In this way, to overcome from these real issues, another class of hackers appeared and these hackers are named as ethical hackers or white hat hackers. Along these lines, this paperportrays ethical hackers, their aptitudes and how they approach helping their clients and fitting up security openings. In this way, if there should be an occurrence of computer security, these tiger groups or ethical hackers would utilizesimilar traps and strategies that hacker utilizes yet in a legitimate way and they would neither harm the objective frameworks nor take data. Rather, they would assess the objective framework's security and report back to the proprietors with the vulnerabilities they found and guidelines for how to cure them. This paper will characterize ethical hacking, show a portion of the ordinarily utilize terms for aggressors, give a rundown of the standard administrations offered by means of ethical hacking to battle assailants, talk about issues and their preventions.

2. Embedded System and RF Hacking

Introduction to embedded devices:
Embedded systems are said to be combined of hardware and software an electronic system that has computer software which is embedded in computer hardware.

However, embedded system is destined to do a single particular task .For eg. Pacemaker.

Some other examples of embedded systems are microwave oven, washing machine, printers telephones, etc.

Steps to Analyzing Hardware
1) Research the device
2) Identify the components
3) Identify debugging ports
4) Dump the flash
5) Extract/analyze firmware

3. Methodology

The methodology for embedded systems hacking is to look for its 3 best interfaces which he/she will find in most of embedded systems:
1) UART: It is a computer hardware device for asynchronous serial communication in which the data format and transmission speed are configurable.
2) JTAG: It is an electronics industry association formed in 1985 for developing a method of verifying designs and testing printed circuit boards after manufacture.Hardware debugging tool.
3) SPI: It is a synchronous serial communication interface specification used for short distance communication, primarily in embedded systems.
4) FTDI cable: for UART and 3.3v vs 5 v.
5) BUSPirate: Talks lots of protocol like UART, SPI, I2C. Can use python to control it. Used for dumping flash, modifying EEROM, Program AVR.
6) JTAG Debugger
7) JTAGulator: Tool to find JTAG.

Equipment's required
- Some PCB does not label the port so we have to identify them by using tools and most commonly used tools are multimeter, UART adapter, logical analyzers, power supply, JTAGulator, Buspirate.
- Logical analyzers: They are protocol aware help you with pinouts for specifically debugging parts. 1's and 0's, convert signals to data.
- JTAGulator, Buspirate: These are used for UART, JTAG, SPI capabilities they are not complete without any framework or computer.

Impacts:
UART, what is it good for?
- Console to the device (telnet ,SSH,NC)
- Helps us monitor and look for offsets, crashes etc.
- Error messages or crash logs are usually extremely verbose.
- Helps us look what is actually running on the device.

JTAG, what can we do?
- We can read and write to memory.
- We can set breakpoints.
- Patch instructions or data into memory.
- Extract firmware.
- Bypass protection, password checks, checksums, etc.
- Simply put, if we've JTAG access we win.

Firmware:
1) Accessible free from almost all vendor websites.
2) Extracting via serial UART, JTAG or SPI flash "if they are available".

Finding Firmware and source code:
To start your research work you need a toolbox of both software and hardware . We will use some of these tools:
1) Firmware analysis
   - Binwalk
   - Firmwalker
   - Open-OCD
   - Firmware modification toolkit [get all software from Github]
2) Reverse engineering / Debuggers/ Disassemblers
   - IDA,IDA pro
   - Radar
   - Hopper disassembler
   - GDB
3) Emulator tools
   - QEMU (No hardware, QEMU will rescue)

Source Code:
- Does the vendor use or publish their software with General Public License, then the source code will be available to you either by download or request.
- Public repos, GIT etc.
- Eg. Lets pick a target. Lets use the Swedish site called Prisjakt which router is most popular in Sweden right now?
  Is ASUS-RTAC68 a good target?
  - Firmware available at the vendors website?
  ……. YES, multiple versions.
  - Some code under General Public License?
  …… Yes!

Check all this….

Introduction to RF Hacking
- Radio frequency (RF) hacking is said to be the most dangerous attack as it can expose some very private communications or by overpowering the legitimate signals attacker can do DDoS or attempt to impersonate legitimate traffic.
- Radio frequency device are used in our daily life cycle can be vulnerable and might take any sensitive data. These radio frequencies have their own wave spectrum where various devices worked on some frequency band.
- For eg. FM radio operating on 100 MHz, GPS and cellphone 1GHz.
- Apart from this there are cars connected to mobile phones and GSm and they operate on 2.4GHz.

- All these can be easily vulnerable with low cost tools such as GNU radio, RTL-SDR, hackRF, etc.

Phases of RF attack

Information gathering -> Frequency -> Modulator -> Transmission

a) *Information Gathering:*
So to gather information of any device is really simple we have to just see for FCCID which is labelled on the device. Through this we get all the information about the device.

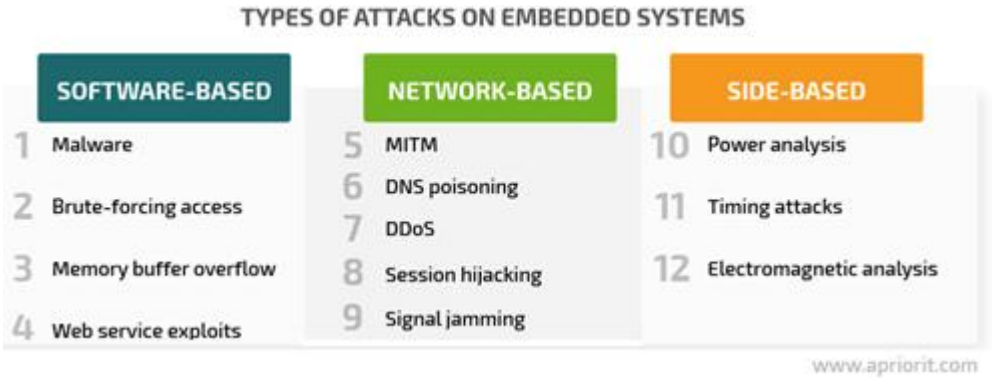
b) *Frequency:*
It is very important to understand the device which we are testing works on which frequency band. So that we can use GQRX which is spectrum analyzer to analyze those FFT and waterfall.

c) *Modulator:* It is like a hiding a code inside a carrier wave. Representing digital data as variations in the carrier wave.

d) *Transmission:* Now from all this study we know the frequency of a device and then modulation of a device now we have to transmit this signal through tools i.e. GNU Radio and etc.
To transmit the signal we need to know frequency, modulation, Bitrate, sync word, Preamble.

e) *Bitrate:*
It is a transmitting rate where per seconds how many samples are transmitted .In simple words it is a sample/sec.

f) *Sync word and Preamble:*
These are the wakeup signals .Every time this will be same for every IoT and RF devices.



4. Conclusions

Embedded devices have made our life more easy and comfortable by meeting almost all the real-time constraints. Although it is very popular among the mass people but they are quite unconscious about the probable security threats till now even the manufactures and the engineers associated with embedded devices. Expert hackers from the different parts of the world have already found many security pitfalls of the embedded devices and they are further working on it. So, it is very clear that it could create a huge blow in near future for the technological industry if the engineers and the manufactures do not take the necessary security solutions as proposed in this paper to protect the unauthorized access from the unsecured third party. We heartily believe that more concentration on cryptography, tamper-resistance techniques, advanced microcontroller and algorithms can mostly make the embedded devices secure enough. At the same time, it is also important for the manufacturer companies to design and implement the whole embedded system with much more security concern.