SOFTWARE DEFINE RADIO (SDR)

PARKER SWISTON
Mentor: Ming Chow
12/15/15

Abstract

With ever growing air traffic for communication, the drive to increase efficiency in relaying information using smaller ranges of frequencies with less interference has skyrocketed. This search has had positive and negative consequences. One method that has greatly contributed to a solution for this problem is software defined radio. However, its has also made access to the radio waves emitted from our devices easily accessible. Software defined radio is a system for radio communication using software replacements for historically hardware roles. This design allows for the radio to receive and transmit using a wide range of protocols which can be leveraged by any communication service. Previously significantly theoretical, the concept of software defined radio has seen massive advancement in feasibility in recent years as a result of advancements in digital electronics. Looking to the future, software defined radios have the potential to become the prevailing technology in radio communications, which has a large impact on everyone using electronics. This paper provides background on software defined radios, identifies current and predicted uses, and assesses security ramifications. It is becoming more and more of a necessity for solutions like software defined radios to satisfy a world that craves more and more remote communication, which in turn requires the community to understand it in order to protect itself from exploitation.

1. Introduction

A radio is any device that can transmit or receive signals wirelessly using the radio frequency in the electromagnetic spectrum. This includes everyday gadgets like cell phones, computers, vehicles, and televisions. A traditionally constructed hardware radio limits cross-functionality and can only be physically modified. This has cost and efficiency consequences which are addressed by software defined radio. A software defined radio is any radio device that includes a software replacement of some or all of the physical components. Supplementing the radio with software components allows radios to be much more flexible, capable of having multiple modes, bands, and/or functions, and can be upgraded using software updates.[1]

“Software radio” was first used as a term in 1984 by E-Systems inc. (now Raytheon) to describe a digital baseband receiver. The receiver was created out of necessity because their general purpose computer did not have the capacity to run a radio signal processing technique that was being developed.[2] It was later reinvented independently in 1991 by Joe Mitola in a plan to combine a digital receiver with a digitally controlled communications jammer in order to create a true software based transceiver. In the early 1990's, the software defined radio was improved upon through research for the SPEAKeasy program.

The support of a number of research reports conducted in 2006 indicate that software defined radio is in the early stages of defining the mainstream market. Widespread use of software defined radio technology has increased drastically in the last few decades. They have been successfully used in defense, cellular infrastructure systems, cellphones, satellite modems, and many more situations. Applications will only increase as the technology improves.

2. To the Community

It is important to keep software defined radio in mind as it becomes a bigger and bigger

part of everyday life. Communication is consistently increasing between people and between devices. Every electronic is giving off radio waves whether we intend for it to or not. Phones, baby monitors, garage door openers, and wireless car keys are just some of the many examples that we all have at some point in our lives. This opens you up for exploitation like mentioned in Melissa Elliot's Defcon 21 presentation where she mentions that her father was able to over hear a man threatening to kill his wife. In that case, it was good that someone was able to tune in on the baby monitor that picked up the conversation, but what else could someone have listened in on? Someone listening in could also hear personal conversations if they wanted to, or worse, figure out the habits of the family and rob the house or kidnap the baby. The radio emissions are giving off some information at all times and someone listening can use that information if they are paying attention. [3]

Why is this important? While it is illegal to monitor certain frequencies, it is possible for an attacker to monitor any electronic device and use whatever information they gather. It is important to be aware what information you are leaking. If you are OK with leaking information about yourself, there is no need to take further steps. If you wish to know what information is getting sent out into the world so you can protect yourself, there are steps you can take detailed in the application section below. By monitoring yourself using software defined radio, you can be aware of what a potential attacker can find out about you and then do what is necessary to give yourself enough security to be comfortable.

3. Action Item

As mentioned above, software defined radio can be used on an individual level. There is a wide range of gadgets that will allow a user to monitor different frequencies. This ease of access means that attackers have easy access to these tools, which makes it more imperative that

individuals equip themselves as well. By knowing what information is getting leaked and how it is getting leaked, measures can be take in order to prevent the leak of private and important information. There are cheaply available radio tuners, which do not require in depth radio engineering knowledge, that capture and dump the data which can be interpreted with software. Examples are an RTL 2832 U, or HackRF ONE, which are USB software defined radio peripherals that allows your computer to receive or transmit signals.[3][4] Both allow a user to see what an attacker may find by monitoring frequencies that can be interpreted by software on a general computer. After identifying some leaks, some basic interference techniques include removing batteries of electronic devices if possible, wrapping devices in tinfoil (not completely practical if the device has a human interface), cellphone blockers which interfere the radio frequency of a cell phone, or storing devices in a microwave (making sure not to run the microwave). These are some drastic measures that are inconvenient and are probably not necessary unless incredibly sensitive information is being leaked. The most important thing is to realize that information about you is being broadcast to the world there just like when something is posted online.

4. Application

One of the original purposes for software defined radio was for the military. The goal of a U.S. Military program called SPEAKeasy was to develop a radio that was capable of communication at frequencies ranging from 4MHz to 400MHz. This provided 5 major military benefits: Interoperability, Flexibility, Responsiveness, Mobility, and cost reductions. Interoperability included emulating legacy systems, a bridge between ground force radios, Air Force radios, Naval Radios, and satellites. Increased flexibility meant a reconfigurable, modular, and scalable systems. Responsiveness meant reprogrammable and enabling P3I. Mobility

entailed reducing logistics and terminals. Lastly, initial production and equipment costs were reduced. The first phase emphasized development on the modem only, but the second phase focused on building the entire radio. After continuous technological advances from the 1990's to the present, the result is that now, soldiers can leverage a flexible new approach to meet diverse communication needs through software programmable radio technology.[5]

5. Conclusion

In conclusion, software defined radios and radio transmissions are all around us and are not going away soon. There can be many benefits to all the technological advances we have like cellphones, military communication, laptops, smart watches, baby monitors, and remote controls, but it comes at a cost. Personal data is becoming more and more publicly available without the average Joe taking any notice. It is important that we realize what is going on and identify our weaknesses so we can know when we are vulnerable and prevent exploits when possible as tools like software defined radio capabilities and and convenience expand.

6. References

1. "Software Defined Radio."*Cognitive Radio Networks* (2009): 41-58. *Wireless Innovation*. Wireless Innovation. Web. 15 Dec. 2015.

2. TEAM 5 (1985): 2. Web. 15 Dec. 2015. <http://chordite.com/team.pdf>.

3. Elliott, Melissa. "DEF CON 21 - Melissa Elliott - Noise Floor Exploring Unintentional Radio Emissions."Y*ouTube*. YouTube, 6 Sept. 2013. Web. 15 Dec. 2015.

4. Ossmann, Michael. "Software Defined Radio with HackRF, Lesson 1."*Great Scott Gadgets*. N.p., n.d. Web. 15 Dec. 2015.

5. "2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks."*2006 1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks* (2006): n. pag. *Bldrdoc*. Bldrdoc. Web. 15 Dec. 2015.