Work Experience - RF Guide

Patrick Mintram

April 18, 2019

Contents

List of Figures

1 Introduction

This guide has been produced to help you work through the RF workshop as part of your work experience. In this workshop you will learn

1. What things use RF.
2. How we can make something that uses RF.
3. How using RF can expose your projects to vulnerabilities.
4. What tools we can use to help when using RF.

.

By the end of this workshop you should be able to use gnuradio, and an SDR to perform a MITM attack on a system which has two devices talking to each other via RF. If you don't know what these things are yet, that's ok, you will find out by working through this guide.

1.0.1 Using this guide

There may part of this guide which aren't explained very in depth, that is because the subject of RF and signals is really complicated, so the detail has been left out. If you want to find out more there are some good overviews available online[1]. This guide is meant at more of a practical wrokshop than an academic exercise, so if something is glossed over a useful link will be provided in the footnotes, as you have already seen.

2 Equipment

The equipment we are using

3 How to use this Guide

Do I need this?

4 Setting Everything Up

How to set things up

5 gnuradio

This is a description of gnuradio and how to use it

5.1 The Spectrum

This is a brief description of the spectrum on gnuradio and what it shows

[1] http://www.ti.com/lit/ml/slap127/slap127.pdf, for example

6 Real World Example

RTL-SDR