



Features Business Explore Marketplace Pricing

This repository Search

Sign in or Sign up

cn0xroot / RFSec-ToolKit

Watch 61

Star 460

Fork 111

Code

Issues 2

Pull requests 0

Projects 0

Insights

Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

RFSec-ToolKit is a collection of Radio Frequency Communication Protocol Hacktools.

radio sdr hackrf bladerf limesdr usrp gnuradio iot fuzzing

30 commits

2 branches

0 releases

3 contributors

Branch: master

New pull request

Find file

Clone or download





cn0xroot Update README.md

Latest commit b3c4708 13 days ago

BladeRF

Add some Resources For BladeRF

7 months ago

 HackRF	Add some Resources For HackRF	7 months ago
 LimeSDR	Null	7 months ago
 PlutoSDR	Null	7 months ago
 RTL-SDR	Null	7 months ago
 USRP	Null	7 months ago
 README.md	Update README.md	13 days ago

README.md

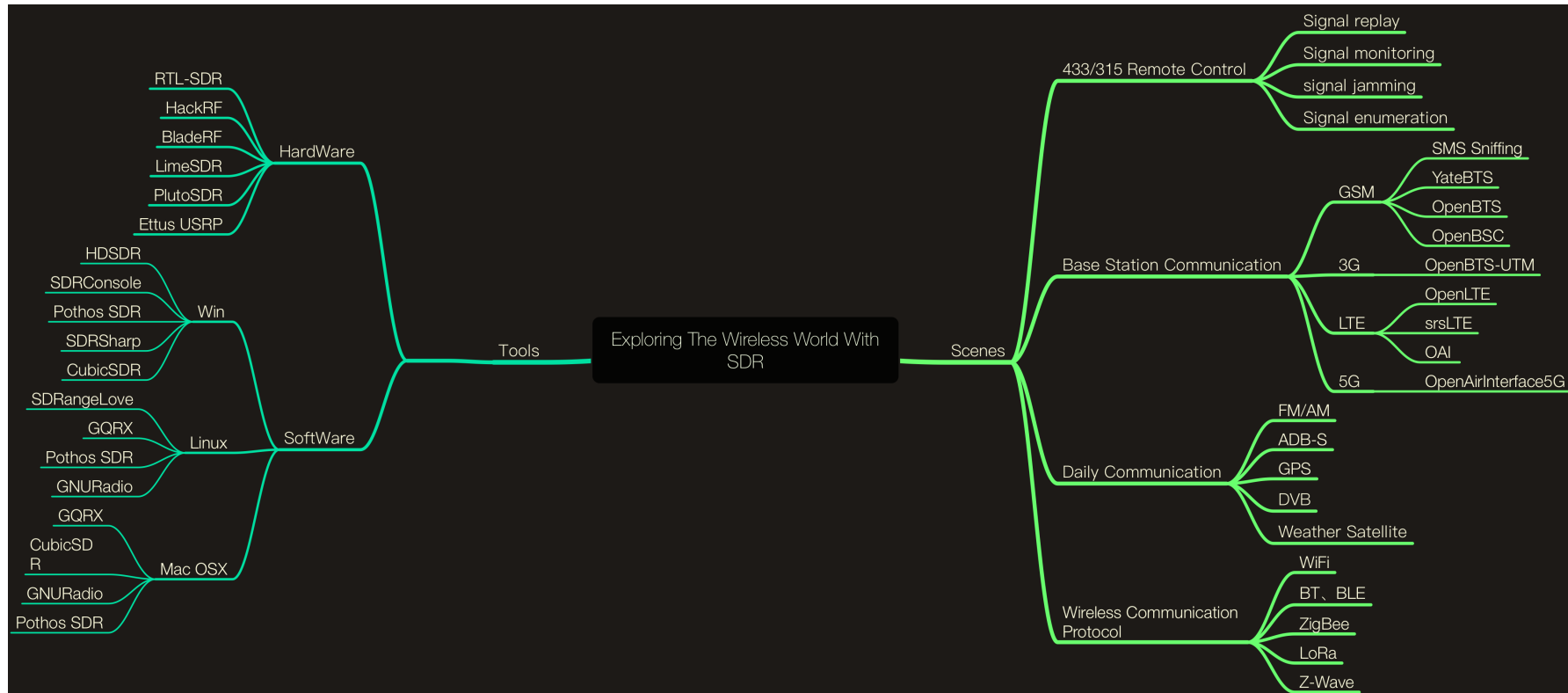
RFSec-ToolKit V 2.0

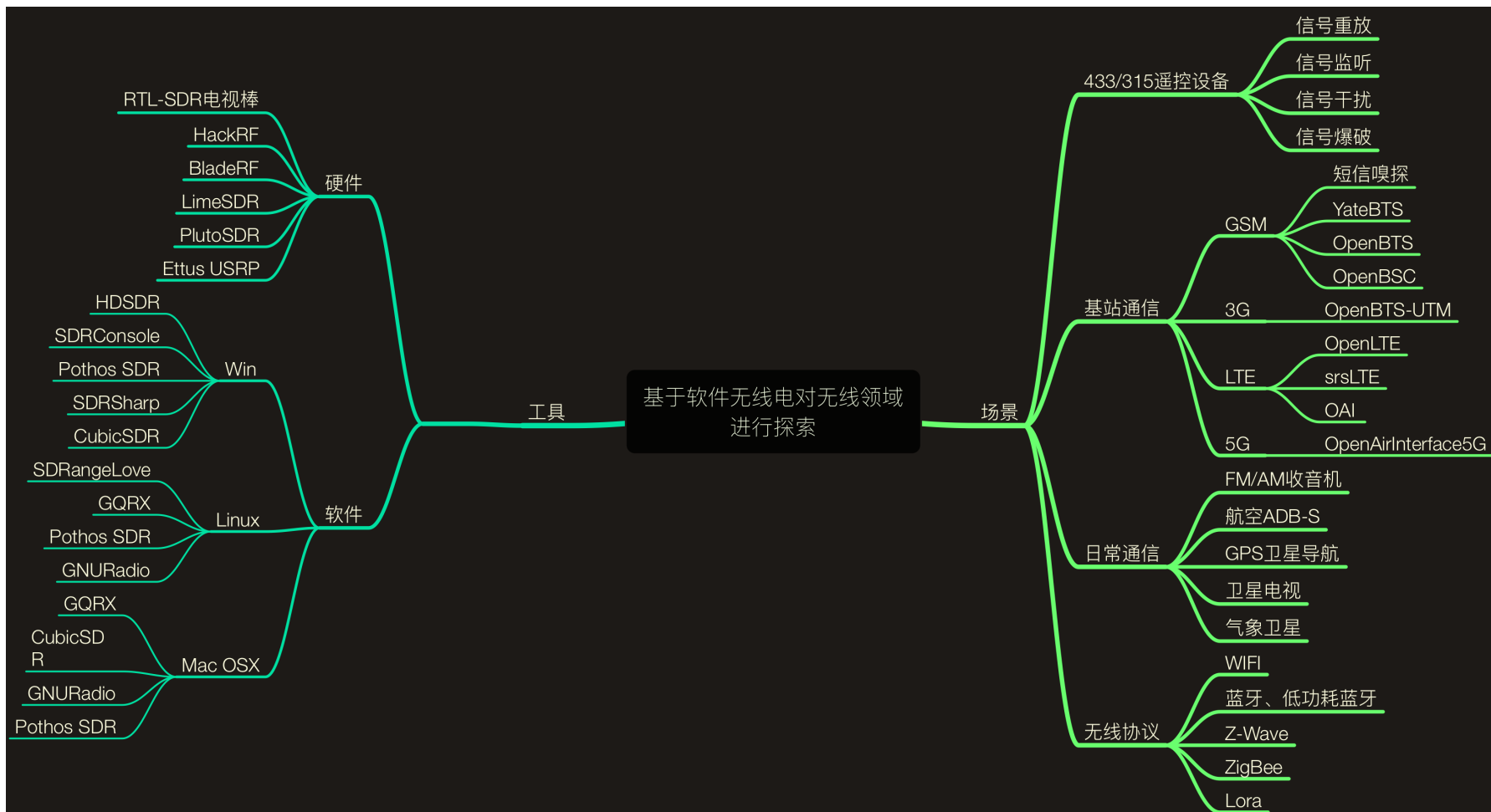
Project Description

RFSec-ToolKit is a collection of Radio Frequency Communication Protocol Hacktools which are from the github platform, and Hacking Tutorial from youtube、blog post, including SDR、2G GSM、3G 、4G LTE 、5G、NFC&RFID、ZigBee and so on.

What can we do with Software Defined Radio?

Some Cool things to do with SDR





Resources Collection by [雪碧 0xroot.com] (<https://cn0xroot.com>) [Twitter@cn0xroot](#)

SDR Resources

SDR-HardWare

RTL2832U:RTL-SDR is a very cheap software defined radio that uses a DVB-T TV tuner dongle based on the RTL2832U chipset.

HackRF:low cost software radio platform greatscottgadgets.com

BladeRF:bladeRF is a Software Defined Radio (SDR) platform designed to enable a community of hobbyists, and professionals to explore and experiment with the multidisciplinary facets of RF communication. [Nuand.com](https://nuand.com)

USRP: The USRP software defined radio products are designed for RF applications from DC to 6 GHz, including multiple antenna (MIMO) systems. ettus.com

LimeSDR:LimeSDR is a low cost, open source, apps-enabled software defined radio (SDR) platform that can be used to support just about any type of wireless communication standard.[Lime Microsystems](https://limesystems.org)

SDR-SoftWare

GQRX:Software defined radio receiver powered by GNU Radio and Qt

SDRSharp:Airspy is a popular, affordable SDR (software defined radio) based communication receiver with the highest performance and the smallest form factor. It is a serious alternative to both cost sensitive and higher end scanners while featuring the best radio browsing experience of the market thanks to the tight integration with the de facto standard SDR# software.[@airspy_com](https://airspy.com)

SDR_Console:SDR-Radio.com is a Windows console for Software Defined Radio (SDR) receivers and transceivers. Designed for the commercial, government, amateur radio and short-wave listener communities, the software provides a powerful interface for all SDR users. [Suport Hardware List](#)

HDSDR:HDSDR is a freeware Software Defined Radio (SDR) program for Microsoft Windows 2000/XP/Vista/7/8/8.1/10.

CubicSDR:Cross-Platform Software-Defined Radio Application

[sdrangel](#):SDR Rx/Tx software for Airspy, BladeRF, HackRF, LimeSDR, RTL-SDR, SDRplay RSP1 and FunCube

[shinysdr](#):Software-defined radio receiver application built on GNU Radio with a web-based UI and plugins. In development, usable but incomplete. Compatible with RTL-SDR.

[openwebrx](#):Open source, multi-user SDR receiver software with a web interface.

[luaradio](#):A lightweight, embeddable software-defined radio framework built on LuaJIT.

[qspectrumanalyzer](#):Spectrum analyzer for multiple SDR platforms (PyQtGraph based GUI for soapy_power, hackrf_sweep, rtl_power, rx_power and other backends)

[PandwaRF](#):PandwaRF: RF analysis tool with a sub-1 GHz wireless transceiver controlled by a smartphone.

[rpitx](#):RF transmitter for Raspberry Pi. rpitx is a radio transmitter for Raspberry Pi (B, B+, PI2, PI3 and PI zero) that transmits RF directly to GPIO. It can handle frequencies from 5 KHz up to 500 MHz.

[pifm](#):Turning the Raspberry Pi Into an FM Transmitter.

[rpidatv](#):Digital Television Transmitter on Raspberry Pi.rpidatv is a digital television transmitter for Raspberry Pi (B,B+,PI2,PI3,Pizero) which output directly to GPIO.

[PSDR](#):PortableSDR - A Stand Alone HF Software Defined Transciever.

[gr-cc11xx](#):GNU Radio OOT module for communicating with TI CC11xx based devices.

[spektrum](#):Spektrum is spectrum analyzer software for use with rtl-sdr.

[OpenUSRP](#):using LimeSDR to simulate USRP B210,OpenUSRP can using LimeSDR to simulate USRP B210 Device

[kalibrate-rtl](#):GSM frequency scanner and frequency offset calculator use with rtl-sdr devices

[kalibrate-hackrf](#):kalibrate for hackrf

[kalibrate-bladeRF](#):kalibrate for bladeRF

[GNURadio](#):GNU Radio is a Free & Open-Source Toolkit for Software Radio [GNURadio.org](#)

[Universal Radio Hacker](#): The Universal Radio Hacker is a software for investigating unknown wireless protocols

[gr-recipes](#):Main GNU Radio recipe repository for use with PyBOMBS

[gr-etccetera](#):This repository stores additional recipes for GNU Radio.

[RangeNetworks/dev](#):A collection of tools to make working with the numerous software components as painless as possible.

[OpenBTS](#):GSM+GPRS Radio Access Network Node

[YateBTS](#):YateBTS is a software implementation of a GSM/GPRS radio access network based on Yate and is compatible with both GSM/GPRS SS7 MAP and LTE IMS core networks integrated in our YateUCN unified core network server.

[OpenLTE](#): OpenLTE is an open source implementation of the 3GPP LTE specifications. The focus is on transmission and reception of the downlink.

[OpenBTS-UMTS](#):3G UMTS Data Radio Access Network Node

[Cellular Infrastructure](#):This is a group of Osmocom programs implementing cellular network infrastructure components for GSM, GPRS, EDGE, UMTS, HSPA, LTE and their associated interfaces and protocol stacks. [360 Unicorn Team's Demo](#)

[OpenBSC](#):This is a project aiming to create a Free Software, (A)GPL-licensed software implementations for the GSM/3GPP protocol stacks and elements.

[OsmoBTS](#):OsmoBTS is an Open Source GSM BTS (Base Transceiver Station) with A-bis/IP interface.

srsLTE:srsLTE is a free and open-source LTE library for SDR UE and eNodeB developed by SRS

srsUE:srsUE is a software radio LTE UE developed by SRS . It is written in C++ and builds upon the srsLTE library

srsGUI:srsGUI is a free and open-source graphics library for SDR using Qt and Qwt. The library provides a number of useful plots for graphing real and complex numbers.

IMDEA-OWL:OWL stands for Online Watcher of LTE. imdeaOWL is a free and open-source LTE control channel decoder developed by IMDEA Networks Institute and based on srsLTE, an LTE library for SDR UE and eNodeB developed by SRS

OpenAirInterface:The OpenAirInterface Software Alliance is a non-profit consortium to develop ecosystem for open source software/hardware development for the core network and both access network and user equipment (EUTRAN) of 3GPP cellular networks.

OpenAirInterface5G:Openairinterface 5G Wireless Implementation.

LTE Base Station Software:LTEENB allows to build a real 4G LTE base station (called an eNodeB) using a standard PC and a low cost software radio frontend. All the physical layer and protocol layer processing is done in real time inside the PC, so no dedicated LTE hardware is necessary. <https://www.amarisoft.com/products-lte-ue-ots-sdr-pcie/#software>

OsmocomBB: OsmocomBB is an Free Software / Open Source GSM Baseband software implementation. It intends to completely replace the need for a proprietary GSM baseband software.

gr-gsm:Gnuradio blocks and tools for receiving GSM transmissions

gr-lte:The gr-lte project is an Open Source Software Package which aims to provide a GNU Radio LTE Receiver to receive, synchronize and decode LTE signals.

LTE-Cell-Scanner:OpenCL, SDR, TDD/FDD LTE cell scanner, full stack from A/D samples to SIB ASN1 messages decoded in PDSCH, (optimized for RTL-SDR HACKRF and BladeRF board)

[gps-sdr-sim](#):GPS-SDR-SIM generates GPS baseband signal data streams, which can be converted to RF using software-defined radio (SDR) platforms, such as bladeRF, HackRF, and USRP.

[gr-fosphor](#):GNURadio block for spectrum visualization using GPU

[gr-nordic](#):GNU Radio module and Wireshark dissector for the Nordic Semiconductor nRF24L Enhanced Shockburst protocol.

[gr-lora](#):GNU Radio OOT module implementing the LoRa PHY

[gr-ieee802-11](#):IEEE 802.11 a/g/p transceiver for GNU Radio that is fitted for operation with Ettus N210s and B210s.

[gr-keyfob](#):Transceiver for Hella wireless car key fobs.

[gr-rds](#):FM RDS/TMC Transceiver

[gr-radar](#):GNU Radio Radar Toolbox

[gr-air-modes](#):gr-air-modes implements a software-defined radio receiver for Mode S transponder signals, including ADS-B reports from equipped aircraft.

[gr-ais](#):Automatic Information System decoder for shipborne position reporting for the Gnuradio project

[gr-dvbt](#):DVB-T implementation in gnuradio

[spectrum_painter](#):A tool to converts images to IQ streams that look like this when viewed in a waterfall plot.

[gr-paint](#):An OFDM Spectrum Painter for GNU Radio [Tutorial](#)

[gr-baz](#):Collection of new blocks for GNU Radio

Environment Build Tools

[HomeBrew](#):The missing package manager for macOS

[MacPort](#):The MacPorts Project is an open-source community initiative to design an easy-to-use system for compiling, installing, and upgrading either command-line

[Pybom](#):PyBOMBS (Python Build Overlay Managed Bundle System) is the new GNU Radio install management system for resolving dependencies and pulling in out-of-tree projects.

RFSignal Reverse Tools

[Audacity](#):Audacity® is free, open source, cross-platform audio software for multi-track recording and editing.

[Baudline](#):Baudline is a time-frequency browser designed for scientific visualization of the spectral domain. Signal analysis is performed by Fourier, correlation, and raster transforms that create colorful spectrograms with vibrant detail.

[Inspectrum](#):inspectrum is a tool for analysing captured signals, primarily from software-defined radio receivers.

[Dspectrum](#):Automated RF/SDR Signal Analysis [Reverse Engineering]

[rtl_433](#):Application using librtlsdr to decode the temperature from a wireless temperature sensor

[ooktools](#):On-off keying tools for your SD-arrR [leonjza.github.io](https://github.com/leonjza/ooktools)

YouTube Video Tutorial

Roberto Nóbrega: Michael Ossmann Software Defined Radio with HackRF)<https://www.youtube.com/user/liquen17/playlists>

Hardware Hacking By Samy Kamkar <https://www.youtube.com/user/s4myk>

Radio Hacking: Cars, Hardware, and more! - Samy Kamkar - AppSec California 2016 <https://www.youtube.com/watch?v=1RipwqJG50c>

GNURadio: GRCon [<https://www.youtube.com/channel/UCceoapZVEDCQ4s8y16M7Fng>]
(<https://www.youtube.com/channel/UCceoapZVEDCQ4s8y16M7Fng>)

Balint256:GNU Radio Tutorial Series、 Cyberspectrum<https://www.youtube.com/user/balint256>

Crazy Danish Hacker: <https://www.youtube.com/channel/UCIg0eyJTbAZaYuz3mhwfBBQ/playlists>

Ettusresearch <https://www.youtube.com/user/ettusresearch/feed>

Anders Brownworth Well Tempered HackerOpenBTS <https://www.youtube.com/playlist?list=PL892EE6BB9D10192F>

Gareth's SDR Tutorial <https://www.youtube.com/channel/UCYJO5ecRhbwARNcsDIFffPg>

Software Defined Radio Academy <https://www.youtube.com/channel/UC1GAlgAQrkjeeLmlkCB8pgQ>

雪碧 0xroot's SDR Hacking <https://www.youtube.com/channel/UCVc4stniRjRfOi1eY-0lj2Q>

26C3: Using OpenBSC for fuzzing of GSM handsets <https://www.youtube.com/watch?v=oGPOscdLPFQ>

27c3: SMS-o-Death <https://www.youtube.com/watch?v=J-IUL3E-uPc>

27c3: Wideband GSM Sniffing https://www.youtube.com/watch?v=fH_fXSr-FhU&feature=youtu.be 28c3: Introducing Osmo-GMR <https://www.youtube.com/watch?v=BSW-V94uZZQ&feature=youtu.be>

29C3: Further hacks on the Calypso platform <https://www.youtube.com/watch?v=xFjVcxMpA6c&feature=youtu.be>

[FOSDEM 2014] osmocom: Overview of our SDR projects <https://www.youtube.com/watch?v=hsKvdga2eQg&feature=youtu.be>

Sylvain Munaut: osmo-gmr: What's up with sat-phones ?https://www.youtube.com/watch?v=ROppOLeB6_I&feature=youtu.be

DeepSec 2010 OsmocomBB A tool for GSM protocol level security analysis of GSM networks <https://www.youtube.com/watch?v=9cBJV3yTaQo&feature=youtu.be>

DeepSec 2010: Targeted DOS Attack and various fun with GSM Um by Sylvain Munaut <https://www.youtube.com/watch?v=7tc4hD7ckZY&feature=youtu.be>

UnicornTeam of Ir0nSmith <http://v.qq.com/vplus/9427cc31bad2413591069f1800862a96>

Twitter&WEB Site

[@rtlsdrblog](#) RTL-SDR.com

[Wireless frequency bands](#): Frequency / Arfcn caculator for LTE, UMTS, GSM and CDMA, and Carrier Aggregation combination info

[@scateu](#) HackRF.NET

[@AndrewMohawk](#) andrewmohawk.com

[@bastibl](#) bastibl.net

[@csete](#) OZ9AEC Website

[@samykamkar](#) Samy Kamkar

[@cn0Xroot](#) cn0xroot.com spriteking.com

[@fairwaves](#) fairwaves

[@gareth__](#) Gareth codes

[@mpeg4codec](#) ICE9 Blog

@marcnewlin Marc Newlin

@drmpegW6RZ

@CrazyDaneHacker Crazy Danish Hacker

jxjputaoshuJiao Xianjun (BH1RXH)'s tech blog

@bastillenet Bastille

@embeddedsec

@RadioHacking

@elasticninja

@devnulling

@uber_security

@TresActon

@Kevin2600

@BE_Satcom

@lucasteske

@giorgiofox

@xdzou

@090h

[@rfspace](#)

[@mobios](#)

[@lambdaprog](#)

[Ruten.proteus](#)

NFC&RFID Resources

HardWare

[ProxMark3](#): The proxmark3 is a powerful general purpose RFID tool, the size of a deck of cards, designed to snoop, listen and emulate everything from Low Frequency (125kHz) to High Frequency (13.56MHz) tags.

[ACR122U](#):

SoftWare

[miguelbalboa/rfid](#): Arduino library for MFRC522 and other RFID RC522 based modules.

[RFIDIOT](#): python RFID / NFC library & tools

[RFIDler](#): RFIDler - Software defined RFID (LF) Reader/Writer/Emulator

Tutorial

[cn0xroot.com](#)

[FreeBuf.com](#)

BLE Resources

HardWare

Ubertooth: Ubertooth ships with a capable BLE (Bluetooth Smart) sniffer and can sniff some data from Basic Rate (BR) Bluetooth Classic connections.

TI CC2540: The CC2540 is a cost-effective, low-power, true system-on-chip (SoC) for Bluetooth low energy applications.

SoftWare

TI PACKET-SNIFFER: The SmartRF Packet Sniffer is a PC software application that can display and store radio packets captured by a listening RF device. The capture device is connected to the PC via USB. Various RF protocols are supported.
<http://www.ti.com/tool/packet-sniffer>

libbtbb: A Bluetooth baseband decoding library

crackle: crackle exploits a flaw in the BLE pairing process that allows an attacker to guess or very quickly brute force the TK (Temporary Key). With the TK and other data collected from the pairing process, the STK (Short Term Key) and later the LTK (Long Term Key) can be collected.

spectool: Spectools is a set of utilities for using various spectrum analyzer hardware. It supports the suite of Wi-Spy devices (original, 24x, 24x2, DBX, DBX2, 900, 24i) by Metageek LLC and the Ubertooth. Spectools includes userspace drivers for the hardware itself, a graphing UI built GTK and Cairo, network protocols for remote device capture, and simple utilities for developing additional tools.

spectool-web: A web viewer for WiSPY and Ubertooth spectrum data

gatttool : Get Started with Bluetooth Low Energy on Linux

[hctool](#):hctool is used to configure Bluetooth connections and send some special command to Bluetooth devices.

[BLE-Security](#):Bluetooth door hacking scripts that require Ubertooth or other devices to passively sniff.

[BLESuite](#): BLESuite is a Python package that provides an easier way to test Bluetooth Low Energy (BLE) device (By NCC Group)

[BLESuite-CLI](#):BLESuite_CLI is a command line tool to enable an easier way to test Bluetooth Low Energy (BLE) devices

[BLE-Replay](#):BLE-Replay is a Bluetooth Low Energy (BLE) peripheral assessment tool

[Blue-Hydra](#) Bluetooth device discovery service built on top of the bluez library. BlueHydra makes use of ubertooth where available and attempts to track both classic and low energy (LE) bluetooth devices over time.

[BTLEJuice](#):BtleJuice is a complete framework to perform Man-in-the-Middle attacks on Bluetooth Smart devices (also known as Bluetooth Low Energy).

[wireshark](#):Wireshark is the world's foremost and widely-used network protocol analyzer.

Tutorial

[BLE Hacking : ble scan and sniffer withu bertooth-one](#)

[Ubertooth – Bluetooth Sniffing Updated for 2014](#)

[Spectrum Tools and Ubertooth One](#)

[BLE Fun With Ubertooth: Sniffing Bluetooth Smart and Cracking Its Crypto](#)

[Ubertooth Spectrum Analysis \(Kali/Chromebook\)](#)

[Sniffing/logging your own Android Bluetooth traffic](#)

ZigBee Resources

SoftWare

[gr-ieee802-15-4](#): IEEE 802.15.4 ZigBee Transceiver

[SecBee](#): SecBee is a ZigBee security testing tool developed by Cognosec. The goal is to enable developers and security testers to test ZigBee implementations for security issues.

#Thanks

[Axiligator](#)

[@vileer_com](#)

