LOW POWER TO
THE PEOPLE

PROGRAMMING THE HARD WAY
LOW POWER TO THE PEOPLE

PROGRAMMING BLE THE HARD WAY

BY

HTTPS://MERIAC.COM

MILOSCH@MERIAC.COM

MILOSCH@MERIAC.COM
WHO AM I?

★ Love breaking things
★ Co-Founder of various open source and open hardware projects like OpenPCD.org, OpenBeacon.org where I designed the first open 13.56MHz hardware design.
★ RFID & Hardware Security Researcher (broke HID iClass security)
★ Enjoy designing secure ultra low power wireless sensors with privacy-enabled protocols and services.
★ In my private time I love making/grokking things. I am currently playing with RGB strips to create light paintings.
OPENPCD.ORG

★ Open Hardware and Open Firmware
★ ARM Cortex-M3 LPC134x - flashed via USB Mass Storage
★ Security Research Tool: boatload of test signals for Oscilloscope via two U.FL sockets
★ Compatible to LibNFC and MIFARE Classic cracking tools
★ See also RFID sniffer tools

PASSIVE RFID

13.56 MHz WITH NFC SUPPORT

OPENPCD.ORG

Fork me on GitHub
ACTIVE RFID TAG

REAL TIME CONFERENCE TRACKING

★ Started with tracking 1000 people at the CCC conference in Berlin in 2006
★ 2.4GHz + 8bit PIC microcontroller
★ Detects human interaction in real time
★ Open Hardware & Software
★ 960 wireless OpenBeacon 2.4GHz AC dimmers
★ per-floor wireless-toEthernet gateways
★ real time UDP protocol, each floor forwards only the data for its lights
★ one wireless packet per floor
★ Chaos Communication Protocol for resilient realtime animations
OTHER PROJECTS

If you have interesting projects or need my help - feel free to contact me at meriac.com
2.4GHz ISM
- 2402-2480 MHz
- 1 Mbps
- GFSK (modulation index 0.5)
- range between 30m to 150m

40 Channels
- 3 advertisement channels (2402, 2426, and 2480 MHz)
- 37 data channels with 2 MHz spacing

Simple
- 1 byte preamble 0xAA or 0x55
- 4 byte access address for target (0x8E89BED6 for advertisement channel)
- 2 to 29 byte Protocol Data Unit
- 3 byte CRC for PDU
- PDU & CRC whitened per channel

Bluetooth Low Energy

Bluetooth 4.0
OPENBEACON HARDWARE

LATEST HARDWARE

HARDWARE SPECIFICATION

★ Bluetooth Low Energy Protocol
★ 3D accelerometer for real-time movement detection
★ OpenBeacon proximity & tracking protocol
★ 8MB of external flash for offline-logging of tag-to-tag proximity encounters and movement
★ 32-bit ARM Cortex M0 CPU based on the nRF51822 SoC from Nordic Semiconductors
★ 256KB flash & 16KB SRAM
LATEST READER

★ BeagleBone Black Cape
★ Add precision RTC with CR2032 battery buffering
★ 3D accelerometer for theft detection
★ 2 nRF51822 Interfaces better reception (Diversity)
★ WIFI-Compatibility RPSMA antennas (5dBi)
★ 100 MBit Ethernet
★ WIFI Meshing planned
DEBUG ADAPTER

- Interfaces to JLink SQO/JTAG Debugger or nRF51-DK with integrated SWO debug interface
- Provides serial over USB serial interface for convenient printf debugging
- Spring loaded pogo pins for flashing a large number of tags
- Provides 3.3V power over USB
- Can act as a reader in combination with a tag
- Fastening clip for tags available
Development is possible on OS X, Linux (Fedora or Ubuntu). Development on Windows might work with Cygwin, but is not supported by our Makefiles.
The physical web beacon firmware allows advertising of URL’s - clients are available for IOS and Android. Due to Bare Metal Access to the radio interface, mischievous Bluetooth devices can be easily created. The first example in a series of upcoming devices allows the creation of an arbitrary amount of virtual BLE devices on the fly to confuse people scanning for their devices.
EXAMPLE CODE

★ Nice starter example - try modifying the URL in the example software.
★ Make sure to update the length field in the protocol header to reflect your new string length
★ Resulting firmware is around 4.7k - including C-library functions like printf
★ UART debug support
ADVANCED EXAMPLE

const char g_prefix_metric[] = "\n\0Aerotono\0Alcohol\0Alc\n\0Aniso\0Anthraco\0Anthra\n\0arsenal\0asbestos\0as";

(Contaminated Dromograph) (Brontoscopic Hemato) (Subtropic Ampullary)

(Malodized Nephrograph) (Dyslexic Hemacytometer) (Subterranean Elliptometro)

(Osteoblastic Chirograph) (Amphitelecenter) (Subtherapeutic Episcopes)

(Zoologic Episcopes) (Dyslexic Hemacytometer) (Subterranean Elliptometro)

(Atroscopic Dendrogram) (Dyslexic Hemacytometer) (Subterranean Elliptometro)

(Insipiameter) (Slippery Tricho-omid) (Subterranean Elliptometro)

(Teleautograph) (Rheumapping) (Subterranean Elliptometro)

(Geological Hemacytometer) (Glyceridemic Hemacytometer) (Subterranean Elliptometro)

(Carcinomatous Apheresiscope) (Comatose-oc-12-trene) (Subterranean Elliptometro)

(Miscorrelated Hectorgraph) (Clariomorphous Osmography) (Subterranean Elliptometro)

(Predigested Aeshmeter) (Subterranean Elliptometro) (Un-leren-liefen)

(Unidametric Elenograph) (Un-leren-liefen) (Un-lern-liefen)

\0Stoichio\0Subgeo\0Sym\n\0Thermo\0Tinto\0Titiri\0T"\n\0Ungeo\0Unhygro\0Un\0Unl

MISCHIEVOUS TAG

★ Shows chaining of hardware Events to allow low power
★ Radio initialisation and BLE advertisement state machine is just 259 lines of code
★ Simulates at any given time 23 concurrent BLE beacon with names that are constantly changing
★ To confuse people more, the names are made up on the fly from a word snippet database

ANNOY YOUR PEER GROUP
See OpenBeacon Tracker API Installation for setting up the server API and example code applications on your own server. Feel free to browse our git source code repository or download the source code as Unix tar.bz2 archive file or Windows ZIP file.
THANK YOU
FOR YOUR ATTENTION.

HTTP://WWW.OPENBEACON.ORG/