Open Hardware is game changer!

Open Hardware - documentation, schematic, gerbers, source available
If it’s not open hardware, open it and start hacking on it!
Overview

- wireless 2.4GHz keyboards with nRF24L01
- RTL-SDR as universal RF receiver
- IMS RF band: 315, 433, 868, 915 MHz
- IR receiving, analysis and sending
- some microcontroller choices
  - Arduino - AVR, 5V, ARM 3.3V
  - Bus Pirate - PIC, 1.8-5V
  - r0ket, Maple Leaf - ARM Cortex M3, 3.3V
  - Raspberry Pi, ARM, 3.3V
  - CubieBoard, ARM A10/A20, 3.3V, more pins
- other useful supporting hardware
  - USB microscope, solder station...
Wireless keyboards

http://blog.rot13.org/2012/12/is-wireless-keyboard-safe-for-your-passwords.html

Three basic types of RF connectivity

1. KeyKeriki v1.0 - 27 MHz
   http://www.remote-exploit.org/articles/keykeriki_v1_0_-_27mhz/index.html

2. KeyKeriki v2.0 – 2.4GHz - nRF24L01 - 1 or 2 Mbit/s
   http://www.remote-exploit.org/articles/keykeriki_v2_0_-_8211_2_4ghz/index.html

3. Ubertooth One - 2.4 GHz - Bluetooth
   http://greatscottgadgets.com/ubertoothone/

All somewhat complicated (KeyKeriki uses multiple radios), requires soldering or expensive kits

But seed of doubt is planted: are they secure?!

Most newer 2.4GHz (not bluetooth!) keyboards (with dongle) use nRF24L01
nRF24L01 - cheap module

http://arduino-info.wikispaces.com/nRF24L01-Mirf-Examples
http://www.ebay.com/itm/251044600998 - buy in pair!
Can we sniff with nRF24L01?

http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html
Arduino ping-pong

https://plus.google.com/u/0/115404771036822212816/posts/efMJQPTi2su
Open Logic Sniffer in the middle

http://github.com/jawi/ols.git  ols-0.9.7-RC1 self-compiled on Debian sid amd64 (Java librxtx is pain otherwise!)

http://saturn.ffzg.hr/rot13/index.cgi?open_logic_sniffer
nrf24L01_plus

**Dobrica Pavlinušić** Shared publicly Jul 20, 2013

I'm looking for #nRF24L01 #Arduino library for which I can specify number of bytes in address (so, no `#define` please!) Should I write another one?!

**Damjan Georgievski** Jul 20, 2013

Doesn't look as a big patch to make the address length an extra argument

https://github.com/kehribar/nrf24L01_plus/blob/master/nrf24.c#L69

**Dobrica Pavlinušić** Jul 21, 2013

True, but I also need much more low-level access because I'm porting [http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html](http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html) (and have no use for most of this library).

If I'm not mistaken I saw R0ket in Kika, so you might try [http://sarwiki.informatik.hu-berlin.de/R0ket_Keyboard_sniffer](http://sarwiki.informatik.hu-berlin.de/R0ket_Keyboard_sniffer) and let me know if it works because I'm basing my port on that code as opposed to combination of C and python which Travis did.

**Dobrica Pavlinušić** Jul 22, 2013

+**Damjan Georgievski** I read through source code of ntf24L01_plus and it really is nicest library I've seen so far. It's not Arduino API based, so I'm somewhat reluctant to base my solution on it (since part of the goal is to show how Arduino based code can be run on different platforms since I think that Arduino API is new standard for embedded development -- blog post about it is pending :-)

+**Damjan Georgievski**
First try: port r0ket sniffer to Arduino

- [http://www.pollin.de/shop/dt/ODE4OTgxOTk-/Bausaetze_Module/Module/Microcontroller_Experimentierplatine_r0ket.html](http://www.pollin.de/shop/dt/ODE4OTgxOTk-/Bausaetze_Module/Module/Microcontroller_Experimentierplatine_r0ket.html)
- [http://sarwiki.informatik.hu-berlin.de/R0ket_Keyboard_sniffer](http://sarwiki.informatik.hu-berlin.de/R0ket_Keyboard_sniffer)
- First encounter with porting Arduino SPI API
- **Utter failure. I can’t sniff a thing!**
- Code does work (somewhat) - there is hope in porting code from one architecture (ARM Cortex M3) to another (AVR)!
MSP430 based, have to solder it!
How about port to Arduino Uno?
It does support few AVR boards...
Arduino Internals by Dale Wheat
...read, read, hack, google, hack…
port to different AVR! (CPU freq)
luckily nRF24L01 is 5V tolerant!

http://git.rot13.org/?p=goodfet;a=shortlog;h=refs/heads/Arduino_Uno
Chicony KG-0609

http://saturn.ffzg.hr/rot13/index.cgi?chicony_kg_0609
http://git.rot13.org/?p=goodfet;a=shortlog;h=refs/heads/Arduino_Uno

dpavlin@blue:/blue-zfs/MSP430/goodfet/client$ ./goodfet.nrf sniffmacs | tee /dev/shm/keyboard
Holding autotune on 2402 MHz
sync,mac,r5,r6
'aa,bffffdea01,02,0f' looks valid 1  0.00094
'aa,bffffdea01,02,0f' looks valid 2  0.00187
'aa,bffffdea01,02,0f' looks valid 3  0.00143
'55,5fffffe500,02,0f' looks valid 1  0.00047
'55,5fffffe500,02,0f' looks valid 2  0.00084
'aa,bffffdea01,02,0f' looks valid 4  0.00154
'aa,bffffdea01,02,0f' looks valid 5  0.00182
'aa,bffffdea01,02,0f' looks valid 6  0.00202
'55,5fffffe500,02,0f' looks valid 3  0.00094

dpavlin@x200:/rest/cvs/goodfet/client$ ./goodfet.nrf tune aa,bffffdea01,02,0f

dpavlin@blue:/blue-zfs/MSP430/goodfet/client$ ./goodfet.nrf sniff
Listening as bffffdea01 on 2402 MHz
  cc  af  f7  bf  ff  1f  e0  19  54  3b  9f  2d  2d  c4  d4  1d  6a  96  d5  16  93  2a  95  b6  2b  74  d4  aa  85  72  91  41
  cc  ef  f7  bc  fe  7f  e0  19  46  c2  5e  b0  c2  5a  54  a5  4d  c2  d2  d5  99  dd  19  7a  aa  a5  85  4a  84  55  15
  cc  2f  f7  bd  42  5f  e0  19  4c  bf  be  dc  d5  69  ab  19  55  8e  95  4f  8f  66  ed  ac  a7  d2  b6  8d  d1  1b  8b  2a
  cc  6f  f7  a2  62  ff  e0  19  58  26  9e  32  25  20  82  0b  56  d5  12  54  3a  a6  bd  5f  7d  75  ed  fd  14  b2  4b  48
  cc  af  f7  a2  7f  9f  e0  19  5b  61  5d  bf  1a  62  50  b6  a9  14  b8  d9  d2  1a  52  11  0a  25  4d  aa  a8  dc  85  1a
  cc  ef  f7  bf  1d  9f  e0  19  53  1f  14  a5  14  54  c3  a2  14  d1  84  59  25  56  09  08  77  55  4a  22  ce  ad  56  91
@travisgoodspeed thanks for goodfet. I ported it to #Arduino Uno and sniffed my #Chicony KG-0609 with #nRF24l01 -
git.rot13.org/?p=goodfet;a=s...
12:57 PM - 10 Aug 13
Logitech - possible?

I guess so! Anybody want to try it out?
buy nRFL01

2pcs NRF24L01+ 2.4GHz Antenna Wireless Transceiver Module For Microcontr

http://www.ebay.com/itm/2pcs-NRF24L01-2-4GHz-Antenna-Wireless-Transceiver-Module-Microcontr-
/251044600998?pt=LH_DefaultDomain_0&hash=item3a736c9ca6

You will need two of them!

http://dx.com/p/upgraded-2-4ghz-nrf24l01-wireless-transceiver-module-for-arduino-black-147596
http://dx.com/p/2-4ghz-wireless-nrf24l01-module-150867
Arduino - API first!


- Arduino Uno - ATmega328
- Arduino Nano - ATmega328 - breadboard friendly
- Arduino Leonardo - ATmega32u4 - USB hacks!
- Arduino Mega - ATmega2560 - bigger, more IO
- Arduino Due - Atmel SAM3X8E ARM Cortex-M3
- Pinguino - PIC18 8-bit or PIC32 32-bit CPUs
- The Maple - STM32F103RB 72MHz ARM Cortex M3
- Energia - MSP430 16MHz board for under $10
- pcDuino - A10 1GHz ARM Cortex A8
- Papilio FPGA - Spartan 3 or 6 FPGA - AVR8 or ZPUino

Many more different boards with (some) API compatibility

5V vs 3.3V, some compatible with Arduino shield pinout
buy Arduino parts


- Solderless Breadboard with 400 Tie-Point
- Breadboard Jumper Wires
- Breadboard Jumper Wire Set
- DHT11 1-Wire Single Pin Thermometer/Hygrometer Module
- DS18B20 Programmable Resolution 1-Wire Digital Thermometer
- Arduino Compatible 1.6" Nokia 5110 LCD Module with Blue Backlit
nRF24L01 + Bus Pirate

http://www.seeedstudio.com/depot/bus-pirate-cable-p-932.html

- Bus Pirate v3.6 universal serial interface
- Different voltages (1.8V-5V from MCU power, sense) and protocols
  - UART, SPI, JTAG, I2C, SUMP logic analyzer (4K samples, <~1Mhz)
- Scripting mode to drive nRF24L01 from python script
  - [https://github.com/dpavlin/nRF24L01-buspirate](https://github.com/dpavlin/nRF24L01-buspirate)
  - My fork, reviewed by someone who knows python, hi Aka :-)
- Different modes have different pinout, take care when connecting!
  [http://dangerousprototypes.com/docs/Common_Bus_Pirate_cable_pinouts](http://dangerousprototypes.com/docs/Common_Bus_Pirate_cable_pinouts)
nRF24L01 + Raspberry Pi

nRF24L01 RF Transceiver

https://github.com/kehribar/nrf24L01_plus
http://arduino-for-beginners.blogspot.fr/2013/02/setup-nordic-nrf24l01-rf-modules-to.html

setup it as hub for your devices

Raspberry Pi is 3.3V device so don’t blindingly connect 5V Arduino sensors to it!
Level shifter comes to rescue:
http://www.ebay.com/itm/121032259497
there are models with less pins too!
RTL-SDR - NSND Osijek 2013


SDR receiver 8-bit, 2.4 MS/s, 24-1766 MHz

http://sdr.osmocom.org/trac/wiki/rtl-sdr

- good for IMS bands (433, 868 Mhz EU) or ADS-B (1090 Mhz) - with home-made antennas! All antennas are not equal!
- weather sensors, blinds, garage doors
What about sending IMS RF?

https://code.google.com/p/rfcat/

CC1111 (RF+MCU) vs CC1101 (RF only)
443 or 868 or 915 MHz - select one
Notice pin spacing! (2mm vs 2.54 mm)

Chronos AP dongle now in with MSP430F5509
and CC1101 so rfcat don’t work anymore!
http://saturn.ffzg.hr/arch/index.cgi?
msp430_chronos
Cheaper alternative for Arduino

- 315 or 434 MHz only, AM modulation
- buy pair - easier to debug and play with!
- [http://www.ebay.com/itm/251044600998](http://www.ebay.com/itm/251044600998)
- Separate sender and receiver module
USB IR Toy - easy IR hacking

http://dangerousprototypes.com/docs/USB_Infrared_Toy

You will need to upgrade PIC firmware first!
Can be used as SUMP IR analyzer
Record and playback IR codes with ease!
IR Arduino alternative

Requires more software tweaking than IR Toy


- you will need additional resistor for IR led!
Arduino Nano + 125KHz RFID

https://plus.google.com/115404771036822212816/posts/VPnpbJqn2xo

It was cheap sell-out component (5V serial)
USB Microscope
http://dx.com/p/s04-25-600x-usb-digital-photography-microscope-magnifier-w-8-led-white-light-grey-black-189450

Good for inspection
640*480 - don’t believe megapixels, has noticeable lag, zoom too high, this is only usable distance!
ERSA analogue soldering station, 80W

570 Kn, Nuškalo, temperature regulation fail > 500°C, burned tip!
Bitcoins in Mojo FPGA

Mining #bitcoins at rate of 35.79 MH/s using +Embedded Micro mojo #fpga board. It's slower than GPU, but fun to watch.

https://plus.google.com/115404771036822212816/posts/4sTk4DEHncH
http://saturn.ffzg.hr/rot13/index.cgi?mojo
CubieBoard
[Link to Google+ post]

2mm pins!
Seeking! Questions?

- Advice on board design (KiCAD? Fritzing?)
- Infrared microwave to convert into reflow oven [http://youtu.be/NCGzKDTFBSQ](http://youtu.be/NCGzKDTFBSQ) (and somebody who wants to have it at home :-)
- everything else I don’t have and don’t know that I need, please donate! I’m starting to learn soldering :-)
- buy me something from my [whishlist at ebay](https://www.ebay.com/)
- always buy more than one component (and pass rest of them to friends)
hardware hacking for software people

Dobrica Pavlinušić
http://blog.rot13.org/
FSEC 2013, Varaždin