ToorCon 14 Badge

The ToorCon 14 Badge is a sub-1 GHz wireless transceiver controlled directly from your computer. It uses the same radio circuit as the popular IM-Me. The radio functions that are possible by customizing IM-Me firmware are now at your fingertips when you attach the badge to a computer via USB.

The badge comes with RfCat firmware installed, courtesy of atlas. RfCat allows you to control the wireless transceiver from an interactive Python shell or your own program running on your computer. The badge also has CC Bootloader installed, so you can upgrade RFCat or install your own firmware without any additional programming hardware.

usage

Download and install RfCat from the repository or the latest repo snapshot.

Connect the ToorCon 14 Badge to your computer with a micro USB cable and execute 'rfcat -r'. This will start an interactive Python session you can use to explore and experiment with RfCat.

A fun first thing to try is 'd.specan()'.

upgrading firmware

The ToorCon 14 Badge comes with the latest RfCat firmware installed, but you can install new firmware if you would like to upgrade RfCat in the future or if you would like to write your own firmware.

The badge design is similar to the CC1111 EMK, affectionately known as "Don's Dongle" in the RfCat community since being popularized by Don Weber. To upgrade or modify the RfCat firmware on the badge, use the RfCatDonsCCBootloader hex file.

It is important to use a firmware image that has been linked properly for use with the bootloader. (Use RfCatDonsCCBootloader, not RfCatDons.) If you write your own firmware, you should take care to link in a similar way.

From the RfCat interactive shell, type 'd.bootloader()'. LED1 should illuminate and remain on, indicating that CC Bootloader is running. RfCat may complain that it lost connection to the device, and you may need to use ctrl-c followed by ctrl-d to break out of the shell.

Use bootload.py to interact with CC Bootloader. You'll need to 'erase_all' and then 'download' the new firmware.

The ToorCon 14 Badge features a GoodFET compatible programming connector that you can use to install or replace the bootloader if you like, but this is not recommended for normal use. There is also a row of test points that can be used with a spring pin adapter similar to the GIMME. I'll have one available for people to borrow at ToorCon 14.

open source

The ToorCon 14 badge consists of entirely open source hardware and software: hardware design files.

thank you

Thanks to atlas for RfCat. Thanks to Fergus Noble for CC Bootloader. Thanks to Adam Laurie for getting RfCat working with CC Bootloader and other RfCat contributions. Thanks to Hak5 and Microsoft for sponsoring the badge. Many thanks to ToorCon!