Cyberspectrum

Contents

The Bay Area SDR Meetup will serve as a forum to exchange knowledge and ideas related to Software Defined Radio (the software and hardware), and generally aim to get people excited about all the applications that can be realised with the technology. At each meetup, attendees will have the opportunity to present their work/ideas to the group.

Engineers, enthusiasts, hobbyists and people of all experience levels are welcome, no matter what your software/hardware background. Everyone is welcome to submit their ideas/presentations to the pool. For each meetup, a fixed number will be chosen to fit the format. Currently there will be a short show-and-tell section, followed by two 20 minute presentations (e.g. an introduction to an SDR topic and analysis of a mystery signal), and then to conclude a 40 minute in-depth presentation on an application. Suggestions/alterations to this format are welcome of course!

Meetup locations will alternate between the South Bay and San Francisco. Meetup presentations will be recorded and posted online (although you can opt out if you wish).

More Information and Upcoming Events: http://www.meetup.com/Cyberspectrum/

https://www.meetup.com/Cyberspectrum/about/

Live Stream: https://www.youtube.com/watch?v=DUGr_Z04SKs

- Kevin Reid (@switchborg): "A Visual Introduction to DSP for SDR"

A tour of DSP topics relevant to implementation of simple software-defined radios. Focuses on visual explanations of fundamental manipulations of digital signals, including analytic signals, frequency shifting, sampling rates, filtering, and the discrete Fourier transform. http://switchb.org/kpreid/

- @SigBlips: the 'baudline' signal analyser, and some interesting signals

Live Stream: https://www.youtube.com/watch?v=Tdn6LDeAdHo

- Nick Foster @bistromath

Satellite communications with GNU Radio, SDR hardware, homebrew antennas and satellite tracking.

- Josh Myer @xek

A couple months back, some friends and I captured a bunch of RF telemetry from a rocket launch down at Vandenburg AFB, down by LA. I'll talk about how we decided what to capture, what we captured, and how we analyzed the many, many gigabytes of RF that wound up on a hard disk that morning.

- Jonathon Pendlum @SDRJon

RFNoC (RF Network on Chip), a new framework for Ettus third generation devices (X300 & E300) that aims to make FPGA acceleration in SDRs more easily accessible. I will cover some background on FPGAs and their use in SDR, the motivation and design of RFNoC, and conclude with a few live demos.

Live Stream: https://www.youtube.com/watch?v=MFBkX4CNb08

- Julian Arnold (AKA Perpetual Intern of the Month, @broadcrap):

A discussion on creating a simple SDR Doppler RADAR, OR decoding WiFi[masked]a packets - which one will he choose!?

- Derek Kozel (@derekkozel):

"Digital modulation schemes such as Phase Shift Keying (PSK) convert data bits to analog signals for transmission. This mapping is known as a constellation. For simple schemes, optimal constellations can be calculated, but for higher-order modulation schemes with more points, it becomes very difficult to mathematically determine an optimal constellation. Evolutionary algorithms provide a simple and pragmatic way to find good answers without advanced knowledge of communications theory. This talk shows a start-to-finish implementation, including an introduction to digital signals and evolutionary algorithms."

- Alex Ray (@machinaut & Team Lunarnaut):

"We'll be talking about some of the radios, antennas and protocols we're working on as part of the just-started NASA Cube Quest Challenge, a competition to get high data rates to small satellites far away from the Earth.

Our team is still in the very early stages, but we've been building and testing antennas, as well as experimenting with modulation schemes. Along those lines, SDRs are great for out needs because we can be extremely flexible with protocols, bands, antennas, and more!

We'll show off what we've been working on so far, and can talk about what we plan on doing next."

Live Stream: https://www.youtube.com/watch?v=Iq07aQaB8mM

- Julian Arnold (@broadcrap) will talk in depth about building a Doppler RADAR with cantennas and SDR
- Ief Kox (@iefkox) will talk from the other side of the world about MultiPSK and use it to analyse all manner of interesting signals: ACARS (HFDL, VDL), STANAG 4285, ALE, AMTOR Navtex, Wefax, DGPS, SSTV and more!
- Jesus Molina (@verifythentrust) will present on "Wardriving in the age of the Internet of Things with SDR":

In this talk I will present information on how to discover and map radio devices utilizing SDR, and I will present a new concept: Warwatching (yeah, watching IoT devices in real time!). Round 10 years ago we drove around picking up wireless signals from WIFI access points. Tools like Kismet were used to collect relevant information, and the data was then post processed to draw heat maps. Then Google crashed the party with their ever present cars, and with increasingly pervasive dynamic AP (phone hotspots, drones) it doesn?t make much sense anyway.

But SDR opens a new world for us: Wardriving in ANY frequency range. The amount of devices equipped with radio transmitting capabilities have increased, and is time to create new tools for discovery and pentesting in the age of the IoT. With SDR we can detect, listen and interact with several ?static? radio devices (cell towers, FM stations, etc), and also we can ?see? dynamic short range devices (drones, Bluetooth) and even actually watch them using augmented reality!. I will provide a short demonstration and the road ahead.

Live Stream: https://www.youtube.com/watch?v=ZxiphlitrAQ

- Kevin Reid (@switchbord): "An Update to a Visual Introduction to DSP"
- Matt Ettus: "Synchronisation and MIMO demystified"

Beyond a single radio, there are multiple antenna systems, geographically separated systems, and all manner of multi-radio configurations in-between. Matt will talk about what is necessary to make these systems work, and the different levels of timing & synchronisation involved.

- Martin Braun (@braun_noise): "The SDR Mythbusters: Is #cyberspectrum hard to do?"

SDR has a reputation for being very difficult. Is this actually true? GNU Radio developer Martin Braun gives a tour through a typical development cycle and the tools GNU Radio provides to make development as smooth as possible.

This talk is geared mostly towards enthusiasts who are looking start their own GNU Radio development, and want to know exactly which resources are available.

Live Stream: https://www.youtube.com/watch?v=GYFalvzo-nk

- Harvind Samra (CTO and Co-Founder of Range Networks):

"OpenBTS: A Software-Defined Mobile Network"

The OpenBTS software is a Linux application that uses a software-defined radio to present a standard 3GPP air interface to user devices, while simultaneously presenting those devices as SIP endpoints to the Internet. This forms the basis of a new type of wireless network which promises to expand coverage to unserved and underserved markets while unleashing a platform for telecom innovation.

- Jason Abele:

"Software Defined Radio without the Radio, using GNU Radio and a sound card to develop a receiver for atomic time from WWVB"

We will talk a little about DIY VLF/LF antennas, the history of WWVB and atomic clocks, and demonstrate how to use GNU Radio to turn a cheap SDR rig into a very expensive clock.

Live Stream: https://www.youtube.com/watch?v=BoFOt9AUWuE

- Moritz Fischer: A quick show-and-tell preview into decoding DECT using GNU Radio
- Surya Satyavolu: RADAR-Guided Wirelessly-Controlled Automated Driving

Surya will cover the technical problems to be solved to realize automated driving. It will focus on achieving reliable lateral guidance using RADAR and hard-real time longitudinal control using wireless, as well as current advances in RADAR technology that would help in realizing the vision.

- Balint Seeber: Walk-through on creating a simple wireless video streaming system using a webcam & GNU Radio

Live Stream: https://www.youtube.com/watch?v=HsDpMffRafg

- Matt Reilly: "SoDaRadio - A General Purpose Transceiver"

http://sodaradio.sourceforge.net/Site/SoDaRadio.html

- Josh Myer: "Decoding Radio Data System (RDS) from FM broadcast stations"

...is a great introductory in-depth SDR project. Josh will walk through his implementation in IPython, starting with sample capture and ending with decoding some of the RDS protocol frames.

Josh lives in the radio noise mess that is San Francisco, and is currently working on data acquisition and signal processing for a biofeedback product. He?s also in the beginning stages of a few radio capture and direction finding projects. You can find more of his bite-sized radio projects at his SDR Snippets page: http://www.joshisanerd.com/projects/sdr_snippets/

Live Stream: https://www.youtube.com/watch?v=NBfBnPPcuJw

- Martin Braun's to-be-regular update on GNU Radio news
- Tom Tsou: "A Guided Tour of LTE on SDRs"

Tom will speak about LTE fundamentals, the many available stacks that can run with SDRs, what their capabilities are, and what the future holds. He will also do some live demos!

- Moritz Fischer: Decoding DECT with GNU Radio - update

Live Stream: https://www.youtube.com/watch?v=eebEKbdFL-g

- "Using SDR & GNU Radio in Radio Astronomy" by Richard Prestage, NRAO
- Tim O'Shea on some more cool GNU Radio hackery

http://oshearesearch.com/tag/lambda-blocks/

GNU Radio Lambda blocks are a simplification of pure-python blocks for GNU Radio which allow for writing a new block from within GRC with a simple python lambda expression. We'll demonstrate the great signal processing hackery that can achieved with the stream and message versions of this block!

- "PSK Modems in GNU Radio" by Kiran Karra

https://kirankarra.wordpress.com/2015/08/26/qpsk-burst-receiver-synchronization/

PSK Modems in GNU Radio have typically used tracking loops which take time to converge and do not leverage reference signals, through re-thinking the approach to PSK demodulation in a message and burst based context we demonstrate a robust new way to build modems!

- "Hacking an RF Shock Collar" by Tim K

GNU Radio is an awesome tool for reverse engineering, but people seem to get stuck somewhere between "Complex to Mag", Audacity, and MS Paint. It's not as hard to get packets out in "real time" as you might think. In this session, I'll build a transceiver from the ground up for the shock collar from DEFCON 23's Wireless Village.

Live Stream: https://www.youtube.com/watch?v=tG70c3Zadek

- "Etch-A-SDR" by Nate (@devnulling)

In this talk I will be doing a quick show and tell of building the 'Etch-A-SDR'. The 'Etch-A-SDR' is a digital Etch-a-Sketch, that doubles as a fully contained SDR platform.

I am a programmer by day, SDR Enthusiast / Hobbyist, Maker, and Amateur Radio operator by night.

- Spread spectrum SATCOM Hacking: Attacking the GlobalStar Simplex Data Service" by Colby Moore (@colbymoore)

Recently, there have been several highly publicized talks about satellite hacking. However, most only touch on the theoretical rather than demonstrate actual vulnerabilities and real world attack scenarios. This talk will demystify some of the technologies behind satellite communications and do what no one has done before - take the audience step-by-step from reverse engineering to exploitation of the GlobalStar simplex satcom protocol and demonstrate a full blown signals intelligence collection and spoofing capability. I will also demonstrate how an attacker might simulate critical conditions in satellite connected SCADA systems.

In recent years, Globalstar has gained popularity with the introduction of its consumer focused SPOT asset-tracking solutions. During the session, I'll deconstruct the transmitters used in these (and commercial) solutions and reveal design and implementation flaws that result in the ability to intercept, spoof, falsify, and intelligently jam communications. Due to design tradeoffs these vulnerabilities are realistically unpatchable and put millions of devices, critical infrastructure, emergency services, and high value assets at risk.

Colby Moore is Synack's Manager of Special Activities. He works on the oddball and difficult problems that no one else knows how to tackle and strives to embrace the attacker mindset during all engagements. He is a former employee of VRL and has identified countless 0-day vulnerabilities in embedded systems and major applications. In his spare time you will find him focusing on that sweet spot where hardware and software meet, usually resulting in very interesting consequences.

Live Stream: https://www.youtube.com/watch?v=1K6LUAZpaWg

- Marcus Leech from SBRAC: "An integrated proof-of-concept 'all-digital' feed for 21cm radio astronomy"

We show ongoing work in designing and building a proof-of-concept 'all digital' feed for 21cm radio astronomy experiments. While manyprofessional radio astronomy observatories are using "digitize at the feed" techniques, amateur experiments (and successes) in this areaare very close to non-existent.

Digitizing at the feed carries many advantages, including overall system gain stability, and the ability to carry signals over cheap ethernet-over-fiber links. We'll show an example feed arrangement that uses a differential radiometry approach, and does much of the initial processing right atthe feed, including radiometry and spectral calculations, sending summary data to an ordinary PC host over ethernet.

Challenges and pitfalls will be discussed.

- Tobias Zillner from Cognosec: "ZigBee Smart Homes - A Hacker's Open House"

ZigBee is one of the most widespread communication standards used in the Internet of Things and especially in the area of smart homes. If you have for example a smart light bulb at home, the chance is very high that you are actually using ZigBee by yourself. Popular lighting applications such as Philips Hue or Osram Lightify and also popular smart home systems such as SmartThings or Googles OnHub are based on ZigBee. New IoT devices have often very limited processing and energy resources. Therefore they are not capable of implementing well-known communication standards like Wifi. ZigBee is an open, public available alternative that enables wireless communication for such limited devices.

ZigBee provides also security services for key establishment, key transport, frame protection and device management that are based on established cryptographic algorithms. So a ZigBee home automation network with applied security is secure and the smart home communication is protected?

No, definitely not. Due to ?requirements? on interoperability and compatibility as well as the application of ancient security concepts it is possible to compromise ZigBee networks and take over control of all included devices. For example it is easily possible for an external to get control over every smart light bulb that supports the ZigBee Light Link profile. Also the initial key transport is done in an unsecured way. It is even required by the standard to support this weak key transport. On top of that another vulnerability allows third parties to request secret key material without any authentication and therefore takeover the whole network as well as all connected ZigBee devices. Together with shortfalls and limitations in the security caused by the manufacturers itself the risk to this last tier communication standard can be considered as highly critical.

This talk will provide an overview about the actual applied security measures in ZigBee, highlight the included weaknesses and show also practical exploitations of actual product vulnerabilities. Therefore new features in the ZigBee security testing tool SecBee will be demonstrated and made public available.

Live Stream: https://www.youtube.com/watch?v=eEMYA-nzATM

- "GNU Radio Update" (Martin Braun)

Martin is a long-time contributor to the GNU Radio project and the GNURadio community manager. Most of the stuff he touches is SDR-related,and his day job is writing software for Ettus Research, where he's spenta lot of time on RFNoC among other things.

- "A Hands-On Introduction to SDR with GNU Radio & USRP" (Neel Pandeya)

We begin a series of hands-on introductory SDR tutorials using USRP hardware and GNU Radio software on the Linux platform. In this first instalment, we review SDR concepts, explore the USRP hardware, walk through the installation of UHD and GNU Radio on an Ubuntu system, and construct and run a few basic flowgraphs to get familiar with GNU Radio.

Bring your laptop and SDR to follow along!

First installment of a new tutorial series!

In an effort to cater to all skill levels, we'll be running tutorials so everyone can get up to speed with the basics, and new tips and tricks. The goal is for everyone to enjoy SDR regardless of experience/hardware/software/etc...

- "Interrogating Passive, Wireless SAW RFID Sensors with the USRP" (James ?Trip? Humphries)

Passive, wireless sensor design typically dictates many strict performance requirements for the sensor interrogation system in terms of bandwidth, output power, and data capture rate. In the past, this implied that a custom interrogator design would need to be implemented, requiring considerable time and effort as well as being unable to adapt to new sensor requirements. This proves to be particularly challenging in a research environment where sensor specifications may change rapidly. Recent advances in commercial-off-the-shelf (COTS) software defined radio (SDR) platforms have enabled rapid interrogator development while being able to meet the strict requirements of passive, wireless RFID sensor tags.At the University of Central Florida, we have utilized the universal software radio peripheral (USRP) B200, from Ettus Research, to implement a pulsed interrogation system for wideband, wireless surface acoustic wave (SAW) RFID sensors. In this talk, we will discuss the implemented SDR system with consideration given to FPGA modifications, external RF component integration, and post-processing. The system operates at 915MHz with 56MHz bandwidth and has output power of greater than +20dBm. A demonstration of the system will also be given with wireless SAW temperature sensors.

Live Stream: https://www.youtube.com/watch?v=qxPv2bSli6o

- Paul David: "gr-minecraft"

Paul will show off a Minecraft hack where one can stand up Lua "computers" within the game and talk to the outside world through TCP or HTTP. This was used to create a Minecraft frequency display linked to GNU Radio where periodic magnitude values are sent from GNU Radio and reflected on a redstone frequency display within Minecraft.

The gr-minecraft idea was inspired by a similar project to control a Wi-Fi lightbulb from within Minecraft. It's a great illustration of how easy it is to get data in and out of GNU Radio, and a testament of the endless possibilities within Minecraft itself.

- Matt Knight: "Attacking ZigBee Locks with Commodity Wireless Tools"

ZigBee and[masked] are two widely proliferated wireless protocols that are commonly associated with the Internet of Things. This talk will delve into some of the practical aspects of attacking devices that utilize these protocols. In addition to presenting a live demo of a recently developed attack on a ZigBee lock, I will discuss the drawbacks of SDR-based tools and walk through a scenario where using a hardware-defined technology was advantageous.

- Marc Newlin: "MouseJack" (special remote appearance)

Marc will join us from Atlanta to discuss the keystroke injection vulnerability he discovered that affects seven vendors' wireless mouse dongles, allowing an attacker to transmit unencrypted keystrokes into a victim's computer.

Live Stream: https://www.youtube.com/watch?v=-JEv2Yq_sc8

- Martin Braun: "GNU Radio Community Update"

The latest news on all things GNU Radio.

- Kevin Reid: "An Audible Waterfall Plot"

AM receivers are useful for detecting a variety of signals (and noise sources) even when they are not deliberately amplitude modulated. It is possible to implement a non-selective AM receiver, one which receives signals in a very large input bandwidth. This has been done in hardware; the classic crystal radio is an example, but more advanced designs are also made for aviation radio enthusiasts. A further refinement allows the signals to be spatialized, producing a stereo audio output where the sound is panned according to the relative RF frequency of the input, thus creating an ?audible waterfall?.

- Paul David: "Adding Dual 10 Gigabit Ethernet Capability to the USRP X300"

The USRP X300 currently supports a single 1 or 10 Gigabit Ethernet connection to the host computer. In this talk, I will discuss the various design challenges in adding support for two simultaneous 10 Gigabit links, from the perspective of the FPGA, the UHD software driver, and different Ethernet cards, as well as give a brief demonstration showing the real-time monitoring of 400 MHz of instantaneous bandwidth to view WiFi and LTE signals over-the-air.

- Balint: "Couple of interesting experiments"

GNU Radio Spot Jammer FMCW RADAR analysis

Live Stream: https://www.youtube.com/watch?v=mgbepw3G-uo

- "GNU Radio Tutorial Part 2" with Neel Pandeya

The tutorial series will continue! This time we will look at how to construct an FM radio receiver, and decode the RDS digital subcarrier. This will include:

- Explain concepts behind commercial FM and RDS
- Receiving mono FM using a from-scratch flowgraph
- Showing how to build 'gr-rds'
- Demonstrate stereo FM+RDS reception using 'gr-rds'
- Building GQRX
- Demonstrate FM reception using GQRX

Make sure you bring along your laptop and SDR!

- "Understanding the LTE Physical Layer" with Sandor Szilvasi (@sszilvasi)

LTE is an incredible, yet complex, cellular networking standard. Sandor will break it down and explain how a LTE signal is constructed. He will also live demo the demodulation and decoding of local carriers.

- Interactive Install & Setup-fest" with the group

We would like to open up the forum to those who wish to get set up with SDR (hardware and/or software). Bring along your equipment, and as a group we can look at/debug the steps required to get you up and running. This could also include setting up an app, or fixing an Out-Of-Tree module, or even an environment issue on your laptop.

Live Stream: https://www.youtube.com/watch?v=c8MW7N2RxqU

- "The Land Mobile Radio Spectrum: What is out there, how it works, and how you can hear it" with Desmond Crisis (@dcrisis)

Wireless two-way is the technology that keeps the world working in sync. I'll explore the various public safety, private enterprise, and personal communications services from[masked] MHz. We?ll discuss the occupied spectrum, modulation bandwidths, trunked radio schemes and digital transmission modes currently in use on the band as well as what lies ahead. Bring your SDR kit and play along!

- An Academic Look at Interference & Jamming
- Installfest / Hackfest / Debugfest

Bring your laptops, SDRs and signals along, and we'll try to work on getting some cool projects running on your machines!

Have a module that's not quite working? Need help with implementing some code? This is the time to get help from the group!

Live Stream: https://www.youtube.com/watch?v=AL1kcy4e92w

- SlackRadio: Turning your Slack channel into a radio station" with Nate Temple

Slack is a popular real-time messaging system designed for team use. I will demo a small application built with GNU Radio and the Slack API that turns your Slack channel into a real radio station for your office.

- "Pothosware" with Josh Blum

Pothosware: An open-source software stack for the SDR community including the Pothos framework for creating interconnected topologies of processing blocks, Pothos GUI for graphical designing, controlling, and visualizing topologies, and SoapySDR - a SDR abstraction layer. The talk will present and overview of the software, cover the inner workings of the framework, and demonstrations with the GUI.

- FPGA-based ADS-B SDR Receiver with Brian Padalino

Brian will discuss the design and implementation of an ADS-B receiver in the FPGA over the BladeRF.

Live Stream: https://www.youtube.com/watch?v=L5iw_hpKhPE

- SDR Polyamory (Jared Boone, @sharebrained)

Jared discusses non-GNU Radio approaches to doing radio signal reverse engineering, prototyping, testing, and transmitting.

- SDR is hard, but installing GNU Radio is not -- Bootstrapping your bench with PyBOMBS and CGRAN" (Martin Braun, @braun_noise)

Want to get started with GNU Radio and SDR? Let's not worry about anything and use some tools that'll get you set up nearly automatically.I'll show you how to use PyBOMBS to get a setup running on most systems without effort -- even for cross-compile setups!In the second part, we'll talk about some of the more advanced features of PyBOMBS and how YOU can use it to distribute your work.

- "Disposable, Stealthy, Cheap SIGINT" (Chris Kuethe, @kj6gve)

This presentation covers some observations and considerations for using inexpensive and compact ARM boards for signals analysis. Topics may include: power budget, air interface, attributability, performance tuning, lolcats and doges.

- "Osmocom-GMR: Quick introduction to receiving the Thuraya and Mexsat satellite phone systems" (Sylvain 'tnt' Munaut, @tnt)

GMR-1 is an ETSI standard for satellite phones heavily derived fromGSM. The main/only commercial provider using this standard used to beThuraya, mainly used in the Middle-East and Asia and didn't provideany US coverage, but recently the Mexican government deployedMorelos-3 which carries a GMR-1 3G payload and can be received fromthe US. Osmocom-GMR is a free-software project from the Osmocom family toreceive and decode those signals, going all the way from RF to packetsin wireshark or audio files. This talk will be a quick introduction to GMR itself, the project and how to get

started using it.

Live Stream: https://www.youtube.com/watch?v=hPiUncCs6Lg

- ?L-Band WX Satellites? (Joe Steinmetz @usa_satcom)

This presentation will cover most aspects of receiving, demodulating and decoding current L-Band Weather Satellite signals (NOAA, MetOp, Meteor, FengYun, GOES). Topics will include hardware, software, de-modulation/decoding techniques, challenges, flows as well as cool sample images and data.

- "Disposable, Stealthy, Cheap SIGINT" (Chris Kuethe, @kj6gve)

This presentation covers some observations and considerations for using inexpensive and compact ARM boards for signals analysis. Topics may include: power budget, air interface, attributability, performance tuning, lolcats and doges.