# SCOPE

# THE PALOMAR AMATEUR RADIO CLUB NEWSLETTER

# Good News From PARS

I am writing to share some absolutely INCREDIBLE news with you.

Last night (August 5th 2014), the Poway City Council approved an amateur radio ordinance that allows a ham to erect up to a 65 ft high amateur radio antenna with just a building permit.

This is an incredible victory for amateur radio! For many of you who have followed this saga, for a City that has never allowed anyone, even the Federal Government, to erect anything over 35 ft, this is amazing!

Poway hams began the quest for this solution since 1999! Over the past three years, and recently with the assistance of the ARRL and an exceptionally gifted attorney Poway hams prevailed!

THANK YOU, THANK YOU, THANK YOU Here in Poway we are extremely grateful for the support we received from hams throughout San Diego County . Their attendance at the Council meetings gave clear indication to the Council members that this matter needed to be taken seriously. We Poway hams thank you for taking the time, even on a nice summer evening, to attend what had to be one of the longest meetings in history!

I must remind myself that we saw Democracy in action! It is like making sausage, but in the end, we got great bratwurst!

Again, thanks for your support!

73 de NN3V Charlie

# Come to the Faire

November 2nd 2014 PARC will participate in the Carlsbad Street Faire. Save the date and let Dennis KD6TUJ know if you are available to volunteer at the PARC booth.



# Save the Date

#### Club Meeting 3 September 2014

There will be a program.

#### **Board Meeting** 10 September 2014

Palomar Amateur Radio Club board meeting at 7:00pm at W6GNI QTH.

### **Club Events** 12-14 Sept 2014

ARRL Southwestern **Division Convention** see page 4

# Advertisements are free for members

Have items that need to find a new home? Advertise here! Send your ads to scope@palomararc.org

#### FOR SALE

Free. Telescoping Antenna Mast, 3 section @ about 10'. Escondido, 760-333-5599 Gilbert Warila

The Ham Radio Lunch Bunch meets Fridays for lunch and socializing at any one of a number of restaurants on a rotating schedule.

The Lunch Bunch signup is http://w0ni.com

Reminders are sent out on Wednesdays. All are welcome for food and fun!

Some of the restaurants on the schedule are Fuddruckers, UTC Food Court, Spices Thai, Savory Buffet, Denny's, Callahan's Pub and Grill, and Phil's BBQ.



[special] to our sponsors

# Please support our advertisers. Their support of the club is vital.





Astron, Drop in to see our display AEA, of working equipment. **OUTBACKER** Find out about Pkt location Larsen Antennas determining equipment TEN-TEC (APRS). Check our Hy-gain, Tri-EX, complete line of Cushcraft And Others magazines. ARRL books. t00 license manuals, and Numerous to Bulletin Board with all Mention! sorts of Goodies listed.

Directions: On 163, take Clairemont Mesa Blvd. off ramp to East. Stay in right-hand lane. Turn right at stoplight. As you are turning right you can see our beams in this shopping center. Travel 100 yds. On Kearny Villa Rd. and U-turn back to shopping area and HRO sign. Be sure to see our equipment in action on real antennas!

SCOPE page 3



Highlights

Testing

• Venders

• Swap meet

Π

• Tech Forums

Amateur Radio







#### The 2014 Convention is at the Sheraton Four Points San Diego 8110 Aero Dr.

Located on Aero Drive near the Montgomery Field airport which is the Same location of the 2010 Convention.

Ticket prices will be listed starting as "early bird", "pre-registration" and "door price." Please check for the upcoming dates. Our convention will feature tech forums, vendor's exhibits, on site radio station, grand banquet, flea market and many more activities. Check this site often to get the latest news regarding our ongoing convention events. We Plan to have over \$5000.00 in Prizes...



Main Prize ICOM IC-7600



Across 1. Rearrange races 6. Lentinula edodes 13. Eccentric 14. seeing with sound 15. Run off to the chapel 16. not UTC 17. Blemish 18. What politicians do. After the mudslinging. 19. diminuitive of mother in Northumbrian dialect 20. can't be satisfied 22. Central points 23. A highball drink made from gin or bourbon, half of a lime squeezed and dropped in the glass, and carbonated water. 24. Call on 25. A drying rack for laundry 26. Mainly Ca2SiO4 27. Tricky pitch 28. Abutment of an arch. Carries the entablature 29. Cavalry member 30. Frightening, but a variant spelling. 31. Anagram of a word for a clearing in a forest. 32. Decayed wood 33. Big mouths 34. Not an elevation. 38. "My man!" 39. All the collections of all the organisms in a region. 40. Halo, e.g. 41. The TSA ruined it. 43. Breathing problem 44. Put down 45. Started 46. Acceptances 47. Salad green



See page 8 for a report about amateur radio activities at DEFCON 22. Above is this year's event badge (the large white circuit card on the right) and on the left is a 3D printed medallion given to all who passed their Element 2 exam at the convention. It says DC22 /AT.

#### Down

- 1. Fragrant resin
- 2. Sage
- 3. Opposite of heats.
- 4. Keepin up
- 5. "The Catcher in the
- 6. Largest island in the Mediterranenan Sea
- 7. Ancient
- 8. "Cast Away" setting
- 9. "Sesame Street" watcher
- 10. Antipathy, hostility
- 11. An alloy of iron and nickel, found only in meterites on Earth.
- 12. Recluse
- 14. B-52
- 16. Ellsberg, Snowden
- 18. Pointless arguments. Like about code vs. no code.
- 21. Teed off
- 22. If you don't have this, coffee making is messy.
- 24. Took evasive action
- 25. Skin infection due to a fungus.
- 26. Really old word for an inflammatory swelling or sore
- 27. What some of us are making during the week.
- 28. De facto
- 29. Dance music from Pará, Brazil.
- 30. Covered with ash.
- 32. \_\_\_\_ of people at Dayton!
- 34. Colossal
- 35. Fencing action
- 36. Bailiwicks
- 37. Indian breads.
- 39. Breakfast staple
- 42. Athletic supporter?
- 43. "20/20" network

# User's Perspective of the Baofeng UV-5R

By Assi Friedman KK7KX/4X1KX August 12, 2014 The US market has been flooded by very cheap radios starting with the \$100 class Wouxuns, and more recently, the \$40 Baofengs. Many howto, performance review, and comparison articles have been written about them; this article attempts to evaluate the merits Boafeng UV-5R as a practical travel radio.

In June of 2014, my family embarked on a three-week vacation abroad. As a devout Ham, I wanted to take a handheld transceiver along in order to explore the airwaves as time allowed. Initially, I considered taking my very old Icom handheld transceiver, but I did not want to risk having it lost, stolen, or confiscated by customs or local officials along my journey. The Baofeng UV-5R, however, fit that bill perfectly. Coming in at less than \$40 – what can go wrong?

For the trip, I purchased a UV-5R, a USB cable programmer, and a 12V DC car charger from my favorite online retailer, named after a famous rain forest in South America. The radio comes with a drop-in charging tray and ear-piece style speakerphone. The radio, itself, is very small and feels surprisingly sturdy. It's obvious that Baofeng has been making commercial radios for a while. The belt clip is spring loaded and compared with some of my past radios – is very functional. I used it both on my belt (as intended) and on the strap of my backpack. In both cases, it held on securely.

The radio does not sport a direct DC power connection, and hence, it cannot charge the battery. The drop-in charger connects directly to the battery via three large, exposed tabs in the back of the battery. This poses two issues. First, you have to mind where you put the radio or risk shorting the tabs. If you're like me and like to toss the radio in the vehicle's cup holder, it may make contact with coins, keys, or anything else that may be there. One obvious solution is to cover the contacts with electrical tape, but that means they would need periodic cleaning to remove the adhesive residue. I did not notice any evidence of accidental shorting, but it's definitely something to keep in mind.

The second issue is that in order to charge the radio in a vehicle, you have to use the dropin base with the 12V cigarette adapter. My experience was that this does not work from a practical perspective. It's impossible to both find a convenient location for it and keep the radio in the drop in charger while driving without it tipping over. As a result, I reverted to keeping the charger at home and leaving every day with a full charge. If you plan on operating heavily, you better bring along a few more charged batteries.

The radio has just one knob – an integrated power switch and volume control. The audio comes out of an estimated 1" speaker. Audio quality is high-pitched, and comparing it side by side with my old Icom handheld – it leaves a lot to be desired.

The radio includes "bling," it includes an alarm and a flashlight feature. If you push and hold the call button, the bright white LED will flash on and off, the LCD display will flash orange, and the speaker will produce an alarm sound. I haven't figured out how that's useful – but it's there. The White LED also doubles as a flashlight. I found this handy at night if you leave the radio on the night stand.

The LCD display is functional, but I did find a few interesting "features." The S-meter graphic was fashioned after the cell phone signal strength indicator, only that it's not an S-Meter – it's a two- level squelch, on/off indicator.

The battery level indicator has three levels, but it didn't seem to respond linearly to battery life left.

Channels can be displayed as a frequency or a 7 character alpha numeric name. The radio had both A and B sides. The display mode for each side can only be frequency or alpha numeric for the entire side and cannot be intermingled. I found this to be a major functional annoyance.

The radio supports both VFO and memory modes like typical ham radios, but since it does not have second knob, all frequency/memory tuning is done via the keyboard. I did not find that very pleasing since pushing the Up/Down buttons is much slower and less comfortable than a rotary knob.

Configuring typical operating modes such as repeater shift, tone, and tone squelch is all done via the built in menu system. Getting in and out of the menu takes a minimum of 5 key strokes. To rapidly switch modes, this can get quite tedious.

Programming memory channels is the most counter intuitive procedure, and mastering it will take a number of failed attempts. The most practical approach to programing memory channels is to use the USB cable. I tried the Boafeng software unsuccessfully but did have good luck with CHIRP.

The scan rate in either VFO or memory modes is done at a rate of roughly two steps per second. Compared to typical radios, this is obscenely slow. For all intents and purposes, the scan mode is useless.

One feature that I was looking forward to is the broadcast FM receive mode. Sensitivity in broadcast mode is mediocre, but that's comparable to other radios and is sufficient to pick up local stations. One major annoyance is that while in broadcast mode, the radio will also monitor the A Side channel and switch over if the squelch is broken. After the first time this occurs, the radio will begin to ping pong between the broadcast and Side A channel repeatedly even if there is no activity on the Side A channel.

A feature that I like a radio to have is AM receive mode, which is fun, especially if air travel is involved. The Baofeng, however, does not support AM receive mode.

Overall, the radio was very disappointing as compared to main stream, handheld radios. It wasn't practical for band monitoring, scanning, or entering newly found repeaters. It is, however, small, light, and sturdy. If you intend to pre-program channels for your destination (using the cable), it won't let you down. If you lose it, you won't shed a tear. Personally, I plan to only use it for fixed channel operation, but for future travel, I will sport a main stream handheld radio.

Closing comments:

1) the manufacturer's User's Manual is useless, use the version authored by the "Radio Documentation Project".

2) Only purchase USB programming cables with FTDI chipset, and avoid Prolific chipsets at all costs.

3) CHIRP seems to work ok for programming the radio. Information, drivers, and software for all of the above is available at:

http://www.miklor.com/uv5r/



The Baofeng UV-5R, photos courtesy of The Internet

# Amateur Radio at DEFCON 22

By Michelle W5NYV. Amateur radio was prevalent at DEFCON 22, held in Las Vegas 7-10 August 2014. Two of the talks were about amateur radio, and a record-setting license exam session was held. Summaries of the talks follow.

Steganography in Commonly Used HF Radio Protocols Paul Drapeau PRINCIPAL SECURITY RESEARCHER, CONFER TECHNOLOGIES INC. Brent Dukes

Imagine having the capability to covertly send messages to an individual or a larger audience, without the need for large centralized infrastructure where your message could be observed, intercepted, or tampered with by oppressive governments or other third parties. We will discuss the opportunities and challenges with steganography implementations in widely used amateur radio digital modes, and present a proof of concept implementation of hiding messages within innocuous transmissions using the JT65 protocol. This technique could theoretically be used to implement a low cost, low infrastructure, covert, world wide short message broadcasting or point to point protocol. No messages in codes or ciphers intended to obscure the meaning thereof were actually transmitted over the amateur bands during the creation of this talk.

Paul Drapeau is currently the Principal Security Researcher for Confer Technologies Inc. He has held senior level IT security roles and consulted on information security topics for various organizations for over 15 years. Paul has a bachelor's degree in computer science from the University of Rhode Island and has been licensed as an amateur radio operator since 1986.

Brent Dukes has a decade of experience working in software and systems engineering roles. He spends his nights tied to various hardware hacking projects sitting in pieces all over his lab, and participating in CTFs. His idea of fun is reverse engineering and modifying toys and consumer electronics for the purposes of good. Brent has been a licensed amateur radio operator since 2006.

The second amateur radio related talk was about how RF fields can interrupt GFCIs. In some cases, RF can destroy them.

#### Girl... Fault-Interrupted.

Maggie Jaurequi SOFTWARE SECURITY TEST ENGINEER GFCI's (Ground Fault Circuit Interrupts) are a practically unnoticeable part of our daily lives, except maybe for when you have to fumble around with the Reset button on your hair dryer to get it to work, of course.

I discovered a way to completely melt (magic smoke demo included!) the GFCI mechanism for several off-the-shelf electro domestics wirelessly using specific RF frequencies. Similarly, I'm able to trip other GFCI's (the type built-in to several apartment/home walls) creating a DoS on running electro domestics.

Electro domestics might not be the worst this vulnerability has to offer, since GFCI's are used on many different types of electronics.

I plan on building a directional antenna to hopefully perform remote electro domestic DoS. I will list all vulnerable patents, my discovered vulnerable products, all applicable frequencies, and all affected switch types (such as AFCI's). I also commit to do responsible disclosure of any sensitive electrical attacks, such as RF interference for equipment upon

which people's lives or livelihoods may depend.

Maggie Jauregui (@MagsJauregui) LinkedIn: http://www.linkedin.com/ pub/maggie-jauregui/46/26a/358

The license exam session was held on Sunday, August 10th from 12:00pm - 3:00pm. In previous years, the session was walk-in with minimal wait. Usually a couple dozen people sat for the exam with no waiting. For a variety of reasons, in 2014, the response was greatly increased. The prevalence of amateur radio in the talks and the growing realization that amateur radio allowed for greatly increased opportunities to experiment and hack were obvious reasons, but in talking with the people in line, a diversity of reasons were revealed. Some people wanted to collect the credential as a status symbol. Some viewed it as a way to get an objective measure of their technical knowledge in wireless communications. Some wanted to be able to experiment with highpowered WIFI. Some wanted to explore topics raised by the Steganography talk. Many others had no specific reason for getting their license, other than it was cool, their friends had it, there was a community of people out there that "did radio" and they wanted to join. And finally, at least one person in line was there because his mother (me!) made him take the exam that weekend. That person was Michael Easton.

At 13, this was Michael's first trip to DEFCON. My first trip was DEFCON 2, in 1994. Now it its 22nd year, the computer security conference has grown from a single-tracked punk no-one-givestheir-real-name party where the hotel phone system and elevator controls were routinely vandalized, into an epic multilayered sponsored celebration of all hackable things, with people standing in line for 3 hours to take a test that inserts their real name and address into an FCC database.

For DEFCON 2, you were lucky to be given a laminated badge. For DEFCON 22, your badge had a processor, a port, LEDs, and could be hacked to do all sorts of amazing things (photo pg 5). Over the past several years, competitions to hack the badges and make them do cool tricks has resulted in badges that flew dirigibles in the main hall that followed the loudest noise, badges that measured radiation to provide truly random numbers over wireless links, and badges that were expanded with screens and speakers to provide visual and auditory entertainment suitable for Las Vegas tastes.

For DEFCON 2, there were t-shirts available. For DEFCON 22, there were t-shirts, bags, notebooks, lab coats, work shirts, and a large vendor area with dozens of people and companies selling all sorts of goodies, ranging from lockpicks to software defined radio cards.

For DEFCON 2, you had amazing comraderie. For DEFCON22, you had... amazing comraderie! It's not common that an annual event can evolve so dramatically yet still have the same spirit, but DEFCON is one of those events that has not only kept the spark alive, it's grown the spark into a fire.

The room for the amateur radio exam served as the Cryptography Village during the other days of the convention. Villages at DEFCON are subject-specific areas where people can get hands-on experience. Lockpick Village, Hardware Hacking Village, Wireless Village, and Cryptography Village were some of the villages in 2014. Below is a video of the lengthy line.



With a bit of assistance, Michael obtained his FRN, filled out his Form 605, paid his \$15 to the ARRL test team (http://conham.org) and joined the line at 11:45am. It took about 2 hours to get into the test room, with batches of people steadily going in to the exam room, and a good number of newly minted hams steadily coming out. Each successful examinee received a 3D printed ornament for their convention badge lanyard, and had their CSCE in hand. People in line enthusiastically congratulated the successful and commiserated with those that didn't quite make it. After a long 30 minutes, Michael emerged, crestfallen. He'd missed passing by two guestions. He had one chance to retake it, and decided to go for it. After another long 30 minutes, at almost 3pm, he emerged triumphant, solidly passing his Element 2. His mom couldn't be prouder. After all, he's now a fourth-generation ham. At 205 candidates, he was also part of the largest test session to date, beating the rumored record of 202 set at Davton Hamvention.

## Club Email Discussion and Announcement Lists

by Michelle W5NYV

f

PARC has two email lists. The two lists offer additional ways to stay up to date with your fellow amateur radio operators. Signing up is very simple.

Go to http://www.palomararc.org/mailman/listinfo

Click the link corresponding to the list you want to sign up for.

Fill in the form, and you're on the list.

PARC-Announce is a very low-traffic mailing list for announcements approved by the club. Expect only a few messages per month, maximum, including a notice about each club meeting. If you have an announcement you'd like to have published to this mailing list, please send your request to

board@palomararc.org for approval

PARC-Talk is an open list for PARC members to discuss anything related to amateur radio and to the club. Please post in plain text. Don't attach files.

We will not use Scope-notice, Scope-pdf, Meeting-remind or any other mailing list for unsolicited messages or announcements.

Don't forget - PARC is on Facebook too!

Find us at https://www.facebook.com/groups/194674987710/

Palomar Amateur Radio Club





It is not too early to start thinking about who will serve as the President for the next year. Dennis will not be available due to health concerns expressed by his wife. (Longevity will be severely shortened if he continues.) Please consider who can serve.

Q

## Palomar Amateur Radio Club Annual Auction

Always in October!

Bring your tired items, your can't-get-round-to-its, your duplicates, your what-is-its.

They get a new home, and you get some cold cash.

1 October 2014 at 7:00pm

SCOPE P.O. Box 73 Vista, CA 92085-0073

Return service requested

Scope Volume # 46, Issue # 6 (USPS #076530) is published monthly by the Palomar Amateur Radio Club 1651 Mesa Verde Drive, Vista, CA 92084.

POSTMASTER: Send address changes to SCOPE, P.O. Box 73, Vista, CA 92085. Periodicals postage paid at Vista, CA 92084 and at additional mailing offices. Dues are \$20 per year or \$35 per year for a family. Dues include a subscription to Scope.

You can join or renew your membership on the club's web site http://www.palomararc.org

Editor: Michelle Thompson W5NYV Submissions: scope@palomararc.org Questions? Ideas? Comments? W6NWG@amsat.org

#### **Featured Program:**

At 7:30pm on 3 September 2014, Palomar Amateur Radio Club will present a program.

We look forward to seeing you at the Carlsbad Safety Center, 2560 Orion Way, Carlsbad, CA.

Sign up for the PARC Email Lists:

http://www.palomararc.org/mailman/listinfo