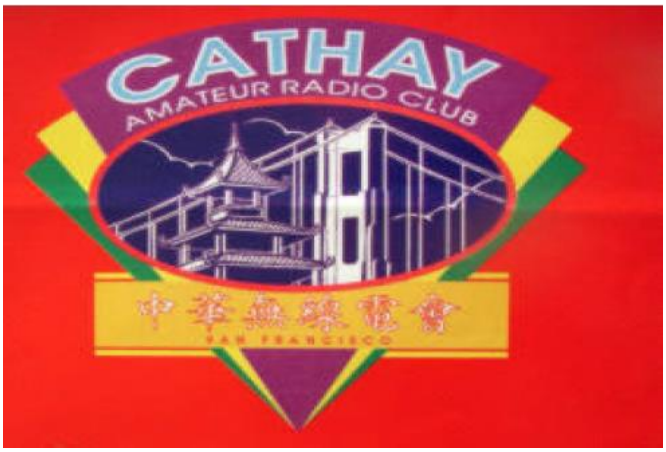

Cathay April 2016

www.cathayradio.org

President: George Chong, W6BUR **email:** *W6BUR@comcast.net*

Vice President North: Leonard Tom, *NX6E* **email:** nx6e@hotmail.com

Vice President South: Bill Fong, *W6BBA* - **email:** w6bba@arrl.net

Secretary/Membership: Rodney Yee, *KJ6DZI* - **email:** rodyee2000@yahoo.com

Editor: Rodney Yee, *KJ6DZI* - **email:** rodyee2000@yahoo.com

Treasurer: Vince Chinn aka Mingie, *W6EE* - **email:** vince@vincechinncpa.com

Web Master: Edison Fong – *WB6IQN* - **email:** edison_fong@hotmail.com

Mission: The Cathay Amateur Radio Club is basically an active social club of Ham Radio Operators and their spouses. We support local community requests for HAM emergency communications. Several of us are trained in CPR/ First Aid and are involved with community disaster preparedness.

Monday Night Net Time: 9 PM Local Time/PST, Frequencies: 146.67MHz -600KHz PL85.4 and 442.70 +5MHz PL 173.8. The repeaters are linked only during the CARC Monday night net.

Update: Link to repeater 442.70 is currently not active until further notice.

The CARC Monday night net is the best way to find out the latest club news.

All check-ins are welcome.

Message from the President: George Chong, *W6BUR*

Hello CARC Members and Friends;

With the presidential race going on and with income tax season we have a lot of additional distractions in our daily lives.

I wish to thank our CARC members that set aside their valuable time to participate in our Monday night's nets.

Tech Article Introduction

This month's article deals with the FBI's on going investigation of the San Bernardino Shooter's Apple iPhone.

The overall public sentiment was in favor of Apple cooperating with the FBI to have complete access to the shooter's Apple iPhone 5c even in the light of the successful 3rd party hack of the iPhone 5c.

What is surprising is how public the issue has become. I would assume it would have been quietly handled behind the scenes with Apple and that the phone would have been completely unlocked.

Apple is very acutely aware their whole business model of Apple Pay on the iPhone as a completely secure branded electronic wallet is being undermined with the proposed government hacking.

Although the Apple iPhone is at the center of the controversy of government access vs privacy, the eventual outcome will have a much wider implication that will extend all to all other mobile communications devices/platforms (ie: Blackberry, Android to just name a few).

Now that I have piqued your interest, please read the full tech article.

CARC Final Wrap-up News

Chat sub s'em to all you CARC members! - George W6BUR.

Public Service Announcements

HAM CRAM / HAM Licensing

For upcoming HAM Licensing locations please refer to:
http://www.arrl.org/find-an-amateur-radio-license-exam-session

Auxiliary Communications Service (ACS)

The Auxiliary Communications Service (ACS) was organized by the San Francisco Office of Emergency Services (OES) following the 1989 Loma Prieta Earthquake to support the communications needs of the City and County of San Francisco when responding to emergencies and special events.

The Auxiliary Communications Service holds General Meetings on the third Tuesday of each month at the San Francisco Emergency Operations Center, 1011 Turk Street (between Gough Street and Laguna Street), from 1900 hours to 2100 hours local time. All interested persons are welcome to attend.

The ACS Net begins at 1930 hours (7:30 p.m.) local time each Thursday evening, on the WA6GG repeater at 442.050 MHz, positive offset, tone 127.3 Hz. The purpose of this net is to practice Net Control skills, practice checking in with deployment status in a formal net, and to share information regarding upcoming ACS events. Guests are welcome to check in. ACS Members should perform Net Control duty on a regular basis. On the second Thursday of each month, the net will be conducted on the output frequency of the WA6GG repeater, 442.050 MHz no offset, tone 127.3 Hz, simplex.

For more information, please attend an ACS meeting or check in on a net, or call 415-558-2717.

Upcoming meetings: Tuesday 7pm, Apr 19, 2016
Tuesday 7pm, May 17, 2016
Tuesday 7pm, Jun 21, 2016
Tuesday 7pm, July 19, 2016

Gilbert Gin (KJ6HKD)

Free Disaster Preparedness Classes In Oakland:
http://www.oaklandnet.com/fire/core/index2.html

CORE is a free training program for individuals, neighborhood groups and community-based organizations in Oakland. The underlying premise is that a major disaster will overwhelm first responders, leaving many citizens on their own for the first 72 hours or longer after the emergency.

If you have questions about the recertification process, you may contact the CORE Coordinator

at 510-238-6351 or core@oaklandnet.com.

Free Disaster Preparedness Classes In San Francisco – NERT Taught by San Francisco Fire Department (SFFD)

Upcoming events

April 2016

2 Neighborhood Command Operations II (Prerequisite NCPI)
5 Staging area command post set up & operations
17 8:30 – 3pm NERT Citywide Drill (Sunday), Marina Green

May 2016 – Sept 2016 (TBD)

October 2016

7-9 Fleet Week Humanitarian Village; NERT Outreach/Education booth. 9:00a-3:00pm, Marina Green near Scott St.
15th: Save the Date! NERT drill

RSVP to sffdnert@sfgov.org or call 415-970-2024 to register.

Visit ***www.sfgov.org/sffdnert*** to learn more about the training, other locations, and register on line. Upcoming Special NERT Events.

San Francisco Police Department: Auxiliary Law Enforcement Response Team (ALERT)

The Auxiliary Law Enforcement Response Team (ALERT) is a citizen disaster preparedness program designed. The ALERT program is for volunteers 16 years of age or older, who live, work, or attend high school in San Francisco.

Graduates of the San Francisco Police Activities League (P.A.L) Law Enforcement Cadet Academy are also eligible to join.

ALERT volunteers will first complete the Fire Department's Neighborhood Emergency Response Team (NERT) (www.sfgov.org/sfnert) training and then graduate into an 8 hour Police Department course specifically designed for ALERT team members.

ALERT members will work closely with full-time and/or Reserve Police Officers in the event they are deployed after a disaster. The Basic ALERT volunteer will have no law enforcement powers other than those available to all citizens.

SFPD ALERT Training

The next ALERT training classes have been scheduled for Saturday June 18, 2016. The class will be held at the San Francisco Police Academy, in the parking lot bungalow, from 8am-5pm (one hour lunch break).

IMPORTANT- All participants must complete the background interview process in order to be eligible to attend the ALERT training class.

Eligible ALERT participants may register for a training class by contacting the ALERT Program Coordinator, Mark Hernandez, at sfpdalert@sfgov.org, or by telephone at 415-401-4615.

SFPD ALERT Practice/Training Drill

All active/trained ALERT members are asked to join us for our next training drill, scheduled for Saturday May 7, 2016 9AM – 1PM. Details will be emailed to active ALERT members, prior to the date of the exercise. Participation is not required, but strongly encouraged.

For more information on the San Francisco Police Department ALERT Program, email us at sfpdalert@sfgov.org, or call Sergeant Mark Hernandez (SFPD, Ret.), SFPD ALERT Program Coordinator, at (415) 401-4615.

For additional information on the web please refer to:
http://sf-police.org/index.aspx?page=4019

Tech Article

Hacking into the San Bernardino Shooter's iPhone

4/1/2016
Rodney Yee

Splash across the news headlines was the FBI inability to retrieve information from the San Bernardino Shooter's iPhone 5c running the iOS9.

The shooter, Mr. Syed Rizwan Farook 's phone is actually the property of his employer: San Bernardino Department of Public Health.

Apparently Mr. Farook had activated an Apple software password lock and data encryption feature that prevents access to the iPhone without the proper pass code. If the wrong pass code is entered 10 times consecutively, the phone will erase all the data contained in the iPhone 5c thus stopping any further investigation on the iPhone.

Most people assumed that Apple would assist the FBI in the criminal investigation by using a backdoor pass code to simply unlocking the iPhone and give it back to the FBI. The only problem with this assumption was that with Apple's goal of providing enhanced iPhone security; Apple did not build in such backdoor with the current security software installed with iOS9 on the iPhone 5c.

Once the FBI was made aware that no backdoor pass code existed and Apple's refusal to hack the iPhone 5c in question, a court order was submitted to Apple.

Now this is where things get very interesting with FBI's battle with Apple. The FBI instigated a Federal Court order that wants much more than merely unlocking the iPhone and handing it over to the FBI. The court order wants Apple do the following:

- Create a custom firmware that resides in RAM memory / updating the BIOS.
- The custom Firmware will only load on the targeted phone
- Bypass the limit of 10 consecutive incorrect passwords limitation
- Remove time delays between entering incorrect passwords
- A software/hardware interface for brut force automating entering of passwords

For more information see the below link:

http://blog.trailofbits.com/2016/02/17/apple-can-comply-with-the-fbi-court-order

On March 29, 2016 the FBI announced with help from an unnamed third party, the iPhone 5 used by Mr. Farook has been successfully hacked and the data has been retrieved. The FBI has withdrawn the Federal court order forcing Apple to comply with unlocking Mr. Farook's iPhone. Just who did the hack and how it was performed on the Apple iPhone is the subject of much speculation and has not been made public.

Well it appears that the big argument between the FBI and Apple is now over for the time being. However in reality it is just the opening salvo between the US Government's wanting to access encrypted information on all mobile communication devices.

Back on March 1, 2016 FBI Director James Comey testifying under oath before the House Judiciary Committee in Washington DC; stated there are several investigative cases pending (Local, State and Federal) that would want to gain access to encrypted Apple iPhones.

The implication is that the flood gates would be open to further hack request from authorities on all Apple iPhone and perhaps all other mobile communication devices.

FBI Director Comey also acknowledged unlike the iPhone 5c that Apple's latest iPhone 6 has security built into the hardware such that there would be no way for law enforcement to "pick the lock" on the iPhone 6 models because there is no door to open.

The irony of this access situation is that current Apple iPhone users could simply switch over to several free 3rd party software vendors to encrypt their data with a built in self destruction mode thus potentially rendering all Apple Hack useless. More information on that can be found at: http://betanews.com/2016/03/16/iphone-backdoor-is-useless/

In the long term any iPhone hack provided by either Apple or unnamed third parties may be rendered useless with the advancement of new hardware, alternate mobile platforms/devices, new/enhanced operating systems, and advanced 3rd party encryption software. Also in question is that the current Apple hack would apply to any other current brands of mobiles devices.

In response to the current successful hack of the Apple iPhone 5c, Apple has announced that it is committed to closing up any loop holes to prevent future hacks. Of course Apple needs to know exactly how the hack was done but the FBI is not talking …. what a twist of fate! The current speculation is that the iPhone 5c hack allowed an unlimited number of guesses on the password which eventually lead to the phone being unlocked.

Now that a hack was publicly shown to be possible on the Apple iPhone 5c, cyber criminals will be embolden to replicate and expand the scope of the hack for their illegal activities.

This set of unusual circumstances suggests that Congress would need to pass a law that all smart phone companies and 3rd party vendors provide a secure backdoor into smart phones to bypass security. This action would put all smart phones at a security risk and would be nearly impossible to enforce.

When Bill Gates founder of Microsoft was asked about his opinion on the conflict between Apple and the US government below is reply:

http://money.cnn.com/2016/03/08/technology/bill-gates-reddit-ama/index.html?iid=ob_article_hotListpool&iid=obnetwork

Question: What's your take on the recent FBI/Apple situation? What would you do if you were Apple?

Reply: There needs to be a discussion about when the government should be able to gather information.

I think very few people take the extreme view that the government should be blind to financial and communication data, but very few people think giving the government carte blanche without safeguards makes sense.

Maybe [Apple] could propose an overall plan for striking the balance between government being able to know things in some cases and having safeguards to make sure those powers are confined to appropriate cases. There is no avoiding this debate, and they could contribute to how the balance should be struck.

In the future, perhaps a means of hacking the semi-conductor memory chip directly may be the only way to access the encrypted data stored on a mobile device and that it would still need to be decrypted by other means. See the following link for additional information: http://www.wsj.com/articles/chip-hacking-might-help-fbi-unlock-iphones-1457050959

In the meantime, there will be many more on going debates on issues of privacy verses the government's request for access to mobile communication devices especially as they become more prevalent, used for point of sales, and are used to interface with other devices along with containing extensive financial/personal information.