Jericho Report

Michelle Thompson
GNU Radio Conference 2017 CTF

September 9, 2020

Julius Schnorr von Carolsfeld (1794-1872), The Battle of Jericho.

Abstract

This is a summary of the challenges in the wireless Capture the Flag (CTF) competition at GNU Radio Conference 2017. The competition was codenamed Jericho. This report has been written to provide a background and baseline for the type and scope of challenges in a CTF using GNU Radio. The goal was to give a variety of challenges, from easy to hard, and to provide both collaborative and competitive opportunities. Challenges were available from a web server running CTFd (https://github.com/CTFd/CTFd). Competitors logged in and selected challenges to solve. After entering in the correct key, points were awarded. More points were awarded for harder challenges. CTFd provides automated scoring and live statistics. Challenges can be unveiled over time manually or automatically. The event was a success, was highly rated in the participant survey, and resulted in contributions to GNU Radio codebase.

Introduction

The CTF was the product of a small team of people working together for 9 months to construct, produce, and manage the hardware and software required for a set of themed wireless challenges. GNU Radio was a central part of each challenge. Challenges were intended to range from easy to hard, with multiple entry points and starting points, and no bottlenecks.

The essential requirement of this CTF was to provide a friendly and supportive environment to both learn and compete. If participants got stuck or wanted to learn how to solve the challenges, then the volunteers would explain. Participants were encouraged to work together. Teams or individuals could compete. Top 5 winners were awarded small California-themed gifts (journals, tote bags) at the end of the event on Friday.

The volunteers brought and gifted 25 customized RTL-SDRs for participants that did not have any hardware at the event.

Updates about the challenges, number of participants (over 50), and leaderboard summary were given several times during the week from the main stage. Live leaderboard and statistics through CTFd were available on an easily accessible website posted at the registration desk.

Challenges

Here are the reconstructed list of challenges and some analysis. Lessons learned and some suggested improvements are given. Original CTFd files were lost due to a hard drive failure.

Hello Kitty

We set up what we believed to be several easy trivia questions about our favorite character, Hello Kitty. The goal was to get people familiar with entering keys to questions and getting scores in the web interface of the CTFd software.

However, the regulator expression calculator in CTFd didn't work as well as expected. The question "What does Hello Kitty Bring?" had the answer "Peace and Love". This was answered out loud multiple times during the first day of the conference and written out at the conference registration desk on a piece of paper. However, even a slight difference caused trouble.

Lesson learned: regular expressions are (still) hard.

Easy questions are a good idea! It does work out well to have something that does not require any hardware or software to get up and running and working, so that people have a score on the board. It reduces the barrier to entry and makes the event more accessible.

Pass the Salt

We obtained a set of reservation pagers. These are the objects that are often handed out in a restaurant so that when your table is ready, they flash and buzz. There is a base station that transmits signals to the customer pagers, a charging carrel, and the customer pagers.

The first challenge was to figure out which one was missing.

For this challenge, the missing pager was in the possession of one of the GNU Radio Conference volunteers. In order to figure out which pager was missing, one had to figure out how the base station called the pagers, call a pager, monitor the transmission, reverse engineer it, figure out the mapping from the buttons on the base station to the individual pagers, then recreate the missing pager

transmission, and call it. The volunteer with the pager would come to the participant and then manually assign the points in the CTFd software.

The second challenge was to make them all go off at once.

This could be accomplished one of several ways. Sending a vector that maps to all at once, or sending all codes sequentially. This was the "clear the room" part of the challenge.

What made this hard?

Usually, a commercially available wireless device in the US has an FCC ID. A good reverse engineer will take this number, look it up in the FCC database, and get all sorts of technical information for essentially free. This is a big head start for anyone wanting to do hardware hacking or signal intelligence. However, this restaurant pager did not have an FCC ID. It was not printed on the system anywhere. It was not in the manual (paper manual provided, pdf easily found online). It was substantially harder to figure out the frequency and modulation of the controlling transmissions without the FCC ID. There was a tiny hint. The frequency was printed on a sticker in very tiny text on the bottom of the base station.

Lessons learned: exceeded our expectations. This challenge was popular enough that another hardware hacker bought the system at the end of the conference to use in workshops and demonstrations.

Potential improvements: Use features like the advertising faceplates to hold more puzzle content. Running this challenge was loud. It's difficult to run it without disturbing people that are trying to enjoy a conference talk.

The Bins

This challenge involved two large bins turned over and placed down on a folding table. The challenge was to 1) control something inside, 2) identify a symbol inside, and 2) identify the color of the symbol. Each bin was a separate challenge. This was multipart and relatively difficult. Two controllers that appeared to be remote control toy controllers were on a table in the CTF

headquarters behind the registration table. This was a hint. If participants needed more of a hint, then they were told they were remote controllers.

In order to get points for controlling something inside, the participant had to reverse engineer the 50MHz remote controller and then make the toy move around inside the bin. A volunteer confirmed movement. Usually it was obvious as the toy bonked around inside the bin. The two toys had different controllers with different radio aspects, as each bin was a separate parallel challenge.

In oder to get points for identifying a symbol inside (video game logos), the participant would have to figure out that there was an NTSC backup camera inside each bin, transmitting an NTSC signal from inside the bin. Now, the bins are dark. Running to each bin was a programmable LED light strip with a BlueTooth controller. The part of the cable with the FCC ID for the BlueTooth controller was deliberately left outside the box. If you found the right Android or iOS app to run the LED light strip and turn it on, illuminating the inside of the box, and if you intercepted and viewed the NTSC signal from the box, then you would see the printed out and taped up video game logo inside the box. Google or a video game fan could help identify the logos.

The color of the symbol, which was not the standard logo color, could only be revealed if the participant was viewing a color NTSC signal. The backup cameras transmitted in color, but commonly available GNU Radio flowgraphs for receiving NTSC were all Black and White. This took some effort, but color NTSC flowgraphs were developed by the participants, and color was observed.

Another way to figure out the color was to set the BlueTooth LED strips to various colors and note the response of the image. With care, this would reveal the color of the printout without developing a color NTSC receiver flowgraph. At least one team successfully solved the challenge with this approach.

What made this hard?

Reversing a remote control is a time-honored basic GNU Radio exercise. However, usually one has the device and can look up an ID or product and get a head start. With the controlled device in a bin, and only the remote, it took scanning the usual frequencies used by these controllers to find them, identify

them, reproduce them with a transmitter, and make the device move.

Noticing the NTSC signal emanating from the bins, recognizing it as a video transmission, figuring out how to light the inside of the box, receiving the video signal, and then adding color were challenging. Showing how truly interesting and clever backwards compatibility in color NTSC television was a big motivation for putting together this challenge. We spend a lot of emphasis and time on new designs. Backwards compatibility is often overlooked, but there is many innovative and compelling aspects to designing something that works with existing standards and equipment. In the case of NTSC, it was backwards compatible for many decades of deployment.

Lesson learned: don't have color as a keyword (or any other small alphabet) because it's too easy to guess. Points had to be manually awarded after participants figured out it was easy to just guess the color, since standard colors are from a limited palette.

Pink Heart

Pink Heart was a BluetTooth LED neopixel ring headset. Find the recipe for constructing it here: https://learn.adafruit.com/bluetooth-controlled-neopixel-headphones

The headset was placed on a styrofoam head and connected to external power for the week. In order to answer the various questions about Pink Heart, one had to figure out how to connect to the Adafruit Bluefruit Feather. The easiest way to do this is to go get the Adafruit Bluefruit LE connect app for iOS or Android. The functions in the standard example program that comes from Adafruit were modified. On a regular basis, the headset LEDs would flash a morse code message about Pink Heart and the Mayan Warrior. These are theme camps at Burning Man. If the message was decoded then points were automatically awarded by the CTFd software.

Intercept

This was scored as the most difficult challenge. A transmission in the 2m ham band would be made on request. The question was “What is revealed?”

The transmission was the image transmitted by using Yaesu System Fusion’s camera microphone feature. The .jpg image was sent in data mode. The image was the nameplate from one of the hotel’s suites on an upper floor. The name of the suite was the key.

Intercepting and decoding the Yaesu System Fusion picture transmission in GNU Radio was accomplished, and the System Fusion blocks in GNU Radio were updated as a result.

What made this hard?

Reconstructing the way Yaesu handles data took effort because it’s not fully documented. There were a variety of basic signal intelligence techniques employed by teams to decode the image. Recognizing headers, recognizing the modulation scheme, looking up details about Yaesu System Fusion, and error correction.

Radio WGNU

A flow graph transmitting very low power broadcast FM radio with Radio Data Systems (RDS) was set up. RDS adds digital data to conventional analog FM broadcast signals. The easier parts of this challenge were to answer questions from the 10-minute custom audio loop in the stereo FM broadcast that was recorded for the CTF. Trivia questions about the identity of speakers, details from the interview, factoids from the “advertisements” - these could all be obtained with nothing more than an RTL-SDR and an easily built or obtained FM receiver flow graph.

There were several answers built into the digital data in the sidebands. A swarm of locusts was in the weather alert, for example.

What made this hard?

FM RDS transmits the digital data in a 57kHz subcarrier. We simply moved the digital sidebands to another frequency. Since they were in a non-standard location, off-the-shelf RDS receive flowgraphs did not see this portion of the signal. One would have to look at the spectrum, notice the difference, modify a

GNU Radio flow graph to properly receive the digital data, and then figure out if there was anything even more buried or obfuscated in the digital data.

Potential improvements: we ran out of time to include things like a slow variation in the carrier frequency to communicate a morse code message. Also, there's other subcarriers included in the RDS ecosystem that we didn't take advantage of. The first is DirectBand, and the second is Audos. Including those in the challenge would have increased the variety and difficulty. Any complex broadcast standard has a lot of potential. FM RDS provided a big dynamic range, from easy to hard, and made for a great challenge.

HD Radio

We invited donated challenges from the floor, and Clayton Smith @argilo submitted a challenge involving HD Radio. Specifically, NRSC-5 digital radio stations using an RTL-SDR dongle. An additional twist was the use of gr-paint to put a picture into the signal spectrum.

See https://github.com/theori-io/nrsc5 for more details about this type of radio transmission.

Problems & solutions:

Found It (100 pts?)
Q: What is the center frequency of the signal (in MHz)?
A: 445.5

First (100 pts?)
Q: What is the first flag?
A: wrathful potato

Second (200 pts?)
Q: What is the second flag?
A: spurious mailbox

Third (400 pts?)
Q: What is the third flag?
A: steadfast pinch

Transmit (400 pts?)
Q: Transmit your own signal at 918 MHz, and include your team name in an ID3v2 Artist tag.

Lesson learned: Accepting challenges at the event required good technical and customer support. It paid off.

BlueTooth Fast and Slow

Keith Wheeler @FirmWarez donated several BlueTooth challenges. There was a variety of questions ranging from easy to difficult.

Lesson learned: Accepting challenges at the event required good technical and customer support. It paid off.

BlueTooth Wristbands

BlueTooth Wristbands, given out at concerts and promotional events, were displayed in the main conference room. If you could "convince" them to flash a certain color, then you won points. This was relatively simple bluetooth hacking, but did require some sort of development kit or board or environment to connect to them and command them.

Mistaken Challenges

Several amateur radio beacons on the microwave band were mistaken for

challenges. Including them would have been a good idea for a themed challenge.

Notes for Next Time

GNU Radio attracts a lot of people that bring their SDRs. Advertising in advance did increase the number of SDRs at the event, but additional advertising and specific hardware suggestions would have made it even more easy to participate.

Providing RTL-SDRs was a good idea and was greatly appreciated, but does require an expenditure of funds that not every volunteer team should be expected to repeat.