The Local Oscillator

The Newsletter of Crawford Broadcasting Company Corporate Engineering

SEPTEMBER 2026 • VOLUME 36 • ISSUE 9 • W.C. ALEXANDER, CPBE, AMD, DRB EDITOR

Last month, Amanda and I were honored to be guests on Kirk Harnack's *This Week in Radio Tech* (TWiRT) on August 20.

Kirk is a great host with a wealth of radio and other broadcast experience on both sides of the mic and camera as well as having worked for Telos for over 20 years. That gives him a unique perspective on our industry as a whole as well as on the underlying technologies.

The day prior to our TWiRT appearance, Kirk was the guest presenter at the SBE Chapter 48 (Denver) meeting. In both the SBE presentation and the TWiRT episode, he brought up some things that have had me thinking.

The SBE48 presentation was on cybersecurity, both the FCC's new cybersecurity/EAS rules that go into effect later this month and cybersecurity good engineering practice (GEP) in general.

The FCC's new rules, specifically 47 C.F.R. §11.35, have three basic requirements. One, change from the default password and employ a password with a minimum of 15 characters and does not use a dictionary word and is not used for any other accounts, equipment, applications or services. Two, install security patches and firmware updates promptly. And three, use a network firewall or comparable network segmentation practice that limits remote management access to authorized devices and users. Easy enough, right?

Kirk brought up access to audio routing as an included component of at least the spirit of the new rules, and I don't disagree. Could someone get into your automation system and make changes to the playout, or gain access to your AOIP system and change the audio routing to put something on the air that shouldn't be broadcast? If that is a possibility, it must be addressed, even though it is not a specific requirement of the new rule.

So do we need to put a 15-character minimum unduplicated strong password on every Zetta user account login? What about on Wheatnet Navigator? What about codecs? Microwave links? Transmitters? Remote controls? If the answer is yes, that would be a lot of initial work and a lot of ongoing password resets when users can't remember their credentials, a nightmare for our engineers.

Thinking through this, I have concluded that if it is properly done, the "network firewall or comparable network segmentation practice" will provide a tall, electrified, razor wire topped security fence around all six sides of our networks. The main firewall is the first and primary line of defense, and at each transmitter site with a secondary (backup) ISP connection, the router/firewall there is another panel of that security fence. Connections between the main studio technical network and the transmitter site networks are made through permanent tunnels. Inside our networks, a user can get to everything, but from outside, only those with a valid VPN key can establish a tunnel and connect, and we can restrict users to certain devices or network segments as an additional security layer,

Inside the fence, we still keep doors locked with passwords, so not just any guest can walk in our door and gain access to systems and equipment; only those that have been issued "keys" (login credentials) can do that, and they can only access the specific devices or systems for which they have credentials. Even then, we can further limit a user's capability by assigning permissions for those specific tasks and functions to which they need access. Guest access to WiFi within our facilities is outside the firewall.

I am confident that our firewall/router/tunnel network segmentation architecture fully satisfies the new rules. At this writing, we have this in place in many markets with just a few locations remaining to

complete the work. It's likely that by the time you read this, we'll be done.

So is the FCC going to send an enforcement team around to check on our networks and EAS units? I can just about guarantee that they won't; they simply don't have the manpower. I believe that as it is with many other areas of the FCC rules, enforcement action will come after a breach has occurred and somehow comes to the attention of the agency. That's when the "insult to injury" comes into play – an FCC forfeiture would be added to whatever damage or injury was caused by whatever cyber-miscreant got into a device or system at the station or group and did mischief. That in no way lessens our responsibility as licensees to fully comply with the FCC's rules, and we must, at license renewal, certify that we have in fact complied.

The New York Minutes
By
Bill Stachowiak
Chief Engineer, CBC – Western New York

Greetings from Buffalo!

Josh and I installed three TP-Link Omada routers at our transmitter sites in order to comply with the new FCC regulations. We set up three new subnets to accommodate three transmitter sites. This worked out very well for us and actually made it easier to access equipment located at those sites.

Josh is going on vacation this week as I write this, so we plan to do WLGZ as soon as he comes back. This will be a little different, since we will be setting up on Unifi. I have already done some testing, so I am confident that everything should work perfectly. If I have any problems, I know where I can get help.

Occasionally, I get asked to assist my son, who is a regional engineer for Town Square Media. In this case, he had a problem with a Harris HT35CD. He was getting a major arcover in the high voltage power supply.

The first thing I did was to check for shorts in some of the obvious places, like the output of the rectifiers, to make sure we didn't have a shorted stack. I also disconnected the secondary on the plate Troubleshooting on modern transmitters is a lot simpler than what we had to do with the older transmitters that didn't have microprocessors watching over everything. Now, when a problem occurs, we really don't have to do much thinking about it. We get a message on the display telling us exactly what the problem is. In most cases we just change a module. I think it is still important to understand how your transmitter works. Read the principles of operation and study the schematics in your manual so that when you are notified of a problem, you can apply what is happening to what you know about the transmitter.

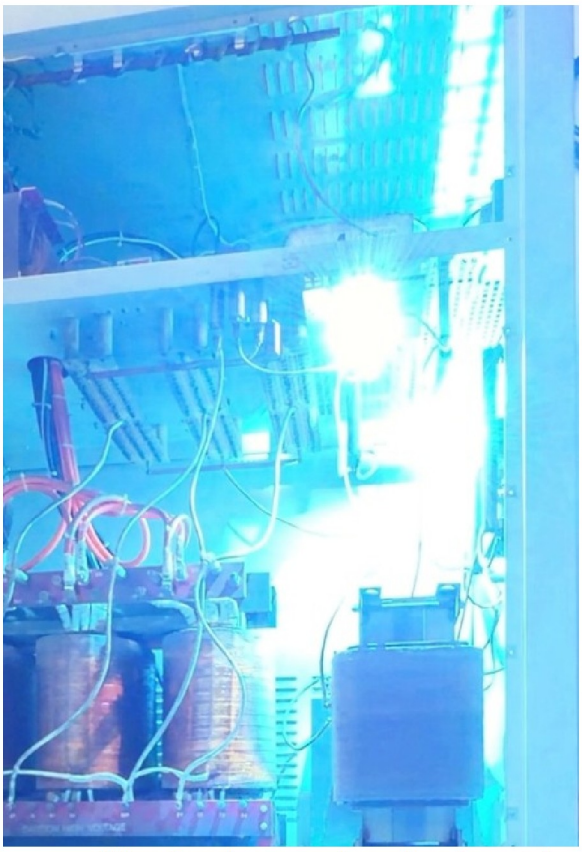
When I work on any piece of equipment, I make sure that what I am seeing makes sense. It is possible that you might get informed that something is wrong, but it really doesn't make sense.

It was, so we reconnected the secondary and switched to the half voltage position. There is a knife switch that switches ground from the center tap on the plate supply or negative of the rectifiers. In the low voltage position, there is only half wave rectification, but it is only intended for emergency use. Under those conditions the supply came up fine.

After we switched back to full supply, we got a huge arc over. Here are a couple of photos that I lifted from a slo-mo sequence that we recorded when we turned on the supply. The photo on the left below shows the arc as it first started, and the one on the right shows the fully-developed arc. Those photos showed us right where the problem was.

So what was the issue? It was a ground wire for which the insulation had become brittle, cracked and fallen off. It was close enough to a high-potential spot on a bleeder resistor that it would arc when the high voltage came on. We fixed the wire and rerouted it so that this problem cannot ever occur again, at least not in that spot!

Troubleshooting on modern transmitters is a lot simpler than what we had to do with the older transmitters that didn't have microprocessors watching over everything. Now, when a problem occurs, we really don't have to do much thinking about it. We get a message on the display telling us exactly what the problem is. In most cases we just



change a module. I think it is still important to understand how your transmitter works. Read the principles of operation and study the schematics in your manual so that when you are notified of a problem, you can apply what is happening to what you know about the transmitter.

When I work on any piece of equipment, I make sure that what I am seeing makes sense. It is possible that you might get informed that something is wrong, but it really doesn't make sense.

That's all for this month. See you next time.

The Motown Update
by
Mike Kernen, CPBE
Chief Engineer, CBC–Detroit

FCC Takes Measures to Enhance Broadcast Infrastructure Security

Readers here are more than likely familiar with the recent FCC Report and Order in PS Dockets 25-224 and 22-329, "Modernization of the Nation's Alerting Systems; Protecting the Nation's Communications Systems from Cybersecurity Threats." There were a couple of other proposed rule changes in the R&O, but those deal with specific EAS system changes and are not yet the law of the land.

To comply with the newly-enacted regulatory changes, Crawford took steps in each area. Changing passwords from dictionary words to strong complex un-hackable strings is easy and should have already been done – even on devices obfuscated by firewalls!

- (Old Password) Time to crack your password: 4 hours
- (New Password) Time to crack your password: 2 trillion years

The next step was to move the internet audio links to our transmitter sites without dedicated, secure microwave links

(STLs) from unencrypted Real-time Transport Protocol (RTP) streams over the open internet to persistent, encrypted VPN connections. This greatly reduced the risk of the streams being interrupted and/or replaced with unauthorized audio intended to cause harm or deception. Although such incidents may seem unlikely, several have already occurred. The FCC is seeking to harden broadcasters' security, ultimately protecting the public from STL attacks which could cause confusion at a minimum or possibly block or alter urgent public safety information.

In Detroit, our combination of transmitter sites, primary and backup internet service providers and STLs via internet led me to create 6 VPNs. Using our Unifi routers, I was able to create WireGuard tunnels and force the STL traffic onto them. This was not difficult is what I would like to be able to say, but I cannot.

To be fair, this was not the fault of the Unifi equipment or software. No, this was me learning on the job (as usual) and having to reset my way of thinking a few times over. Ubiquiti is famous for its user interfaces and straightforward approaches to networking. However, much of their equipment lacks thorough documentation and support is pretty much limited to chat sessions.

Once I reached the apex of the learning curve, I was able to get the system to force STL traffic over the intended VPN without calling an ambulance.

The next thing was to create new networks in the firewall. We do not use Unifi routers and firewalls, so this was a manual process – shout-out to Todd Dixon for once again bailing me out and helping me understand what to do. I'm not complexity averse, but I do appreciate the assist from time to time if for no other reason than to keep myself from bricking our entire network.

A Tribute to the "Department of Redundancy Department"

Back in the late crustaceous analog period, I worked at a recording studio and post-production company. This is where I learned how to wire things out-of-phase. It wasn't my fault – there was beer in the soda machine… Anyhow, we had a reasonably large duplication department that served as the final step of our services to clients. We'd duplicate and distribute the commercials we'd help them create in our suitably named "Department of Redundancy Department" (it said that right on the door).

Working there taught me the value of redundancy. Not because we duplicated reel to reel tapes but because we had redundant equipment at every workstation. If something failed, we never had to stop production – just move on with something else so the radio and TV station always got the ads we produced without delay.

Subsequently working for four major market top 10 radio stations hammered home the idea that I should always be aware of single points of failure and work to eliminate them wherever possible. While creating six VPNs for our STLs wasn't off-the-charts complicated, and they work like a hose, the Ubiquiti Dream Machine Pro that they're running on means three of our four stations are but one switching power supply failure away from silence. Fortunately, Ubiquiti has thought about that and has allowed for a "High Availability" configuration. This requires a second UDM Pro and a way to split ISP and host connections for both units.

To divide the ISP connection, I added a simple Unifi Cloud Gateway Ultra and used a VLAN to connect it to the standby UDM Pro. The UDM Pro units are in complete synchronization, so having the same ISP connection details on both pathways was imperative. The Unifi Cloud Gateway sits isolated with its WAN connection using one of our unused fixed outside IP addresses. The hosts are split via one Unifi 24 port switch.

I realize this is not without its single points of failure. Building completely redundant systems can be prohibitively expensive, and one must consider risk factors when constructing any system. Since routers (which the UDM Pro certainly is) require periodic updates and have unique configurations, it made sense to duplicate them. A switch can be replaced in short order by an inexpensive spare.

The new UDM Pro sits in "shadow mode" constantly synchronizing any changes with the primary and waiting for the possibility that the primary stops sending its heartbeat signal. If that happens, the shadow unit wakes up its ports and establishes the VPNs and assumes the other duties of the primary, including operation of the front door card access system – all within 3-5 seconds. Pretty cool redundancy!

Miscellaneous Ramblings and Goings On

As usual, lots of other things have been going on here in the Detroit market.

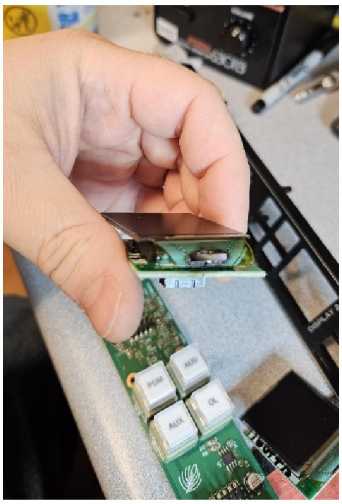
The Verizon 4G LTE service that I reported on last month is running supremely well, so well that I've ordered and configured two more to complete replacement of our satellite delivered internet services at our transmitter sites. Their significant

lower monthly cost gives us a perpetual savings along with a much more robust connection. The devices have a built-in battery and a heavy-duty enclosure. They also have wired ethernet ports so they can be connected to professional routers, but if you want to use it, they also have a nice little router on board.

Those of you with Wheatstone consoles know they have numerous tiny OLED displays. We noticed on one of our consoles that all 39 OLED screens were so dim as to be nearly unreadable. Some had already failed completely and had been replaced one at a time, but the time had come for a complete restoration.

All new bright and beautiful OLED screens have, in addition to a thorough scrubbing, returned this LXE to like-new condition.

Upon receipt of 40 little OLEDs, Steve was handed the unenviable job of replacing each one and meticulously cleaning the entire console. He removed each minute display, a couple of uneaten French fries, and a quarter cup of coffee from the WCHB control room console, cleaned five years of finger grunge off the surfaces and reassembled the entire thing, all while balancing high above the big top floor and all without a net! Even though one defective display nearly caught fire after two days taking the entire console down with it, Steve lives to tell the tale. Kudos Steve!



39 of these OLED screens are used in each of our LXE surfaces.

News from the South
by
Todd Dixon, CBRE
Chief Engineer, CBC–Alabama

Heavy Lifting

Nearly a year ago, I heard about a challenge that DARPA (Defense Advanced Research Projects Agency) was putting on. They were challenging aeronautical engineers, weekend garage enthusiasts, and small companies to advance drone lift capacity and apply any number of technologies at their disposal to do it.

For those of you that are not FAA Part 107 pilots, the license gives the RPIC (Remote Pilot in Charge) the ability to fly a drone that weighs over 0.55 pounds and under 55 pounds. While Part 107 pilots are limited to 55 pounds including vehicle and payload, traditional thoughts on any flight limits has essentially limited lift capacity to near 1:1 ratios, notwithstanding lighter than air vehicles. Even heavy lift helicopters like the Sikorsky S-64 Skycrane, which has a 19,500 pound empty weight, is only rated for lifting 20,000 pounds.

Keeping to the spirit of the Part 107 license in place, the DARPA challenge limited teams to a maximum vehicle weight of 55 lbs., which included any fuel or battery source as well. The additional payload weight for the challenge would be provided in the form of Olympic style barbell plates that had the typical ranges from 45 pounds down to 2.5 pounds. Since these types of weights are easily accessible, it gave each team the ability to design and test their vehicles with the exact same weight conditions they would have at the real competition.

The flight requirements of the competition were that the vehicles had to travel four nautical miles with a minimum of 110 pounds of weight attached, land and drop their weight, and then fly an additional one nautical mile before safely landing the vehicle back at its starting

point. This entire operation had to be done with a 30-minute time frame from beginning to end. Additionally, once the vehicles reached an altitude of over 100 feet, they had to maintain flight within a height window between 100 and 200 feet.

The Part 107 license itself requires that a pilot is always under the limit of 400 feet above ground level, unless an obstruction (like in our case, a radio tower) is in the path which allows for 400 feet above the obstruction.

The event was held at Wright Patterson Air Force Base and Flight Museum in Dayton, Ohio. The flight field was setup as 15 "lanes." These lanes allowed the DARPA flight safety coordinators at the event to make sure that teams not only flew within their prescribed lanes but also created plenty of space between competing teams so that the field was not overrun with flight activity and chaotic in nature. At any one time, only three or four lanes were being occupied by active teams, and they were all being monitored by a flight operations team in a building just beyond the field.

Safety, even among casual pilots, is of utmost concern when flying any drone, but in this particular environment, where a number of experimental drone designs were being tested at their physical limits, it was paramount that all safety protocols were being followed to the letter.

The purse for the DARPA challenge was to offer $2.5 million dollars to the first-place team, $1.5 million to the second-place team, and $1 million to the third-place team. Other $500k categories that were more subjective in nature were "Most Revolutionary Aeronautical Design," "Most Revolutionary Powertrain Design," and "Most Promising Design."

The caveat for the heavy lift portion was that in order for a team to collect the full prize winning amount, they had to meet or exceed a ratio of 4:1. To put that in perspective, a 55-pound drone was being asked to lift more than 220 pounds in order to collect the full cash prize. If a team didn't reach the 4x lift, they received half of the allotted challenge money.

The challenge lasted from the August 3rd to August 9th, with qualifying runs beginning on Wednesday, August 5th. One of the interesting things about the challenge was that current FAA statute doesn't allow for a drone to "legally" fly in airspace if it weighs more than 55 pounds. So how were these teams expected to test their designs if they couldn't fly them out in the open? One way would be to fly the drone in an indoor facility because when you are indoors you are not in airspace. Another way to test would have been to tether the drone to the ground so that there was no way it could fly off and all participants could be outside the radius of the tether. Of course, the tether might create a weight constraint or cause instability in controlling the flight.

With that in mind, you can only imagine that there were really a bunch of genius designs that needed to be tested and a number of them failed spectacularly. There were also a number of them that succeeded beyond their creator's wildest imagination. There were wing foils with small drone prop motors that were attached at the ends that spun the foil in a helicopter fashion, standard helicopter designs with gas motors that turned a generator that gave steady DC battery power to drone motors, a specialized inflated fabric that acted as a rigid (and I mean RIGID) frame for its drone that only weighed 2.2 pounds and could be folded into a backpack, and even a couple teams that were using diametrically opposed, tethered RC planes to create the lift necessary to pull weight up into the air. It was really inspiring to see not only real ingenuity at work, but also the spirit with which competing teams helped and encouraged one another.

I was catching the footage on the DARPAtv YouTube channel when I could. They were keeping track of teams and their ratios, but it was one of those events you watched because you weren't exactly sure what would happen next. Would a team complete the challenge or would their design, that was fine with 55 pounds on it, fold in two from 150 feet when it had 110 pounds attached to it? That was always the hook for me.

In the end, no team achieved the 4:1 (or above) ratio, but several did get close with the winner, Avidrone, completing their run with a 3.86:1 lift ratio. One team named Defendtex got nearly three miles through their competition run before their battery power simply ran out and they fell from the sky. Their drone was carrying 112.4 pounds, but the drone only weighed 11.7 pounds (!!!), which gave it a 9.61:1 ratio. Just to provide a reference point, the DJI Phantom 4 Pro drones that we use for flying our towers are 2.2 pounds.

So why is any of this important? I am sure that DARPA was looking for ideas that would possibly skew a battlefield in our favor. What if the gas motor/generator/battery combination were combined with a handful of other designs and a 6 or 7 times capacity could be maintained in a simple, easy to deploy design? What about other industries, maybe a search and rescue drone could drop a fair amount of food or medical supplies to someone while a team prepares a rescue or thousands of drones with heavy

lift capacity were able to be used to fight fire with water or chemical with surgical precision? How about a tower crew being able to bring 150 pounds of tools and materials to a climber that is already in place? The possibilities are endless, with only a few changes in FAA rules that could facilitate an incredible jump in technology and in usage limits.

The entire challenge and the resulting competition piqued my interest because I am FAA Part 107 certified and it really brought together a number of my interests. I hope it did for you as well, and I also hope that we begin to see the effects of this DARPA heavy lift challenge in near future.

Attitude

I had already completed almost all of my article for this month fairly early, but something happened yesterday within my life sphere that made me want to add this additional part to this month's submission. Jack Bonds and I both live in Calera, AL, a suburb about 25 miles south of the Birmingham metro area. An interstate widening project is currently underway that is adding a third lane for traffic in about a seven-mile stretch of the roadway. The seven-mile stretch includes an exit that includes the Shelby County airport. With all of the work happening on the project, you can imagine that there are a number of heavy equipment machines that are being loaded and off loaded for the work to be completed.

Yesterday, the overpass bridge at the airport exit was struck by a vehicle carrying some of that heavy equipment. With rubble all over the road and several other passenger vehicles involved, it shut down the interstate and the associated overpass until it could be cleared by DOT engineers. It turned my normal 30-minute commute (and tens of thousands of others) into about an hour and a half commute. During that drive home last night, the Waze app took me through several neighborhoods and roads that I had never been on before. Actually, other than tripling the time factor that was involved, the drive was relatively pleasant and peaceful.

While I was reflecting on it, a quote that I had been thankfully confronted with really early in my life came to remembrance. It is from Chuck Swindoll and it is called Attitude:

"The longer I live, the more I realize the impact of attitude on life. Attitude, to me, is more important than facts. It is more important than the past, than education, than money, than circumstances, than failures, than successes, than what other people think or say or do. It is more important than appearance, giftedness or skill. It will make or break a company...a church....a home. The remarkable thing is we have a choice every day regarding the attitude we will embrace for that day. We cannot change our past...we cannot change the fact that people will act in a certain way. We cannot change the inevitable. The only thing we can do is play on the one string we have, and that is our attitude...I am convinced that life is 10% what happens to me and 90% how I react to it. And so it is with you...we are in charge of our attitudes."

— Charles Swindoll

So true. I don't want to drive an extra hour every day, but yesterday, I was thankful for Waze, thankful for my vehicle and thankful for a different perspective. I am also thankful, today, that I-65 southbound at that Airport exit is back open and the overpass bridge that was hit had cars going across it.

All of us are faced with crazy things every day, but the attitude with which we approach every circumstance is the real limiting factor.

Have a great month and I'll see you in these pages in October.

Tales From Cousin IT
by
Stephen Poole
CBC Corporate IT Specialist

Cris and Amanda were featured on Kirk Harnack's podcast (This Week in Radio Tech, or "TWIRT") the other day. Among the items discussed was the FCC's recent emphasis on securing broadcast facilities. The Alabama Broadcaster's Association is sponsoring a webinar here on this same topic, and other industry groups are doing that same all over this country. Everyone's talking about it.

You know me (whether you want to or not): I'm going to take a different angle here. I'm not going to discuss the obvious: any communication between your studios and transmitters should be encrypted, with access carefully limited. If you're sending live audio over the public Internet, this is especially important. And so on.

To really be secure, you must learn to think like a Bad Guy. This doesn't mean that you should wear a weird outfit and cackle maniacally; people will start arranging lots of furniture between you and them. Keep it up and some serious-looking people will show up with a long-sleeved white jacket and you'll find yourself chortling in a padded room.

I've been amazed at the number of people who will install a nice deadbolt lock ... in a door with thin glass windows. They'll put video cameras and motion lights on the porches and ignore the rest of the property. If a break-in occurs, they'll run to look at the video ... only to discover that the thief was wearing a mask. (My favorite happened at the 850 AM site here some years ago; the thieves wore Groucho glasses. I'm not kidding.)

Unfortunately, many of us make equivalent mistakes when securing our data. Here's a prime example: you can use the latest and tightest VPN to encrypt everything between the studio and transmitter, but if there are wireless devices at either end that could be hacked, you're not protected. Criminals can get into your systems through unpatched WiFi routers, wireless cameras and cheap, consumer-grade "Internet of Things" gadgets. You should address that.

So ... here's tip one. If you have an old D-Link WiFi router at a transmitter site that hasn't had a firmware update since the Bush administration, you might want to replace it. It may cost a bit of money, but you should budget to regularly replace devices, especially once they've passed End of Life ("EOL").

My Background

A lot of what I just said is (or should be) obvious. But let me briefly describe my background and point of view. Many years ago, back in the MS-DOS era, I developed anti-virus software (the term "malware" hadn't been invented yet). My partner and I decided that the last thing the world needed was another scanner.

This hasn't changed since we released our ARF Anti-virus in the late 1980s. To this day, most anti-malware systems can only protect you from known threats. If a novel piece of bad software pops up, it will take time for it to be analyzed and addressed.

This was actually a bit hilarious (in a sad way) in my anti-virus heyday. Scanners didn't look at an entire file; that would take too long. Instead, they

Figure 1 - Hope the password has been changed on this camera...

looked for short virus signatures. So ... the virus writers simply rearranged their code from time to time to obscure the signatures. The scanner companies looked like Sebastian the Crab in The

Little Mermaid; their jaws dropped and a loud chorus of "wuhh" was heard.

To be fair, the latest scanners do all sorts of things to address this, and in the main, they're decent. And I'll admit that the odds are in your favor; no single, specific user is likely to be hit on a given day. But ironically, that leads to the worst enemy of all: complacency. Because you've never been hit, you blithely assume that it will continue.

Instead of scanning for known threats, our software looked for weaknesses and secured them. I wrote a device driver that would install itself during bootup, then check critical parts of the operating system for changes. To poke the scanner folks in the eye, we actually borrowed the main idea from the virus guys: we would "inoculate" each system file with a wrapper that checked for alterations and would only allow the original code to run if no changes were detected.

Here's the bottom line. Of course it's not possible to protect against every possible threat. But think like a Bad Guy. Walk around your facilities and inspect carefully on a regular basis. Check for firmware updates. Replace old devices. Watch for rogue WiFi access points that aren't on your list (or were installed by an employee without your knowledge; ask me how I know!). Use a firewall that will let you track each connected device and watch for a sudden increase in traffic, especially if it's between your studios and Russia or North Korea (duh). Look for changes.

Alert Board

We're back on some projects that were pushed aside for other things. The Alert Board that Cris showed you in a previous issue is gaining the ability to flash images on selected inputs. If, say, someone is at the front door, the control room may not notice a static "Front Door" image popping up. But if it flickers on and off, it'll catch their eyes.

For those who care, the code that does the important work isn't a big deal. Providing a useful interface that will allow people to configure things without having to edit cryptic files? That, and thorough testing, are what take most of the time. For now, I've been using simple web interfaces. The Raspberry Pi units can easily support a "lamp" stack (Linux, Apache, MySQL and PHP), and I already have a bunch of code that I can quickly modify to make stuff for this.

Sorry for all the gibberish I had to use this time. I can sum it up the security thing with some immortal words from a sign that once hung on the wall of a music store in Southern Pines, NC: "Be Alert! This Nation Needs More Lerts!" Stay alert and think like a Bad Guy!

Figure 2 - Things like this rain gauge are often overlooked.

 The images came from Wikimedia Commons: the wireless camera is from user Acabashi and the digital rain gauge is from user Missvain. Because of course she is. Until next time, keep praying for this nation!

The Chicago Chronicles
by
Rick Sewell, CSRE, CBNT, AMD
Engineering Manager, CBC–Chicago

Welcome to the new Tornado Alley.

I don't know if the Midwest can now truly claim to be the new Tornado Alley because what they now call "Dixie Alley" in the South has also seen a rise in tornado activity in the last two decades as well.

The Midwest has more tornados than the South with a 9-percent increase since the year 2000. The South has had a greater increase in activity going up 22-percent since the start of the century. These stats come courtesy of https://www.tornadopath.com/tornado-alley.

I am quite sure the staff at our Birmingham operations would probably proclaim that they have noticed this change. I certainly noticed it here. Still, growing up in the St. Louis area for most of my life, I don't remember hearing about tornados in the Chicago area too much, and being on the trailing edge of the traditional Tornado Alley, it seemed to be that my area certainly received many more threats of this type of weather than the Upper Midwest did.

When I first moved here in 2014, within a few months we had a storm that brought 11 tornadoes to the area. That seemed to me to be something way out of the norm for this area. I chalked it up to something that happens every couple of decades, and while we didn't make it through unscathed, it was something that wouldn't be repeated any time soon.

However, I eventually changed my thoughts after these events continued to be repeated. Some years are better than others. That brings us to this year, we have had three multiple tornado events in the south suburban neighborhoods and Northwestern Indiana in the past three months.

It's been a rough summer, and this last round on August 11th was very devastating. It wasn't just the fact that there were two tornados in the immediate vicinity of our studios and several transmitter sites, it also wasn't the high straight-line winds that came with this and a couple of the other events. In this last case, we had what is called a derecho. In some ways it has more devastation than a tornado because it is so widespread in the damage it causes. There was some speculation that the tornados may have actually protected some areas from the derecho. I don't know if it really mattered if it was true.

From our standpoint as a cluster of four stations amid all of this, we came away in pretty good shape, considering what could have been. When it hit, we lost power at the studio almost immediately, but the outage only lasted about ten minutes.

One of things I have never seen before was rain coming in the top of our back door that faced the storm. It is covered by an awning, so the rain was not coming down the building so much as the wind was forcing rain directly through the weather stripping around the door. This wasn't just a trickle but actually pouring over the top of the door.

Every site we have ended up with the generator coming on except for the Lansing, Illinois site, the one that has generator problems and also was closest to the path of one of the tornados. That was a blessing, because the backup generator is not available to the auxiliary transmitter that we can use for the sister station WPWX located at our Burnham, Illinois site.

At the Burnham site, we lost electricity quickly after the storms. We had a near full propane tank, but we acted quickly and ordered a delivery of more fuel because we cut through about 25% of the tank a day even with the transmitter at half power. Even with the transmitter off we probably go through about 10-percent a day.

I would like to think that our quick reaction saved us, but that was not the case. Once we realized that our Lansing site was stable with power remaining on, we moved the station from the Burnham transmitter to the auxiliary site at Lansing.

It was good that we had this capability, as we did not get another delivery of propane until eight days later. This is the third time that we have been saved this year from being off air due to a combined lack of utility and generator fuel. The foresight and investment in building this auxiliary site infrastructure have really paid off.

We are not totally satisfied with the current set up as we need to get a generator in place at that site that can handle the load of that transmitter. That is in the works even as I write this article.

Rocky Mountain Ramblings
The Denver Report
by
Amanda Hopp, CBRE
Chief Engineer, CBC - Denver

Raise Your Hand If You're Tired of Talking Cybersecurity!

Cybersecurity is something that needs to be taken seriously by all. I think many people don't realize how much is on the internet. There are people or bots who have a mission of hacking, of gaining access to personal information. Some will ransom it back for a hefty price, others steal identities, while others just want to interrupt life. We've heard about it repeatedly.

It happens on a personal level but also on a professional level. Radio station files have been ransomed, and air streams have been hacked and malicious audio put on the air. I can't say it enough, having a good password is important. Kirk Harnack has done some TWiRT's covering this topic and he also presented to the Denver chapter of the SBE. Hearing his thoughts and discussing with others has got my brain going.

To prepare for the new rules, we have begun creating a VPN tunnel from the studio to each transmitter. I'm sure I annoyed Todd Dixon, who helped figure all this out, with all my questions. The more I thought about what we were doing, the more complicated I made it when it's not. Once I took a step back it all made sense, and I now have a decent grasp of it.

Part of getting things ready to go is having to change the network at a few of the sites. When we first installed our dual-WAN routers, we set each transmitter up at 192.168.1.X. Normally, this wouldn't be a big deal, but since we are going to VPN each location, there was a greater risk (or rather an assured risk) of conflicts.

As I am getting the tunnels set up, I am having to go to each site and change the IP scheme to help avoid these conflicts. It's a tedious process, as some of the equipment can only be changed on the unit itself. I have three of our five locations done at this writing. I am hoping to get the last two sites done by the end of the first week of September.

The Quietest Site Has Given Us the Most Grief

I would say KLDC, since moving to Englewood, has been the quietest site we have. Lookout Mountain would be the other one. I rarely have to make a trip out to the KLDC site in Englewood. August was the exception. All my transmitter trips for the month have been out there.

The first trip was to get the network changed and to learn how to get the new tunnel working. I had to get Todd on the phone, and he poked around for a good long while before finally realizing the issue. Off the top of my head I don't remember, but I think it had to do with a step he included in his instructions that actually didn't need to be there. Once he made the change and removed what I had done, things fell into place.

The other issue is that the Cambium microwave link for the site would disconnect randomly. I could get to the Cambium radio on the tower, but it would show it didn't have any Ethernet connectivity to the network at the site, which would mean I had to go into the site via our backup internet. Thankfully, that was solid, as it kept audio on the air.

We had originally found a broken ground on the shielded RJ45 connector at our isocoil. Once it was soldered back on properly, the link came back and was solid for a few days.

I was watching the site closely and noticed on the 15th an alarm showing the Ethernet connection from the Cambium radio on the tower to network at the site was down. I immediately hopped on and found that I could not get to the Cambium on the tower or anything else at the site (through our backup internet). I went to Xcel Energy's website and looked at the outage map and saw an outage in the area. All I could do was wait.

Once the power came back up, I noticed the J1000 main transmitter wasn't responding. We have it connected via SNMP, and everything was greyed out. I was able to put it on the backup transmitter, our trusty old ND1, and left it there for the rest of the weekend.

On Monday, we went to the site and found the breaker tripped for the J1000. We reset it and it immediately tripped again, but a second reset seemed to fix it. While I dealt with another issue, my dad went through the transmitter settings and had to reset

Chris Clare of 3dB Networks changing the Ethernet cable out on the KLDC tower.

a few things before it would come up and operate.

After this I kept noticing that microwave link's Ethernet connection to the building coming and going as it was before. We decided the next step was to replace the cable going up the tower. We got that done on the 25th.

In the process of dealing with this, I found that my cheap cable tester wasn't working properly anymore as it would show wire 2 as not being there when it was (I tested with a known good cable). We used an ohmmeter and confirmed the connections were good. At this point, only time will tell, but we are praying that the new cable up the tower fixes our connectivity issue once and for all.

Inventory

We were given our inventory lists and now Daniel and I are working to get that done as soon as possible. I'm letting Daniel do most of the transmitter sites so he can become familiar with what equipment is at each site while I am working on inventory at the studio.

Inventory isn't my favorite time of the year. While I have tried to keep better track of things and make sure locations get changed in the database as they occur, things still are forgotten and it becomes a search to find it. I look forward to getting it done and moving on with my work.

Looking Ahead

As mentioned, the plan is to finish getting our network changed up a bit and a tunnel set up at my last two sites. Beyond that, I really don't know what's next. Fall is quickly approaching, which is just crazy to think about.

I hope with Autumn it comes a time of slowing down. I haven't had a real day off in a long time. I even worked a little bit nearly every day while on vacation. The constant issues every day are beginning to wear on me. I could definitely use a break.

I think that about covers it for this month. I pray you all stay safe and well!

KBRT • Costa Mesa - Los Angeles, CA
740 kHz/100.7 MHz, 50 kW-D/0.2 kW-N, DA-1
KNSN • San Diego, CA
1240 kHz/103.3 MHz, 550W-U
KCBC • Manteca - San Francisco, CA
770 kHz/94.7 MHz, 50 kW-D/4.3 kW-N, DA-2
KLZ • Denver, CO
560 kHz/100.7 MHz, 5 kW-U, DA-1
KLDC • Denver, CO
1220 kHz, 1 kW-D/11 W-N, ND
KLTT • Commerce City - Denver, CO
670 kHz/95.1 MHz, 50 kW-D/1.4 kW-N, DA-2
KLVZ • Brighton-Denver, CO
810 kHz/94.3 MHz/95.3 MHz, 2.2 kW-D/430 W-N, DA-2
WDCX • Rochester, NY
990 kHz/107.1 MHz, 5 kW-D/2.5 kW-N, DA-2
WDCX-FM • Buffalo, NY
99.5 MHz, 110 kW/195m AAT
WDCZ • Buffalo, NY
950 kHz/94.1 MHz, 5 kW-U, DA-1
WDJC-FM • Birmingham, AL
93.7 MHz, 100 kW/307m AAT
WCHB • Royal Oak - Detroit, MI
1340 kHz/96.7 MHz, 1 kW-U, DA-D
WRDT • Monroe - Detroit, MI
560 kHz/107.1 MHz, 500 W-D/14 W-N, DA-D
WMUZ-FM • Detroit, MI
103.5 MHz, 50 kW/150m AAT
WMUZ • Taylor - Detroit, MI
1200 kHz, 50 kW-D/15 kW-N, DA-2
WPWX • Hammond - Chicago, IL
92.3 MHz, 50 kW/150m AAT
WSRB • Lansing - Chicago, IL
106.3 MHz, 4.1 kW/120m AAT
WYRB • Genoa - Rockford, IL
106.3 MHz, 3.8 kW/126m AAT
WYCA • Crete - Chicago, IL
102.3 MHz, 1.05 kW/150m AAT
WYDE • Birmingham, AL
1260 kHz/95.3 MHz, 5 kW-D/41W-N, ND
WYDE-FM • Cordova-Birmingham, AL
92.5 MHz, 2.2 kW/167m AAT
WXJC • Birmingham, AL
850 kHz/96.9 MHz, 50 kW-D/1 kW-N, DA-2
WXJC-FM • Cullman - Birmingham, AL
101.1 MHz, 100 kW/410m AAT

Crawford

Corporate Engineering
2821 S. Parker Road • Suite 1205
Aurora, CO 80014