The Local Oscillator

The Newsletter of Crawford Broadcasting Company Corporate Engineering

MAY 2026 • VOLUME 36 • ISSUE 5 • W.C. ALEXANDER, CPBE, AMD, DRB EDITOR

NAB Convention

Another NAB spring convention is in the books, and I sat this one out. For decades, I made every NAB spring convention (and a few fall radio shows, too). I always looked forward to making those trips, seeing all the new gear, seeing people I hadn't seen since the last show, and sitting in on various technical sessions. I do miss that, but the reality is that the Las Vegas NAB convention is a very expensive trip, and in my estimation does not have a lot of value for this company, which is the only figure of merit that really counts.

The good news is that I can purchase the Broadcast Engineering Conference Proceedings after the show and pretty much learn everything I would have gotten in person. And it seems that most of the people we do business with come through Denver at some point during the year and I get to see and visit with them without the expense of a multi-day Las Vegas trip.

So… for those of you who made the convention this year, I am a bit envious, but all things considered, not too much. And I'm certainly not as tired!

Tiny Parts

Surface mount technology, or SMT, has been around for a good while now. Contrasted with "through hole" component mounting, it is more efficient and allows for a greater component density. Also, at VHF and UHF frequencies, the lack of lead inductance is a real advantage.

SMT requires a whole different technique for manufacturing and population of circuit boards, using stencil printing, robotic "pick and place" component placement, and reflow soldering. It's very efficient, I'm told, and we've all seen the results.

But what about component replacement in the field during the repair process? That is a horse of an entirely different color, let me assure you. Over the years, I've done a good bit of repair work on SMT circuitry, but recently I had to deal with replacement of a truly tiny SMT component, and it was a challenge.

The issue was with a Nautel NX50 PA module from KCBC. One particular modulator, a power MOSFET, kept going shorted. Steve Minshall followed Nautel's troubleshooting procedure to isolate the bad modulator, replaced it and put the module back in the transmitter. It worked for a few seconds and then tripped off. Unable to find anything else wrong, I had him send me the module.

When I got the module, I repeated the MOSFET replacement and got the same result – no surprise there – and confirmed that it was the same modulator that failed. With that in mind, I started looking at other components in that circuit. There is in the gate circuit a 22-ohm SMT resistor in parallel with an SMT diode. I had to unsolder and remove the 22-ohm resistor to check the diode, but when I did, I found that there was another current path across the diode through the inverter/buffer driver, and that device is a six-legged TO-220 package device. I had to unsolder and lift the leg that connects to the diode and resistor before I could get a good check of the diode, which I found to be open.

Amazingly, I had a supply of those SMT diodes on hand. The problem: that diode is about the size of an anthrax spore, barely visible with the naked eye! I had a lighted magnifying light on the bench to look through, and it was still extremely tiny!

It took some doing, but somehow, I managed to get the bad diode unsoldered and off the board (easy) and the new diode on the board and in place (hard!). But before I soldered it into place, I had to use my DVM to figure out which end was the cathode, since the markings were too small to see.

Getting the diode properly oriented and in place was a real trick. Even static electricity would cause it to move. I eventually used the tip of a piece of 24-gauge solder wire to nudge the diode into position, and then somehow managed to get some solder to flow and make contact with one side of the diode and secure it in place. The trick then was to lift the soldering iron and not have the diode come up with it.

I eventually got both sides soldered into place, double-checked and confirmed the correct orientation with the DVM, and then soldered the 22-ohm resistor (which was a lot bigger than the diode) into place. Then I reconnected the driver leg, replaced the modulator MOSFET and put the module back together. Amanda put it in the KLTT transmitter and ran it for a few minutes, watching all the module parameters for any issues, All good!

Is there a better way to work on such a tiny component? Some might suggest a hot air solder setup, but it occurred to me that even a breath of hot air would cause that tiny diode to move, so that's probably not an option. I suppose muddling my way through it like I did is probably the only real option.

Old eyes and shaking hands are not your friends when working on this tiny stuff, but thank God, I somehow got it done. Hopefully it's the last time I'll have to do that for a while!

The Radio Business

People ask me from time to time how things are going in the radio business. It would be easy to give a "standard" response, as we all do when someone says, "How are you doing?" "Fine, fine. And you?" We all do it, and sometimes it's a lie.

The truth is that the radio business is changing. It wasn't all that long ago that radio was ubiquitous and *the* source for aural entertainment, news, weather, traffic and all that. Now, with the continued expansion of the internet and connected devices, people have at their fingertips many, many choices for aural entertainment that extend far beyond the presets on their car radios.

And speaking of car radios, those have morphed into something entirely different. Instead of separate devices that offer FM, AM and maybe SiriusXM reception as well as playout of MP3 and other digital recorded material, in many vehicles they are integrated into the vehicle's user control system that includes driver assist options, entertainment, navigation, climate control and vehicle settings. Often it takes some effort to navigate to the "radio" screen.

So rather than being *the* entertainment source, over the air broadcast radio is one of too many to count. Many millennials and younger people don't listen to broadcast radio at all. Some don't even know it exists.

And yet, recent surveys show that over-the-air AM/FM radio still tops the list of preferred in-vehicle listening. People still tune in and listen, many faithfully. It's true that many of these people are older, but they are still listening, and as long as they are, we will keep playing the hits and providing the quality programming that those listeners want to hear.

What we can't do is take our audiences for granted. Their loyalty and lifetime listening habits aside, they still have choices, and if we don't provide what they want to hear, or worse, irritate them, they may well begin to explore some of those other options. We can't let that happen.

All that means that we have to work harder than ever before to be competitive, and in far different ways than ever before. We've not only got to provide unique and compelling programming and sound deliciously good (far better than low-bit-rate compressed on-demand streams), but we have to *look good* as well.

We're in competition on the vehicle dashboard with all the other whiz-bang eye candy, and we can't just be the numbers representing a frequency or a callsign. We've got to have attractive logos displayed and put up album art and other images related to programming, even our commercials.

And don't forget that metadata. It's got to be there, it's got to be right and it's got to be time-synched with what's playing.

That is our challenge in the 2026 radio business.

So how are your stations doing?

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

Greetings from Buffalo!

I was thinking about some of the cool projects I have been involved with, and one comes to mind.

When I first started working at WPHD and WYSL, the AM audio was on a 15 kHz equalized phone line and the FM had two discreet Marti STLs.

When phone lines really became expensive, we decided to install a new Mosely PCL606 composite system for the FM. This left us with the two discreet Marti STLs to use as emergency backup for the FM audio and also serve as the STL for the AM.

I wanted to be able to switch both STLs around so if one failed, I could still use the remaining one for ether station.

I decided to set up bidirectional control on our Mosely MRC1600 remote control. If you aren't familiar with the unit, it is a very basic remote control with 16 channels of metering control and status. The studio unit and transmitter unit were connected with a phone line for the AFSK data.

I needed to set up bidirectional control, meaning that I had to bring the 16 status bits out so that I could use them to do more than turn on LEDs. Fortunately this turned out to be quite easy, as the LEDs were driven by open collectors internally.

We brought the open collectors out to a type D connector, which we mounted on the back panel. We built two interfaces and ran the FM and AM audio through it to each STL input.

Conversely, at the other end (at the transmitter site), we had a similar interface to direct the receiver outputs to the AM audio processer or a second Optimod that I had on a homemade composite switcher so that if the main STL failed, I could switch to the backup. Of course the audio was in mono in that case. The receiver switching panel also had closures for status. As I previously explained, those status bits were decoded at the studio. This is how I kept both panels in sync.

One day, the PCL606 went down, so I immediately switched the FM over to the backup Optimod. All seemed to be okay, but somehow the two interfaces got out of sync and FM audio was on the AM and AM audio was on the FM!

I got to the studio as soon as I could only to find the announcers had come up with the most logical solution: they switched studios! We got a good laugh out of that.

In the original design, we had capacitors in series with the bases of the relay driver transistors to create a momentary pulse. We removed them so that the open collectors would hold a constant low on the base so that it would be impossible for the two interfaces to get out of sync.

This past month, at the WDCX transmitter site, the air conditioning stopped working, causing the room temperature to reach around 100 degrees. After resetting the breaker, everything seemed to return to normal operation.

This caused me to realize how important it is to be able to keep tabs on the temperature in your transmitter rooms. The only way we knew something wasn't right was that the HD signal kept dropping out. We could reset the exporter remotely, but it would only stay up for a short time and crash again, evidently because of the high temperature.

I am going to install a smart thermostat so that I will know about the problem before equipment starts failing.

We had a tower crew out at the WDCX AM transmitter site in Brockport to work on some tower light issues we had. All has been fixed.

At the WDCZ AM transmitter site, we are waiting for some parts to come in to fix a few lighting problems that we are having.

That's about it from Buffalo for this month!

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

Cisco Not Perfecto, Part Two

As reported last time, one of our normally trustworthy Cisco 3560CX switches exhibited an unusual problem where it would act normally and pass TCP packet data, but its multicast functionality would fail. We use Wheatstone's Wheatnet audio over IP system which is, like others, dependent on multicast networking. This malfunction interrupted audio in the studio, but administrative connections to the Wheatnet related hardware remained up.

Replacement of the switch with another 3560CX has so far been a remedy. However, Detroit has been receiving a remarkable amount of rain and wind this spring causing unstable power at our studios. A few days ago, while working in that studio, we lost power briefly. All of our studios have UPS systems, but for whatever reason this one allowed the power to drop. Could this short drop be causing the Cisco switch to malfunction rather than restart entirely? I may never know and the offending switch will never see duty on the AOIP network again.

TRE+

For some reason that no one can seem to find, our HDRadio Artist Experience images have stopped being triggered. Logs and screenshots have all been sent to the developers. For reasons unapparent, only the station logo appears and the text corresponding to the message being transmitted from TRE+ is working. I'm hoping someone will swoop in and figure this out because I'm out of things to try – or am I?

I decided to try reducing the delay which I presume is there to keep message displays in alignment with program audio. We need about 48 second to account for our profanity delay and the diversity delay introduced by HDRadio itself. Bingo! Remove the delay and everything works! Reintroduce it to any significant amount and TRE+ malfunctions.

I'm guessing the TRE+ dev team will be debugging this and hopefully providing a fix in their next release. For now, things are working, but our linked message timing is way off.

Genny Genny, to Whom Can I Turn?

Last month, I wrote about our studio/FM site generator and our ongoing battle to make it happy with its fuel supply. Since it was placed on site, we've had to have a completely new service brought in from the street with larger pipe, new regulators, and a new meter. They allowed us to raise our supply pressure from ¼ PSIG to ½ PSIG or 13.8-inch water column. Our generator calls for between 7 and 11 inches of water column, which converted is about .25 PSIG to .4 PSIG

Once we got our new natural gas supply, we had more than enough pressure, which was, as luck would have it, too much. Too much pressure exceeds the range of the generator's governor and causes about 30 to 45 seconds of surging where the generator runs but hunts for the 1800 RPM required by the engine to produce 60 Hz AC at the proper voltage. This causes the transfer switch to delay moving the building to emergency power sometimes, and other times it transfers to the unstable power.

The answer to this should have been to place a regulator alongside the generator to drop the pressure from the 15.5 inches we have to around 10 or 11 inches. We installed that regulator last fall, but soon noticed a completely new set of issues.

With our new regulator, the generator would start reliably with no hunting or surging. This we thought was the answer to our problem, and it did prevent the surging, but what we didn't know was that under load, the generator would starve for fuel. That new regulator was either defective, or it severely limited the generator's gas volume. Under load, we were seeing less than 1 inch of pressure causing the generator to stall.

I quickly condemned the no-brand generic regulator and bought a Maxitrol. The plumber installed it, but issues remained. With the adjustment screw run all the way down, the generator only received about 6" WC, which certainly helped but was nowhere near the 9" WC I'd hoped for.

A gas regulator's range is set by the amount of pressure placed by a spring on a diaphragm. Pressure can be adjusted by changing spring itself for a course adjustment or by moving a screw up or

down that presses on the spring for a finer adjustment.

9 inches almost on the nose under load.

I decided to call the supply house and order every size spring available for the Maxitrol. I also ordered my own manometer. Once these things arrived, I was easily able to dial in the exact pressure I wanted, which I settled on 9", splitting the difference between 7" and 11". The generator starts every time without hunting and performs as it should at full load.

I also noticed and tightened six or seven exhaust manifold bolts that were backing out of the cylinder heads.

GV40 Monkey Business

During the latest round of springtime power outages, I decided to keep our GV40 from throttling all the way up to our TPO of 27 kW while the generator was on. Full transmitter power output was stalling the generator (see story above), and since the Burk remote control system knows when we transfer to generator power, it was easy to make the GV40 change to a lower power preset.

The trouble was that when the power failed, the GV40's single board computer lost power, too, and rebooted, resulting in the GV being blind to SNMP commands for a few minutes. By the time it restarted, the GV's independent control had ramped the power up to the point where the generator would stall and the SBC would restart again.

Nautel provides a completely isolated single-phase input for the SBC computer and exciter, which I had wired to a breaker during installation. Although the panel containing that breaker was on emergency power, it wasn't on a UPS, meaning it was dead while the generator started. I wired in an APC 400VA UPS to cover the brief time while the generator starts so we don't lose SNMP or any functionality of the GV40's user interface.

The UPS now feeding the GV40's SBC.

Miscellaneous Ramblings and Goings On

This month has brought with it the April ample precipitation promised by the old saying "April showers bring May flowers." This means we haven't had an opportunity to spray, and I'm betting the weeds are tall enough to whisper in your ear! Hopefully, the next few weeks will dry out, and we can get them sprayed rather than having to cut them down with a machete.

We bought several UPSs at the same time. Guess what all their batteries are doing? Fortunately, Home Depot sells them for way less than you'd pay going through your friendly IT retailer. Check them out next time you need a sealed lead-acid battery. Plus, they deliver!

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

Ready or Not, AI-Assisted Quantum Computing is Here

For a long time now, most white-hat cyber security experts have taken the position that their companies just needed to keep ahead of their black-hat counterparts by removing the low hanging fruit and thereby knocking out 95 to 98 percent of the possibility of a security vulnerability crippling their organizations.

The "fruit removal" involved working to keep security patches updated on network routing and switching equipment, keeping computer operating systems and other hardware up to date, educating users about making their passwords difficult, and making sure firewalls and VPNs were guarding access to all that data in the first place. Overall, we've done a reasonable job of keeping ahead of most of the script-kiddies and people with moderate to low level hacking skills. There is this one pesky hacker from Portland that Stephen has gone around with on several occasions, but we typically have been ahead.

That is, until recently. We're coming into some scary times regarding the protection of data that even the best of practices will have a hard time combating against. Quantum computers have been coming of age for a while now.

Unlike the device you're probably reading this article on that uses binary 0's and 1's called bits of data) computing to efficiently chew through the math required by your programs and to generate content, quantum computers use a quantum bits (qubits), where the bit value can be both values at once at the same time. The power in quantum computing comes when the hardware is able to begin reading multiple qubits, which expands exponentially as 2n, where n is the number of qubits. Quantum computers are similar to the computers you are familiar with, but they all get better computationally with more powerful processors and additional cutting edge hardware.

Is there some kind of difference in performance? That question is loaded. It all comes down to the different math that can be done with each. Getting back to the security bent with which I started the article, binary computers are great for a lot of computations and have advanced our civilization at breakneck pace, but they are really awful at cryptography math. That is, the encryption that powers most of the internet, the fundamental math that keeps your well thought out password safe or the website encryption that we count on to make sure we're looking at a "secure" site.

Most of that encryption cannot be easily broken with the binary computers. (Check your password here to see how long the current estimate to break your password would be https://www.security.org/how-secure-is-my-password/).

In contrast, quantum computers' mathematical ability is fantastic at encryption style math. In 2024, Google's Willow quantum chip, a state of the art 104-qubit processor, performed a specific computation in five minutes that would have taken a traditional supercomputer 10 septillion (1025) years. Obviously, the "specific" may have been a well-engineered problem, but the fact remains that I've got five minutes to wait, I don't have 10 with 25 zeros years to wait.

Why does all of this even matter? Most quantum computing specialists believed that a quantum computer could break most RSA-2048 encryption with a computer that contained between 100,000 to 1 million qubits. Just this month, both Google's Quantum AI team and a Cal Tech startup named Oratomic both produced papers that stated that they had figured out a way, with the help of AI, to reduce the necessary number of qubits in a quantum computer to down around 10,000. When Cloudflare, a company that manages about 25% of internet traffic, saw these papers, they moved their timeline for having necessary post-quantum encryption up from 2035 to 2029 – a six year reduction.

The real problem with this I see is twofold. First of all, the problem is massive. It affects financial institutions, any internet entities, governments and big businesses. Most companies (or people) simply aren't ready for what is going to be necessary to protect themselves.

The second, more sinister nature of the issue

is that there have been entities stealing encrypted data for a long time that have been waiting for this opportunity to come around. These "Harvest Now, Decrypt Later" folks clearly didn't have the time or resources available to purchase a supercomputer and wait for the results, but they could hang on to entire lists of encrypted passwords and data and store them...and wait. They have all been continuing to collect and sit on the data with the thought that eventually quantum computing would be more ubiquitous and they would be able to begin drilling down on the data they've collected and have a payday.

I know it sounds like the internet is basically planning to eat itself for dinner, but there are things we begin to do ahead of all of this to make sure that we are somewhat better prepared. The first thing to do is realize that you cannot afford to continue keeping your passwords simple, cute phrases, or birthdays or anything that can be remembered. I suggest beginning to use a password manager. There are a number of them out there, but when you use a password manager, your password can be longer which will allow the de-encryption to require more time.

The second consideration is to begin to use 2-factor authentication (2FA) with as many accounts as you can. Generally, 2 factor authentication not only requires your password, but you also have a physical device that gets texted or emailed to you with an actual code that you have to use in order to access your accounts. This requires an "Authenticator" app that is up and running on your device, but it is tied to the account so that when a request for access to the account is asked for, you are notified and asked to give the code. If the code isn't provided, then no access is granted.

The fact remains that a lot of us have traded ease and convenience for our digital security and the two are things are diametrically opposed. A user that has a lot of convenience baked into their digital data life has weakened, or at the very least, minimal security. I fear that we're moving toward a time when making things more difficult for yourself will not only put a hedge of protection around all of your data, but also make it more difficult for others to get to as well You've got a three year head start, but don't be surprised if, with AI's assistance, that time frame gets shortened again.

If One AI Story Wasn't Enough…

Another story that brewed up in April 2026 was that Antropic AI's Mythos AI code model was found to be incredibly good at finding vulnerabilities in software. In fact, it was so good at finding those issues that they didn't end up releasing it out to the wild, but took an entirely different path. They handed it to the likes of Broadcom, Cisco, PaloAlto Networks, Google, Crowdstrike, Apple, Microsoft, The Linux Foundation, Nvidia, AWS, and JP Morgan Chase and told them to use Mythos to make sure their software stacks were free of any crippling bugs. Bugs that might show themselves if other frontier AI models, like DeepSeek, ChatGPT, or God forbid, human hackers were unleashed into their code.

As I mentioned an article or two ago, the mental model we need to be holding onto is not that there has been an AI model named Mythos that can or could hack everything, but that the skill floor for doing sophisticated cyber hacking is dropping, that you, or I, could sit down at a computer in an afternoon and bring multi-billion dollar entities to their knees. Truly, AI is taking the technical out of the technical at a frightening pace.

With that, I apologize for the fatalistic themes that show up in my articles. Until the next apocalyptic calamity, may the Lord bless the work of your hands.

Tales From Cousin IT
by
Stephen Poole, CBRE, AMD
CBC Corporate IT Specialist

It has been 15 years since Sandy and I were awakened by the sound of a tornado approaching our neighborhood. Thank God, it was dissipating by then but was still more than scary enough to go along with. We suffered some roof and siding damage; our neighbor up the street had his home knocked off its foundation and destroyed.

This was part of the April 27, 2011 outbreak that killed hundreds of people and destroyed countless businesses, homes and cars. Many of you were watching live coverage of the Tuscaloosa tornado that afternoon. Figure 1 is a radar image that I've seen many times since moving to Alabama: the classic tornadic "hook" signature. This EF4 twister tracked through T-town, stayed north of Birmingham and hit Fultondale before dissipating just past 850 AM's transmitter site near Tarrant, AL. It passed within 1000' of tower #5 of our array.

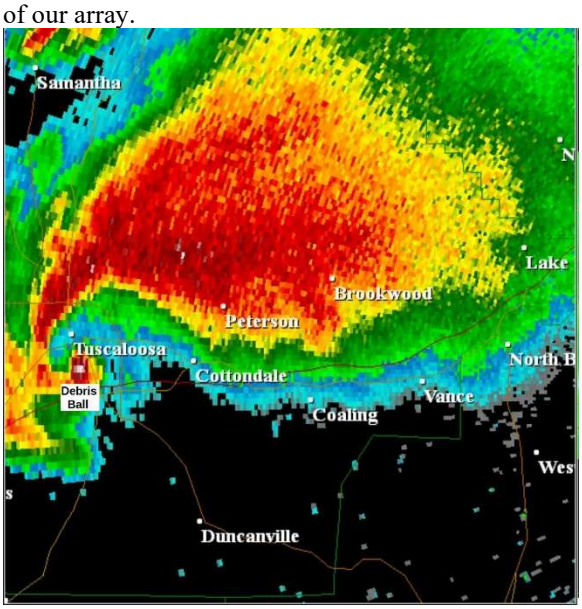


Figure 1 - Classic 'hook' signature with debris ball for the Tuscaloosa twister

You may also have seen videos of the EF3/4 that tore through Cullman, AL, after first crossing within a couple of miles of our 101.1 FM in nearby New Hope. But we had another city of license that was devastated by TWO tornadoes on that same day but received very little coverage: our 92.5 FM is licensed to Cordova, AL (Figure 2). We rebuilt that site when we purchased it back in the early 2000's, installing a new ERI antenna and a new Nautel transmitter. The tower itself is in the middle of nowhere, in a little neighborhood called Pumpkin Center. Alabama Power gave us a Quinton, AL address.

I used to enjoy driving through the countryside out that way. It takes time, but it's very pretty. More than once, I took back roads through Cordova headed back to Birmingham. It really wasn't much of a town; it had a small early-1900's style main street and boasted of its own Piggly Wiggly. But on April 27, Cordova was destroyed (including that supermarket) by not one, but two tornadoes.

Figure 2 - EF4 headed to Cordova, AL on 04/27/11

The first was part of the same storm that had shaken my house that morning; it did quite a bit of damage as an EF3 twister that passed through downtown Cordova. Later that afternoon, an EF4 twister with 170 MPH winds came through, finishing what had been started that morning. There were still work crews trying to restore power and remove debris when the second tornado warning was issued. No doubt they looked at each other and said, "No way!" ... and then ran for cover.

Hackleburg, Phil Campbell, Cordova, Ruth ... small towns that you've never heard of and all destroyed on April 27. They didn't get the attention that Tuscaloosa did and that's understandable.

Sometimes it's just a matter of a city or town being large or notable enough to support a media presence. But I'll never forget that afternoon, driving around to check on our sites, only to receive one call after another from Sandy and Todd Dixon saying, "No, don't go that way!" I finally just went home; the roads to our sites would have been inaccessible, anyway.

The Mail Server!

Thanks to Amanda Hopp, Todd Dixon and Jack "Dangerous Man" Bonds, we got this done on Wednesday, April 22. I had planned for a nice, orderly day, with The Big Move scheduled for that evening after hours. That plan flew out the window when I checked my email again around 10 AM and received a "bad certificate" warning. I had generated an SSL certificate for the new server, but GoDaddy canceled the old one sooner than I had planned. Yay.

I briefly considered regenerating a certificate for the old server so that we could follow my original plan, but that could have taken hours (speaking from experience; GoDaddy can take that long or worse). I'd then have to regen again that evening (and wait for hours) for the new server. I alerted Cris and contacted Amanda, Todd and Jack and said, "Help, we need to switch servers now!" They pitched in and we had everything essentially done in just under an hour.

We're still fixing the occasional glitch: missed accounts that didn't get transferred, settings that had reset to the defaults on the new server, passwords that weren't updated, that sort of thing. But all in all, it was much smoother than I had feared.

Up until the weekend before, I was still having trouble making our Barracuda Spam Firewall "talk" to the new server. I finally ironed that out, though, and we were ready to move, thank the Lord!

This new mail server is much faster than the old one. There's no comparison; it's night and day. We have trimmed a bunch of older accounts and webmail access has been disabled. Just eliminating the web access has drastically trimmed the number of hacking attempts, so that tells me something. I had received a Red Alert warning about bugs in Zimbra's webmail that hackers were specifically targeting, so getting rid of the webmail interface turned out to be an even better thing than I'd planned!

There's still one annoying guy in Portland who is determined to get into our mail system. I have to be careful about blocking his IP addresses, because they're part of the same Comcast/Spectrum group that some of our sites use (as I mentioned last time). It's always something, but God is good!

Figure 3 - Jimmy Parker's view of the Artemis 2 launch!

Cris and I have anxiously awaited the completion of the mail project because there are so many other things that we want to do. I'm back on the idea of putting SNMP access into our older Nautel transmitters.

There's also a need for an Enberg-type alert display for phone calls and EAN activations. I'd never heard of Enberg until Cris asked if we could do something like that (in NC, most of my stations were too poor to buy fancy gadgets; we did well to stay stocked with light bulbs and coffee).

A Bit More Info on Encrypted Connections ...

I want to add a caveat to what I discussed last time. I implied that public-private key encryption couldn't be tapped. It can, but only by a man-in-the-middle ("MitM", because of COURSE we need another acronym) attack. This is where a Bad Guy literally sits in the middle, whence the name. You establish the connection, the MitM captures your request, then makes his own connection to the other end, relaying and examining everything from that point on.

It would take a lot of work, but it can be done. If you're a cynical, suspicious sort of fellow, you might wonder about your third-party VNC service. Sure, they absolutely promise – spit-dog-swear! – that they would never sniff your data ... but, well, you know. (Heh.)

I've given some thought to building our own little test setup that could sniff encrypted links. OpenSSL, the package that almost everyone uses, is understood by Wireshark, and the latter can be instructed to grab the secret key before it starts sniffing packets. It can then use that secret to decode things back to unencrypted data.

Jimmy Parker

You may remember this fellow. Jimmy worked with us as an assistant engineer starting in 2006 for the new studio buildout at 120 Summit. He married a sweet Christian girl in Huntsville and eventually moved up there to work as an engineer for a TV station.

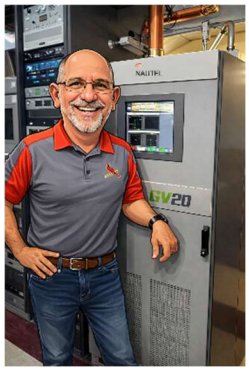
Todd told me that he's now in Florida, working for NASA, so I texted him. He's in their public information department, helping with the technical details. He had a great view of the launch of Artemis II; see Figure 3, which is a capture from a video that he made on his phone.

Until next time, keep praying for this nation!!

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

"I've been hacked"!

That's not a phrase that I heard when I was young. It certainly isn't something IT and engineering likes hearing. But at least several times a year something like this is said.



Internet security is always a topic that we must face as broadcast engineers. This past month certainly made me realize that it is not something you look at occasionally, like a spring cleaning. We must be diligent daily.

I am always amazed at two things: one, how good hackers are at breaking carefully constructed, complicated passwords; and two, how average users still use super easy passwords.

I was forced to look at both sides of this coin recently. First, as we transitioned to the new Crawford email server, I needed to collect users email passwords. I was stunned at how simple some of the passwords that our staff was using. Stunned but not totally surprised, as we have hacked email accounts on a regular basis. Of course, the other side of this was the users who don't know their password.

I took pride in crafting complicated passwords that I and our local engineering staff could remember so we wouldn't be spinning our wheels in an emergency trying to login to something because we forgot the password.

So, a few weeks ago, I had a piece of equipment with a GUI get hacked, and whoever did it changed the passwords (which were not the factory defaults, by the way). This happened to be at a site that was 100 miles away, so it not only was it a potential liability, but I had to take that long drive to deal with the problem.

The other part of this was the manual didn't have any instructions on how to factory reset it from the local box. I both called and emailed support, but it took a long time to hear back after I already had left the site.

While all that was annoying, I realized I had a piece of equipment with what I considered a fairly strong password behind a firewall. This meant that this password was compromised and that anywhere I was using it would have to be changed, especially at this site.

I also had a strong suspicion that the local router was not as secure anymore. It was an older model in which the manufacturer had not released any updates for years. I had already been in the process of replacing it because of these reasons and a new one was being shipped.

I have shaken my head at the stories where someone has a piece of broadcast equipment with the default password, and it's not even behind a firewall. Just like I do with the passwords that are so simple. I have always tried to have at least a modicum of security measures. But I realize that I probably need to step my efforts even further.

I am glad that our company is no longer allowing users to select their own passwords for their email accounts. Long, complicated passwords are a pain to use, but worse is your email not getting where it needs to be due to the domain being listed as spam.

The reality is that internet security is a weak link function. That sounds like a cliché, but it is true. You're only as good as your weakest link. Do we know what our weakest link is?

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

I feel like a broken record, but where has the time gone? Spring is here. Winter never showed up in Colorado.

In Aurora, where the studios and my primary residence are, we are in a "stage one" drought. We can only water lawns twice a day, restaurants can't just bring water out to a table unless a person requests it to drink, and I'm sure there are more restrictions, but those are the two I know of for a fact.

At home I am doing my best to restrict the water I use. At the office I am having to remind people not to run our dishwasher every night (we shouldn't be doing this anyway) but only when it is full.

Many reservoirs and lakes around Colorado are significantly low. One of which is so low they are going to pump the water out and move it to another, deeper reservoir because if they don't, the water will just evaporate and be wasted.

In town, it doesn't really seem to be a huge deal. Yes we are on restrictions, but there isn't a sense of fire danger and for one reason or another, the fact that water supply is low just isn't a thought to cross anyone's mind.

In the mountains, where our second home is located, it's another story entirely. Beetle kill in years past has devastated trees all over, the East Troublesome fire and many other wildfires over the last six years have burned up a lot, leaving dead and downed trees in their wake.

What this means is that even the tiniest of sparks can start another wildfire. The need to keep the growth cut at our cabin is an absolute must, something we are already good at doing. We can only do our part, and hope others do too.

There are some who will be brainless (and who have already done so) and will do a controlled burn, have a campfire, shoot a gun or do some other careless act and will cause a fire to start. All we can hope for is that they will get under control quickly.

My Second Job as a Plumber

A true broadcast engineer's job is not just fixing transmitters. We have other equipment to deal with for the on-air side. All of us these days do IT work, and many transmitters are now equipped to be accessed on the internet, which is crazy.

I recently found myself trying to fix the dishwasher at the studio. Our sweet receptionist came to me one day saying that it wasn't working. It had power, but we never heard any water run. I know nothing about dishwashers or any appliance really. So I went to my trusted assistant, Google.

Google had several thoughts on what to check. I also discussed it with my dad. I first replaced the float switch. If this is stuck in one direction or another, it can either tell the dishwasher to stop filling or to keep filling. Since it wasn't filling at all, this was a good possibility and a cheap fix. Unfortunately, this did not fix the issue.

I then replaced the drain pump. There was some water standing in the bottom of the dishwasher, so perhaps it senses that water and since it can't drain, it just doesn't work. That was not the issue.

My dad finally got some free time and came to investigate with me. I had noticed on the door switch connector (behind the cover) a white connector that was discolored. It didn't look too bad at that time, and since the steam comes out near the top, I figured this was normal.

On the day my dad looked at it, it had gotten worse. It was blackened and parts of it were falling out. This indicated an actual burn of some kind. We checked the wires from there to the various other parts and found that there was a disconnect. The solution was to replace the door switch. This is what finally solved the problem.

Sometimes it takes a second pair of eyes and someone who might know a bit more about appliances to find the issue.

UPS Batteries

I think I've mentioned before that I have been working on getting UPS batteries replaced throughout our facilities in Colorado. A few years ago, I created a spreadsheet with each UPS with the

location and what the battery replacement is and when the battery was last replaced.

Typically, I wait until I see the dreaded red light to change out the batteries. That isn't very smart, and it's not necessarily something I meant to do. The goal is to replace them before it's needed to help keep things going.

The battery packs that many of the rackmount UPS units use cost a few hundred dollars. We have found that we can buy the individual batteries (on Amazon or from Home Depot) for a fraction of the cost of the entire pack and just disassemble the battery pack. The hardest part is getting the old, original battery unstuck from the cage it's on. Going forward, since all batteries have been replaced, they shouldn't be stuck.

Spring Is Upon Us

Thankfully, we've gotten some wonderful spring rain in the last couple of days. Not a ton, but some. I wish that smell could be bottled and saved.

What rain means for me is growth. You've seen me write about it a lot over the years. Daniel worked hard over the winter to get the brush hog repaired. The metal has weakened in areas and needed to be welded. And the blade needed to be sharpened. He did a beautiful job with the weld work. To be honest, it looks so much better than when we hired a professional welder to fix it. He was also able to remove the blades and get them sharpened. He has been working on all our site maintenance equipment, getting it ready for the work that is ahead.

We have had some growth from last year, which while dead, still needs to be cut to lower the fire danger. Plus, the weeds. I don't care how dry it is… I think Colorado could turn into a desert (it's getting close now!) and the weeds will still grow and be green and happy.

It is really my hope that with Daniel on board with us, together we can stay on top of the growth. With the fire danger so high, I really want to get each site cut better than it has been in years. I am going to look into buying some weed spray for our site up in Brighton, CO. We've had some good luck spraying after we mow. Maybe with some teamwork, Daniel and I can get it sprayed and keep the growth to a minimum this year.

Coming Up

Did I mention spring has sprung? I think mowing season will be here in a matter of weeks. So of course, we will begin focusing on that. I do not want things to get out of control like they did last year.

I also plan to do some spring cleaning. At the office, the studios all need a good cleaning. From vacuuming dust to wiping down, carefully, the equipment.

The tower sites are all in decent shape thanks to Daniel checking in on them periodically and cleaning up. This will be a good time to do something more in depth. I may take the power cubes out of the ND transmitters at the four sites and clean them really well. I know at KLTT, I've seen some mouse poop in there when they've been removed. Not something we want. It doesn't appear the mice have caused damage as the transmitter still runs great.

It has been many years since I've done a cleaning like this on these transmitters. I remember something always blew up once I put it all back together. I hope this time, it goes better. At least it will be good practice on repairing the old transmitter.

As I look through my things to do list for each site, the theme is consistent. Clean. Clean inside buildings, clean up equipment, clean the growth or a better term would be clear out the growth. Clean up cameras, clean up lock boxes and keypads. Clean transmitter filters (or change depending on the type of filter). Change out AC filters.

I am grateful to have help this year from someone who is eager to work and genuinely seems to enjoy it. It is going to be a great season ahead for us.

That about covers it for this edition. Until next time, 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