The

Broadcasters' Desktop Resource

www.theBDR.net ... edited by Barry Mishkind – the Eclectic Engineer

Doing IT Right

Securing Gear On The Internet

By Bill Putney

[March 2017] Recently a series of radio station program hijackings have brought attention to those using digital links over the public Internet without proper protection – and ending up running offensive audio. Can a station protect itself without spending exorbitant amounts of money? Bill Putney discusses the problem and solution.

The public Internet is a worldwide party line. As soon as you attach something directly to it you can safely assume everyone everywhere has access to your device and someone will find a way to abuse that access.

Anything you can do they can do. If you are operating a modern computer-controlled transmitter they can change power, frequency, or program source to feed their choice of program instead of what you are sending from the studio. If it is your STL codec they just have to pretend to be you and your station has become an outlet for whatever is their current cause or whim.

If this alarms you, it should.

REGULATORY IMPERATIVE

As broadcasters, we have a regulatory responsibility to maintain control of our stations and protect them from being operated outside the limits of the station's license restrictions.

Thus far, the FCC has been very understanding about the incidents of station takeovers via the Internet. However, I cannot imagine they will continue to give stations a pass on this. I do not think that connecting a non-secure device directly to the Internet is ever the right thing to do.

Ultimately I think the FCC will see this as negligence akin to having no lock on an unattended transmitter building door. At some point they are going to pull out their NOV books and start writing tickets.

FREE IS NOT ALWAYS FREE

The siren song from something that seems to be "free" is a hard one to resist.

Indeed, after so many years of paying big sums of money for the Telco's to provide conditioned an audio circuit, ISDN, or T1 for program and control in radio stations, the Internet was finally deemed "Good Enough" and free – an engineer's dream come true."

And with some care it can be a powerful tool.

But, in reality, the Internet is not a private closed-circuit like a leased line and engineers can put their stations in jeopardy by not understanding the risks and taking steps to reduce them. In that case, it could lead to a situation where, as the song says, "*Free(dom) is Just Another Word For Nothing Left To Lose."*

THE DEFAULT DANGER

The password is your first line of defense Immediately changing it on any new device is something you should do without thinking twice.

First of all, most of the default passwords for the devices we use are in publically available user manuals or Internet groups. And, if you have changed a device's password to "PASSWORD" or "123456" or something equally as guessable, you can count on someone eventually breaking into your device.

If you read your server access or error log, you will be stunned to see how many times each day an automated script "tests" your gear's front line defenses. They come at you hour after hour, banging on your door, asking to be let in.

STRONG PASSWORDS

The password should not be obvious. The bad guys use automated scripts to find passwords, and they will just pound away – often multiple times a second, using what is called a "dictionary attack" – until the password is found.

Here is a simple way to test your password: put your password in the Google search window and if it returns *anything at all*, change the password to something that does not. Change it now.

Longer passwords are better than short ones. Anything shorter than eight characters is generally just asking for trouble. As on TV or in the movies, the scripts will test each character in each place in the password. Given enough time, the script will eventually crack your password.

Fortunately, for most sites, the "script kiddies" eventually will get bored if cracking the password takes too long, and move on to easier places to crack, (Still, I have seen one IP address trying hour after hour for over three weeks to break in on a site!)

Passwords with mixed upper and lower case letters, numbers and punctuation marks work better, increasing the time it takes to crack them.

On the other hand, if there is an exploit for your device, a password alone will not protect you from a determined malicious attack. In the end, passwords, even good passwords, basically just keep honest people honest.

YOU REALLY ARE NOT HIDDEN

Some folks think, even on the Internet with all the scripts running, testing each IP address in turn, that their particular situation is "hidden by obscurity."

Think again. There are websites like Shodan.org which specialize in finding and identifying different types of equipment. Recently, a government agency entered the name of a popular codec and – in seconds – found what appear to be some 250 broadcast-oriented IP addresses.

Think there are some bad guys that already know about this? That is a very good bet – or, actually, a losing one, if you are not protecting your gear.

It is bad enough if an attacker has broken into your device. But, they now may have access to everything else on your LAN by using your device as their gateway.

PROTECTION VIA AN AIR GAP

The best protection is to put an "Air Gap" between the public Internet and the LAN that has become such an integral part of modern broadcast plants.

An Air Gap means that there are absolutely no connections, directly or indirectly, between the public Internet and your LAN, period.

Of course, that makes some of those rich remote access and control features of these devices a little less useful, but it is ultimately the safest way to operate. Still, it can be a lot to give up if you do need the remote access to provide program audio or remote metering and control.

So, sometimes you do have to violate the Air Gap, and we need to discuss how to do that in the least risky way.

UNDERSTANDING THE FUNCTIONS

Broadcast device manufactures who build things like transmitters, audio over IP codecs, and remote controls have their focus on providing you the best functionality for that class of device.

For that very reason, network security is often just a password. You can pretty much assume that the password protection on your device will do little more than keep honest people honest on your own LAN.

As we have already seen, you should absolutely change passwords, but they are not a protection against a determined malicious attack.

SOME MIGHT CALL IT PROGESS

It really is no wonder that a manufacturer of a broadcast device, with all they have on their plate, cannot protect you from all the bad actors on public networks.

With that in mind: When was the last time you applied security patches to any of the broadcast hardware items you have installed?

Do not think this is optional. Every year there are security conferences that focus explicitly on how to protect devices attached to public networks. Each year, it is a foregone conclusion that last year's "fool proof" defense will be broken, sometimes within days of a defense being implemented.

THE RIGHT PERSON

Would you go to a podiatrist for brain surgery? Not, you would go to a specialist in that field.

That means, as nice as they are, and as helpful they try to be, you simply cannot expect a broadcast device manufacturer to protect you from complex network attacks.

For this reason, the network security specialist of network devices is really your primary firewall. And that is the key word to learn: Firewall.

People who produce firewalls spend their entire focus on keeping the bad guys out of your network. They produce software patches as often as it takes to keep up with new attacks and all you have to do is install the patches and not find your own clever ways to defeat the firewall you installed.

THE FIREWALL LINE OF DEFENSE

To better understand what makes a firewall, let us first note the two kinds of network addresses:

Public addresses, unique in the world, that are used as destinations for Internet connections, and "Private" addresses (like 192.168.X.Y) that are blocked from the public Internet.

Similarly, there are two broad categories of firewalls. The first is the consumer style firewall that is part of a DSL or cable modem.

These generally employ "Network Address Translation" (NAT) as their only firewall mechanism. NAT hides all of your LAN devices behind a translator that keeps track of your outbound connections and creates a way for the outside world to reply.

All the world sees is your "Public" network address and your "Private" network addresses are mostly safe behind the NAT wall. NAT firewalls are not foolproof but they make the risks very low unless you do something to defeat them.

These firewalls are intended for use by consumers with relatively little to protect and they will keep the neighbor kid from looking at the email on your laptop.

Yes, the companies that make consumer firewalls go to all those same security conferences and are always looking for ways to improve their firewalls. But there is only so much they can do with a NAT firewall, and they tend to issue very few security updates as consumers generally do not install many of the updates that are available.

THE NAT VULNERABILITY

The principle way people sabotage themselves with NAT firewalls is by poking holes in them using the "Port Forwarding" feature of many of these firewalls.

To direct a connection to a device, the Internet communications connections protocols require a device address *and* a service port number. Any networked device has an address and each networked service on that computer has one or more service port numbers associated with it.

For instance, there are "regular" ports the computer uses for replies to connections it has made to other devices. These are well-known port numbers like port 80 is HTTP (web servers), port 53 is DNS (domain name lookup service), and so on, for special services or users use.

By using port forwarding you can allow devices outside the firewall to connect to a LAN device just as if the LAN device's address was the public address of your firewall. But here is the problem: in general there are no restrictions on who can connect to a port-forwarded port, so it is once again open to the world.

Once an attacker has found any port number that responds at a public IP address they will try every other possible port number, too. In other words, as soon as you have set up a port forward, you have defeated the firewall and left that LAN device to protect itself from attack.

If the device if hardened against attack this can be an acceptable risk but as I have noted, most broadcast plant devices are not first and foremost security devices.

FILTERING

The next class of firewalls are called "Filtering Firewalls" and they are what the big kids use.

These frequently incorporate NAT but *also* allow more restrictive filters to be placed on connections. They can hide in plain sight and be invisible to everyone except the people you want them to be seen by.

As an example, they can react and open up only if they see the right IP address "calling" *and* other filters and various tests can be added as necessary to create a cryptographically secure connection over the public Internet, called a

"Virtual Private Network" (VPN) between, for example, your control point and the transmitter.

Some of these solutions can cost tens of thousands of dollars per site to implement and the more frustrating thing for a broadcast engineer is that some of these firewalls are configured in ways only an IT geek could love.

It may not be a career change you want to make right now.

But fear not, there more reasonably priced and less arcane firewalls available.

In the second part of this article, we will show you exactly how to build a good firewall without spending a fortune.

- - -

Bill Putney is the Chief Engineer for KPTZ, Port Townsend, WA. You can contact Bill at: billp@kptz.com

- - -

Would you like to know when more articles like this are posted?
It takes just 30 seconds to sign up – right here - for the one-time-a-week BDR Newsletter.

- - -

Return to The BDR Menu