4-6 Perry Street
PO Box 1662
Wapakoneta, OH 45895

Located in historic downtown Wapakoneta, Ohio, FNGi has been instrumental in developing and supporting Internet Networks across the U.S. since 1993. The FNGi team can assist you with all phases of your Internet Network from initial planning through long-term support.

www.network1.net
800.578.6381

FOCUS Newsletter

Spring has sprung and as the season of renewal begins, we need to renew our commitment to making sure all of our systems are safe, secure and as stable as they can be. We're looking at the newest security on the horizon for Wi-Fi technology. Learn how to keep your DHCPatriot safe and secure with our easy and robust maintenance contract.

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS April – June 2018

In This Issue

Wi-Fi Protected Access v3

Currently, the best way to secure your wireless networks is using Wi-Fi Protected Access v2 (WPA2). However there are still some issues regarding how this system functions. Last year's KRACK vulnerability has proven that this 13 year old security protocol needs redone.

At this year's Consumer Electronics Show (CES2018), the Wi-Fi Alliance debuted the version 3 of WPA, increasing the security capabilities of the process in several ways.

WPA3 will now support 192-bit encryption natively (with an assumed 48-bit initialization vector) and the Dragonfly Protocol (aka: Simultaneous Authentication of Equals (SAE)). Even the link between the device and the router, for example in on a public network, will be entirely encrypted as well.

The Dragonfly Protocol (SAE) allows for a cryptographically strong shared secret for securing other data-- e.g. network communication. SAE is resistant to passive attack, active attack, and dictionary attack. It provides a secure alternative to using certificates or when a centralized authority is not available. It is a peer-to-peer protocol, has no asymmetry, and supports simultaneous initiation. This will take most of the pressure off of users who do not create secure of varied enough network passwords and make linking devices (mesh networks) easier and just as secure.

The Wi-Fi Alliance has just finalized the spec on WPA3, so don't look for it to enter the consumer realm in the current hardware cycle. Devices that feature WPA3 abilities are expected to reach the market in Q3 of 2018. WPA3 will only work if both devices are capable of using it and first party support from all major operating system vendors is expected in a timely manner. Until then and even after, WPA2 is not going away entirely. This cut over to WPA3 will be a natural and gradual process as new equipment and software come out that can utilize it.

While waiting for WPA3 firmware and hardware to be released to the public, currently the safest method of securing your WIFI is to utilize WPA2 security with AES encryption. While there are ways around WPA2, the likelihood of that happening compared to other security measures is quite low. Other best practices is to remember to rotate your password every few months or not broadcasting your SSID so people out snooping won't even see your network. It's also a good idea to log into your router and check the various devices attached to your network and take an inventory every few months as well.

FNGi
First Network Group Inc

New Threats, Old News?

In January, we heard a lot about Meltdown and Spectre, and the vulnerabilities of microprocessors. One set of theories speculates that the flaws that allow these exploits have existed since 1995. The scariest scenarios proclaim that microprocessors always have and always will be vulnerable to exploit. While that is probably axiomatic, cooler heads take note of the following:

- → The industry has been aware & working on this for some time
- → Some OS fixes were in place before the "news" ever broke
- → Other OS remedies were quick to follow
- → The exploits gain access to data in memory through browsers or other running software with a user interface, so resist the urge to condemn your routers and switches because they are running a listed processor.

The important lesson is to keep all PCs, servers and other systems up to date with current operating systems and software. Hackers are always looking for new exploits and developers are always working to improve security as well as performance.

Fortunately, as hard as some outlets tried to make this the first cyber horror story of the year, the panic was relatively short lived and contained.

In mid-March (2018), the Department of Homeland Security (DHS) issued a follow-up warning to a March 2016 report that Russian cyber attacks have targeted US and European power plants and utility infrastructure.

Once again, phishing has been a primary tool to gain access to systems and plant malware. I understand that DHS and FBI have offered advice and assistance to operators of vulnerable critical infrastructure. As we have discussed in the past, there is no substitute for sound fundamental cyber security policy.

--Steve Walter
Founder, President and CEO

Secure Your Out-of-band Management!

Out-of-band management is an important part of ensuring a quick response to outages in your network infrastructure. For decades, many customers have used old Cisco dial routers as makeshift terminal/console servers. However, they were not originally intended to serve that purpose, and as such can be difficult to configure and cumbersome to use. More importantly, many systems still in use do not support ssh or any other secure access, which puts your network at risk of attack or infiltration.

We, at First Network Group, have tested several replacement solutions over the years. Several years ago, that culminated in our selecting Opengear as our vendor of choice. Opengear offers a wide array of console servers and remote site management units that provide secure access to serial and USB console ports.

Some key features available include:

- → SSH and HTTPS access
- → Cellular out-of-band connectivity
- → Backup WAN connectivity via cellular
- → SFP fiber network ports
- → serial port densities ranging from 4 to 96
- → support for newer USB console ports

As an Opengear partner, First Network Group can provide an out-of-band management solution to fit your needs. Let us help you secure your management and provide a key component to ensure the resiliency of your network.

— Randy Carpenter,
rcarpen@network1.net or 1-800-578-6381 x1

5 Things Your Maintenance Contract Covers

The rock solid, stability and accessibility of the DHCPatriot is enhanced even further with it's annual maintenance contract. We want to take the stress out of a new system purchase. So we provide the DHCPatriot's comprehensive maintenance contract for free for the first year of ownership.

We know you'll be so pleased with your purchase and our service that continuing the maintenance contract after the first year will be a no-brainer. You may already be familiar with maintenance contracts on other vendor's equipment. Our commitment to our product and to you, includes more help and support than you will find in many of them.

The DHCPatriot maintenance contract provides full phone support for any part of the software or the system. We will give you as much or as little help as you like. We will even configure the machine for you, if you'd like.

Software updates are a breeze. You will always have access to the latest and greatest builds of the DHCPatriot software. We call you when the update is available and schedule a time to install it that fits your schedule.

The system's hardware, at any age, is fully protected with an active maintenance contract. Once a fault is found we will expedite shipping of a replacement device in the event of hardware failure. And since the DHCPatriot has back-up systems built-in a hardware failure will rarely take it fully offline. We are proud of our 99.999% uptime and we think you'll be pleasantly surprised as well.

As rugged as the DHCPatriot is, all hardware ages and all needs grow. Your maintenance contract affords you access to our industry-leading trade-in program. You can upgrade to the latest fastest DHCPatriot hardware at a significantly reduced price! We offer a massive credit on the trade-in of the old equipment.

And to keep everything running as smoothly as possible, your DHCPatriot's health is monitored 24 hours a day 365 days a year. If any issues should arrive, they are dealt with and resolved immediately. We want your experience with the DHCPatriot to be the easiest of any of your IT solutions. This level of care is unheard of in offerings from other equipment manufacturers!

We've crafted the DHCPatriot and its maintenance contract to be as hassle free as possible. We've all dealt with vendor issues and limited warranties that always seem to fail the day after the coverage is over. We want you to experience a completely different approach with our product. You will never have to worry about the system as we will be day and night making sure that it is working for you just as hard on day one as day 3,000!

Did You Know?

Hearing music while we're on hold waiting to talk to a company representative is so common today that it's hard to imagine there was a time where people just sat around listening to nothing at all while waiting on hold. What's fascinating about hold music, or Music On Hold (MOH) as it's known in the industry, is that it was completely accidental.

While you'd assume that hold music was purposely created for the benefit of bored customers stuck waiting on the line (and to indicate that the line was still active and hadn't been disconnected), it was created (and subsequently patented) by accident. In 1962, callers put on hold when calling the factory of Alfred Levy were treated to music. The customers complimented him on the nice touch (a touch which he had no idea existed) and he set to work investigating it. It turns out that a loose wire was touching a large metal girder in the factory which turned the metal shell of the factory into a huge antenna. When the calls were put on hold, the radio signal was able to overpower the line signal and the callers could hear music from the local radio station next door to the factory.

Levy patented a more purposefully designed hold music system in 1966 and the rest is history: now we all get to enjoy smooth jazz or sanitized pop songs while waiting to talk to our insurance agents.

Via Howstuffworks

A Few of Our Proud Partners

22 Years — Proudly Serving Our Customers