FNGi
First Network Group Inc

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

FNGi
First Network Group Inc

FOCUS Newsletter

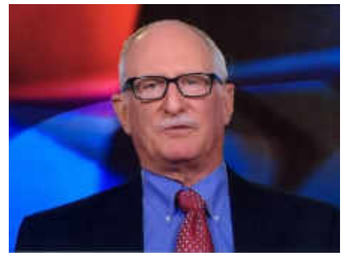
In this issue we explore strong and easy to remember passwords. We talk about how to protect our networks from attacks all over the world and we delve into the mysteries of DHCPv6 as part of the IPv6 rollout and compliance on the DHCPatriot.

YOUR CONNECTION TO FIRST NETWORK GROUP NEWS Jan — Mar 2018

In This Issue

¶Λ$$W0®d5

We've all been thru setting up a password and told to use upper and lower case letters, special characters, symbols and numbers. They can be annoying and make passwords difficult to remember.


Bill Burr

Well you have a man named Bill Burr to thank for this concept. In 2003 Bill was a manager at the National Institute of Standards and Technology (NIST). He created a guide on how to create secure passwords, known as the "NIST Special Publication 800-63. Appendix A."

Ever since then software and websites have relied on the suggestions of this document to create secure passwords. The only trouble is that when Mr. Burr wrote this document he was not well versed in computer security practices. The core idea is that a short password made up of random characters and symbols would be much harder to break down than a short password that's more human friendly. And while that does hold true, short random passwords are not as secure as once thought.

Even though Mr. Burr has admitted that he now regrets most of what he did, it's not all his fault. Fifteen years ago, we all knew much less than what we know now about what it takes to crack passwords.

The best passwords are long passwords that can be easily remembered phrases instead of shorter passwords with a random use of characters.

Example: `P@55w0rd` would take between 9 and 24 hours to brute force or solve.

Example: `MonkiesdrivecarsonThursdays` would take 17 octillion years to brute force or solve. And it's much easier to remember.

While including upper and lower case, numbers and symbols can help secure a password, ultimately password length with a minor mixture of randomness creates the most secure passwords.

No matter how secure your passwords are it's always a good idea to change them routinely (at least once a year). And using a more human-friendly long password will take some of the sting out of remembering all new passwords again.

Enemies Here & There

Major cyber threats have been on the rise and many, like Wanna-Cry, originating in North Korea, have caused massive issues with government and business networks and data.

While North Korea, Russia and China come to mind as the top risks for hacking, this threat shares no specific geographical origin. Concerns over hacked infrastructure have been headlined since journalists heard the word Internet, but foreign actors are even more likely to seek disruption and financial disaster with their hacking.

The #1 security measure against all hacking is to keep your software patched and up to date. Server, home computer, tablet, phone or IoT device, it is imperative to keep up with updates if you want a secure environment, it is the place to start. Remember that updated Windows machines were saved from WannaCry.

If you have routers, servers or even workstations that are too old to update, they are also too old to be secure. Legacy Operating Systems like Windows XP (probably my favorite version) are simply not worth running if the computer is connected - even by modem. Encourage your users to stay current, and lead by example. Skipping an update might be short term savings and long term disaster.

From all of us at First Network Group - we wish you a safe, happy and prosperous 2018!

--Steve Walter
Founder, President and CEO

Did You Know?

A number of flora and fauna cause damage to fiber. Some birds really like Kevlar reinforcing material and think it makes lovely nests for their babies, so they peck away at the fiber-optic cables to get at the Kevlar material.

Several different types of ants seem to enjoy the plastic shielding in their diet, so they nibble at the underground fibers. Sharks have been know to chomp on cable near the repeating points. A plant called the Christmas tree plant think that fiber-optic cable is a tree root and wraps itself around it very tightly and chokes it off.

Telecommunications Essentials, Second Edition: The Complete Global Source By Lillian Goleniewski, Kitty Wilson Jarrett (editor)

Network Attacks

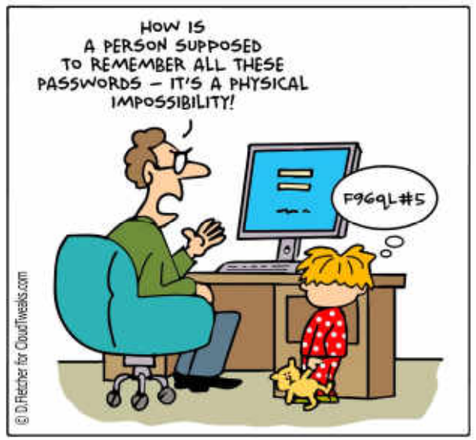
Denial-of-service and other similar network attacks are becoming more common than ever. All it takes is for one of your users to make themselves a target by upsetting a malicious user online. That malicious user could employ a botnet to launch a distributed denial-of-service (DDoS) attack against your user, which could flood your incoming internet connections and overload your routers.

Recently, there has also been an outbreak of attacks against a newly discovered vulnerability in the Network Time Protocol (NTP). This vulnerability allows an attacker to send very small packets to affected servers and routers, which reply with much larger packets. The destination of those reply packets is spoofed, so that a huge flood of traffic ends up coming from your network in response to a fairly small attack that is sometimes hard to identify and trace.

Those are just a couple examples of attacks that can be difficult to deal with. Some attacks can be prevented outright by proper configuration of your equipment. Others are difficult without dedicated hardware to prevent, detect, and respond to more complicated attacks. It is extremely important to keep your equipment up to date and well managed on an ongoing basis to protect against vulnerabilities, which is very difficult without proper software updates and hardened configurations.

First Network Group can assist you in assessing your preparedness, and building a good defense against network attackers. We can help you build proper configurations on your existing gear, or suggest new or additional gear to protect your network. We also provide ongoing maintenance plans as well as 24/7/365 network monitoring and response to help your network perform at its best, and protect against the aforementioned attacks.

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



DHCPv6 Authentication

The upcoming version 6.2.0 will feature captive portal authentication with DHCPv6. Previously, DHCPv6 did not feature the ability to force authentication using the captive portal on the DHCPatriot system.

Each shared network in DHCPv6 now features a checkbox that turns it into an authenticated network. A couple of new subnet configurations have been added to the DHCPatriot system in support of this. The first is “Pre Auth Subnet” which allows the addition of one or more DHCPv6 subnets to a shared network that the DHCPatriot will allocate to unknown devices. These subnets should then be routed to the DHCPatriot device for captive portal authentication using policy routing. This would cover devices connected directly to the network, but what about devices behind a router?

We have also added “Pre Auth Prefix” which allows the addition of one or more DHCPv6 prefix delegation subnets to each “Pre Auth Subnet”. These are subnets that can be allocated to a customer router for use on the LAN interface of said router. This occurs automatically during the DHCPv6 process should the customer router ask. The reason for this is that IPv6 does not support NAT like IPv4 did. Therefore, typically, global addresses must be used on the inside LAN interface of the customer router. These subnets should also be policy routed to the captive portal on the DHCPatriot system for authentication. The DHCPatriot knows which router these belong to and will authenticate both types of subnets simultaneously.

While, typically globally routable IPv6 addresses would be used for subnets and prefix delegations, that is not necessary for these “Pre Auth” subnets and prefix delegations. We recommend using RFC 4193 “Unique Local Address” defined addresses.

The reason for this is that these addresses are not going to be used outside of the local ISP network. Therefore, there is no reason to use addresses from the ISPs globally routable subnets.

The operation of the captive portal in DHCPv6 is very similar to that of DHCPv4. In fact, the same captive portal configurations are used. We will also have various methods that attempt to avoid requiring authentication twice in most situations (once each for DHCPv4 and DHCPv6).

Phonetic Alphabet

Letter	As In ...
A	Alpha
B	Bravo
C	Charlie
D	Delta
E	Echo
F	Foxtrot
G	Golf
H	Hotel
I	India
J	Juliet
K	Kilo
L	Lima (lee-ma)
M	Michael (or Mike)
N	November
O	October
P	Papa
Q	Quebec
R	Romeo
S	Sierra
T	Tango
U	Uniform
V	Victor
W	Whiskey
X	X-Ray
Y	Yankee
Z	Zulu

Provided by First Network Group, Inc. www.network1.net