TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

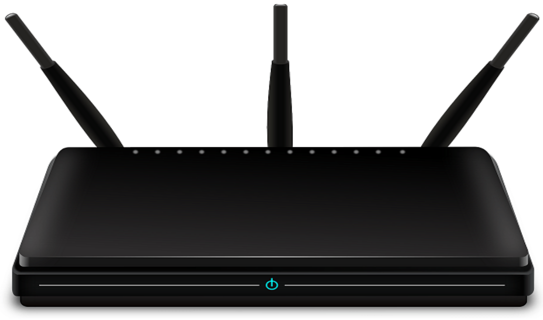
In the News:

- [How To Lose $8k Worth of Bitcoin in 15 Minutes with Verizon and Coinbase](#)
  - Medium
- [How a Few Yellow Dots Burned the Intercept's NSA Leaker](#)
  - Ars Technica
- [OneLogin Suffers Breach — Customer Data Said To Be Exposed, Decrypted](#)
  - Ars Technica

current courses >>>

Non-Standard Communications

This course is designed to teach students how to communicate securely while protecting their identity by employing digital signature reduction measures and digital tradecraft through the use of commercial off-the-shelf technology (COTS), readily available open source technology, and best practices. Students will learn a variety of critical skills utilizing the host nation's commercial digital infrastructure.



Ultimate Router Configuration

Configured with security in mind

When properly configured, your router/modem is the only device that is publicly accessible on the internet. Most routers use what's called NAT to share your public IP address with all the devices under your router. This also helps keep all of your local devices protected by adding a buffer between them and the internet. As we talked about in the last issue, "doors" can be opened on your router, often called ports, without your knowledge. These ports can allow direct access to the devices on your local network. Below is a list of every router setting that has potential benefits or disadvantages pertaining to security. Before changing any settings on your router, make sure you're aware of what you're changing. If your router has a back-up option, it's worth backing up your original settings.

Admin Credentials: Routers come out of the box with default credentials (admin, password, 1234) and these should always be changed. This is your first line of defense to the admin settings of your router. Anyone who is on your local network can access the admin portal and change your router settings. This can also be done remotely if you have remote management turned on.

Wi-Fi Settings: We covered several security practices on Wi-Fi in depth two issues ago. The most important things to consider here are SSID and Wireless Security. You should always be using the WPA2 standard. Both your password and SSID should, under no circumstances, contain personal information.

Remote Management: This setting allows you to remotely manage your modem or router from the public internet. This is almost never necessary and should be turned off. If your situation requires remote management, be sure to choose strong credentials and, if available, change the default port. Changing the default port will prevent automated scanners from trying to log in with default credentials, but this should not be relied on.

Continued on page 2 —>

Threats and Vulnerabilities >>>

The Issue With WPS

We have stated in numerous issues of the digital update and in previous courses about how bad the WPS protocol for routers is and how you shouldn't use it, but we have never really explained why. That's because there is no quick answer and there's not just one reason.

The most practical reason is because it undermines the need to use a password on your wi-fi network. You can have a strong, random 63 character password, but it would be undermined by the eight digit pin that WPS provides. You go from a very hard to guess password with a full character set to a numeric only pin that, in comparison, is laughable as an authentication method.

Another reason boils down to lack of physical security. Who has access to your router? If an attacker can gain physical access to your router, they can either read the pin on the bottom of the router or simply just push the WPS button to connect to your router without authentication. This not only applies to WPS, but this applies to the entire router. How difficult is it to plug directly in via ethernet?

The more complex reason starts with implementation of the protocol by the router manufacturers. Random numbers are very hard to produce and require a lot of entropy created from many different data sources. Some router manufacturers take the easy way out and generate their random numbers using the same algorithms and the same starting values. This results in predictable WPS pin codes on every router made by that manufacturer. This makes attacks like the Pixie Dust Attack quick and easy.

If your router is not vulnerable to this attack, an attacker can still brute force your WPS pin which should be 100,000,000 possible combinations, but because the pin is split in half before being checked and the last digit is only a check digit, we get down to only 11,000 possible combinations. That's still a lot of pins to run through, but it's only a matter of time. For more info contact: admin@tpidg.us

Upcoming Events:

Associated Locksmiths of America Security Expo

June 16-22 2017, Rosemont, IL

National Technical Investigators' Association (NATIA) Annual Conference

July 12-23 2017, Tampa, FL

BlackHat USA

July 22-27 2017, Las Vegas, NV

DEFCON 25

July 27-30 2017, Las Vegas, NV

The easy button >>>

Ultimate Router Configuration

Cont. from page 1

WPS: This protocol has been broken and insecure since its conception. Many router manufacturers use unreliable random number generators that can be easily predicted and cracked in a matter of seconds. This should be turned off and never used because it makes your strong, random password absolutely useless and bypass-able. See above for more details on why WPS is a bad protocol.

Port Forwarding: This setting gives you the ability to open a door on your router and allow an incoming connection to one of your local devices. This can be useful if you are running a server, but can be dangerous if it is open for no reason. Any and all ports that are not being used should be closed, which you can accomplish by deleting the appropriate port forwarding rules.

DNS: Domain Name Servers play a very important role on the internet: translating domain names to IP addresses. While no content actually goes to these servers, it can still be dangerous to use untrusted domain name servers. For example whoever owns your domain name server could point you to a fake site pretending to be google.com. On the subject of Google, they have their own DNS servers at 8.8.8.8 and 4.4.4.4. If you have attended one of our NSC courses, you know that we tend to stay away from Google products, so we do not recommend using these DNS servers or any others that store logs of which sites you ask for. While they cannot see what content you are sending to and from the sites you go to, they can see where you are going and link that to your IP address.

Check back next issue for part two!

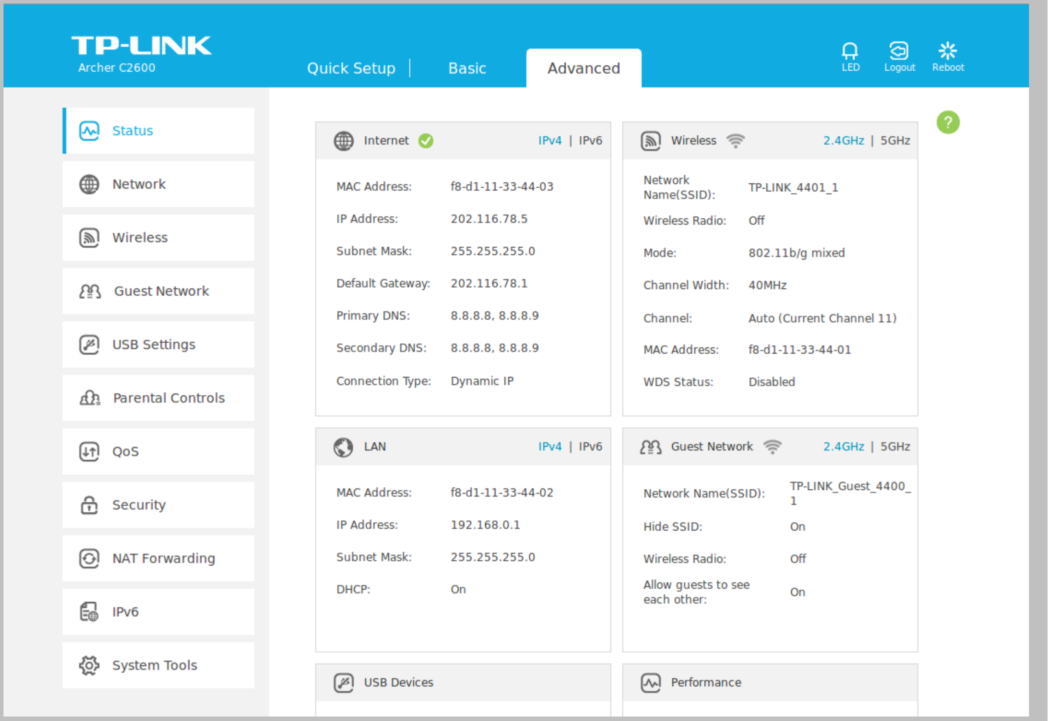
Bonus Materials >>>

Router Emulators

Test settings with an emulator

If you want to try out the settings in the first article of this newsletter without the risk of messing up your router or if you have internet downtime while you change the settings, we recommend using a router emulator. Some router manufacturers offer an emulator as part of their support documentation. It can be very useful to play around with router settings before purchasing or switching to a new router, as some routers support different features and all manufacturers use their own custom router firmware. Many manufacturers don't publicly post on their website that they offer emulators, but a quick search for "router emulators" returns quite a few results for them.

Below are links to a few router emulators that you can try out for free:



Internet ✓ IPv4 | IPv6

MAC Address: f8-d1-11-33-44-03
IP Address: 202.116.78.5
Subnet Mask: 255.255.255.0
Default Gateway: 202.116.78.1
Primary DNS: 8.8.8.8, 8.8.8.9
Secondary DNS: 8.8.8.8, 8.8.8.9
Connection Type: Dynamic IP

Wireless 2.4GHz | 5GHz

Network Name(SSID): TP-LINK_4401_1
Wireless Radio: Off
Mode: 802.11b/g mixed
Channel Width: 40MHz
Channel: Auto (Current Channel 11)
MAC Address: f8-d1-11-33-44-01
WDS Status: Disabled

LAN IPv4 | IPv6

MAC Address: f8-d1-11-33-44-02
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0
DHCP: On

Guest Network 2.4GHz | 5GHz

Network Name(SSID): TP-LINK_Guest_4400_1
Hide SSID: On
Wireless Radio: Off
Allow guests to see each other: On

[TP-Link Routers (Various Models)]

[Linksys Products (Various Models)]

[Netgear Prosafe Wireless Access Point WG102]

[D-Link WBR-2310 Router]

[Belkin F5D8236-4 Router]

Update Corner >>>

Website Updates

Updates to https://www.tpidg.us for the month of May. For comments or suggestions email admin@tpidg.us

Login Changes

- Added ability to change username
- Added ability to change password
- Added upcoming events to main profile page

OSINT Changes

- Added the following APIs:
  - Pipl
  - Gravatar
  - Twitter
  - Flickr
  - Twilio
- Updated the way people are displayed (click on results for more info)
- Added a page for external tools
- Added a Google Hacking page (still in beta)

coming soon >>>

In Future Issues...

Ultimate Router Configuration Pt. 2

USG USB Firewall

Private Domain Name Servers

The Dangers on USB devices