in this issue >>> V.1.19


```
   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3177:d8c:a694:b42%13
   IPv4 Address. . . . . . . . . . . : 10.5.10.6
   Subnet Mask . . . . . . . . . . . : 255.255.255.252
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:
```


TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- ATM Skimmers: A Closer Look
  - Krebs on Security
- Tips From Ex-Burglars On Making Your Home More Secure
  - Lifehacker Security
- US Navy Laptop Breached—134,000 Sailors' Data Compromised
  - Ars Technica
- Ultra-Secure Android Phone: Tor Phone
  - Ars Technica
- One Million Google Accounts Compromised by Android Bug
  - Ars Technica

TMAC

MAC Spoofing Made Simple

A computer's Media Access Controller (MAC) is an identifying number burned into the machine's hardware. When you connect to a Wi-Fi router, this address is stored by the router. This is necessary for the router to keep track of what computers are connected to it. These records are stored in the router's logs, and can be accessed by anyone with access to the router. This might be undesirable if you are trying to keep a low profile.

Fortunately, it is possible to force the computer to transmit a temporary MAC that is different than its permanent MAC. By using a randomly assigned MAC, the computer can connect without fear that his or her true MAC will be recorded by the router. This process is known as "MAC Spoofing". MAC Spoofing has traditionally been somewhat difficult and required knowledge of command line. Fortunately a program for Windows computers called TMAC makes MAC spoofing a very simple task. TMAC requires only a single click to temporarily change the computer's MAC.

If you need to conduct business that can't be traced back to you, spoofing your MAC on a public Wi-Fi network is a good way to do it. Another protection that MAC spoofing offers is privacy. Users who frequent a particular Wi-Fi hotspot risk revealing details about their real-world and online habits. Using a randomly generated MAC each time allows these users a degree of anonymity.

Many operating systems including Android, iOS, and Windows 10 already use MAC spoofing or "MAC randomization" to conceal a user's true MAC address when a device is transmitting Wi-Fi probe requests. This is to prevent users from being tracked through the MAC contained in these requests. However, these automated MAC randomization protocols switch off when the device actually connects to a network. Spoofing on a more persistent basis requires a user implemented solution.

Using the program is simple. First, download the application from **https://technitium.com/tmac/** and install it. Upon opening it your MAC will automatically be changed. If you would like to change it again, click "Random MAC". This will display the new MAC address, and the hardware manufacturer associated with that MAC (i.e. Cisco or Intel). Clicking "Change Now" will change the MAC again. MAC spoofing has traditionally been accessible only to those with considerable technical know-how. Tools like TMAC place it within reach of even the most casual user.

set the stage >>>

Local Backup Basics

Last week we discussed the importance of backups and we discussed some cloud storage options. We also discussed some best practices for cloud storage backups. Though data stored offsite is much more resilient against local disasters, it can have its downsides, too.

If you lose data and need it immediately, that may not be an option with cloud storage that depends on a stable internet connection for access. By placing data in the cloud you are also exposing it to serious risk of compromise—both on the cloud server and while in transit. Data breaches happen on a regular basis and to think it couldn't happen to a cloud server is faulty. Cloud storage also comes with a pretty significant expense. Depending on the amount of storage your require this monthly fee can add up quickly.

Local backups have the benefit of being free, aside from an initial investment in a hard drive. When looking for a hard drive you should consider one that is at least twice the size of your computer's internal hard drive or SSD. Backups can take up a lot of space, and you will probably want room for at least a couple of incremental versions.

Backups should also be encrypted to the same level as the original data. If your backup hard drive is lost or stolen you don't want the data on it to be readily accessible. There are a couple of ways we can go about protecting this data. Some programs like Mac's Time Machine allow you to encrypt the backup itself. Even if the hard drive is encrypted, a decryption password is required to access the backup.

An alternative strategy would be to encrypt the drive containing the backup. This can be done through a number of utilities. The best strategy for Windows users is BitLocker. VeraCrypt would be a good alternative, but we have found that some backup utilities won't recognize a VeraCrypt-encrypted drive. Mac users should stick with FileVault for encrypting their external hard drives.

Upcoming Events:

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

National Technical Investigators' Association Annual Training Conference

July 12-23, Tampa, FL

Associated Locksmiths of America Expo

16-22 June, Rosemont, IL

The easy button >>>

Local Backups: OS X

One of the best backup systems we've encountered is the Mac OS X Time Machine backup utility. This setting allows users a very intuitive way to create good local backups and it can work in any of several different ways. Setting up Time Machine is incredibly simple. Attach your storage device and open the Time Machine settings, located in System Preferences. Select your disk and Time Machine will take care of the rest. In the future when you connect the disk a backup will be automatically started. Initially a full backup is created. As changes are made on the host computer, incremental backups are made to keep your data as current as possible.

You can also use Time Machine in conjunction with Apple's AirPort Time Capsule. The AirPort is a Wi-Fi enabled hard disk drive that functions as a Wi-Fi access point for your home. When your computer is plugged into power and you are connected to the Wi-Fi network your computer will automatically back-up to the AirPort's hard drive. This system keeps your backups current without requiring any additional effort from you. They are encrypted to the access point with WPA2 encryption.

Speaking of encryption: the backups themselves can be encrypted within your Time Machine settings. In the Time Machine setup menu you can click the "Encrypt Backup" option. This will ensure that your backups are protected. As mentioned previously, external media like your backup hard drive can be encrypted using Apple's native FileVault encryption. This creates a very robust solution for protecting your data.

Apple also offers seamless backups for iPhones, iPads, and iPods. These can be backed up to a Mac or Windows computer using iTunes. This backup can be kept completely locally and can be independently encrypted. This backup is stored on your computer and is copied when your computer is backed up.

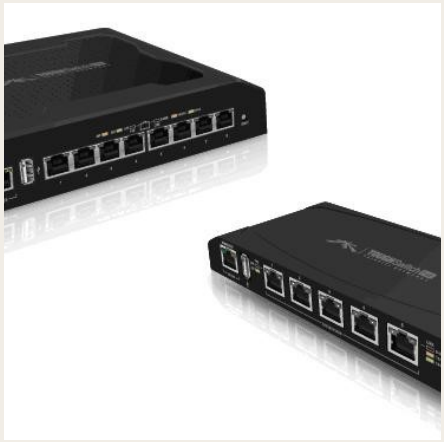
ToughSwitch

PoE Security Camera Switch

The ToughSwitch is another networking device made by Ubiquiti (like the EdgeRouter X we reviewed in a previous update). The ToughSwitch is a managed PoE (Power over Ethernet), 10/100/1000 compatible switch and it comes in three different versions: 5 port, 8 port and 16 port. All versions support Power over Ethernet, which allows compatible devices with an Ethernet port to accept power and data over a single cable. This makes networking cameras and other small devices so much easier because you only have to run one cord to the device instead of two (this is assuming you don't trust Wi-Fi).

The 5 port version only support 24V PoE, so you're limited to what can be powered, but the 8 port and 16 port both support 24/48V PoE. Unlike some other devices on the market, the ToughSwitch supports PoE on every port, and each port can be turned on or off as necessary. The device boasts an intuitive interface and Gigabit connections on every port. The interface allows you to do things like set up alerts for network activity, configure VLANs, setting up remote logging and normal switch settings you would find on any other switch. The VLAN setup is very easy to configure, just tag which ports you want on the VLAN and un-tag the rest. As we've mentioned before though, do not rely on VLANs for network segregation because it is possible to hop VLANs.

Overall, the ToughSwitch does everything you could hope for in a switch. You could set up an entire surveillance system with just one ToughSwitch using the PoE capability to power the cameras. Ubiquiti makes some really good products and we will definitely be looking into more of their products. For additional info or questions, contact admin@tpidg.us



coming soon >>>

In Future Issues...

Unifi Video

Firefox Focus

Mailfence

Wire

CRITICAL TOR VULERNABILITY

Mozilla, the software company behind the open source Firefox web browser, has recently released an update for the version of Firefox used in Tor. This update patches a critical zero-day vulnerability that is under active attack right now. This attack allows Tor users to be de-anonymized, which can lead to exposure of their true identities. If you are a Tor users, **update immediately** to the latest version at **https://www.torproject.org/download/download-easy.html.en**

The threat itself is very specific: when users visit sights that run scripts to display vector graphics, their real IP address and MAC may be transmitted. This defeats much of the protection offered by Tor. Mozilla and the Tor Project rate this vulnerability as "critical". In addition to updating Firefox, The Tor Project has also updated the NoScript script-blocking software that is included with Tor.

Because scripts are allowed to execute in this version of Tor, it is also potentially a problem in the more mainstream Firefox browser. Users should update their version of Firefox, as well.