in this issue >>> V.1.13

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Password Strength Meters Still Aren't Trustworthy
  - Lifehacker Security
- NIST's New Password Rules You Need to Know
  - Naked Security
- Opt-Out of WhatsApp Sharing Your Phone Number with Facebook
  - Naked Security
- Meet USBee: Air-Gap Jumping Malware
  - Ars Technica
- iOS Hack in the Wild: Update iOS Immediately
  - Ars Technica

CradlePoint AER-1600

In a previous issue, we reviewed the Cradlepoint MBR 1400 which is a router aimed at SOHO networks. The AER 1600 is similar in many ways to the MBR 1400, but there are many key differences that we would like to highlight. First off, the AER 1600 is one of the newer models of Cradlepoint routers and it's more geared for primary, application specific and micro branch networks. As such, it has a faster processor and more interfaces to keep up with a small to mid-sized network. The beauty of the AER 1600 is the self-contained solution it provides with the box itself being fairly small, the WiFi antennas and the LTE modems being internal, and the only external component being the antenna for 3g/4g. The device supports multiple connection types for internet access including Ethernet, WWAN (WiFi as WAN) and it supports LTE as a failover network, meaning it kicks on after you lose your current connection. Some testing showed it takes about 20 to 30 seconds for LTE to fully come on after a connection is lost. Cradlepoint sells modems for many different cellular carriers including Verizon and T-mobile which support dual SIMs. The AER 1600 supports dual modems as well, which allows the use of two different cellular networks at once. It has five switchable 10/100/1000 WAN/LAN ports which can switch between LAN and WAN to allow multiple or no Ethernet connections to the internet at once. As for WiFi, the AER 1600 supports dual band connectivity (2.4 GHz & 5 GHz, 802.11 a/b/g/n/ac), which is nice considering the MBR 1200 only supports one band at a time. Each band allows for four separate networks in the air at once and they can each be put on their own separate VLANs allowing for further customization of your networks depending on your networking needs. As with all Cradlepoint routers, we have options to fine tune the firewall to meet specific needs, MAC filtering, content filtering, and VPN support (IPSec, OpenVPN and L2TP) to connect to a bigger network to gain access to network resources or to connect securely to a network you trust. We also have the option of paying for cloud management which allows for remote access to your router from anywhere in the world. Cloud Management comes with a fancy looking user interface that allows us to monitor data usage, network details, configuration settings and even GPS location. The AER 1600 is a bit on the pricey side, but it is definitely worth the investment if you are looking for a good, solid router. For additional info or help with troubleshooting or setting up your Cradlepoint router, contact admin@tpidg.us.

set the stage >>>

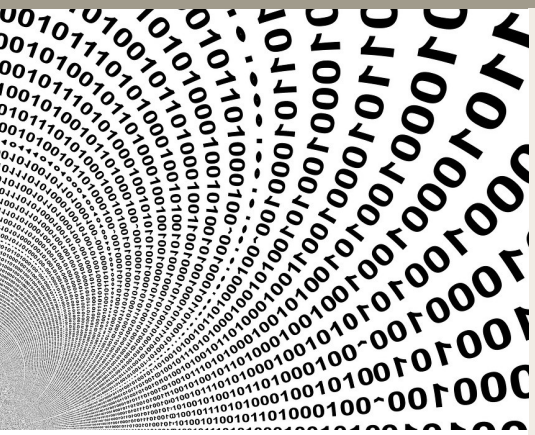
Mobile Device Security: Pt VII

Over the last six issues we have covered a number of aspects of mobile device security including OS and app updates, app permissions, and virtual private networks. In this final installment we will discuss lost phone tracking software. Both Android and iOS devices offer the ability to track a lost device. On Android devices this is done through Android Device Manager. On iOS devices this is called "Find My iPhone" and is done through iCloud. Both of these services also have similar function sets. They allow you to track and retroactively lock a lost device, and wipe all the data from the device.

Before enabling (or disabling) these services you should be aware of the benefits and disadvantages. We have worked with both Google Device Manager and Find my iPhone, and have found them both to be surprisingly accurate. In fact, they rival nearly any GPS for location accuracy. If you lose you phone it should be very easy to locate it, assuming it has not powered down. On the other hand, your geolocation is stored in either a Google or iCloud account. Should your account be breached an attacker could track your location until the breach is discovered. It is up to you to choose what the greatest risk is based on your personal and operational threat model(s).

Android: You don't need to do anything to enable this function. Simply login to your Google account (the one used on your Google Play account). Once logged in search "Find my phone" and Google will open a map page with the current geolocation of your device. To turn it off, you must go into the account settings and disable Android Device Manager.

iOS: Navigate to Settings>>iCloud. Toggle "Find My iPhone" on (requires an active iCloud account). Now login to your iCloud account on another device and select Find My iPhone.



The easy button >>>

Kismet Smarter Wi-Fi Manager

We recently discussed the dangers of Wi-Fi on mobile devices in the Mobile Device Security segment. As we mentioned there are a number of threats that are made possible through an active Wi-Fi interface. As we also mentioned, keeping your Wi-Fi turned off is the safest and surest mitigation to these vulnerabilities. We recognize that it can be a annoying to constantly have to toggle Wi-Fi on and off. We also recognize that toggling it off is easily forgotten. Fortunately there is a solution that can automate this process for us.

Kismet Smarter Wi-Fi manager is a mobile application for Android devices. As the name implies this application manages your Wi-Fi networks with security and privacy in mind. The app "learns" where you use Wi-Fi by monitoring where you connect to Wi-Fi. If you connect to your home network, your work network, and a local coffee shop, Kismet Smarter Wi-Fi Manager will automatically turn Wi-Fi off whenever you are not in one of those locations. It will also turn Wi-Fi back on when you return to one of those locations.

This allows you to "fire-and-forget" Wi-Fi by enabling it and leaving it alone. Kismet works by creating geofences (a geographic boundary) around the locations where you use Wi-Fi. These geographical boundaries are defined by the cellular towers in the area. Kismet Smarter Wi-Fi Manager can also allow you to disable Wi-Fi during time ranges, and it can ignore selected networks that you don't wish to connect to in the future.

Giving the application access to your location data requires a certain level of trust. Kismet's code is open source. If that weren't enough, it has also been used as part of the Blackphone's standard OEM software load.

Kismet Smarter Wi-Fi Manager is $1.99 and is available from Google Play.

Upcoming Events:

Fort Mead Tech Expo

01 September 2016, Ft. Mead, MD

Ft. Gordon Cyber Security & Tech Day

19 October 2016, Augusta, GA

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

For more information go to www.tpidg.us

Online Account Security

Usernames

Recently we have talked quite a lot about two factor authentication. We have also frequently mentioned password managers and the need to use one. Both of these are things you should be doing. If you are doing these things and you still want to increase the security of your online accounts there is one additional factor you can look at: usernames. Usernames are almost never discussed as a security measure. This is because of bad training—by services like Gmail—that your email address IS your username. Few have considered that there is another way. Usernames should be the very first line of defense for online account security.

If an attacker is after one of your online accounts he or she has a couple of options. First, it is logical to attempt your email address. Most people use their email address as their username on most sites. Some sites do not allow a username; in this case people usually use easily-guessable information like their last name plus year of birth (i.e. johnson87). By knowing your username, the hacker already has an excellent starting point from which to launch the attack. Fortunately this easy to prevent.

When you create usernames you should use a different one on all your online accounts. The username should be a random string of letters and numbers, and should be as long as the site allows (usually 24-32 characters). This makes it extremely hard to guess and makes even finding the right account to attack difficult. However, some sites require an email address to be used as a username. In this case we recommend using a service like Blur.

Blur offers a function called "Masked Emails". These email addresses can be created on Blur's web interface or in your mobile app. They forward mail to your real email address so you don't have to check multiple accounts. And they betray nothing about you: Blur email addresses are random and look like **7UGC37A@opayq.com**. You can create as many Blur email addresses as you like. You can also turn each one off if you no longer need or begin receiving spam from it.

This will not protect you against a couple of things. First, it will not protect you against broad, unfocused attacks. These are the types of attacks that breach hundreds of thousands of email accounts a year. The hackers behind these credential thefts don't care about you specifically. Your account is just a number. Using a random username will also not protect your account in the event of a large-scale data spill. It will still protect your privacy however.

Anyone seeing a random username will not know that a particular account belongs to you. For example, you may not want anyone to know you participate in a certain dating site or social network. If you username is random/unique, you can prevent them from correlating an account with your name.

Using different usernames on all your accounts may seem challenging. In reality it is no more challenging than using different passwords, assuming you are using a password manager. This is an overlooked and tool that can greatly increase your online security.

coming soon >>>

In Future Issues...

Blur

Privacy.com

Critical iOS Update

Patches In-The-Wild Exploit

Earlier this week Apple announced the release of iOS 9.3.5. This new operating system deals with three different critical zero-day vulnerabilities. These vulnerabilities (dubbed "Trident") allow an attacker to steal confidential messages from WhatsApp, Gmail, Facebook, and other apps on the device. Researchers believe the exploit has been in circulation for some time—months to years. Because of it's criticality the exploit kit sells for $8 million (for 300 licenses) it is most likely employed by state actors.

If you have not already done so, **update your iOS operating system(s) immediately**. This includes your iPhone, iPad, and iPod Touch. We have said it here before and will say it again: nothing is free from vulnerabilities. Updating software including the OS and installed applications is the surest and most effective way to deal with them.