in this issue >>> *V.1.10*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Baton Rogue Police Information Made Public By Hacker
  - Naked Security
- Oklahoma Police Department Exposed by Database Leak
  - Naked Security
- Android's Full Disk Encryption Just Got Much Weaker—Here's Why
  - Ars Technica
- Ten Million Android Phones Infected with Auto-Rooting Malware
  - Ars Technica
- BOLO: Mac Backdoors Found In the Wild
  - Ars Technica

TILE Bluetooth Tracker

Convenience Vs. Security

The TILE is a Bluetooth tracking device that is used to find various things attached to it. For instance, you can put a TILE on your keychain or glue one to your laptop. It's so inexpensive you could have one for every valuable in your house for a few hundred dollars. It is a great device to use if you've ever lost your keys and you couldn't find them.

The device runs by connecting to an app installed on your smartphone. The app requires both your Bluetooth and Location Services to be on at all times while using the app. The TILE communicates with your smart phone up to 100 feet via Bluetooth. You can make the TILE play a ringtone until you find it or you can press a button on your TILE and have it ring your smart phone. The Location Services come into play with keeping track of where in the world your TILE is or was to assist you in finding it if you lost it.

If you have completely lost your device and don't know where to begin looking for it, you can enable TILE's lost function. This sends a request to their servers and alerts every phone with the TILE app installed. Every one of the phones then probes for your lost device and you receive a notification when your device is found. This is a really cool concept, but it is a privacy and security nightmare. At any given time, your phone could be looking for several other lost devices around it. Not to mention, TILE collects all of this information and keeps it for the life of your account. A quick read through their privacy policy gives a bit of hope. TILE does not share your information with anyone that doesn't absolutely need the information for TILE to operate.

You are, however being tracked 24/7 with this app running and one breach of TILE's servers could tell hackers where you and all of your valuables are. They could also establish a pattern of life, seeing where and when you go to work or what places you like to visit throughout the day. The TILE is a really neat and inexpensive device to keep track of your lost things, but it also tracks your every movement. Good news is you don't have to worry about TILE, you just have to worry about the people trying to hack into TILE.

For more information on the TILE visit https://www.thetileapp.com/. Touchpoint is currently looking at this device from both offensive and defensive standpoints.

set the stage >>>

Mobile Device Security: Pt IV

In the fourth installment of this series we will discuss passcodes. Though this might not seem like the most interesting topic, it is incredibly important to protecting the data that is stored on your mobile device. This data includes access to your email accounts, your personal photographs, text messages, phone calls, and internet browsing history. If you use mobile banking or ecommerce apps, getting into your phone might also give an attacker access to your financial information.

Regardless of what kind of phone you use, you should use a good, strong passcode. Android and iOS devices differ only slightly in the passcode options they offer. One notable difference is that Android offers the "pattern" unlock that allows you to swipe a pattern on your display. Because of the limited number of options in a pattern, this is not recommended under any circumstances. Patterns have also proven to be terribly predictable. Additionally, patterns are easy to see in imprinted on the screen.

To access your passcode options, in Android open **Settings >> Security >> Screen Lock**. In iOS open **Settings >> Touch ID & Passcode >> Turn On/Change Passcode** and tap the blue "**Passcode Options**".

Both Android and iOS offer the ability to use custom-length numeric passcodes. These let you use a long numerical code, while still using the more user-friendly numeric keypad. Android phones allow up to 16-character passcodes; iOS devices place no restriction on the length of passcodes. We recommend using the longest passcode you can manage, and recommend a minimum of eight characters.

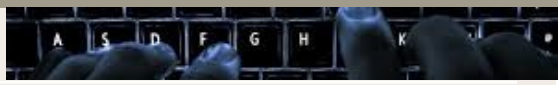
Using an alphanumeric password is the best practice, but we realize few are willing to use the full keyboard to unlock their phone.

Upcoming Events:

-Blackhat 30 July-04 Aug 16
Las Vegas, Nevada
- Ft. Meade Tech Expo, Sept 01
Ft. Meade, MD
- Military, Police, & Law Enforcement Expo
Sept 14-15, Ft. Leonardwood, MO
- Marine Military Expo, Sept 27-29
Quantico, VA

For more information go to www.tpidg.us

The easy button >>>



COMSEC: Key Fingerprints

If you are a graduate of our NSC or Data Protection courses then you understand the importance of protecting the content of your text and voice comms. Verifying key fingerprints is an important step in knowing who your communications are coming from.

Most reputable encrypted messaging apps offer a way to verify key fingerprints. Wickr, Signal, and Threema (which we have covered here in the past) offer ways to verify that you are talking to the person you *think* you are talking to. These are called "fingerprints". Your device's unique encryption key produces a reliable output of letters and numbers that collectively are referred to as its fingerprint. Duplicating a fingerprint is mathematically improbable to the point of near impossibility, so if you verify another user's fingerprint, you can have high confidence that you are talking to that person.

In Signal, when you open a conversation with someone you can look at both fingerprints (yours and theirs) by opening the conversation and tapping the contact's name (Android) or long pressing their name (iOS). This will open a screen with both users' fingerprints. How do you know you are seeing the correct fingerprint? You have to get the user to send his or her fingerprint to you via another communication method.

Sending through another method is incredibly important. It should be a pathway that a hacker would not know. When I verify my Signal fingerprint, I usually send it via Wickr to the recipient's Wickr ID. While it is possible that one of these mediums has been compromised, it is very unlikely that an attacker has compromised both.

When you receive the other party's fingerprint in Signal you have to visually compare them to ensure they match. If they don't stop immediately—something is wrong!

CradlePoint

Tactical-Capable Wi-Fi Router

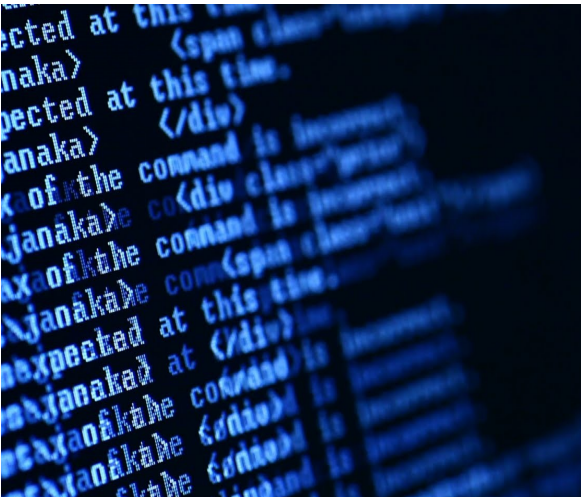
The CradlePoint MBR 1400 is a high powered router with many features aimed at small businesses, temporary command centers, home offices, recreational vehicles, and mobile networks. It is designed to be plug and play for any scenario that involves multi-client access to the same network. The MBR 1400 does not provide internet, but it does make it easy to connect it to the internet. It offers several different means; one way would be using WWAN (WiFi as WAN) where you can connect the MBR 1400 to an existing WiFi network giving you internet access. Another way would be to connect it to 3G/4G which is as simple as plugging a MiFi or a USB compatible modem into any of the three available USB ports on the device. CradlePoint also sells dedicated 3G/4G modems that snap into the base device and add their own dedicated antennas.

Because this is a router type device, it has Ethernet ports on it allowing for a normal wired connection and giving clients the choice of connecting via an Ethernet cable. The MBR 1400 comes with 5 Ethernet ports: one for WAN and the rest for LAN access. As for WiFi, this device is capable of operating four WiFi signals at once on either the 2.4Ghz or 5Ghz band, but not both. It also runs all the networks on the same channel, so careful planning will be needed to avoid clogging up a single channel. Each WiFi network and physical Ethernet port can be on the same network or separated into their own networks with different permissions or features. For instance, you could have two networks, one-set up for physical connections and one for WiFi.

The physical network could be assigned a 192.16.0 network, have access to the router administration page and be able to see all other clients. For the WiFi network, you could assign a 172.16.0 network, deny access to the router admin page and completely isolate each wireless client. In the same sense, you can set restricted websites based on what network the client is on or you can do it by MAC address which is not recommended (any MAC based rule is easily bypassed). You can also set up networks to be hotspot networks where clients have to agree to a custom terms of service page before being granted internet access.

The firewall capabilities on the MBR 1400 are pretty intense and you could spend hours micromanaging all of the individual settings it provides. You can set the firewall as an implicit deny and only allow what you feel is appropriate for your situation or you can set it as an explicit deny and only block certain services. The things you can block include: certain ports, IP addresses or protocols and you can do this based on MAC address (again not recommended). This device also has the capability to connect to a remote VPN, cloud management, custom DNS servers, GPS (with a GPS enabled device), port forwarding, several options for NAT and much more. Overall this device is a very nice router with several necessary features in it and could be very useful in any situation where networking is difficult.

For more information on the CradlePoint MBR 1400 contact us at admin@tpidg.us. We are happy to assist you in the purchase, setup, or troubleshooting of the CradlePoint router.



Google's Allo

Insecure By Default

Google recently announced a new messaging application called Allo. Allo is similar to Apple's iMessage platform, but differs in one important way. Although it is capable of secure end-to-end messaging, it isn't setup that way by default. Instead, Allo is setup to send all messages in plaintext by default.

Users can configure Allo for secure messaging, but this is a bad precedent. Because most users will be unaware of this setting, most will probably continue to use the app in its default configuration. This is bad for two reasons. First, it is a huge missed opportunity to encrypt a huge number of communications by default. Second, many users who do configure this setting to secure their messages will probably communicate with people who don't. This compromises everyone's security.

Allo is available in the Play Store but at this time we do not recommend its use. There are just too many good alternatives available.

coming soon >>>

In The Next Issue

CradlePoint AER-1600

Mobile Device Security: Part V

Virtual Machines