in this issue >>> V.1.9

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- The Best and Worst Encrypted Messaging Apps
  - Gizmodo
- Comparison of Secure Messaging Apps
  - The Intercept
- Severe Bugs Found in 25 Security Products from Symantec/Norton
  - Ars Technica
- US Customs Wants Your Social Media Accounts When Traveling
  - Naked Security

Tiny Hardware Firewall

Protection on High Threat Networks

Tiny Hardware Firewall (THF) is a small, portable device designed to be used on networks you don't trust and protects you from the dangers of public access internet. It accomplishes this in a few ways, the first way is by sitting between your device and the untrusted network using a wired or wireless connection.

This is not a unique concept to the THF, but it is a very important part of the device. It hides your device's MAC address and protects any ports that may be open on your device from being exploited. The second way this device protects you is by having a built in VPN that you purchase with the device. We would like to see this device allow custom VPN settings instead of being restricted to using the built-in VPN, but the built-in one does a pretty good job with speed and privacy.

Finally, THF is equipped with the capability to connect to the TOR network which runs on top of the already running VPN. If you're feeling extra paranoid, you can connect your device to the THF and then connect your device to its own VPN and run the TOR browser on top of that. Beware though, doing this will slow your internet connection speed to a crawl. Overall, this device is definitely something you should consider using when connecting to untrusted networks or even at home if you don't want your ISP spying on your traffic.

set the stage >>>

Mobile Device Security: Pt III

Installing applications on your mobile device is something that all of us have done. You have probably noticed that when you do, you are sometimes shown prompts, asking you to permit the app to access certain features or functions like your camera, microphone, or contacts. Sometimes, access to these features are necessary.

Our favorite encrypted messenger, Signal, is a good example. Signal requests access to your microphone, contacts, and other services. While microphone access might seem scary, the app needs to access the microphone, otherwise it is not able to transmit your voice calls. Signal also needs your contacts, because this is where it discovers which of your contacts are Signal users.

Some apps, on the other hand, request far more permissions than they actually need. For example, a flashlight app or game has no reasonable need to access many things, including your camera, microphone, location data, or contacts. Many apps "over-request" access so they can record location data, harvest contact lists, and other information. This information is then transmitted (often insecurely) and sold to data marketers.

Both iOS and the Android devices allow you to carefully control each app's permissions (this only applies to the latest version of Android—version 6/Marshmallow. If you have an older version, check for an update.)

iOS: Open Settings and scroll to the bottom where all apps are displayed. Each app will allow you to toggle access to contacts, photos, location services, microphone, camera, etc.

Android 6: Open Settings, and tap Apps. Open each app individually, and tap "Permissions" inside the app. Toggle offer permissions that the app does not need.

Upcoming Events:

-Blackhat 30 July-04 Aug 16
Las Vegas, Nevada
-NATIA 09-15 July 16
Seattle, Washington

For more information go to www.tpidg.us

The easy button >>>

COMSEC: iMessage & FaceTime

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. Apple's iMessage and FaceTime apps give you built-in end-to-end encryption

Millions of people already enjoy Apple's organic iMessage and Facetime applications. These apps let you communicate over Wi-Fi-only connections, and don't use up your messaging plan or phone minutes. What most people don't realize is that both of these applications are encrypted, end-to-end. This means that billions of encrypted messages are being exchanged daily iMessage users. If you use either—or both—of these services, you are already using encryption.

iMessage encrypts its content with AES-128 encryption. The initial handshake between devices occurs when keys (which are stored on Apple servers) are exchanged between devices. This is how your device "knows" another device is iMessage-capable. Though iMessage encryption is strong, it's implementation is aging. Some security researchers believe it is time for a major security upgrade. Also, we should point out that a vulnerability was recently discovered that can allow photo and video attachments to iMessage to be intercepted. FaceTime also encrypts your voice-only and video chats using the same algorithm.

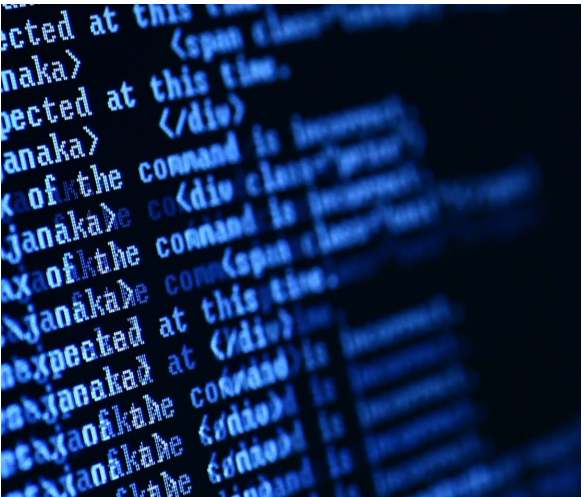
Both of these apps offer decent security. Perhaps the best thing about both is that they won't raise suspicion because they don't present as security apps. Unfortunately, these apps are only available on Apple devices. Although Apple theoretically could, they have not brought iMessage and FaceTime to other platforms like Android. This would greatly increase the number of people you could securely message.

Windows 10:
Full Disk Encryption?

If you have attended any identity management or digital security course, you know that we highly value full-disk encryption. Full disk encryption protects the entirety of your computer's hard drive, including its operating system, programs, and all files and metadata. Full disk encryption comes with a slight cost in performance. Decrypting files as they are used does use some processing power and may slow your computer down slightly. This is really the only disadvantage. Full disk encryption is transparent to the user and provides excellent protection for your data-at-rest.

With the release of Windows 10 we have encountered some problems applying full disk encryption to some computers. Specifically, computers that meet the following criteria: have a solid-state drive AND run Windows 10. Historically we have used TrueCrypt and VeraCrypt to protect system hard drives. With computers with this configuration, VeraCrypt is unusable because it cannot process Windows' new GPT architecture. Using full disk encryption is still incredibly important, regardless of what operating system you use, so we have been searching for a free, open-source solution to this issue. Unfortunately we have yet to find one.

As a result, we are now (reluctantly) recommending you use Windows' native BitLocker. There is nothing wrong with BitLocker and we believe it provides strong encryption. BitLocker is also full-featured, also allowing you to encrypt removable media like flash drives and external hard drives.



Our primary issue with BitLocker is that it is not available to all Windows users. BitLocker is only available with the premier versions of Windows 10 (Pro and Enterprise). If you have Windows 10 Home, you will have to pay $99.99 to upgrade to Pro. We believe the ability to full disk encrypt is worth the upgrade price, but realize that many cannot afford to pay a hundred dollars (hence our hesitation with this recommendation).

If you choose to upgrade to Windows 10 Pro, the process is fairly painless. Open your Settings, then System, then About. Click the "Change Product Key or Update Your Version of Windows" link. This will take you to the Windows website where you can purchase the Windows 10 Pro Pack, which contains BitLocker.

Once you have upgraded, you can enable BitLocker and fully encrypt your computer's hard disk drive. Open your systems' Control Panel. Select "BitLocker Drive Encryption". Your computer's hard drive(s) will be displayed. Choose the drive you wish to encrypt and click "Turn on BitLocker". You will be prompted to choose an encryption password. Of course we recommend you choose a very strong one.

Next, you will be asked where you wish to save your recovery key. This key will be used to unlock your computer if you lose your password. We recommend saving this information with one of the local options and NOT "Save to your Microsoft account". This prevents it from being uploaded to the cloud where it could be potentially compromised.

In the future, when you turn on your computer you will have to enter your password. Other than this, BitLocker is completely transparent and you don't have open any special programs to access your data. We hate asking you to spend money, but full-disk encryption is a necessity for those in high-threat digital environments.

FDE on Other OSs

Earlier Windows and LINUX

Earlier Windows operating systems can use the free and open-source VeraCrypt software. This method of encryption can be slightly trickier since it is not a native Windows application. Additionally, it will require that you burn a "recovery disk" that can be used to restore your hard drive should the encryption become corrupted. Full instructions are available in the VeraCrypt User Guide. To open the User Guide install VeraCrypt. Click Help, then User Guide. For Linux users, you will be using LUKS (Linux Unified Key Setup) for full disk encryption. Linux makes this really easy and transparent on installation of most distros by choosing the encryption option on the installation target screen and entering a password for encryption. It will fully encrypt everything on your drive besides the partition with the boot loader. For true full disk encryption, we recommend putting the bootloader on an external drive and booting from that every time. You will be prompted for an encryption key every time you boot into your Linux distro.

Mac OS X

If you are a Mac user, we recommend using Mac's built-in FileVault software. FileVault is simple to use and intuitive, and provides strong, AES-256 encryption for your entire hard drive. To access FileVault open System Preferences and click Security and Privacy, then FileVault.

coming soon >>>

In The Next Issue

Cradle Point

COMSEC: Allo

Mobile Device Security: Part IV