in this issue >>> V.1.7

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Credit Card Skimmers Found at Wal-Mart
  - Krebs on Security
- Facebook Tracking and Showing Ads to non-Facebook Users
  - Naked Security
- HaveIBeenPwned?: Invaluable Resource in Hacking Age
  - Vice
- US Nuclear Program Still Run on 1970s Tech: 8" Floppy Disks
  - Gizmodo
- Checksums Updated
  - Your Ultimate Security Guide

SyncStop:

Charge Your Devices Safely

Jacob Alexander

The SyncStop, formerly known as the "USB Condom", is a device designed to protect your USB devices from an unwanted data connection when plugged into an unfamiliar port. Plugging in any device into a USB port can be dangerous because USB allows data to pass to and from your device while it is plugged in. This could allow an attacker to upload a malicious file to your device while it is charging.

Fortunately, the SyncStop device offers a solution to this: remove the data connection and only allow power to pass through. It accomplishes this by physically removing the connection on the data pins of the USB connector, rendering the inert. This is the best way possible as software fixes might be vulnerable to bugs, too. This completely removes the possibility for any data to be transferred, whether to or from your phone, table, or other USB device.

This is a great device to have when you phone is dying and you don't' know what's on the other side of your power source. USB chargers in hotel rooms, airports, rental cars, and even on airplanes should be suspect. To use the SyncStop simply plug it into the charging port, then plug your device into the SyncStop. Power will be transferred but nothing else. You may even want to use the SyncStop when your only charging option is your work computer. This will ensure your selfies don't inadvertently get uploaded to the company's server.

The SyncStop is available for $20 from http://syncstop.com/. Or you can build your own. We use this as an introductory soldering project in our Commercial-Off-The-Shelf (COTS) Course. For more information contact admin@tpidg.us.

set the stage >>>

Mobile Device Security: Pt I

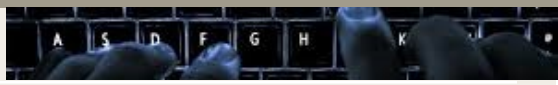
Today begins another multi-part series in the Digital Update: Mobile Device Security. Though this series can't possibly begin to tackle all of the different devices out there, we will try to offer some general principles that can help you keep the data on your device safe from prying eyes.

This week we are going to make a couple of very basic recommendations. While they may not seem military, these will have perhaps the most impact on the security of your devices. The first of these is **keep your OS and apps updated**. Apps for both iOS and Android devices can be checked in the Google Play and App Store, respectively. Checking your OS will require a bit more digging.

For Android devices go into your Settings. Scroll to the bottom to "About Phone" or similar. On the following screen tap "System Updates". You should either see a notification to update your device, or one saying your device is good to go (exact terminology varies device-to-device). On iOS devices tap the Settings icon. Scroll down to General. On the next screen tap "Software Update". If an update is available you will be notified.

It is easy to ignore those warnings letting you know you need to update your apps or your operating system, but it is unwise. Malicious software exploits the mistakes in the underlying code that these updates are written to repair.

The easy button >>>



COMSEC: WhatsApp

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. The extremely popular messaging application WhatsApp recently made a significant upgrade to its encryption protocol.

With over a billion users, WhatsApp is one of the most popular messaging apps on the market. WhatsApp recently upgraded its security to offer true end-to-end encryption for its users. The app integrated the protocol from Signal Private Messenger, which we consider to be one of the best-in-class secure commo apps. The Signal protocol (former known as the "Axoltl Ratchet) is a form of perfect forward secrecy (PFS). PFS means that each message is protected with a new encryption key. If an attacker breaks the key he or she only has access to a single message. This is a major upgrade.

This is great news as many of you and those you know and work with already use this app. We also like to pedestrian nature of this app as it doesn't scream "security". Be aware, however, that the encryption provided does not protect your metadata. The Facebook-owned application still records who you talk to and how often you talk. Depending on your threat model this may be a serious consideration. On the other hand, all other messaging apps have access to this information by default, as well.

If you don't already have WhatsApp, it is free to use. Just download it from your app store and install it. You will then have to verify the app using your mobile number. If you already have WhatsApp, check with your app source to verify that you are running the latest version.

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 Tor Network: Part III

The Tor Network has been demonized by the media as a tool for hackers. However, this DOD-funded browser has applications for anyone who needs strong online privacy

The Tor Network offers the closest thing one can get to anonymity in the digital environment. To take advantage of this anonymity you must follow some basic best practices and be aware of some potential pitfalls. In the third and final piece on the Tor Network, we will cover some of these vulnerabilities to help you stay safe.

Browser Fingerprinting: Every internet browser has a "fingerprint" that is comprised of several factors. These include add-ons installed on the browser, languages, cookies stored in history, and screen size, resolution, and color depth. When you visit a website it can (and frequently does) record your browser's fingerprint to identify you the next time you visit that site.

Unfortunately, this is one of the most difficult tracking mechanisms to defeat. The Tor Browser's answer to this problem is twofold. First, you are warned not to install any additional add-ons on to the browser (NoScript and HTTPS Everywhere come standard). These could make you unique. Next, Tor opens up at a minimized view (NOT in full screen mode). By opening in a smaller window, the full size of your screen is not recorded. Tor recommends never maximizing to full screen.

Session Correlation: Another major potential vulnerability that can pierce your anonymity is correlating true-name activities with your browsing. For example, if you log into your "real" email account through Tor, you have associated your real name with that session. Additionally, when you log in to a service a cookie is placed on your computer. This cookie can record and transmit information about you, again tying you to that browsing session. If you access a service that is correlated with your true identity you should close the browser and open a brand new session before continuing.

Opening Attachments: Attachments and downloaded files like Word documents, PDFs, JPEGs, movies, or audio files can contain macros that communicate back to the Internet. Though the Tor Browser routes your browsing traffic through the Tor Network, other traffic on your computer is often routed through your normal (unmasked) internet connection. If you open an attachment that attempts to "phone home" it will likely do so without the protection of Tor. This can leak your true IP address and identify you as the user.

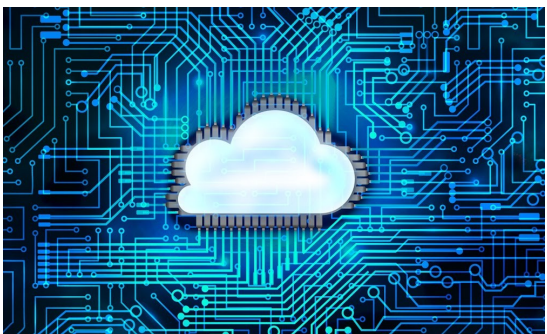
To avoid this type of compromise the fix is simple. After you have downloaded the files in question, close your Tor session. Next, break your internet connection entirely. Now you are safe to open the attachment without fear of it exposing you.

Exit Node Poisoning: One of the most dangerous aspects of working on the Tor network is the security of the exit nodes. As we described in the first part of this series, Tor routes your traffic through a series of relays called "nodes". Your traffic is heavily encrypted between these nodes, but the encryption is stripped off as it exits the Tor network (it has to be so packets can "find" the correct website and return packets to the correct person).

Exit node tampering is dealt with by the inclusion of HTTPS Everywhere in the Tor Browser Bundle. This ensures that (provided the site has an HTTPS connection) your traffic is still strongly encrypted when it leaves the Tor network. You should always ensure you have a good HTTPS connection before you enter login credentials to any site (we will cover how to read SSL information in the next issue).

Bottom Line: The Tor Network offers an incredibly robust layer of security and privacy. The last two installments of this series have focused on negative aspects of using this tool, as with most things, though, it is not a "fire and forget" solution. You have to take a great deal of care to do things the right way, otherwise you are defeating the purpose of using Tor.

In the next issue we will take a look at which solution is better: Tor or Virtual Private Networks.



coming soon >>>

In The Next Issue

Tor vs. VPNs: Which is Better?
Reading SSL Certificates
COMSEC: Privnote
Mobile Device Security: Part II
Tiny Hardware Firewall