TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- ID Thieves Exploited Equifax's TALX Payroll Division
  - Krebs On Security
- How to Keep Your Data Safe When Traveling Abroad
  - Lifehacker
- How to Build Your Own VPN if You Are Wary of Commercial Options
  - Ars Technica
- Breaking Iris Scanner on Samsung Galaxy S8 is Laughably Easy
  - Ars Technica
- Radio-Controlled Pacemakers Easier to Hack Than You Think
  - Ars Technica
- YahooBleed Leaked Private Attachments to the Internet
  - Ars Technica

Shodan.io

The Search Engine for Internet Connected Devices

Traditional search engines such as Google, Bing, and Yahoo search web servers for content and keywords. They do this by searching a particular place where a website tends to be, tries to make sense of the website and adds it to an index to be searched by you later. These particular places are often referred to as ports. In essence, a port is just a little door in a router to only let certain traffic through. The ports are assigned by numbers ranging from 0 to 65535, with webservers typically using port 80 (HTTP) or port 443 (HTTPS). It's important to note that search engines don't only search these places and are not restricted from searching everywhere, but the majority of website content lives on these ports.

Shodan differs from traditional search engines because it searches multiple ports, tries to connect, and sorts what it finds based on what ports are open and the header information returned from the connection. This a great tool to use to discover what is exposed on the internet, but it's also quite alarming the first time you use it. You can access publicly available webcams, databases, routers and even SCADA systems! Some things are password protected, while others allow admin access without the need to ever supply any sort of credentials. The devices that do have some sort of password often use system defaults (admin, password, 1234, etc.) and can be accessed very trivially. The header information shown often gives information such as OS, type of hardware default credentials and more.

Why are there so many devices indexed by Shodan? Shodan is just doing the work that anyone could do manually with traditional scanning software; they are not actually hacking anything. They are only showing what is freely available on the internet, indexing them and putting everything in a searchable list. The issue is not that hackers are using Shodan to compromise devices on the Internet, the issue is devices are allowed on the Internet immediately out of the box with default credentials. Another big issue is improper router configuration. Your modem/router is the gatekeeper to the Internet and it should be properly set up best to protect you. In the next issue, we will cover in depth the absolute best way to setup your router to prevent leaks. For additional info contact: admin@tpidg.us

Faraday Bags: The Ultimate Tracking Protection

If you have concerns about your mobile phone tracking you, you are not alone. Mobile phones contain multiple interfaces including Wi-Fi, GPS, Bluetooth, and NFC that can be used to track your location. A cell phone triangulating itself on cell towers can also be used to track your location, and is much harder you to control. If you really want the ultimate protection for sensitive meetings, off-the-books activities, or to give your phone company a little less information about your daily pattern of life, you should consider a Faraday bag.

A Faraday bag (named after Michael Faraday, inventor of the Faraday cage) is a bag with a metallic lining. The lining blocks signals to and from the device within a specified band, and can block all of the signals that can be used to track you. If you work in a high-risk occupation, the Faraday bag can also give you some protection from electronic eavesdropping through your smartphone.

TouchPoint recently partnered with Silent Pocket, a manufacturer of extremely high-quality Faraday bags. Silent Pocket offers a number of sizes tailored for different applications. The core of their product line is smaller pouche designed for the storage of smartphones. Smaller bags are available for special-purpose applications, such as very small bags designed to protect RFID badges or key fobs, as well as a line of RFID -blocking wallets and passport covers. Silent Pocket also makes larger bags, including waterproof dry-bags as well as backpacks and briefcases. Most of Silent Pocket's lineup includes full shielding against cellular, Wi-Fi, Bluetooth, GPS, NFC, and RFID signals.

TouchPoint customers can receive a discount on Faraday bags from Silent pocket by contacting us directly at **admin@tpidg.us**.

Upcoming Events:

Associated Locksmiths of America Security Expo

June 16-22 2017, Rosemont, IL

National Technical Investigators' Association (NATIA) Annual Conference

July 12-23 2017, Tampa, FL

BlackHat USA

July 22-27 2017, Las Vegas, NV

Biometric Authentication

Risk vs. Reward: Is it Worth it?

During the past week we have seen two major news articles about biometric authentication. One of these articles deals with a basic problem with biometrics as authentication measures, and the other raises some difficult questions.

The first of these articles concerns facial recognition. JetBlue airlines is rolling out a new program to use facial recognition to speed up the boarding process. When you arrive at the airport you will check in as usual. When boarding at the gate, however, you will not longer scan your boarding pass. Instead a photograph of you will be taken. It will be sent to US Customs and Border Protection where it will be compared against your passport photograph. JetBlue's stated reason for this is to ease "chokepoints" in the "air travel experience" and it might, but we see some bigger issues. What happens if you are a false negative? What happens to all this data? Who stores it, and how do they protect it?

The other article, mentioned in our "In the News" segment deals with the new Samsung Galaxy S8. Samsung's latest phone has an iris scan to unlock that is extremely easy to defeat. This isn't the first time we've seen easily-defeated biometric measures on mobile devices—Apple's Touch ID has been pretty roundly defeated, too. Which brings up the next question: how do you control your "tokens"? You leave your fingerprints lying around everywhere, including all over the very phone they protect. How do you prevent your photo from being taken?

These questions are not new. Many of these questions have been asked by security theorists for years. We encourage you to think about these before authenticating your phone, computer, or anything else with a biometric token. Is it really worth a small amount of convenience?

Firefox Settings: Privacy

Optimizing Your Browser Security

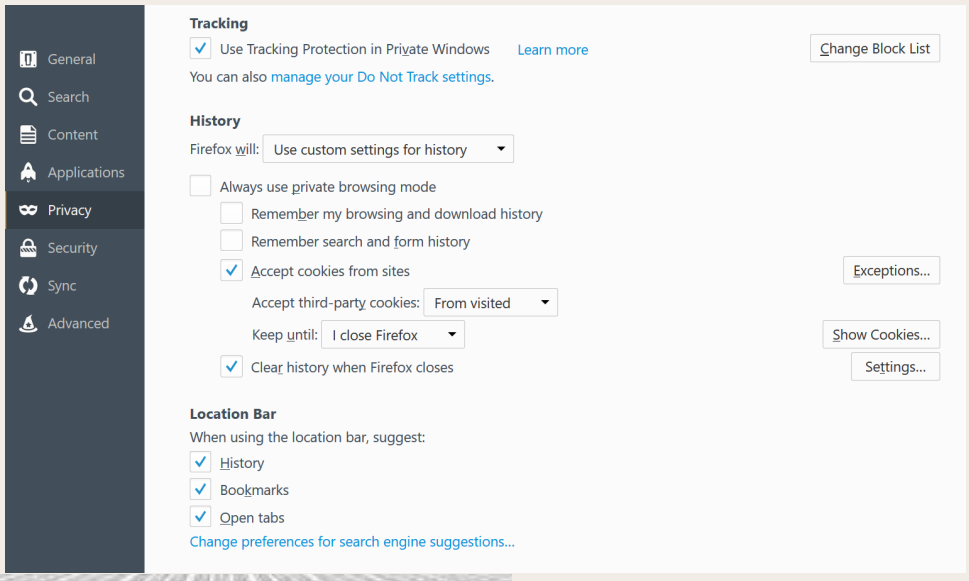
It is no secret that Firefox is our favorite browser. Over the last few weeks we have covered security add-ons for Firefox, including NoScript, HTTPS Everywhere, and Self-Destructing Cookies. All of these doubtlessly make Firefox more resilient, but there is a lot of work we can do in the settings, as well. This week we will cover Firefox's Privacy settings, since this is the most critical group of settings in the browser.

We won't go over this process step by step, because if you "make yours look like ours" using the screenshot below you'll be good to go. We will explain why we are doing this though. The first drop-down menu (use custom settings for history) allows you to choose every single history setting for Firefox. This is something that no other setting does. If you use Private Browsing Mode, you give all the control over what is deleted to Firefox, which is why we choose not to enable this mode. Also make sure to uncheck the boxes that offer to remember browsing, download, search, and form history. All of this data shows exactly what websites you've visited to anyone who sits down at your computer.

The next three settings deal with cookies. Cookies are a necessary evil of the internet but you shouldn't keep them longer than you need them. It is also completely unnecessary to keep cookies from third-party sites that you have not even visited.

One of the most important settings here is "Clear history when Firefox closes". Make sure this box is checked. Next, make sure to click the Settings button to the right. This will open a new dialogue that allows you to choose exactly what is cleared when Firefox closes. You should select all of these options. The location bar items don't make much difference either way. Since the storage of history, bookmarks, and open tabs is controlled elsewhere, enabling these options will not harm your security.

In the next issue we will take a look at some other security and privacy settings in Firefox.



Sudo Adds CallKit Support for iOS

We have talked about Sudo in previous editions. It is a powerful app that allows you to have nine separate phone numbers and email addresses in one convenient interface. Recently Sudo added CallKit support for iOS devices

CallKit is iOS's native phone integration. When you enable this feature in Sudo, you calls to Sudo numbers ring as regular phone calls. This means you do not have to unlock your phone (and the app) to answer incoming calls. It also means that if you are listening to music or other audio when the phone rings, iOS will recognize it as a phone call and pause the audio. Finally, if your "real" phone rings you will not be kicked off of the Sudo call. With CallKit enabled, Sudo calls get the same priority as regular phone calls.

This is a huge feature upgrade for Sudo, but it is not without some downsides. When you enable CallKit you give your phone application access to Sudo calls. This means that records of calls are stored in your phone's "Recents" where they are accessible to persons and applications that have access to your call history. We think this compromise is worth it for the convenience Sudo/CallKit offers.

To enable CallKit open Sudo. Tap the Settings icon (the small gear-shaped icon in the upper right). Scroll down to "Phone Settings". In this menu toggle "iOS Call Integration" to ON.

coming soon >>>

In Future Issues...

Internet Browser Comparison

⇒ ***Chrome, Firefox, Opera***

⇒ ***Mobile Browsers***

Firefox Setup Review

Browser Extensions