in this issue >>> V.1.12

Ubiquity EdgeRouter X
CopperheadOS
Mobile Device Security VI
Two Factor Authentication: ~~SMS~~
Encrypto

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Social Security Administration Now Requires Two-Factor Authentication
  - Krebs on Security
- Facebook Rolls Out Code to Defeat Ad-Block Plus Add-on
  - Naked Security
- Major Qualcomm Chip Flaw Exposes 900 Million Android Phones
  - Ars Technica
- New Air-Gap Jumpers
  - Ars Technica
- Researchers Find Unusually Advanced Malware that Stayed Hidden Five Years—Likely State-Sponsored
  - Ars Technica

Encrypto

Ultra Simple File Encryption

If you have read the Digital Update before, it should be no surprise that we love encryption. Most of our readers have no problem with using strong encryption, but it can be hard to get others on board. This is especially true when encryption programs are complicated or non-intuitive. Thankfully a new program from MacPaw makes encrypting a file on Windows or Mac computers extremely easy.

Encrypto is a super simple desktop application. When the application appears, there are no buttons to click, no drives to "mount", and no accounts to create. To encrypt a file simply drag it onto Encrypto's interface or click the "Add File" or "Add Folder" buttons. Next, you will be prompted to create a password. You will also have the option to include a password hint (obviously we recommend against use a hint that may reveal the password). After you have entered the password click the "Encrypt" button. An encrypted version of the file will be created. Clicking "Save as" will allow you to save this file to local storage. It is important to note that Encrypto does not overwrite the original file—it merely creates an encrypted copy with a *.crypto file extension. The stated purpose of Encrypto is to allow you to create encrypted versions of files that you can then email or upload to the cloud, or save locally.

Encrypto is free and uses AES-256 encryption. We have yet to see an encryption program that is as simple and intuitive as Encrypto. This program is ideal for those who are not technically literate or don't have time to be trained on more feature-rich applications. Encrypto is also designed to work in tandem with another MacPaw app called "Hider 2". Hider 2 creates encrypted containers in which to stash your sensitive files. If you are familiar with VeraCrypt you will recognize Hider 2's containers as functionally similar to VeraCrypt volumes.

For more information on Encrypto visit http://macpaw.com/encrypto

set the stage >>>

Mobile Device Security: Pt VI

Last week in the Update we discussed Virtual Private Networks and protecting the information that is constantly flowing from a smartphone. This week we are going to discuss limiting that information as much as possible. Both Android and iOS phones have multiple interfaces (communication pathways) that can be turned on or off independently. Each of these represents increased convenience, but also increased attack surface.

Cellular connectivity, as well as Bluetooth, Near Field Communication (NFC), and Wi-Fi all offer exploit opportunities. Cellular, Bluetooth and Wi-Fi can all be intercepted, and all can be used to track your location to varying degrees of accuracy. Bluetooth is the most accurate, but also requires that you be closest to a receiver. Cellular data is the most prevalent, but also the least accurate, generally speaking. The accuracy varies depending on the saturation of cellular towers in your area of operation. Wi-Fi is also very accurate, and can place you anywhere within the footprint of a wireless router. Wi-Fi is also incredibly dangerous because your Wi-Fi probes can reveal where you have been historically, and your home, work, and other frequented networks.

We strongly encourage turning Wi-Fi, and Bluetooth off when they are not in use. This can help you limit location tracking. It can also prevent your from connecting to malicious access points (AP). These APs can be used to set up Man-in-the-Middle attacks and collect your traffic. There is also a much more practical reason for leaving these interfaces off when they are not in use: a drastic improvement in battery life.

On Android and iOS devices you can toggle these settings off in the Quick Settings menu (Android) or Control Center (iOS).

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

The easy button >>>

CopperheadOS

Continued from previous page...

Last week we talked about CyanogenMod, an aftermarket operating system for Android phones. While CyanogenMod has achieved an almost “mainstream” status in the world of custom Android builds, another is quickly coming to the front: CopperheadOS. CopperheadOS is built with security in mind from the ground up.

Copperhead addresses many of the problems that end-users can’t address. While the end-user can encrypt and limit app permissions and take other security measures, things like implementing Address Space Layout Randomization (ASLR) and hardened C libraries and compilers is beyond the reach of almost all. This is where Copperhead comes in. The three man team at Copperhead does all this and more including stronger sandboxing for apps, backporting security features, a hardened kernel, and the implementation of a firewall and hardened networking services like MAC randomization. And that’s not all; Copperhead also takes an interest in privacy. Inherent in the operating system is an app called F-Droid. F-Droid is an unofficial app store that allows you to install apps without giving up any personal information or having a Google Play account.

CopperheadOS is available for download but it only works on Google Nexus phones. Copperhead made this decision because of Google guarantees timely software updates for these devices for at least three years (other manufacturers have no financial incentive to keep legacy devices up-to-date and many do not). Devices are also available for purchase with CopperheadOS pre-installed.

Look for a much more detailed review of CopperheadOS in the coming weeks, and as always, if you have questions direct them to admin@tpidg.us or visit https://copperhead.co/android/

Ubiquiti EdgeRouter X

Isolating Wi-Fi Devices

The EdgeRouter X is a tiny 5 port router designed by Ubiquiti for SOHO (Small Office, Home Office) users, but has some features in it that could be very helpful for network security. Isolation has been a very popular topic recently and it is very important as we add more networked devices to the internet. Networked televisions, refrigerators, lightbulbs, among others are collectively referred to as IoT (Internet of Things) devices. These devices are very dangerous for network security as they are often designed by companies who have no experience with security because they never needed the knowledge before IoT devices existed. Our best defense against hackers exploiting these devices and attacking our other devices is isolation by keeping all of the devices on a separate network and never touching our primary network.

Typically, this is done by having three separate routers: one for IoT devices, one as your primary router and one to bridge them to the internet. Another alternative are VLANs (Virtual Local Access Network) which are a solid line of defense, but they are possible to defeat by "VLAN hopping" to gain access to other VLANs. That's where the EdgeRouter X comes into the picture with its logical interfaces. Each port on this device is treated as a separate interface instead of being thrown into a collective pool. This is absolutely perfect for isolation purposes because nothing on each of the interface's networks can talk to each other unless they are bridged together. This device gives you the option of only bridging some of the interfaces in one network, leaving others to be completely isolated which would make them perfect to host an IoT network. You can also use a VPN to bridge your local network with a corporate or home network (PPTP, IPsec and OpenVPN in CLI). You also have the option of layering VLANs on top of the interfaces to segregate the networks even further. The EdgeRouter X also has POE (Power Over Ethernet) capabilities which allows it to be powered and power a device with Ethernet.

Ubiquiti also makes WiFi antennas that support POE which allows you to have a nice wireless setup. This device does not have WiFi capabilities, so additional wireless routers would be needed with this device sitting as close to the internet as possible. The device itself is completely Linux based and has SSH access on by default. You can log in with the same username and password as the GUI and you have full root access. The device seems to be running a modified version of Debian with SELinux implemented minimally.

Overall, this device is a very good networking router with built-in isolation that comes in such a small form factor. It would be nice to see more isolation implemented into modern day routers as we continue to add more and more networked devices. For more information, contact admin@tpidg.us

coming soon >>>

In Future Issues...

Mobile Device Security: Part VI

CradlePoint Router

Encrypto and Hider for Mac

Two Factor News

SMS Gets Downgraded

The National Institute of Standards and Technology (NIST) recently published a paper "deprecating" SMS as a two-factor authentication mechanism. NIST has recommended phasing out SMS as an authentication mechanism because SMS messages are too easily intercepted or forwarded, compromising the security of the system. So what does this mean, and what can you do about it?

First, **you should be using two factor authentication**. Second, even if a site or service ONLY allows SMS as a second factor, you should still use it. An imperfect implementation is still way better than nothing. However, if a site or service offers other means of authentication you should use it instead. Much stronger options like a software token (through apps like Google Authenticator or Authy) or hardware token (like the Yubikey) are available with many sites that offer two-factor authentication.

The number of sites that supports two factor authentication is still a long way from complete, but it is growing. If you've been to our Non-Standard Comms or Digital protection classes you know we highly encourage using it on your personal accounts, or implementing it on your organization's network. For a list of websites that support two factor authentication, visit https://twofactorauth.org and enable it everywhere you can. Just try to stay away from SMS where possible.