in this issue >>> V.1.10

Cyanogen Mod
Mobile Device Security Part V
Mumble

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Rigged YouTube Videos Can be Used to Hijack Siri and Google Now
  - Naked Security
- WhatsApp Isn't Fully Deleting "Deleted" Chats
  - The Verge
- Vulnerability puts Mobile Phones and Towers at Risk of Complete Takeover
  - Ars Technica
- New Attack Bypasses HTTPS on Windows, Mac, Linux
  - Ars Technica
- Over 100 Tor Nodes Found in the wild Designed to Spy on Users
  - Hacker News

Cyanogen Mod

Ultimate Security Android Build

If you have attended our Non-Standard Communications course you know we discourage rooting Android devices because of security risks. CyanogenMod (CM) is a custom version of the Android operating system that requires rooting to install. In this case rooting might actually be a good idea because CM is built around improving security. CM is supported by a wide assortment of phones including many of Samsung's Galaxy phones, the Amazon Kindles and the Moto G (the phone we use in our NSC class). Installing CM is definitely not recommended for the average user who just needs to check Facebook and text their friends because it requires some advanced knowledge of installing custom firmware. After installation, you have root access to your device and you also have a pretty high chance of "bricking" your phone (i.e. rendering it completely inoperable) and never being able to use it ever again.

Risks aside, CM comes with several features to be desired by power users, the security and privacy oriented, and users with a distaste for bloatware. Upon installation, you have a small assortment of apps including a modified chrome browser, screen and sound recorders, and an audio FX app. You will notice that the Google Apps suite is not installed, meaning you will not be able to easily install apps via the Play Store. This is due to licensing restrictions and as such CyanogenMod does not support the use of the apps on their firmware. The Play Store and other Google apps can be installed separately via a third party. Root access to apps is disabled by default, but can easily be turned on by checking the options in developer options.

CyanogenMod also comes with Privacy Guard which implicitly revokes all permissions unless you specifically allow a permission for an app. This is especially useful if you enable this by default for newly installed apps and then explicitly allow only what is necessary for the app to operate. It also includes a CyanogenMod updater to keep up to date

Continued on next page…

set the stage >>>

Mobile Device Security: Pt V

We have talked previously about Virtual Private Networks (VPNs) in the Update. We are addressing them again in mobile device security because they are such a crucial feature. Let's quickly recap what a VPN does—and doesn't do. A VPN gives you a level of security by routing your traffic through an encrypted tunnel. VPNs also give you privacy by allowing to exit at a different IP address than your real IP. Using a VPN is incredibly important on mobile devices—we think it may be more important than using them on desktop operating systems.

Your mobile device is constantly transmitting information in the background. Even when the device is asleep, it is busily checking in for OS updates, notifications, and sharing data about the device's state. All of this information can provide a treasure trove for a malicious actor. Additionally, the communications you transmit from your phone including emails, VoIP calls and texts, internet browsing data, and more are usually plaintext by default. A VPN can protect this sensitive traffic.

The VPN that we recommend and teach in our Non-Standard Communications Course is Private Internet Access. We like this VPN not only because it provides great security, but also because it can be configured as "always" on. This means that when the phone goes to sleep the VPN connection remains active, protecting background traffic.

To use Private Internet Access on your device will require installing the app. Alternatively you can install the OpenVPN app and import PIA's OpenVPN config files, but we have found this to be less reliable (on iOS devices). There are plenty of other good VPNs out there, but always check their privacy and data retention policies first.

Upcoming Events:

Fort Mead Tech Expo

01 September 2016, Ft. Mead, MD

Ft. Gordon Cyber Security & Tech Day

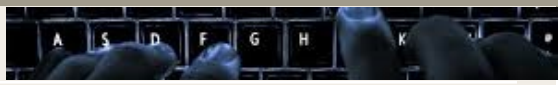
19 October 2015, Augusta, GA

Law Enforcement Intelligence Units

1-5 May 2017, Bloomington, MN

For more information go to www.tpidg.us

The easy button >>>



Cyanogen Mod

Continued from previous page...

with the current version which is normally updated more often than an older model android phone or a phone from a carrier such as Verizon. This is because updates come straight from CyanogenMod developers. This is a major issue with standard Android builds: updates have to go through both hardware manufacturers and carries before they reach end-user devices. Out-of-date operating systems lead to malware and other major security issues.

Everything in CyanogenMod is fully customizable including the status bar, the overall theme, button configurations, the display and notification lights. CyanogenMod is definitely worth installing, but should be done so with caution or else you could brick your phone. CyanogenMod is completely open source and free. There are also some reasons you may NOT want to use CyanogenMod, however. First, it may void your warranty. Also, if you don't know what you are doing it is very possible to introduce more security risks with a rooted phone. As we've pointed out, it is possible to brick your device (we want to be absolutely clear this is a real risk).

CyanogenMod is our recommended custom Android build. CM is lightweight and pushes your system harder for better performance. It is secure: you can remove bloatware which are potential privacy and security threats, have control over apps, and stay on the latest OS version. More information on it can be found here at their website: http://www.cyanogenmod.org/. If you want to give it a try, numerous tutorials for installing CyanogenMod can be found on YouTube. CyanogenMod can also be taught as part of the Non-Standard Communications course of training as a two-day block. Please contact us at **admin@tpidg.us** if interested.

Mumble:

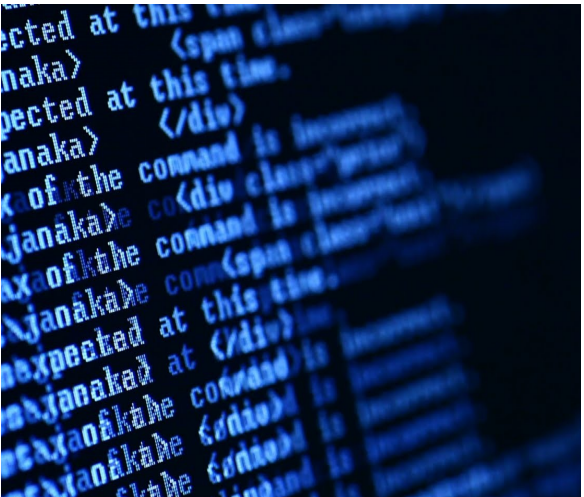
DIY VoIP Solution

Mumble is an open source, high quality, low latency, encrypted VoIP (Voice over Internet Protocol) and chat solution. It is mainly aimed at gamers, but has many more potential uses. All communications transmitted over the Mumble service are encrypted end-to-end using TLS (Transport Layer Security). What makes this program unique compared to other VoIP services (ie. Skype) is the transparent security and the ability to set up and configure your own server on any platform you have available.

The Mumble client can be easily deployed on Windows, OS X, Linux, iOS and Android. The server portion of Mumble (called Murmur) can be hosted on a Windows or Linux based system and can be configured from custom certificates down to the number of users allowed at one time. Murmur gives you the option of either generating certificates automatically or using your existing certificates if you are already running a web server or FTP server. When Murmur generates a certificate, it gives you a rather generic looking certificate, which is difficult for users to verify as authentic (see issue 1.8 for more information on reading TLS certificates). If you use your own certificate, it's already registered to your web server and its authenticity can be more easily verified. If you don't already have a TLS certificate, an easy and free option is "Let's Encrypt", an advocacy group dedicated to bringing encryption to the internet. For more information on free TLS Certificates through Let's Encrypt, visit **https://letsencrypt.org**.

The app itself is actually pretty easy to use. The first time you set it up, it will prompt you to set up your audio settings and to generate a client certificate. You again have the option of automatically generating a certificate or importing your own. You also have the option between creating your own Mumble server or joining one of the publicly available ones. In most cases, if you're not a gamer and you want a secure chat, you're going to have to host your own. Mumble also does you the favor of color-coding the servers, the green highlighted ones have a valid TLS cert and the un-highlighted servers have an issue with their TLS implementation.

Overall, Mumble is a great piece of software that is very easy to set up and use for all secure communications. We can think of dozens of uses for Mumble, from military personnel communicating with spouses back home to law enforcement setting up command centers. The fact that you can see and manage the security behind it and not just believe in the mysterious security behind the curtain makes this program a preferred communication avenue. For more information or to download Mumble visit https://wiki.mumble.info/wiki/Main_Page. For any questions or details on how to set up or use Mumble, contact **admin@tpidg.us**



Netcraft

Firefox Security Add-on

Recently a former student alerted us to a new Firefox add-on called the Netcraft Toolbar. Netcraft is a very full-featured add-on that "blocks phishing sites, and helps protect users from online fraud". It does so by providing you detailed information about the websites that you visit, including risk ratings and detailed reports about the sites you are visiting. Netcraft provides some Cross-Site Scripting (XSS) protection (if you have NoScript you already have XSS coverage) and phishing protecting by maintaining a huge database of known phishing sites.

Netcraft places all of this information in easy view in a toolbar. The toolbar displays the site's ownership information, it's country of origin, how long it has been in business, and a red/yellow/green risk indicator. If you are going for maximum screen space, you may not want to add another toolbar to your browser. For more information or to download Netcraft, visit http://toolbar.netcraft.com.

coming soon >>>

In The Next Issue

Mobile Device Security: Part VI

CradelPoint Router

Encrypto and Hider for Mac

Black Hat After-Action