in this issue >>> *V. 2.03*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- [Adobe and Microsoft Release Critical Bug Fixes]
  - Krebs On Security
- [Majority of Android VPNs Can't Be Trusted to Make Users More Secure]
  - Ars Technica
- [Facebook Upgrades Two-Factor to Include Hardware Tokens]
  - Ars Technica
- [WebEx Plugin for Chrome will Execute Malicious Code; UPDATE NOW]
  - Ars Technica
- [Android Malware "HummingWhale" is Back with >2 Million Downloads]
  - Ars Technica
- [Mac Malware Discovered in the wild; Also Works on Linux]
  - Ars Technica

Intel NUC

Small Computer, Big Performance

The Intel NUC (Next Unit of Computing) is a very small computer (115mm x 111mm x 32mm for the model we purchased) designed by Intel to provide the same processing power as an average Desktop computer. We purchased the NUC6i5SYK model and it is barely bigger than two Raspberry Pi 3's in a standard pi case, but it differs significantly from them. The main distinction would be processing performance and architecture. The Raspberry Pi runs on an ARM architecture which requires a custom operating system to run (ie. Raspian). The NUC runs on a 64-bit architecture, which is typically found in most systems nowadays. This means two things: it supports over 4 GB (up to 32 GB) of memory (DDR4 2133) and it is supported by all the major operating systems including Windows and Linux. The NUC is meant to be used as an ordinary desktop computer with a standard monitor, keyboard and mouse, but it can be used as a small server or a mobile media center as well.

All models support M.2 solid state drives, but only the larger models support 2.5" hard drives. The processor varies by model, but the current generation of NUCs run the Intel Skylake processors and the next generation will run Intel Kaby Lake processors (coming April 2017). The graphics are absolutely beautiful on the NUC, courtesy of Intel Iris graphics 540 and support 4K displays with ease. As for ports, it boasts USB 3.0, HDMI, DisplayPort, a full size SDXC slot and a 10/100/1000 Ethernet port. If you're not a big fan of wires, the NUC has built in wireless which includes IEEE 802.11ac (Wi-Fi), Bluetooth 4.1 and Intel Wireless Display 6.0.

We can definitely see the Intel NUC replacing most desktops used today due to its small form factor and low price without sacrificing any performance. The newer models of the NUC are coming out in April and are said to support up to three 4K displays simultaneously and are adding support for Thunderbolt. If you are thinking of buying a new desktop, definitely consider getting the NUC, but wait for the new models to come out in April. For additional info or questions, contact admin@tpidg.us

iOS 10: Passcode Security Part I

Many of you have asked for copies of Your Ultimate Security Guide: iOS *by Justin Carroll. Due to the book's age it is no longer for sale, but Justin has updated his iOS security guide in a series of blog posts, available at* ***https://blog.yourultimatesecurity.guide****. In this issue we are running the first part of this series. The complete series is available at* ***https://blog.yourultimatesecurity.guide/tag/ios-10/****.*

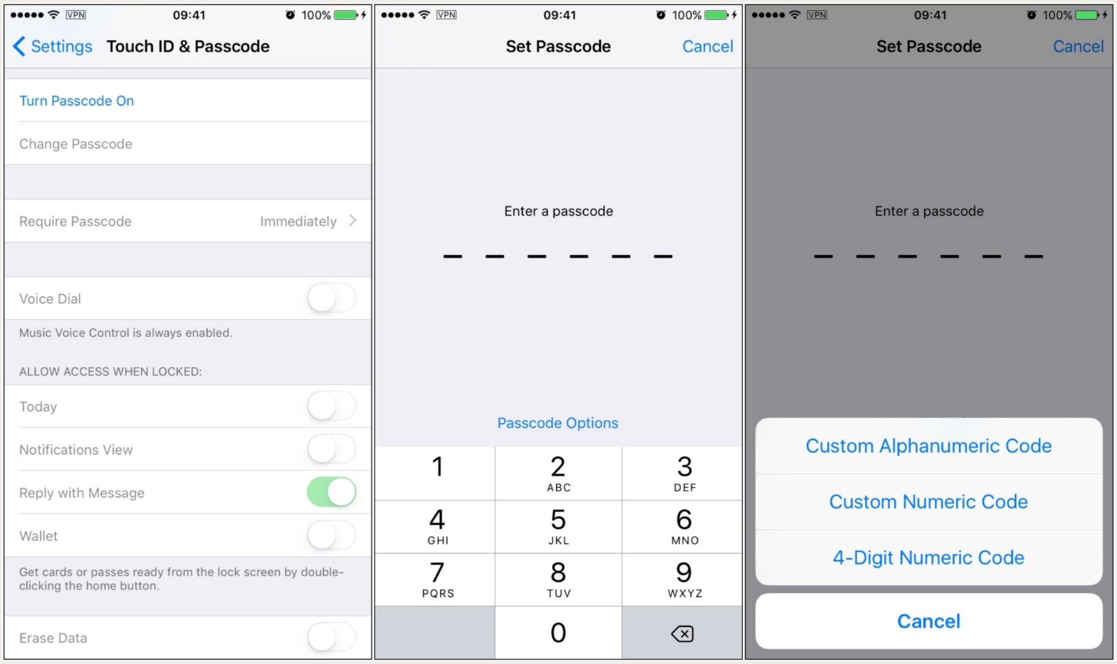
iOS 10 Passcodes and Encryption Part I

Passcodes are perhaps one of the most important considerations to the security of data-at-rest on an iOS device. Apple has used very strong full-disk encryption on iOS devices since iOS 3 and the iPhone 3GS. This encryption is "non-configurable" by the end user, meaning it cannot be disabled, intentionally or unintentionally. However, to take advantage of this encryption you must passcode-protect the device.

When you create a passcode, it is fused with a 256-bit Unique ID (UID). The UID is stored on hardware in the device and is inaccessible – it is burned into a silicon chip within the device and permanently sealed. Although in 2016 the FBI succeeded in breaking the passcode on an iPhone, it was a legacy device that lacked the Secure Enclave. Newer devices (5S and up) are almost certainly invulnerable to the same technique.

Encryption that is tied to hardware is inherently harder to break than software-only encryption. Hardware encryption means that an attacker cannot pull the data off the device and attack it in isolation and at very high speeds. Instead the attack must be attempted on the target device. Apple has put protections in place for this, too. One is "Erase Data", which will be discussed in an upcoming post. Another is an 80-millisecond penalty for each incorrect passcode; this is the time it takes the device to process a passcode attempt. At this speed only 12.5 passcodes per second can be tested. This delay can increase the time to brute-force the passcode to an intolerable length, but only if your passcode is not easily guessed.

Passcode selection is important because it plays a direct role in the encryption of the data on the device by creating entropy when fused with the UID. Additionally, poorly chosen iOS 10 passcodes may be easily guessed. The iOS passcode settings allow you to choose from several different passcode options. The default passcode is a six-digit numerical passcode. However, users may also choose from a four-digit passcode (legacy), custom-length numeric passcode, or custom alphanumeric passcode. Each of these options has benefits and disadvantages, but you should choose your passcode carefully to protect your data to the


Require Passcode: Immediately

Music Voice Control is always enabled.

Get cards or passes ready from the lock screen by double-clicking the home button.

Continued on next page >>>

maximum extent possible.

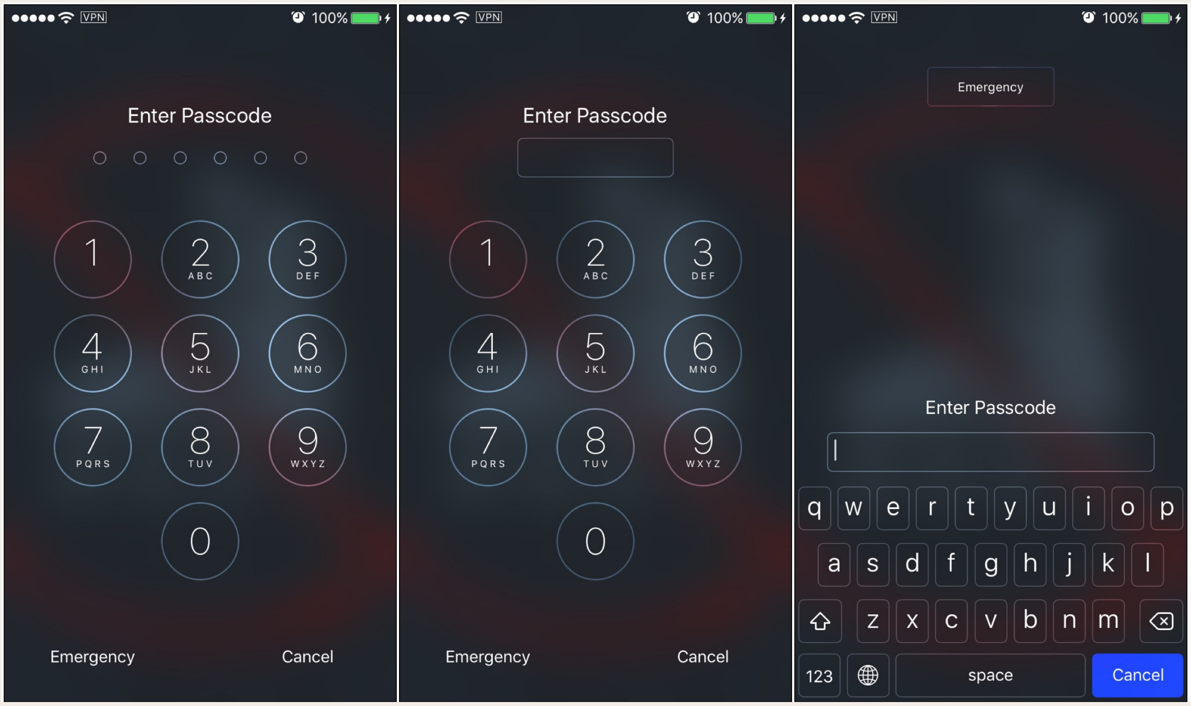
Choosing A Passcode

To set up a passcode for the first time navigate to **Settings//Touch ID & Passcode//Turn Passcode On**. If you are changing your passcode, navigate to **Settings//Touch ID & Passcode//Change Passcode**. This will bring up a screen prompting you to enter a six-digit passcode (see the screen shot on the previous page). If you wish to use a six-digit passcode, enter it now. If you wish to use another option, tap the blue “Passcode Options” label. This will bring up the additional passcode options.

Four-digit Numeric Code: This option is not recommended under any circumstance. A four-digit passcode offers only the barest layer of security for your phone and the information on it. There are only 10,000 possible combinations (0-0-0-0 through 9-9-9-9) in a four-digit numerical passcode.

Six-digit Numeric Code: The six-digit passcode is a substantial upgrade over a simple four-digit passcode, offering a million possible combinations. This may be sufficient for your needs if you have Erase Data enabled. If you do choose to use a six-digit passcode, I recommend repeating one or two (but not more) digits in the passcode. If the numbers used in the combination are discovered (i.e., through your fingerprints on the screen), and they are all different, there are only 760 possible combinations. If you repeat one digit, the number of possible combinations is increased to 1,800. If you repeat two of the digits (or one digit twice) and only use four different numbers in your six-digit passcode, there are 1,560 combinations in the passcode. If more than two digits are used, the number of possible passcodes begins to go down drastically.

Custom Numeric Code: The custom numeric passcode is the option I recommend for most users. This option hits the “sweet spot” between security and convenience. It allows you to use a very long passcode (I have successfully tested up to 40 characters) while still being able to use the numeric-only keypad. This keypad is much easier to manipulate than the full keyboard (see the screenshot below). This passcode also offers another layer of protection: it does not tell an attacker how many digits are in the passcode, unlike four- and six-digit passcodes.



Continued on next page >>>

iOS 10: Passcode Security Part I

How Long Should Your Passcode Be?

Even a seven- or eight-digit passcode is a substantial upgrade over a six-character passcode because there are more combinations, and because the attacker doesn't know how many digits are in the passcode. He or she only knows that there are more than six. Ten digits is my recommended minimum, and The Intercept's Micah Lee recommends an 11-character minimum for iOS 10 passcodes. This is based on the time it would take to crack your passcode. At 12.5 guesses per second, a six-character passcode could protect your data for a maximum of 23 hours – this is the length of time it would take to test every possible combination.

By making your passcode longer by one digit, you increase its strength by a power of ten. While it would take only 23 hours to test all of the combinations in a seven-digit passcode, it would take 220 hours, or over nine days, to test all the combinations in a seven-digit passcode. With a ten-character passcode there are 10,000,000,000 possible combinations and it would take over 25 years to test them all. Be forewarned that your passcode will (hopefully) be somewhere near the middle of the pool of potentials. This will ensure that any data on the phone is no longer actionable by the time it is recovered.

You may also wish to avoid making your iOS 10 passcodes too long. For many months I had a passcode that was thirty characters long. While this provided excellent security, it also had some unintended consequences. First, such a passcode was excessively prone to failed attempts which cumulatively cost me a huge amount of time. Second, such a long password actually tended to draw attention to me. While trying to share contact information or show a picture to someone it was not an uncommon occurance that they would notice the length of my passcode and comment on it. This attention was obviously unwelcome. Shortening the passcode somewhat still allows me to enjoy a level of security that I am comfortable with, but also far fewer incorrect attempts, and less unwanted attention.

To be clear, the custom numeric passcode is a compromise. It does allow an attacker to confine his or her guesses to numerical-only combinations which **significantly reduces the strength of the passcode**. There are some reasons I still believe this is an acceptable option however. If the passcode requirements are overly onerous, users will not want to enter it frequently. As a result, users may increase the Auto-Lock and Require Passcode intervals to longer periods, or take other shortcuts that could compromise security. I believe that with the other protections available in iOS, like the 80-millisecond delay between passcode attempts and Erase Data, this still provides an acceptable layer of security for most threat models.

Custom Alphanumeric Code: This passcode option provides the strongest security of all. This option should be considered if security is the paramount goal. It should also be considered for some other specific scenarios: if you leave your device unattended, or if your device is at high risk of loss, theft, or capture. A custom alphanumeric passcode should also be used if you use Touch ID to unlock your iOS device. This option has one significant downside: it requires the passcode to be entered on the full alphanumeric keyboard. This tiny keyboard offers the most complexity, but is incredibly tedious to work with, especially when you are in a hurry.

You can make a custom alphanumeric passcode even more secure by using some special characters on the iOS keyboard. The letters A, C, E, I, L, N, O, S, U, Y, and Z all contain special (high-ANSI) characters. For instance, the letter “a” contains the following special characters: à, á, â, ä, æ, ã, å, and ā. To access them, press the desired letter and hold. A pop-up menu will appear. Slide your finger to the desired character and release. Because of the immensity of the iOS keyboard's character set, incredibly complex passcodes are possible.

Stay tuned for Part II, where I discuss Passcode Best Practices.

Cloud Storage Insecurity

A Cautionary Tale

Last week, **news broke** that some users of the popular cloud-storage service Dropbox had some of their old files reappear in their storage accounts. The problem, however, is that these users had deleted these files years prior and had an expectation that they had also been deleted from Dropbox's servers. The reappearance of the files is proof that Dropbox had not deleted the files.

We talk about cloud storage a lot. We are sometimes asked, "what's the harm?" or "what's the big deal?" This situation perfectly illustrates the problems with cloud storage: you are handing control of your data over to someone else. When you upload files you are trusting that someone is not looking through them (Evernote **learned the hard** way that people don't like this idea). You are also trusting that when something is deleted, it is truly deleted. Dropbox users just learned the hard way that this isn't always the case.

So how do you prevent this? We have talked about this before, but this topic is worth reiterating. The best and most certain way is to maintain positive control of your data: don't upload it to a cloud storage provider. We aren't just picking on Dropbox here—this applies to all cloud storage services that aren't specifically privacy-focused. If you must upload data, think about what you are uploading and what the implications of it's loss would be. If it contains personal data, it probably shouldn't be stored on the cloud.

Before you upload files, you should also encrypt them. There are numerous tools you can use to do this. Some privacy-focused cloud services like **Spider Oak** and **Tresorit** will do it for you as part of the service. If you are just uploading a few Word documents or PowerPoint slides, you can use the built-in encryption, and of course, there's always VeraCrypt. Regardless of what you use, think twice before you upload files to Box, Dropbox, Google Drive, or iCloud.

coming soon >>>

In Future Issues...

FLIRC

Ubiquiti VOIP

Mini Chameleon

EFF's Privacy Badger

PHOTO TRAP UPDATE: ISSUE FIXED!

In the last edition of the Update we reviewed the **Photo Trap** application for iOS from **Escape the Wolf**. We mentioned that we had contacted Escape the Wolf about issues with comparing the "after" images, but had heard nothing back. Our conclusion was don't purchase the app. We are very happy to report that although we never got a direct response from Escape the Wolf, an update was recently released that fixed this bug. **We now recommend Photo Trap with confidence.**

PHOTO TRAP

Upcoming Events:

Law Enforcement Intelligence Units
May 1-5 2017, Bloomington, MN

Associated Locksmiths of America Expo
June 16-22 2017, Rosemont, IL

National Technical Investigators' Association Annual Training Conference
July 12-23 2017, Tampa, FL

BlackHat USA
July 22-27 2017, Las Vegas, NV