in this issue >>> *V.1.6*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- MUST READ: Find Out Everything Google Knows About You
  - Business Insider
- Wendy's Card Payment System Infected with Malware
  - Naked Security
- Chinese Company Left Backdoor in Kernel for Some Android Devices
  - Ars Technica
- Five Things You Should Delete From Facebook Immediately
  - Voice
- Internet of Fail: How Modern Devices Expose Our Lives
  - HelpNet Security

IronKey:

Ultimate Security for Data-at-Rest

Jacob Alexander

Today we visit a topic most software developers don't like to talk about: software is inherently insecure. No matter how many safeguards you put in place, no matter how much you try to prevent potential flaws in your software, there will always be a security vulnerability. This is because you have several different variables to account for such as: what OS you're running it on, what other programs are running next to it and internet connectivity. This is also true for encryption; software- based encryption utilities are vulnerable to security flaws, just like any other software. Fortunately, IronKey has a fix for this. Instead of using software to encrypt your data, it uses hardware to do the encryption with a chip inside the device specially designed to handle all of the encryption. This removes many of the opportunities for execution of flaws written into the code, and makes data much more secure. All of the data that is written to the IronKey is strongly encrypted at all times.

The device itself is very sturdy and acts just like a normal flash drive, just plug it in, enter your password and you can do what you wish with it. IronKey has a few interesting features, one of which is worth noting. If you forget your IronKey password, you have ten attempts to guess it before it fries the circuit board and renders the entire device useless. Now that's a great feature if your device falls into the wrong hands, but if you forgot your password, you might as well just buy another one.

Ironkey flash drives are available in several size increments for 4 GB to 128 GB. IronKey also manufactures external hard drives, and flash drives with a bootable (and encrypted) version of Windows built in. The downside of IronKey is that this security does not come cheaply. If you are interested in purchasing IronKey for your organization, TouchPoint can assist you with bulk sales. Contact us at **admin@tpidg.us.**

set the stage >>>

TouchPoint "Help" Button

Touchpoint IDG has set up a new system to help us better support our clients. We have added a 24/7 support button on the front page of our website. The button sends you to a form where you will need to fill out some basic information. Before you send your request, you may choose your priority level based on your current needs.

The default priority is low which sends the support team an email and typically gets a response no longer than 48 hours. In the same way, the medium priority sends an email, but typically gets a response within the day. For those in need of urgent support, there is a high priority. This option should only be used if urgent support is necessary as it sends SMS alerts and emails to each member of the support team. You will get a response as fast as humanly possible with this priority level selected. Urgent priority is intended for those in the field who require immediate operational reach-back to TouchPoint.

If your communications need encryption, specify in your first message and we can make the arrangements to use whatever is necessary. As you can probably guess, most of our team use encryption by default. We can support manual PGP, ProtonMail, Tutanota, Signal, and Wickr, and can flex to other systems as needed.

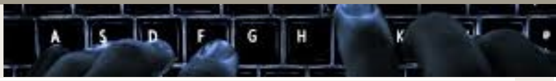
We are proud of the opportunity to support our operational men and women. Please feel free to use this service!

Upcoming Events:

-SOFIC 23-26 May 16
Tampa, Florida
-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 easy button >>>



COMSEC: Threema

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. Threema is a relative newcomer in the encrypted messaging playing field, but one that shows promise.

The world of encrypted messaging applications is a crowded field. Unfortunately, none of these messengers is doing everything to our complete satisfaction, so there is still room for growth in this space. One relatively new application that we like is Threema Secure Messenger. "Threema" is a play on "three 'e'" (End-to-End Encrypted), and that is exactly what it provides.

Our favorite feature of Threema is that it assigns you a random username. We like this because you don't have to give out your phone number to other contacts. We also like that Threema allows you to verify contacts' key pairs physically. If you can meet with a contact, he or she can scan your Threema ID (as a QR code).

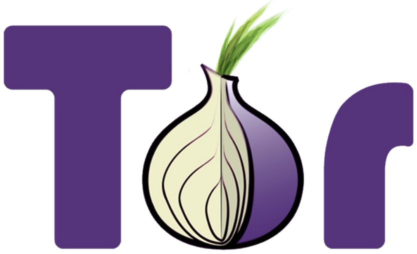
Beyond these features Threema works like most encrypted messaging systems. The texting in intuitive. Icons appear beside each message to let you know it's status (sending, downloaded, read/unread), and you can send photos, videos, files, share your location, or record audio directly into a message.

Threema costs $2.49 for Android, $2.99 for iOS, and $1.99 for Windows Phone.

Threema.

The Tor Network: Part II

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



In the last issue of the Digital Update we talked about the Tor Network and how it can hide your online activities. In this issue we will get into some more specifics of actually using the Tor Network. While Tor is the "nuclear option" for hiding your network traffic, it isn't all that complicated to use. But there are some things you should know before you begin.

Using Tor: To use the Tor Network, you must install a custom, Firefox-based internet browser called the Tor Browser Bundle. Visit https://www.torproject.org/projects/torbrowser.html.en and click the download button. After going through the installation process, the browser will install on your computer.

To use the Tor network, open the browser. You will immediately notice it looks a lot like Mozilla Firefox. This is because it is a custom version of the Firefox browser. This version is optimized for use on the network, and has add-ons for HTTPS Everywhere and NoScript (we recommend both of these add-ons even for the standard version of Firefox). You can now browse the internet as you always would. Type in a URL, and your traffic will be relayed through a circuit of three other "nodes".

You may notice some issues with Tor. First of all, it is slow compared to a non-Tor connection. Routing your traffic through multiple circuits takes a toll on speed. The other issue you may notice with Tor is that some websites may require you to complete a CAPTCHA or restrict you from visiting the site altogether. This is because Tor is used by hacker groups and is a security measure, but it is still an inconvenience.

Threat Modeling: While it would be nice to use Tor exclusively, it may not always be the best tool. You should carefully examine your threat model before you dive in fully to the Tor network from overseas. There are some serious reasons why.

First, Tor traffic "looks" very different from regular traffic if packet inspection is being conducted. This means that your traffic creates a distinctive signature. Though it is impossible for the adversary to tell what the traffic is, it is obvious you are using the Tor network to hide something. This can elevate your profile unacceptably and make you a target for additional digital scrutiny. Tor may also make you a target because it is used by the criminal element to hide their activities. If, however, you know that you are already the target of additional scrutiny, Tor may be your best bet as it provides some of the most comprehensive protection available.

If you are apprehensive about using the Tor network, remember, it was created for the military and intelligence community. Tor is still funded (through grants) by the Department of Defense. Unless your honest, sober threat model contraindicates the use of Tor, it is an excellent tool for obscuring your online activity—though not impenetrable. Stay tuned to find out Tor's vulnerabilities.

Secure Messaging: Our Philosophy

Multiple Platforms

In the past months we have covered several secure messaging systems, including Signal, Silent Circle, Wickr, and now Threema. You may be wondering why we don't settle on a single messaging system and go with it. There are a couple of reasons.

Compartmentalization

First, access to multiple, secure messaging systems allows you to break up messages into smaller chunks. If extreme security is required, you can pass a portion of the message through three, four, or five systems. It is unlikely that they are all broken, and this gives you an excellent layer of additional security.

Resilience

The other major benefit of having multiple messengers installed on your device is resilience in the face of vulnerabilities. If flaws are discovered in one application, you (and those with whom you communicate) can seamlessly roll to another, assuming you are all familiar and already have the apps installed.

coming soon >>>

In The Next Issue

Tor Network: Vulnerabilities

COMSEC: WhatsApp