in this issue >>> *V.1.5*

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- NYPD Contacts Thousands Whose Names Appear on Terror Target List
  - Fox News
- Canadian Police Obtain Blackberry's Global Decryption Key
  - Vice News
- US House Unanimously Passes Email Privacy Bill
  - Naked Security
- Checksums Updated 15 April 2016
  - Your Ultimate Security Guide

YubiKey 2-Factor:

Hardware Authentication Token

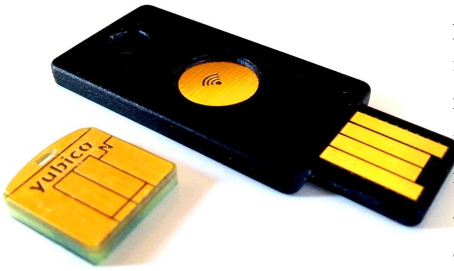
Jacob Alexander

The Digital Update has discussed two-factor authentication in the past. Today we want to focus on hardware-based authentication. This means a small device that provides a token that is very hard to replicate. This is one of the most secure second-factor options available, and one of the best examples of a hardware second factor is the YubiKey. There are three tiers to the YubiKey system:

The first tier is the "U2F/FIDO option which only works with certain services, namely Google, Dropbox, and Github. In addition to your usual username and password, you will also need this token to log into these services (if you enable this function).

The second tier offers all of the above, plus the ability to use "One Time Password" (OTP) mode. This allows you to use two factor authentication to login to your OS or use it to get into your password manager (such as LastPass or KeePass). The final tier offers everything from Tiers 1 and 2, as well as the ability to be used with mobile devices as a second factor. This is accomplished through Near-Field Communications (NFC), a low-powered transmission that transmits the appropriate login data to your device.

The YubiKey requires no drivers to be installed, requires no batteries, has no moving parts, and is nearly indestructible. This is a nearly essential device for providing the utmost security for online and local accounts alike.



The YubiKey resembles a small USB flash drive. To use it you simply insert it into your device's USB port and pair it with your accounts and/or services. This provides absolute, best-in-class security—just don't lose it!

set the stage >>>

ID Management 101 *(Part 5 of 5)*

Part I: The self– assessment.

Part II: the importance of NOT giving information out.

Part III: Removing data

Part IV: Creating disinformation

Part V: Monitoring

If you have been following along with the Identity Management segment of the Update, you know that some effort has gone into securing your identity. After taking all of the steps outlined in the previous parts, it is still important to keep an eye on the information that is available about you. This occurs through constant monitoring.

Monitoring means you should do several things. You should conduct a self-assessment (discussed in Part I) annually. This will help ensure new information has not been publicly released. You should also be requesting your annual credit report from the three credit reporting agencies to ensure you have not been the victim of identity theft. Finally, you can use services like Google Alerts to warn you when a new website shows your personal information.

Wrap-Up

If this seems like a lot of work—it is. Maintaining your privacy and managing your identity is can be difficult. We strongly believe this is important to the safety of our military and public safety personnel, and that of their families.

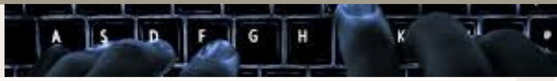
For a much more in-depth look at this topic check out *The Complete Privacy and Security Desk Reference*. One of the authors, Justin Carroll, is a senior instructor for TouchPoint, IDG, and one of the leading experts in the emerging field of identity management.

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: Silent Circle

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. Silent Circle is an easily-scalable solution for organizations with serious data-protection needs.

Silent Circle was founded by former Navy SEAL Mike Janke and PGP-encryption inventor Phil Zimmerman. The company's flagship product, the Silent Circle application allows easy encryption of voice calls and text messages. The encryption used in this product is second-to-none: Silent Circle uses the Zimmerman Real-Time Protocol (ZRPT). Calling and texting functions are available in a single application that is intuitive and easy to use.

Silent Circle is a paid product. Subscriptions begin at $10 per device for the basic service which allows unlimited communication between other subscribers. Enhanced calling plans offer a phone number that can be used to place and receive calls that are encrypted on the subscriber's end. The reason we like this product for military units and law enforcement agencies is its scalability. All subscribers can be managed by a single individual.

Silent Circle is one of the oldest and most trusted names in encrypted voice solutions on the market. For more information visit https://silentcircle.com

The Tor Network: Part I

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

Almost everyone has heard of the Tor Network in some form or fashion. It made headline news when Ross Ulbricht, the founder of the infamous online drug marketplace "Silk Road" was arrested. Occasionally it will still pop up in a public interest piece on hackers, the "dark web" or online cime. Tor certainly gets a bad rap in the media, but it was originally developed by the US Navy intelligence as a tool for agents to use for secure online activity. Like any tool, it can be (and is) used for both good and evil alike.

How does it work? The Tor Network provides the closest thing to online anonymity there is. When you login to Tor (which originally stood for "The Onion Router"), your traffic is routed through three intermediary servers which make up your unique "circuit". This obscures your IP address, making it very difficult for anyone to track the websites you visit or the activities you conduct on these websites. Because your traffic is routed through three servers instead of just one (as would the case with a VPN), it is nearly impossible to link your activity back to you. This protection is made even stronger through robust encryption.

The traffic leaving your computer is "triple wrapped". The first server in your circuit can unlock the first layer and see the next server in the circuit. This process is repeated for both successive servers and ensures no one node in the circuit can see both the content you are served, and your real IP address. The encryption of the Tor Network also means that your data is safe from packet inspection conducted by hackers, your ISP, or rogue access point operators.

The next two parts of this series will cover how to use the Tor Browser and Threat Modeling the Tor Network (hint: Tor isn't always the right tool). Stay tuned!

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

Course Spotlight: Non-Standard Communications

coming soon >>>

In The Next Issue

Secure Data Storage with IronKey

Tor Browser Bundle

COMSEC: Threema

Our Non-Standard Communications Course is our most popular course offering among the SOF community. Taught by expert instructors, this threat-specific course is like no other on offer. It covers basic computer security, protecting data-at-rest, and communicating securely. Though a baseline curriculum is offered, each course is custom-tailored to the using unit. Custom modules include Raspberry Pi VPN projects, custom FTP server setup, and in-depth mobile device security.

For more information or to schedule your course, contact us at:

admin@tpidg.us

Editor's Note: We Want Your Feedback!

In Touch with TouchPoint

The TouchPoint Digital Update was created for you, our readers. We wanted a quick, easy platform to keep you in the loop on the ever-shifting digital landscape. With that in mind, we want to tailor the Update to what is relevant to your and your job.

If there is a topic you'd like to see addressed in the update, please let us know. If you are curious about a computer program, mobile app, a piece of hardware, or a tactic, technique, or procedure, shoot us a quick email and we'll get on it. We are always looking for new content ideas and we want them to be things that help you do your job.

Write for the Update

Likewise, if there's something you'd like to write about for the update, we are always accepting submissions. We recognize the vast body of expertise our readership has, so if there is a piece of that you'd like to share, this is the place to do it. If you worry about attribution, or about revealing your affiliation with your unit or agency, don't worry—we get it.

In either case, drop us an email at:

admin@tpidg.us