in this issue >>> V.1.8

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC

A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

current topics >>>

In the News:

- Mega-Breaches: If Your Re-Use Passwords, Get Ready to be Busy
  - Krebs on Security
- Scammers Already Using Orlando Tragedy to Solicit Donations
  - Ars Technica
- University Pays $16,000 to Recover Data Held Hostage to Ransomware
  - Ars Technica
- Background Check Company Reads Your Private Facebook Data to Compile Marketable Information
  - Naked Security

Qubes AppVMs:

Sandbox Your Programs

Jacob Alexander

Virtual Machines are self-contained machines that run an operating system inside an already running host operating system. Basically it's a machine inside a machine where the host machine shares its resources with the virtual machine, but keeps all of its personal files to itself. The real benefit to running a virtual machine is complete isolation, meaning whatever happens in the VM stays in the VM. That's not to say it's impossible for something to escape from the VM to the host machine, but it is a good first layer of defense.

Qubes takes this to a whole new level and puts all of your individual applications inside their own mini virtual machine. Qubes calls them AppVMs or domains and they can be configured multiple different ways depending on your needs. For instance, if you want to visit a site you don't quite trust, you could run Firefox inside an untrusted domain and Qubes would see it as a possible security threat and block anything Firefox doesn't need to operate such as storage, the camera or the microphone. For more innocent applications, such as notepad, you could run it inside a work or personal domain and you would have a lot more freedom with what notepad could do.

Custom domains can also be created to suit your needs further, if you feel the defaults are too restrictive or not restrictive enough. You can also run multiple applications inside the same domain if they need access to the same resources. Qubes does a great job with isolation and making sure applications mind their own business. Applications should not be allowed to interact with other applications without permission to do so and they certainly shouldn't be allowed to take control of your computer (ie. Ransomware) and Qubes is definitely taking a step in the right direction.

For more information visit https://www.qubes-os.org/

set the stage >>>

Mobile Device Security: Pt II

Last week we began this series by talking about operating system and app updates. These two steps are immeasurably important in the security of any computer, and mobile devices are not exempt. If you make a habit of following that bit of advice, your smartphone is reasonably secure as-is. This security assumes that you **keep the apps on your device to the absolute minimum.** If an app isn't necessary, don't install it!

Applications (or "apps") are the programs we all know and love that make our smartphones more functional and more fun. However, apps also represent the Achille's Heel of smartphone security. Each additional app you install is an additional process that the device has to execute. This makes the system more complex and introduces more opportunity for things to go wrong (maliciously or not). The more complex a system is, the more potential for failure it has.

Aside from making the system needlessly complex, there are some other reasons to minimize the apps on your device. First, apps (yes, even in Apple's App Store) can be malicious by design. Malicious apps can be designed to break your HTTPS connections, harvest data from the device, access your camera and microphone, and track you in real time.

Non-malicious apps can perform some of these same behaviors because you allow them to when you install the app. Many apps that have no legitimate need access your contacts, your camera, your location data, or your browsing history. This information is often transmitted (frequently insecurely) back to the app developer, who compiles it and sells it to third-party data marketers.

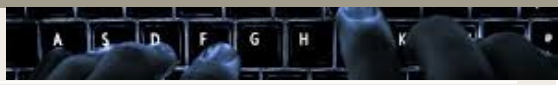
Next week we will discuss reviewing and limiting app permissions in iOS and Android. In the meantime, break the app addiction!

Upcoming Events:

-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: Privnote

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. Privnote is a tool that allows you to pass small amounts of data discretely, and know if it has been read.

Privnote is a website (https://privnote.com) that allows you to type or paste text. When you are ready to transmit it, you click "Create Note". A custom link will be created to your note. You can now forward this via text, Wickr, email, or any other medium to the intended recipient. When they click on the link the message will be displayed. And that is where things get interesting.

When the recipient—or anyone else—views the link, the message will be destroyed. It can only be opened once. This gives you a reasonably good assurance that only the intended recipient can access the contents of the message. There is also another potential benefit to using Privnote.

If your message is opened before it reaches your intended recipient, there is a good possibility that your communications are being monitored. You can even have Privnote alert you when a message has been destroyed. When typing your message you can click "Show Options". This will allow you to input a destruction notification email. Within seconds of your Privnote link being opened you will be notified.

Privnote is an excellent tool for passing small bits of sensitive information. For example, if you need to send a symmetrically-encrypted document, Privnote may be an option for sharing the password (through another medium, of course). Privnote is free, user friendly, and intuitive.

HTTPS Certificates

HTTPS connections are one of the most ubiquitous forms of encryption in use today. They are the backbone of internet security. But how do you really know your connection is secure? Read the certificate!

We have all seen the green padlock in the address bar of an internet browser, letting us know our connection is encrypted. This encryption is done with a protocol known as Transport Layer Security version 1.2. It is usually just referred to as "TLS" or sometimes even "SSL" (which actually refers to an out-of-date version of this protocol known as Secure Sockets Layer).

TLS provides very strong AES-128 encryption between your browser and the site you are visiting. This doesn't prevent someone from seeing what sites you are going to, but it does keep them from seeing the information you are sending and what you are viewing. TLS encryption is not perfect though. It can be stripped away or interfered with through self-signed certificates. There are numerous instances of this happening though malware, malicious Wi-Fi hotspots, and, since we have been talking about the Tor network, at rogue exit nodes.

When using Tor or any other untrusted network (like public Wi-Fi) you should verify that a site's certificate is valid before you trust it with sensitive information including your username and password and/or any financial transaction.

To verify a certificate is valid, you first have to view the certificate. In most modern browsers (including Chrome, Firefox, Opera, and Safari) you can do this by clicking the padlock icon in or beside the address bar. This will open a pop-up displaying some basic information about your connection. To view the actual certificate you will have to expand pop-out. Directions for popular browsers are:

⇒ **Chrome**: Details, then View Certificate

⇒ **Firefox**: Right arrow, then More Information, then View Certificate

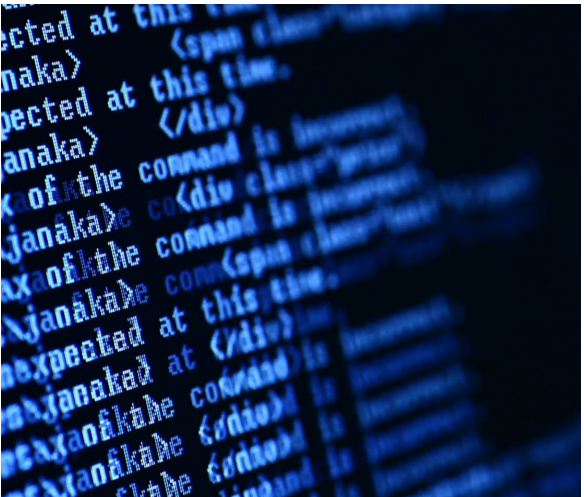
⇒ **Opera**: Details, then click the hyperlink beside "Certificate"

⇒ **Safari**: Show Certificate, then Details

Once the full details of the certificate are displayed there are a couple of quick checks you can make. First, look at the "Issued To" and "Common Name". It should match the site you are visiting. If you are visiting Bank of America's website, you should expect both of these to be some variation of "Bank of America" or "www.bankofamerica.com". If another entity is listed, you have a strong indicator you are currently the victim of a man-in-the-middle attack. If everything looks good, scroll to the bottom of the certificate information.

Here you are looking for a field labeled "Fingerprints". These are cryptographic hashes of the certificate being used to protect your session, but are meaningless without a known good fingerprint for comparison. Fortunately, good comparisons are available on the internet at https://www.grc.com/fingerprints.htm. On this page you can enter a domain name, click "Fingerprint Site" and be given an authentic fingerprint. Compare the SHA-1 fingerprints. If both the fingerprint you retrieved, and the one returned on www.grc.com match, your connection is not being tampered with and you can continue in confidence.

Though this may seem like a lot of work, it is incredibly important when using public Wi-Fi or services like the Tor Network.



Tor vs. VPNs?

Wrong Question

We are frequentl asked, "What is better, Tor or a VPN?" Though this question has some validity, it draws a false comparison between the two. Virtual Private Networks (VPNs) and Tor are designed for distinctly different purposes.

Anonymity vs. Privacy

The Tor Network and the Tor Browser Bundle are tools that are designed to assist users in gaining true anonymity. Virtual Private Networks, on the other hand, are designed to offer the user some enhanced privacy and security and by design cannot offer anonymity.

Tor is an excellent tool, but not ideal for all situations. Many websites disallow logins from Tor connections. It is also difficulty (and possibly undersirable) to route all a device's traffic through Tor. Both of these are areas where VPNs shine. While neither tool is perfect, both should be in your arsenal.

coming soon >>>

In The Next Issue

Tiny Hardware Firewall

COMSEC: iMessage and FaceTime

Mobile Device Security: Part III