Tails: The Amnesiac Incognito Live System – Privacy for Anyone Anywhere

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites/dependencies

Systems that can boot DVD, USB, or SD media (x86, no PowerPC or ARM), 1GB RAM

"We will open the book. Its pages are blank. We are going to put words on them ourselves. The book is called Opportunity and its first chapter is New Year's Day." - Edith Lovejoy Pierce

First and foremost, Happy New Year!

If you haven't read or heard about the perpetual stream of rather incredible disclosures continuing to emerge regarding the NSA's activities as revealed by Edward Snowden, you've likely been completely untethered from the Matrix or have indeed been hiding under the proverbial rock. As the *ISSA Journal* focuses on Cyber Security and Compliance for the January 2014 issue, I thought it a great opportunity to weave a few privacy-related current events into the discussion while operating under the auspicious umbrella of the cybersecurity label. The most recent article that caught my attention was Reuters reporting that "as a key part of a campaign to embed encryption software that it could crack into widely used computer products, the US National Security Agency arranged a secret $10 million contract with RSA, one of the most influential firms in the computer security industry."[1] The report indicates that RSA received $10M from the NSA in exchange for utilizing the agency-backed Dual Elliptic Curve Deterministic Random Bit Generator (Dual EC DRBG) as its preferred random number algorithm, an allegation that RSA denies in part.[2]

In September 2013 the *New York Times* reported that an NSA memo released by Snowden declared that "cryptanalytic capabilities are now coming online…vast amounts of encrypted Internet data which have up till now been discarded are now exploitable."[3] Ars Technica's Dan Goodin described Operation Bullrun as a "a combination of 'supercomputers, technical trickery, court orders, and behind-the-scenes persuasion' to undermine basic staples of Internet privacy, including virtual private networks (VPNs) and the widely used secure sockets layer (SSL) and transport layer security (TLS) protocols."[4] Finally, consider that, again as reported by DanG, a senior NSA cryptographer, Kevin Igoe, is also the co-chair of the Internet Engineering Task Force's (IETF) Crypto Forum Research Group (CFRG). What could possibly go wrong? According to Dan, Igoe's leadership had largely gone unnoticed until the above mentioned reports surfaced in September 2013 exposing the role NSA agents have played in "deliberately weakening the international encryption standards adopted by developers."[5]

I must admit I am conflicted. I believe in protecting the American citizenry above all else. The NSA claims that their surveillance efforts have thwarted attacks against America. Regardless of the debate over the right or wrong of how or if this was achieved, I honor the intent. Yet, while I believe Snowden's actions are traitorous, as an Internet denizen I can understand his concerns. The problem is that he swore an oath to his country, was well paid to honor it, and then violated it. Regardless of my take on these events and revelations, my obligation to you is to provide you with tooling options. The Information Systems Security Association (ISSA) is an international organization of information security professionals and practitioners. As such, are there means by which our global readership can better practice Internet privacy and security? While there is no panacea, I propose that the likes of The Amnesiac Incognito Live System, or Tails, might contribute to the cause. Again, per the Tails team themselves: "Even though we're doing our best to offer you good tools to protect your privacy while using a computer, **there is no magic or perfect solution to such a complex problem**." That said, Tails endeavors to help you preserve your privacy and anonymity. Tails documentation[6] is fabulous; you would do well to start with a full read before using Tails to protect your privacy for the first time.

1 http://www.reuters.com/article/2013/12/21/us-usa-security-rsa-idUSBRE9BJ1C220131221.

2 http://www.theregister.co.uk/2013/12/23/snowden_is_a_liar_and_we_never_fiddled_crypto_says_rsa/.

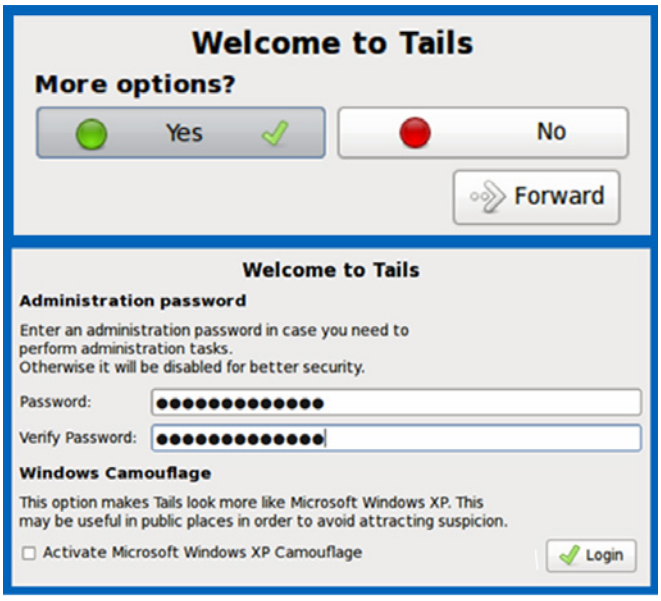
3 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0/

4 http://arstechnica.com/security/2013/09/nsa-attains-the-holy-grail-of-spying-decodes-vast-swaths-of-internet-traffic/.

5 http://arstechnica.com/security/2013/12/critics-nsa-agent-co-chairing-key-crypto-standards-body-should-be-removed/.

6 https://tails.boum.org/doc/index.en.html.

Figure 1 – Tails Greeter



Tails

Tails, a merger of the Amnesia and Incognito projects, is a Debian 6 (Squeeze) Linux distribution that works optimally as a live instance via DVD, USB, or SD media. Tails seeks to provide online anonymity and censorship circumvention with the Tor anonymity network to protect your privacy online. All software is configured to connect to the Internet through Tor and if an application tries to connect to the Internet directly, the connection is automatically blocked for security purposes. At this point the well-informed amongst you are likely uttering a "whiskey tango foxtrot, Russ, in October *The Guardian* revealed that the NSA targeted the Tor network."[7] Yes, true that, but it doesn't mean that you can't safely use Tor in a manner that protects you. This is a great opportunity, however, to direct you to the Tails warning page.[8] Please read this before you do anything else; it's important. Schneier's *Guardian* article also provides nuance. "The fact that all Tor users look alike on the Internet, makes it easy to differentiate Tor users from other web users. On the other hand, the anonymity provided by Tor makes it impossible for the NSA to know who the user is, or whether or not the user is in the US."

Getting under way with Tails is easy. Download it,[9] burn it to your preferred media, load the media into your preferred system, and boot it up. I prefer using Tails on USB media inclusive of a persistence volume; just remember to format the USB media in a manner that leaves room to create the persistent volume.

When you boot Tails, the first thing you'll see, as noted in figure 1 is the *Tails Greeter* which offers you *More Options*.

Figure 2 – Tails warns regarding a VM and confirms Tor

Selecting *Yes* leads you to the option to set an administrative password (recommended) as well as Windows XP Camouflage mode (makes Tails look like Windows XP when you may have shoulder surfers).

You can also boot into a virtual machine, but there are some specific drawbacks to this method (the host operating system and the virtualization software can monitor what you are doing in Tails). However, Tails will warn you as seen in figure 2.

Tor

You'll also note in figure 2 that TorBrowser (built on Iceweasel, a Firefox alternative) is already configured to use Tor, including the Torbutton, as well as NoScript, Cookie Monster, and Adblock Plus add-ons. There is one Tor enhancement to consider that can be added during the boot menu sequence[10] for Tails, where you can interrupt the boot sequence with *Tab*, hit *Space*, and then add *bridge* to enable Tor Bridge Mode.[11] According to the Tor Project, bridge relays, or bridges for short, are Tor relays that aren't listed in the main Tor directory. As such, even if your ISP is filtering connections to all known Tor relays, they probably won't be able to block all bridges. If you suspect access to the Tor network is being blocked, consider use of the Tor bridge feature as supported fully by Tails when booting in bridge mode. Control Tor with Vidalia, which is available via the onion icon in the notification area found in the upper right area of the Tails UI.

One last note on Tor use as already described on the Tails Warning page you should have already read. Your Tor use is only as good as your exit node. Remember, "Tor is about hiding your location, not about encrypting your communication." Tor does not, and cannot, encrypt the traffic between an exit node and the destination server. Therefore, any Tor exit node is in a position to capture any traffic passing through it and you should thus use end-to-end encryption for all communications. Be aware that Tails also offers I2P[12] as an alternative to Tor.

Encryption options and features

HTTPS Everywhere[13] is already configured for you in Tor Browser. HTTPS Everywhere uses a ruleset with regular

7 http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

8 https://tails.boum.org/doc/about/warning/index.en.html.

9 https://tails.boum.org/download/index.en.html - index2h1.

10 https://tails.boum.org/doc/first_steps/startup_options/index.en.html.

11 https://tails.boum.org/doc/first_steps/startup_options/bridge_mode/index.en.html.

12 http://www.i2p2.de/.

13 https://www.eff.org/https-everywhere.

expressions to rewrite URLs to HTTPS. Certain sites offer limited or partial support for encryption over HTTPS, but make it difficult to use where they may default to unencrypted HTTP, or provide hyperlinks on encrypted pages that point back to the unencrypted site.

You can use Pidgin for instant messaging which includes OTR or off-the-record encryption. Each time you start Tails you can count on it to generate a random username for all Pidgin accounts.

If you're afraid the computer you've booted Tails on (a system in an Internet café or library) is not trustworthy due to the like of a hardware keylogger, you can use the Florence[14] virtual keyboard, also found in the notification area as seen in figure 3.

If you're going to create a persistent volume (recommended) when you use Tails from USB media, do so easily with `Applications | Tails | Configure persistent volume`. Reboot, then be sure to enable persistence with the Tails Greeter. You will need to setup the USB stick to leave unused space for a persistent volume.

You can securely wipe files and cleanup available space thereafter with Nautilus Wipe. Just right click a file or files in the Nautilus file manager and select Wipe to blow it away…forever…in perpetuity.

KeePassX is available to securely manage passwords and store them on your persistent volume. You can also configure all your keyrings (GPG, Gnome, Pidgin) as well as Claws Mail. Remember, the persistent volume is encrypted upon creation.

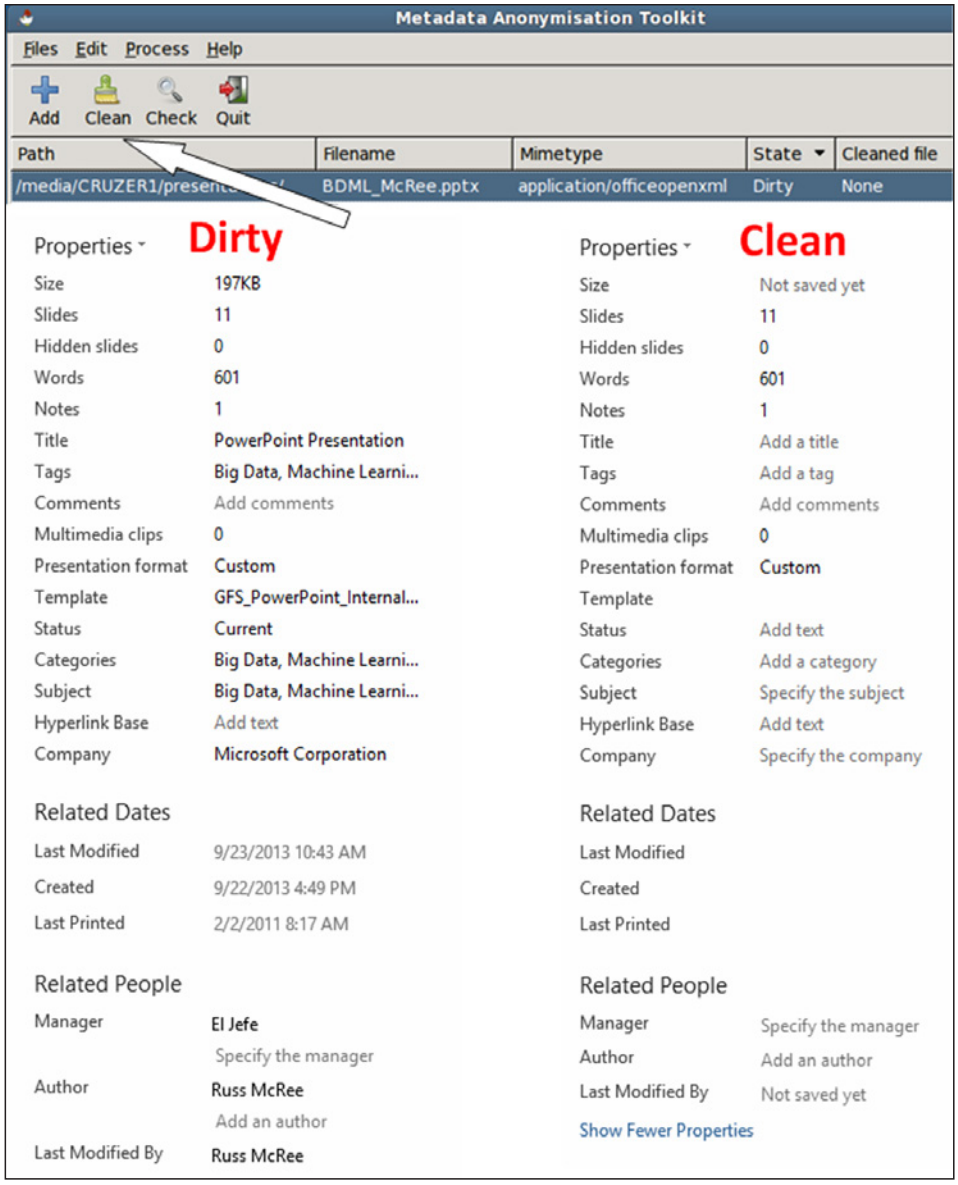


Figure 4 – Metadata Anonymisation cleans up a PowerPoint doc

You can encrypt text with a passphrase, encrypt and sign text with a public key, and decrypt and verify text with the Tails gpgApplet (the clipboard in the notification area).

One last cool Tails feature that doesn't garner much attention is the Metadata Anonymisation app. This is not unlike Informatica 64's OOMetaExtractor,[15] the same folks who bring you FOCA as described in the March 2011 *toolsmith*.[16] Metadata Anonymisation is found under *Applications* then *Accessories*. This application will strip all of those interesting file properties left in metadata such as author names and date of creation or change. I have used my share of metadata to create a target list for social engineering during penetration tests, so it's definitely a good idea to clean docs if you're going to pub-

14 http://florence.sourceforge.net/english.html.

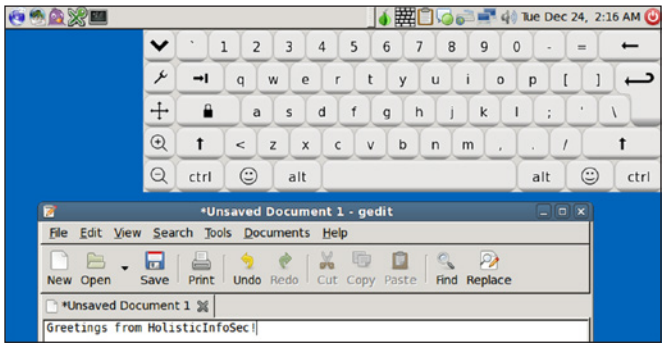


Figure 3: – The Tails virtual keyboard

15 https://oometaextractor.codeplex.com/.

16 http://holisticinfosec.org/toolsmith/pdf/march2011.pdf.

lish or share them if you wish to remain anonymous. Figure 4 shows a before and after collage of PowerPoint metadata for a recent presentation I gave.

There are numerous opportunities to protect yourself using The Amnesiac Incognito Live System, and I strongly advocate for you keeping an instance at the ready should you need it. It's ideal for those of you who travel to hostile computing environments, as well as for those of you non-US readers who may not benefit from the same level of personal freedoms and protection from censorship that we typically enjoy here in the States (tongue somewhat in cheek given current events described herein).

Conclusion

Aside from hoping you'll give Tails a good look and make use of it, I'd like to leave you with two related resources well worth your attention. The first is a 2007 presentation[17] from Dan Shumow and Niels Ferguson of Microsoft titled "On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng." Yep, the same random number generator as described in the introduction to this column. The second resource is from bettercrypto.org and is called Applied Crypto Hardening.[18] Systems administrators should definitely give this one a read.

Enjoy your efforts to shield yourself from watchful eyes and ears and let me know what you think of Tails. Ping me via Twitter via @holisticinfosec or email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

About the Author

Russ McRee manages the Security Analytics team for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.

17 http://rump2007.cr.yp.to/15-shumow.pdf.

18 https://bettercrypto.org.