Security Leftovers

By *Roy Schestowitz*
Created *21/07/2019 - 1:02pm*
Submitted by Roy Schestowitz on Sunday 21st of July 2019 01:02:13 PM Filed under Security [1]

- **Alas, Poor PGP [2]**

  The first is an assertion that email is inherently insecure and can?t be made secure. There are some fairly convincing arguments to be made on that score; as it currently stands, there is little ability to hide metadata from prying eyes. And any format that is capable of talking on the network ? as HTML is ? is just begging for vulnerabilities like EFAIL.

  But PGP isn?t used just for this. In fact, one could argue that sending a binary PGP message as an attachment gets around a lot of that email clunkiness ? and would be right, at the expense of potentially more clunkiness (and forgetfulness).

  What about the web-of-trust issues? I?m in agreement. I have never really used WoT to authenticate a key, only in rare instances trusting an introducer I know personally and from personal experience understand how stringent they are in signing keys. But this is hardly a problem for PGP alone. Every encryption tool mentioned has the problem of validating keys. The author suggests Signal. Signal has some very strong encryption, but you have to have a phone number and a smartphone to use it. Signal?s strength when setting up a remote contact is as strong as SMS. Let that disheartening reality sink in for a bit. (A little social engineering could probably get many contacts to accept a hijacked SIM in Signal as well.)

  How about forward secrecy? This is protection against a private key that gets compromised in the future, because an ephemeral session key (or more than one) is negotiated on each communication, and the secret key is never stored. This is a great plan, but it really requires synchronous communication (or something approaching it) between the sender and the recipient. It can?t be used if I want to, for instance, burn a backup onto a Bluray and give it to a friend for offsite storage without giving the friend access to its contents. There are many, many situations where synchronous key negotiation is impossible, so although forward secrecy is great and a nice enhancement, we should assume it to be always applicable.

  [...]

My current estimate is that there?s no magic solution right now. The Sequoia PGP folks seem to have a good thing going, as does Saltpack. Both projects are early in development, so as a privacy-concerned person, should you trust them more than GPG with appropriate options? That?s really hard to say.

- **Armadillo Is An Open-Source ?USB Firewall? Device To Protect You Against USB Attacks [3]**

  Exchanging data using USB devices is something that we do on a daily basis. But how often do you think that the next USB device that you?ll plug into your PC?s port could be malicious? In the past, researchers have unveiled 29 types of USB attacks that could compromise your sensitive data by simply plugging in a USB device.

  Globotron?s Armadillo is a device that you could use to protect yourself from USB attacks.

- **Open source solutions in autonomous driving: safety is more than an afterthought [4] [Ed: A lot less likely to contain back doors, unlike proprietary software where this has become rather 'standard' a 'feature']**

  In the automotive industry, in-vehicle infotainment (IVI) systems were one of the early adopters of open source operating systems, namely Linux. Today?s innovation and success with IVIs can largely be attributed to this approach.

  Collaborative efforts such as the GENIVI Alliance and Automotive Grade Linux?where automakers, suppliers, and their competitors agree to share common elements of the IVI software stack?are enabling rapid development in this area.

- **New open source solution reduces the risks associated with cloud deployments [5] [Ed: This is an inherently flawed kind of logic because if you handed over control to AWS, then the Pentagon already controls everything and thus you have zero security, you're 'pwned' by definition]**

  The Galahad software will be deployed to AWS and provides a nested hypervisor on AWS instances. There, it will monitor role-based virtual machines virtually across all levels of the application stack including the docker container: the basic unit of software that packages an application to run quickly between computing environments.

- **Open-Source Exploit: Private Keys in MyDashWallet Exposed for Two Months- Users Should Move Funds Immediately [6] [Ed: Highly misleading headline. This has nothing to do with "Open Source"; it's about some fool who uploaded private keys]**

  The private keys of Dash crypto coins being held in online software ?hot wallet? called

MyDashWallet have been exposed to hackers for two months, and anyone using the wallet should immediately move funds out.

A ?hot wallet? is any cryptocurrency software ?wallet? connected to the Internet.

Security

Source URL: http://www.tuxmachines.org/node/126117

Links:
[1] http://www.tuxmachines.org/taxonomy/term/59
[2] https://changelog.complete.org/archives/10010-alas-poor-pgp
[3] https://fossbytes.com/armadillo-usb-firewall-device/
[4] https://www.automotiveworld.com/webinars/open-source-solutions-in-autonomous-driving-safety-is-more-than-an-afterthought/
[5] https://www.helpnetsecurity.com/2019/07/19/reduce-cloud-deployment-risks/
[6] https://www.crowdfundinsider.com/2019/07/149501-open-source-exploit-private-keys-in-mydashwallet-exposed-for-two-months-users-should-move-funds-immediately/