NSA's Greatest Weapon In Surveillance? Outright Ignorance In Tech Consumers

Submitted by Reggie Middleton on 09/09/2013 13:35 -0400

Should MSFT split up

After reading an interesting article in the New Scientist, How NSA weakens encryption to access internet traffic, I was brought to mind a piece that I wrote to address the single most powerful tool in the NSA's arsenal – the blatant ignorance of the common tech enduser. I wrote intensely on this topic in What Angela Merkel Could Learn From Me and Using Glass To Spy On The Spies, to wit:

"…you can see how and why Android is safer to the populace than all of the popular competition. Windows and iOS all have the same problems, except for the facts that

- *You dont have access to the code*
- *You don't have the ability to submit changes to even be*

considered for acceptance

- *With Android, you don't need for Google to accept your personal changes, you can simply roll your own personal version and use it for yourself which should be the preference for the paranoid types. You can't do this with any other popular OS.*
- *The amound of independent eyes on Android trumps that of any other OS, by far. If something has a chance of getting caught (ex. spy code) it will likely get caught on Android code base. This has already happened, read XDA developers code posts for the HTC Evo"*

On that note, quoting the piece from the New Scientist, How NSA weakens encryption to access internet traffic:

The Snowden files say the NSA spends $250 million a year on covertly influencing the product designs of technology companies, suggesting inserting such vulnerabilities is a high priority for the agency.

It could also be swiping keys directly from online service providers, says Kuhn. The TLS encryption protocol, which puts the "s" in secure https connections, relies on servers storing a secret key to decrypt incoming messages or transactions. The NSA could bribe a system administrator or otherwise infiltrate the organisation to gain access to these keys, allowing it to decrypt any intercepted traffic to the relevant server.

To avoid the NSA's gaze, Kuhn says people should turn to open-source software, where many people evaluate the underlying code and can identify any attempts to weaken it. "There is going to be a lot of pressure on IT decision-makers to justify why they gambled the security of their infrastructure on some close-sourced offering that is very likely infiltrated by NSA

programmes."

There's also the news pieces stating that the NSA can access the personal information on popular handsets, including Blackberry, iOS and Android handsets. The NSA apparently had problems with the Blackberry devices, for about a year. Then again, knowing that Blackberry simply handed the keys over to the Indian government, I wouldn't have felt very secure, even for that year.

There are many reasons to avoid closed systems, with security and government systems being just two. There's also downright, market based innovation, as illustrated in this CNBC clip from Thursday…

Here's an example of the innovation that I use for privacy and control – CyanogenMod introduces system level encryption for messaging. The ability to have code scoured, cleaned, and fixed by tens of thousands of others will beat the efforts of any single company – any time of the day. If you really care about your privacy, you should think twice about iOS, Blackberry and Windows.

http://www.zerohedge.com/contributed/2013-09-09/nsas-greatest-weapon-surveillance-outright-ignorance-tech-consumers