بسم الله الرحمن الرحيم

Are Meltdown and Spectre Bugs Part of a Cover up Operation?

News:

Recently researchers revealed that two security flaws, dubbed Meltdown and Spectre, impact billions of devices globally. The flaws enable hackers to steal passwords and other sensitive user data from almost any device employing Intel, AMD and Arm chips [1]. Intel's involvement raises awkward questions about whether this was a design flaw or a disturbing ploy to help American intelligence services spy on foreign as well as domestic adversaries.

Comment:

The Meltdown bug, which is specific to Intel chips, allows hackers to bypass the hardware barrier between applications run by users and the computer's memory, potentially enabling hackers to read a computer's memory. A second bug, called Spectre, impacts chips from Intel, AMD and Arm. This enables hackers to trick otherwise error-free applications into giving up secret information. In the digital age, where most devices are connected to the internet, a powerful state entity or a terrorist organisation could easily manipulate these flaws and wreak havoc across the globe.

Hitherto, the mainstream media has reported these security flaws as bugs, but increasingly there appears to be a sinister side to this story. Only a few years ago, reports surfaced that America's premier National Security Agency (NSA) had a backdoor to Intel hardware. In 2014, during an interview with Reddit the CEO of Intel Corporation, Brian Krzanich refused to answer any questions about NSA's access to Intel hardware [2]. Clearly Krzanich's repeated denials underscore what most independent security analysts have suspected for decades. America's premier chipmaker and NSA are bedfellows. Last week, amidst reports that cloudproviders are looking to switch Intel's competitors, Krzanich tried his best to soothe fears and promised patches to the pseudo bugs.

Intel Corporation is not the only US technology company enjoying clandestine relations with American spooks. WikiLeaks and online blogs, Google [3], Microsoft [4], Facebook [5] and other tech giants enjoy similar relationships with US spy agencies such as the NSA, CIA, and FBI. In the shadows of Silicon Valley, there appears to be growing evidence that some tech startups are intentionally targeted and funded by CIA venture capital. Facebook is the most prominent example.

The clandestine relationship between American security services and tech companies not only erodes confidence in the independence of America's tech industry but makes a mockery of America's free market capitalism mantra where private enterprise is the centerpiece. Just like the oil industry before it, today's tech industry is selectively subsidized either by the US government or through certain US agencies that run such enterprises. Additionally, secretive association between the US government and tech giants reaffirms the longstanding proposition that governments must take the lead in making huge investments in infrastructure, which is inclusive of transport links and technology platforms.

This glaring deceitfulness disqualifies America in preaching to the world about the merits of Western capitalism and the benefits of its products and services. In the digital age, the world more than ever needs devices that are foolproof and do not possess secret back doors for spies to eavesdrop and exploit.

As far as the Islamic world is concerned, it cannot afford to invest in Western, Chinese or Russian technology platforms—all are compromised and serve their masters. The Islamic world must strive to build its own technology platforms but this can only happen under the shade of the caliphate (Khilafah) once political and economic sovereignty has returned to the state.

Written for the Central Media Office of Hizb ut Tahrir by

Abdul Majeed Bhatti

References:

[1] "Intel Chief Says Chip Flaw Damage Contained By Industry". 2018. Mail Online. http://www.dailymail.co.uk/sciencetech/article-5249039/Intel-chief-says-chip-flaw-damage-contained-industry.html.

[2] "Intel CEO Refuses To Answer Questions On Whether NSA Can Access Processors". 2014. Infowars. https://www.infowars.com/intel-ceo-refuses-to-answer-questions-on-whether-nsa-can-access-processors/.

[3] "How The CIA Made Google". 2017. Zero Hedge. https://www.zerohedge.com/news/2017-08-28/how-cia-made-google.

[4] Greenwald, Glenn, Spencer Ackerman, Laura Poitras, Ewen MacAskill, and Dominic Rushe. 2013. "Microsoft Handed The NSA Access To Encrypted Messages". The Guardian. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

[5] "Facebook And It's Connections To The C.I.A. And D.A.A.R.P.A. By Brian S Staveley". 2012. THE REAL NEWS ONLINE.COM. http://www.therealnewsonline.com/our-blogs/facebook-and-its-connections-to-the-cia-and-darpa.