Microsoft 'Encryption' and Intel 'Security'

By *Roy Schestowitz*
Created *06/11/2018 - 3:18am*
Submitted by Roy Schestowitz on Tuesday 6th of November 2018 03:18:34 AM Filed under Microsoft [1] Security [2]

- **You Can?t Trust BitLocker to Encrypt Your SSD on Windows 10 [3] [Ed: Actually, it has long been known that Microsoft's BitLocker has NSA back doors [4]. Even Microsoft staff spoke about it. It's for fools.]**

  > Some SSDs advertise support for ?hardware encryption.? If you enable BitLocker on Windows, Microsoft trusts your SSD and doesn?t do anything. But researchers have found that many SSDs are doing a terrible job, which means BitLocker isn?t providing secure encryption.

- **Flaws in self-encrypting SSDs let attackers bypass disk encryption [5]**

  > Researchers at Radboud University in the Netherlands have revealed today vulnerabilities in some solid-state drives (SSDs) that allow an attacker to bypass the disk encryption feature and access the local data without knowing the user-chosen disk encryption password.
  >
  > The vulnerabilities only affect SSD models that support hardware-based encryption, where the disk encryption operations are carried out via a local built-in chip, separate from the main CPU.
  >
  > Such devices are also known as self-encrypting drives (SEDs) and have become popular in recent years after software-level full disk encryption was proven vulnerable to attacks where intruders would steal the encryption password from the computer's RAM.

- **New Intel CPU Flaw Exploits Hyper-Threading to Steal Encrypted Data [6]**

A team of security researchers has discovered another serious side-channel vulnerability in Intel CPUs that could allow an attacker to sniff out sensitive protected data, like passwords and cryptographic keys, from other processes running in the same CPU core with simultaneous multi-threading feature enabled.

The vulnerability, codenamed PortSmash (CVE-2018-5407), has joined the list of other dangerous side-channel vulnerabilities discovered in the past year, including Meltdown and Spectre, TLBleed, and Foreshadow.

Microsoft Security

Links:
[1] http://www.tuxmachines.org/taxonomy/term/62
[2] http://www.tuxmachines.org/taxonomy/term/59
[3] https://www.howtogeek.com/fyi/you-cant-trust-bitlocker-to-encrypt-your-ssd-on-windows-10/
[4] http://techrights.org/wiki/index.php/Microsoft_and_the_NSA<
[5] https://www.zdnet.com/article/flaws-in-self-encrypting-ssds-let-attackers-bypass-disk-encryption/
[6] https://thehackernews.com/2018/11/portsmash-intel-vulnerability.html