Dalton Murray

INT 7223 Cybersecurity

Dr. Hany Othman

June 12, 2023

Research Assignment #2

Question

12.10 It is recommended that when using BitLocker on a laptop, the laptop should not use standby mode, rather it should use hibernate mode. Why?

There is a long debate about why laptops should use standby mode/sleep or if it should use hibernate mode. In recent years with Windows 10 and Windows 11 you should not use hibernate at all as it has the potential of slowing down the system and causing other harm to it, however, this is in general usage of the laptop and not specifically for BitLocker (https://support.microsoft.com/en-us/topic/use-of-hibernation-may-cause-slower-starts-and-resumes-when-bitlocker-drive-encryption-is-enabled-1006aec5-1f82-9cb0-f479-bcf5ec1f47ed).

For only the purposes of security and BitLocker, it is recommended to use hibernate mode instead of standby mode because if an attacker wants to get recovery keys for BitLocker and gains physical access to the machine, they can use a DMA attack in order to gain the ability to read contents of memory/RAM. However, if the laptop is in hibernation mode the contents of the disk are saved in the hibernation file, which is typically stored on the system on the C drive and prevents the attacker from

gaining access to the recovery keys (https://learn.microsoft.com/en-us/windows/win32/power/system-power-states?redirectedfrom=MSDN). In other words, this means that standby mode keeps the recovery keys/encryption keys in memory which an attacker can access while hibernate erases the key from memory while not in use and stores it in the hibernation file which makes it more secure for the laptop and the attacker cannot access this.

References

Stallings, W., & Brown, L. (2018). *Computer security: Principles and practice*. Pearson.

I have neither given nor received unauthorized aid in completing this work, nor have I presented someone else's work as my own.

Dalton Murray