Bypassing Self-Encrypting Drives (SED) in Enterprise Environments

Daniel Boteanu
dboteanu@kpmg.ca

Kevvie Fowler
kevviefowler@kpmg.ca

November 2nd, 2015

Abstract

Most enterprises employ full-disk-encryption (FDE) in order to protect the confidentiality of the data stored on laptop drives. In the recent past, hardware-based FDE solutions have gained increased popularity. Drives equipped with hardware-based encryption capabilities are called Self-Encrypting Drives (SED) and have the advantage of offloading the encryption from the Operating System to dedicated hardware in the drive.

In this paper we analyze 4 attack techniques that can be used to gain access to the data of a SED managed using the Trusted Computing Group (TCG) Opal Storage Specification standards, if the laptop is powered on or in Sleep Mode. One of these techniques had been previously analyzed for SEDs in the ATA Security Mode whereas the other 3 are to our knowledge novel techniques introduced by this paper.

Although not all configurations were vulnerable to all of attack techniques, we were able to gain access to the data on the SED using at least 2 techniques for each configuration tested.

Responsible Disclosure

The issues identified in this paper surround the usage of SED drives with the Opal standard in enterprise environments. However, these issues are not due to erroneous or incomplete implementations of the Opal standard by the various vendors. Instead, they are due to a limitation of the standard that is not well known within the industry.

We contacted TCG and disclosed our findings with them on July 15th, 2015. A decision was taken by common agreement that TCG would disseminate the information with all members of the Storage Work Group. We also involved CERT in the disclosure process and informed them of the exchanges we had with TCG and the vendors.

Finally, our goal with disclosing these findings is not to facilitate hacking by exploiting the vulnerabilities we identified. Instead, we are disclosing these issues with the purpose of raising awareness that these vulnerabilities exist, to allow for organizations to put in place mitigating controls and for the whole industry to evolve to a more secure state.

Contents

1. Introduction

Full Disk Encryption (FDE) is a technique that consists in encrypting the entire contents of a drive in order to provide data-at-rest protection. Until recently, the most common method of implementing FDE has been software-based which works by having a software component tied in the Operating System (OS) that decrypts or encrypts the data prior to it being read or writing to the drive.

An alternative to software-based FDE is to delegate the encryption logic to a dedicated hardware component in the drive. Drives that implement this feature are called Self-Encrypting Drives (SED). One of the advantages of SEDs is that the encryption is offloaded from the computer Central Processing Unit (CPU). Although this might not have a significant impact with typical hard-drives where the CPU encryption speeds largely surpass hard-drives read/write speeds, with the advent of SSDs that have superior read/write speeds, having the encryption offloaded to dedicated hardware increases the overall speed of the drive when encrypted.

One way to control SEDs is through standard Advanced Technology Attachment (ATA) Security commands. Before the existence of SEDs, the ATA Security commands were used to lock and unlock drives by using a password. Although ATA Security can in theory be used to manage SEDs, it is not wide-spread in enterprise environments. This is due mostly to the fact that it lacks management features required by enterprise deployments such as the use of recovery keys and Single Sign-On (SSO) OS based on user accounts.

Another method for controlling SEDs is by using the Trusted Computing Group (TCG) Opal Storage Specification [1]. The Opal standard provides a richer set of features than ATA Security and is most commonly used in combination with pre-boot authentication software that implements encryption key management and SSO. The TGC Commonly Asked Questions webpage [2] provides a listing of vendors that provide Opal compliant drives as well as software management solutions for Opal drives. Although this information appears to date from 2011, it demonstrates the level of industry acceptance of the standard.

Finally, Microsoft also implements a method for controlling SEDs, called Encrypted Hard Drive or eDrive [3]. This method is similar to Opal and adds specific requirements for drive manufacturers on top of the Opal standard. In the remainder of this paper, we will refer to this method as belonging to the Opal security model category, managed by the Microsoft BitLocker in eDrive mode.

This paper focuses on the analysis of SEDs when used in the Opal mode with a compatible software management solution. Any reference to SEDs used in the ATA Security mode will be explicitly distinguished.

2. Related Work

Müller et al. [4] provide a security evaluation of the hardware-based FDE and compare it to software-based FDE. In particular, they introduce a novel attack technique called “Hot Plug Attack” which involves switching the SATA data cable from the original machine and connecting it to an attacker-controlled machine. Because the SATA power is maintained while the data cable is switched, the drive remains in an unlocked state and the data can be read directly from the attacker-controlled machine.

Müller et al. also adapt and test known attacks for software-based FDE and provide a decision tree for the suitable attack technique depending on the computer’s state. Although they describe both the ATA Security as well as Opal security models, they only perform tests on SEDs managed with the ATA Security model.

2.1 Contributions

In this paper we provide the following contributions:

- *Hot Plug Attack*: We take the technique introduced by Müller et al. for ATA Security drives and test it on Opal drives;
- *Forced Restart Attack*: We introduce a new technique involving triggering a system crash followed by booting the machine from an alternative source. We call this technique the Forced Restart Attack;
- *Hot Unplug Attack*: We introduce and test an extension to the *Hot Plug Attack* technique that bypasses the eventual protection mechanisms that can be implemented in the laptops, such as the one implemented in Lenovo laptops for ATA Security drives;
- *Key Capture Attack:* We theorize about a technique that would allow for the actual encryption key to be captured and used for subsequent unlocking of the drive;
- *Recommendations:* We provide recommendations both for IT administrators on how to harden Opal SED deployments as well as for the SED vendors.

3. Attacks

3.1 Setup

The issues described in this paper do not affect specific drives, specific management software or the laptops and workstations from specific vendors. Instead, to our knowledge, these issues are common to all Opal SED deployments.

Because there are a large number of vendors providing both the drives, management software and computers compatible with Opal SED deployments it is practically impossible to test every single combination of these components. For the purposes of our research, we limited our testing to the following components:

- Drives (with originally supplied firmware):
  - Samsung 850 Pro, SSD, 1 TB, P/N MZ7KE1T0
  - Samsung PM851, SSD, 256GB, P/N MZ7TE256HMHP – 000L7
  - Seagate ST500LT015, HDD, 500 GB, P/N 1DJ142-500
  - Seagate ST500LT025, HDD, 500 GB, P/N 1DH142-500
- Target Computers:
  - Lenovo ThinkPad T440s, BIOS version 2.32
  - Lenovo ThinkPad W541, BIOS version 2.21
  - Dell Latitude E6410, BIOS version A16
  - Dell Latitude E6430, BIOS version A16

- Management Software:
  - Microsoft BitLocker eDrive, Windows version 8.1 Enterprise, Build 9600
  - Wave EMBASSY Security Center (ESC), version 2.11.1
  - WinMagic SecureDoc, version 6.4.0.117-HF1

In addition, out of the 48 possible combinations of the previously mentioned components, we tested the following 12:

- Samsung 850 Pro - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Samsung 850 Pro - Microsoft BitLocker eDrive - Lenovo ThinkPad T440s
- Samsung 850 Pro - Microsoft BitLocker eDrive - Dell Latitude E6430
- Samsung 850 Pro - Wave ESC - Lenovo ThinkPad W541
- Samsung PM851 - WinMagic SecureDoc - Dell Latitude E6410
- Samsung PM851 - WinMagic SecureDoc - Dell Latitude E6430
- Samsung PM851 - WinMagic SecureDoc - Lenovo ThinkPad T440s
- Samsung PM851 - WinMagic SecureDoc - Lenovo ThinkPad W541
- Seagate ST500LT015 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Seagate ST500LT015 - Microsoft BitLocker eDrive - Dell Latitude E6430
- Seagate ST500LT025 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Seagate ST500LT025 - Microsoft BitLocker eDrive - Dell Latitude E6430

For the purpose of simulating the attacker controlled computer, we used typical desktop and laptop computers equipped with a Tableau SATA Forensic Bridge.

3.2 Hot Plug Attack

As described by Müller et al., Hot Plug Attacks rely on the fact that SEDs do not detect when the SATA data cable is unplugged which allows them to be disconnected from the target machine and connected to the attacker-controlled machine. Because the power is maintained while the data connection is switched from one machine to another, the drive remains unlocked and the data is directly accessible on the attacker-controlled machine.

On laptops it is not possible to disconnect only the SATA data cable and usually, the entire drive must be removed from the laptop thus disconnecting both the data and the power connection. In order to overcome this limitation, the attacker puts the laptop in Sleep Mode and connects SATA extension cables between the drive and the laptop. Then, when the laptop is resumed from Sleep Mode, the laptop automatically unlocks the drive and at this point, the SATA data cable can be disconnected while still maintaining power to the drive.

Müller et al. found that modern Lenovo laptops detect when drives are unplugged in Sleep Mode and do not unlock them automatically when waking up from sleep. As mentioned before, these tests and results are limited to SEDs in the ATA Security mode. Although the scope of this paper is to analyze the security of SEDs in enterprise environments which use Opal, we validated the scenario described by Müller et al. on our test Lenovo ThinkPad W541 laptop and confirmed their results - i.e. the laptop detected that the drive was disconnected in Sleep Mode and did not unlock the drive automatically when the laptop was resumed from Sleep Mode.

When performing the same tests on SEDs in Opal mode, we confirmed that this attack technique remains valid. Furthermore, we found this attack to be successful even on modern Lenovo laptops when the drive SEDs are in the Opal mode.

The following configurations tested were found to be vulnerable to this attack:

- Samsung 850 Pro - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Samsung 850 Pro - Microsoft BitLocker eDrive - Lenovo ThinkPad T440s
- Samsung 850 Pro - Microsoft BitLocker eDrive - Dell Latitude E6430
- Samsung 850 Pro - Wave ESC - Lenovo ThinkPad W541
- Samsung PM851 - WinMagic SecureDoc - Dell Latitude E6410
- Samsung PM851 - WinMagic SecureDoc - Dell Latitude E6430
- Samsung PM851 - WinMagic SecureDoc - Lenovo ThinkPad T440s
- Samsung PM851 - WinMagic SecureDoc - Lenovo ThinkPad W541
- Seagate ST500LT015 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Seagate ST500LT015 - Microsoft BitLocker eDrive - Dell Latitude E6430
- Seagate ST500LT025 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Seagate ST500LT025 - Microsoft BitLocker eDrive - Dell Latitude E6430

None of the configurations tested that had the option of Sleep Mode were found to protect against this attack.

Note that Sleep Mode might not be the default installation option or even available at all for some SED management solutions. For example, the standalone Wave EMBASSY Security Center (ESC) 2.11.1 does not support Sleep Mode at all when used in conjunction with SEDs [5]. On the other hand, Sleep Mode is supported in enterprise deployments with Wave EMBASSY Remote Administration Server (ERAS), however, the ERAS Administration Manual [6] encourage the use of Hibernation instead of Sleep Mode due to the fact that when using Sleep Mode, the SED is automatically unlocked when the machine is resumed. McCracken [7] also mentions the issues with Sleep Mode and SED on the WinMagic Security blog and suggests the use of geofencing to move the laptop from Sleep Mode to Hibernation when the laptop is no longer connected to the corporate network. Finally, Microsoft [8] mentions that the use of Hibernation is more secure than Sleep Mode because returning from Hibernation requires BitLocker authentication, although this recommendation is generic to BitLocker and not specific to BitLocker eDrives.

3.3 Forced Restart Attack

As described above, after an SED is unlocked, it will remain in that state until it is powered off or explicitly locked.

If an attacker is able to trigger a soft-reset, the drive will remain unlocked. The attacker then has the option of booting from an alternative source such as CD/DVD, USB or PXE in order to run an OS that the attacker controls and that reads the data off of the unlocked drive.

Default configurations of Windows automatically restart after a Blue Screen of Death (BSOD) crash. An attacker that has physical access to a running Windows machine with an SED and is able to generate a BSOD will be able to employ this technique.

The following configurations tested were found to be vulnerable to this attack:

- Samsung 850 Pro - Microsoft BitLocker eDrive - Dell Latitude E6430
- Samsung 850 Pro - Wave ESC - Lenovo ThinkPad W541
- Samsung PM851 - WinMagic SecureDoc - Dell Latitude E6410
- Samsung PM851 - WinMagic SecureDoc - Dell Latitude E6430
- Samsung PM851 - WinMagic SecureDoc - Lenovo ThinkPad T440s
- Samsung PM851 - WinMagic SecureDoc - Lenovo ThinkPad W541
- Seagate ST500LT015 - Microsoft BitLocker eDrive - Dell Latitude E6430
- Seagate ST500LT025 - Microsoft BitLocker eDrive - Dell Latitude E6430

The following configurations tested were found to be not vulnerable to this attack:

- Samsung 850 Pro - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Samsung 850 Pro - Microsoft BitLocker eDrive - Lenovo ThinkPad T440s
- Seagate ST500LT015 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541
- Seagate ST500LT025 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541

We observed that the two modern Lenovo laptops we tested, ThinkPad W541 and ThinkPad T440s, when used in conjunction with BitLocker eDrives, would lock the drive whenever the machine restarted. This occurred both when performing a standard Windows restart as well as when triggering a BSOD crash. This behavior was not observed on the same Lenovo laptops when used in conjunction with Wave ESC or WinMagic SecureDoc. In addition, this behavior was not observed on the Dell Latitude E6410 and E6430 laptops when used in conjunction with either BitLocker eDrives or with Wave ESC and WinMagic SecureDoc.

The following sections describe different modes that can be used to trigger a BSOD in Windows.

3.3.1 Facedancer Triggered BSOD

The Facedancer [9] is a device that can be used to fuzz USB drivers. As shown by Schumilo et al. [10], there are several bugs in the USB driver stack of operating systems that can cause them to crash.

In particular, we confirmed that the following test cases from USB host security assessment tool *umap* [11] trigger a BSOD on a Windows 8.1 Enterprise OS fully patched as of July 13th, 2015:

- 03:00:00:C:16
- 03:00:00:C:17

- 01:01:00:C:4
- 01:01:00:C:5
- 09:00:00:C:9

3.3.2 USB Hub Chaining Triggered BSOD

In addition to being able to trigger a BSOD sending malformed USB packets, we were able to consistently crash a fully patched Windows 7 32-bit Enterprise machine using a specific combination of off-the-shelf hardware: a SteelSeries Kinzu v2 Pro Edition mouse (P/N: 62025) connected to the USB port of a DAS keyboard (P/N: DASK3ULTMS1SICO) connected to the USB port of a LinksKey 2-port USB KVM Switch (P/N: LDV-302ARC) connected to the laptop.

Note that we discovered this combination of devices that trigger the Windows BSOD by accident which shows that generating a Windows BSOD by having physical access to a machine is relatively easy to achieve.

3.3.3 Memory Pins Short Triggered BSOD

This method of triggering a BSOD involves tampering with the hardware of the machine. Specifically, we found that shorting memory pins of a running laptop for a brief period of time can cause a BSOD. In our testing, we were able to generate a BSOD and have the OS subsequently restart roughly once in every two attempts, with the other attempts resulting in an OS hang. We triggered this by sliding the tip of a screwdriver over the pins of a memory module, as illustrated in Figure 1. Note that although in our tests we did not experience any permanent hardware issues, this technique could have a potentially destructive effect on the memory module or the motherboard.

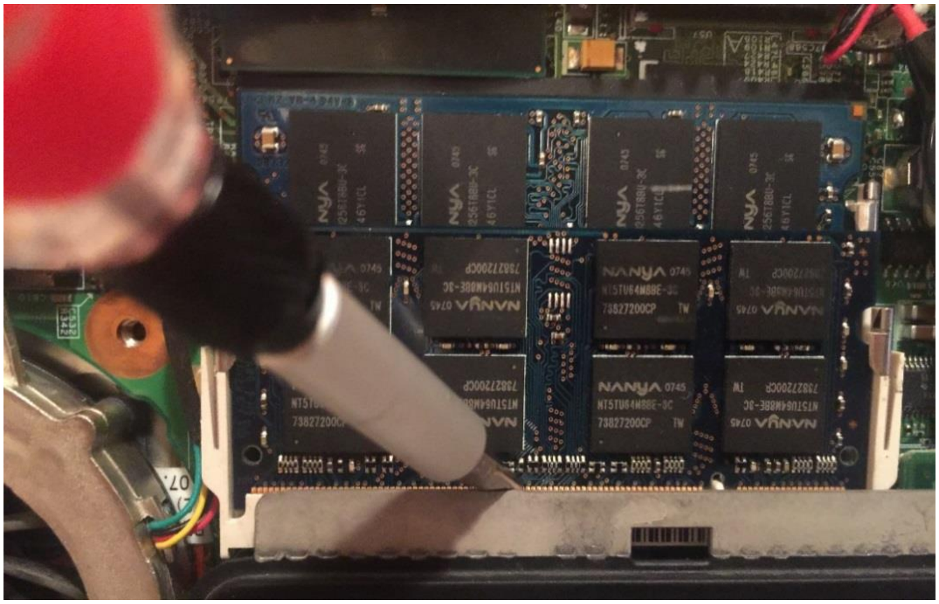

Figure 1 - Shorting the pins of a memory module

3.3.4 Keyboard Triggered BSOD

Windows has a documented way for triggering BSODs using the keyboard after adding a specific key to the Windows Registry [12]. This technique is not a vulnerability and requires local administrative privileged on the machine to perform the registry changes. We found this feature useful because it allowed us to trigger controlled BSOD and more easily verify the behavior of the SEDs when faced with an OS crash.

3.4 Hot Unplug Attack

As described in section 3.2, when performing the Hot Plug Attack technique on laptops, the attacker must first put the laptop in Sleep Mode so that SATA extension cables can be installed. Laptop manufacturers could put in place mechanisms to detect if a drive is disconnected while the laptop is in Sleep Mode and prevent the drive from being unlocked automatically on resume. Although modern Lenovo laptops implement this feature on SEDs in the ATA Security mode, we are not aware of such an implementation for SEDs in the Opal mode.

At a high-level, this technique involves following operations:

1. Expose the drive SATA connector pins while the drive is still in the laptop and is powered on;
2. Supply power to the drive SATA pins from an alternate source;
3. Break the SATA power and data connections between the drive and the laptop;
4. Maintain the alternate power source and connect the SATA data to the attacker-controlled machine.

We attempted two implementations of this technique, one where we taped wires to a plastic card and placed the card on the SATA power pins and another one that where we exposed the power and data pins from an actual SATA connector. The first implementation did not produce the expected results and after several attempts, we ended up accidentally connecting the taped wires to the wrong pins on the drive which rendered the drive permanently inoperable. The second technique produced the expected results and consisted of the following:

1. Expose the drive SATA connector pins while the drive is still in the laptop and is powered on – we opened the drive cover and removed the drive screw; then, we slightly pulled the drive in the direction opposite to the SATA connector in order to expose the SATA connector pins, as illustrated in Figure 2 and Figure 3;

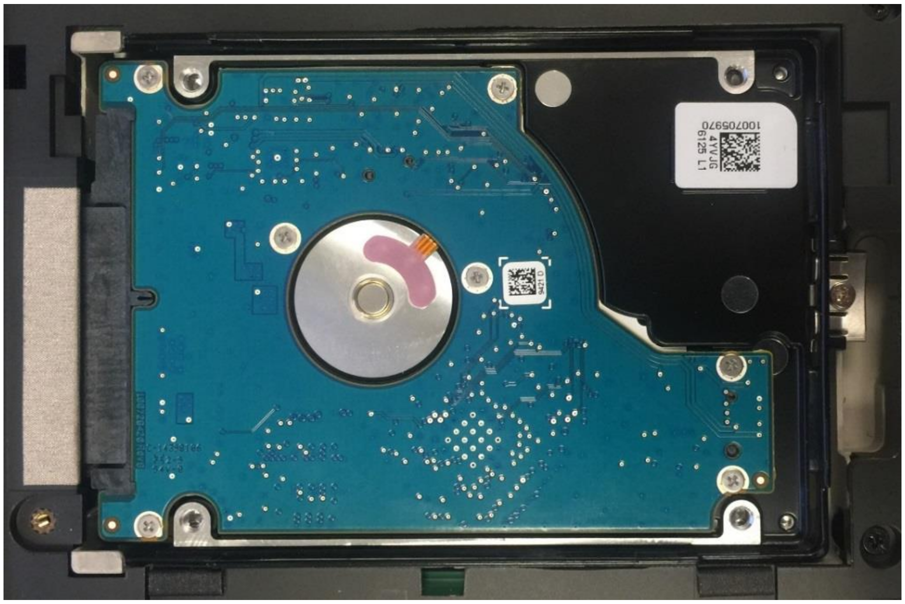

Figure 2 – SED in laptop compartment with cover open

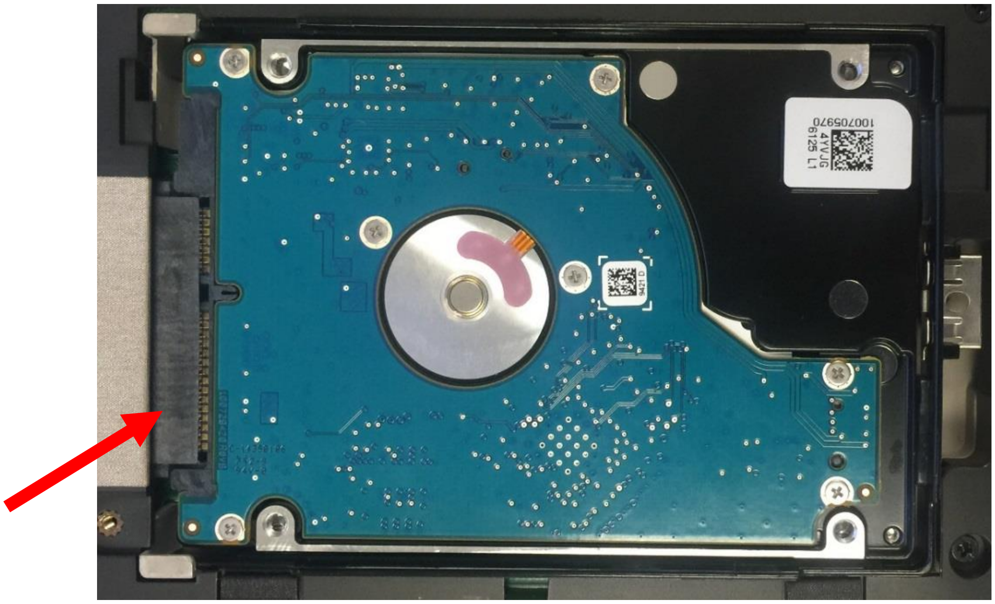

Figure 3 – SED in laptop compartment with cover open and SATA pins exposed (shown by arrow)

2. Supply power to the drive SATA pins from an alternate source – we modified a SATA extension cable in order to expose the pins, as illustrated in Figure 4; this cable contained both data and power connectors but at this stage only power was provided at the other end of the extension cable; we then connected the SATA extension pins to the exposed pins on the drive, as illustrated in Figure 5;

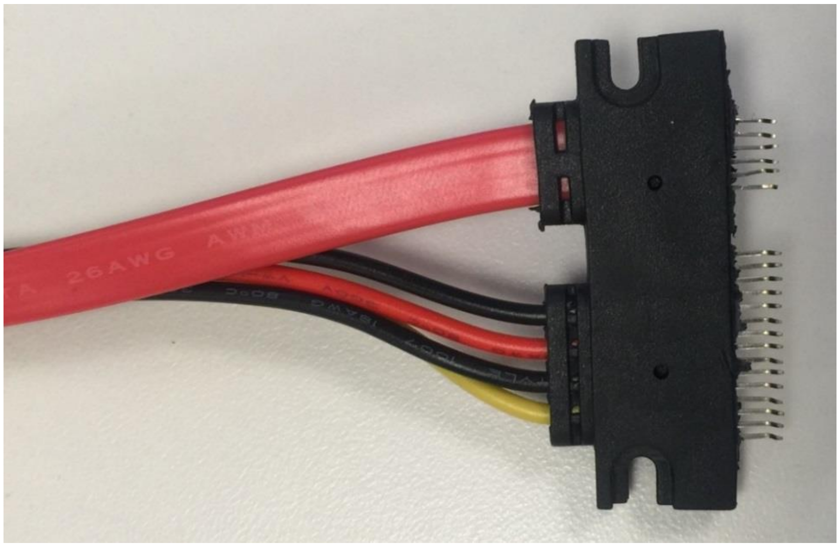

Figure 4 – SATA power and data cable and connector with pins[1] exposed

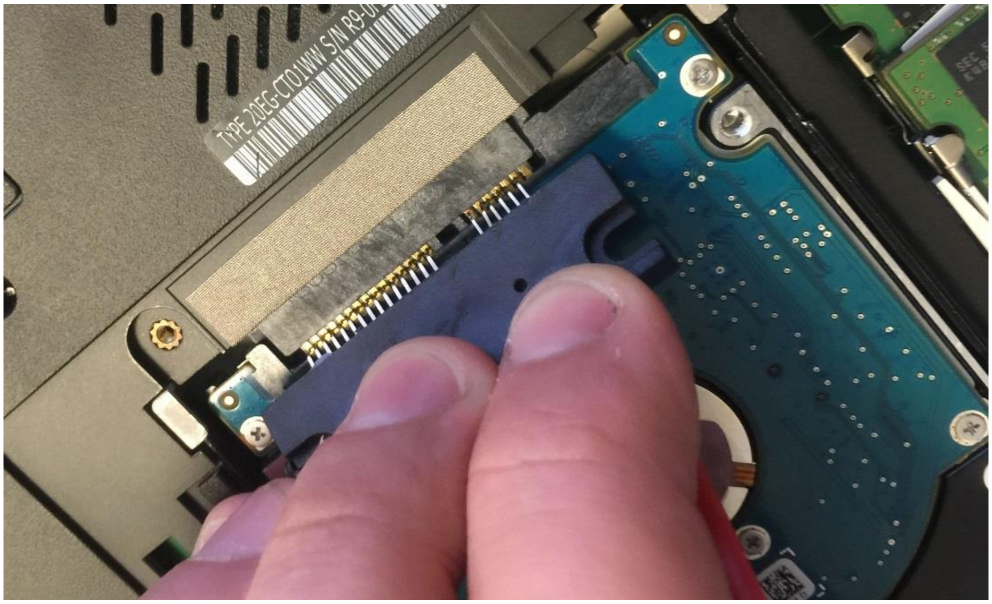

Figure 5 – SATA pins connected to drive while operating

3. Break the SATA power and data connections between the drive and the laptop – we pulled the drive from the enclosure until it was completely disconnected from the laptop SATA power and data connector, while still maintaining the connection with the modified SATA extension cable;
4. Maintain the alternate power source and connect the SATA data to the attacker-controlled machine – we connected the other end of the SATA data extension cable to the attacker-controlled machine and we obtained access to the unencrypted data.

[1] The top-most SATA data pin was accidentally broken when exposing the pins. Because this pin (1) is connected to GND, role also performed by pins (4) and (7), this did not have an impact on our experiment.

The following configuration was found to be vulnerable to this attack:

- Seagate ST500LT015 - Microsoft BitLocker eDrive - Lenovo ThinkPad W541

Note that this technique is similar to the Hot Plug Attack with the difference that it does not require the laptop to be put in Sleep Mode. Consequently, we expect this technique to work on at least all of the configurations that are vulnerable to the Hot Plug Attack as well as to bypass any protection mechanisms that could be implemented in the laptops that would detect and lock drives being disconnected while in Sleep Mode.

3.5 Key Capture Attack

This technique consists in capturing the actual cryptographic keys being sent to the drives to unlock them.

One implementation of this attack technique consists of updating the firmware of an attacker-controlled drive in order to masquerade as a legitimate Opal drive and to capture and store encryption keys. Then, the target machine is put in Sleep Mode and the original drive is replaced with the tampered drive. When the machine is resumed from Sleep Mode, the unlock command and decryption key is sent to the tampered hard drive which records it. Then this key is used to unlock the original drive without other restrictions on an attacker controlled machine.

An alternative implementation of this technique consists of connecting a SATA sniffer to the SATA data cable to capture and decode the authentication commands containing the decryption key while the original drive is being unlocked, for example, when the machine is resumed from Sleep Mode.

Note that we only theorize about the Key Capture Attack and that we did not actually implement or test it. However, this technique could be used to bypass eventual protection measures in the drives that would detect when the SATA data connection of a drive is interrupted and moved to another machine.

4. Recommendations

This section describes the various corrective or compensatory measures that can be put in place to limit the risk that the SED attacks described in this paper pose.

4.1 Recommendations for Enterprises

Enterprises that have currently deployed SEDs may attempt to harden their deployments. In particular the following compensatory measures should be taken into consideration:

- Disabling Sleep Mode: If the availability of Sleep Mode is not required, we recommend disabling this feature in order to prevent against Hot Plug attacks on laptops. Alternatively, some management solutions allow for setting temporal or geographical limitation on the use of Sleep Mode;
- Disabling the restart on BSOD: If the Windows *Automatically restart* feature is not activated, an attacker that has the ability to crash a machine with a BSOD will not be able to boot the machine from an alternative media. This workaround addresses the Forced Restart Attack technique;
- Prevent booting from alternative sources: If the BIOS is locked down to prevent a user from booting for any other device than the main drive, an attacker that is able to trigger a restart would not be

able to boot from an attacker-controlled OS and read the data. This workaround addresses the Forced Restart Attack technique.

4.2 Recommendations for SED Manufacturers

SED manufacturers should consider implementing a feature in the drives that detects when the SATA data connection is lost and locks the drive at that point. This recommendation mitigates the Hot Plug and Hot Unplug Attacks.

4.3 Recommendations for SED Management Software Providers

SED Management Software Providers should discourage or disable the use of the Sleep mode as well as the *Automatically restart* Windows feature, similarly to our recommendations in section 4.1. Note that some SED management solutions already implement this recommendation to a certain extent.

4.4 Recommendations for Laptop Manufacturers

Laptop manufacturers should consider detecting when Opal managed SEDs are disconnected in Sleep Mode and disabling the automatic unlocking of these drives when they are plugged back. Because the unlocking is performed by the SED management software and not directly by the laptop BIOS or UEFI, this recommendation is not straightforward to implement. One way in which this could be achieved would be for the laptop to require a full power off and power back on when such an event is detected.

In addition, laptop manufacturers should consider providing configuration options in the BIOS or the UEFI that would lock the SED when the system is being reset, for example, after a Windows BSOD. According to the testing that we performed, eDrive managed SED have this behavior which mitigates the Forced Restart Attack.

Finally, laptop manufactures should consider providing laptop with tamper detection mechanisms that, for example, would power off the laptop if the drive cover is tampered with, if configured to do so.

4.5 Recommendations for OS Developers

Operating System developers should reconsider the implications of bugs or vulnerabilities in their software that allow an attacker with physical access to the machine to trigger a system crash generating a soft-reset. As shown in this paper, in the context of SEDs, such a system crash may give an attacker access to clear text data on a SED.

5. Conclusions

In this paper, we introduce 3 novel attack techniques for gaining access to the data on SEDs in the Opal security mode, namely the Forced Restart Attack, Hot Unplug Attack, and Key Capture Attack. These techniques, as well as the Hot Plug Attack previously used to gain access to SEDs in the ATA Security mode, all require an attacker to have physical access to a laptop that is powered or in Sleep Mode.

We tested the Hot Plug Attack, Forced Restart Attack and Hot Unplug Attack on various configurations with Seagate and Samsung drivers of different models, on Lenovo and Dell laptops of different models and in conjunction with WinMagic, Wave and Microsoft SED management software.

We found all tested configurations to be vulnerable to the 3 attack techniques, with the exception of the Lenovo laptops when used in conjunction with the Microsoft BitLocker eDrive SED management software. In this specific case, the Force Restart Attack was unsuccessful regardless of the drive being used, however, the other two techniques, the Hot Plug Attack and Hot Unplug Attack were successful and did allow us to bypass the SED data encryption.

We recommend that enterprise deployments of SEDs consider disabling Sleep Mode, preventing Windows to automatically restart following a crash and locking down the BIOS or UEFI. We also provide recommendations for the other industry actors involved in SED solutions, such as, SED manufacturers, SED management software providers and OS developers.

6. References

[1] Trusted Computing Group, Storage Security Subsystem Class: Opal, Specification Version 2.01, Revision 1.00, August 5, 2015

[2] Trusted Computing Group, Commonly Asked Questions and Answers on Self-encrypting Drives, November 18, 2011, http://www.trustedcomputinggroup.org/resources/commonly_asked_questions_and_answers_on_selfencrypting_drives

[3] Microsoft, TechNet, Encrypted Hard Drive, August 23, 2012, https://technet.microsoft.com/en-ca/library/hh831627.aspx

[4] Tilo Müller, Tobias Latzo, and Felix C. Freiling, Friedrich-Alexander - Self-Encrypting Disks pose Self-Decrypting Risks, How to break Hardware-based Full Disk Encryption, Universität Erlangen-Nürnberg, Germany, December 2012, https://www1.informatik.uni-erlangen.de/filepool/projects/sed/seds-at-risks.pdf

[5] Wave, EMBASSY Security Center (ESC) Client Manual, ESC Version 2.11 SP1, October 23, 2014

[6] Wave, EMBASSY Remote Administration Server (ERAS) Administrator Manual, ERAS Version 2.11 SP1, October 22, 2014

[7] Garry McCracken, Sleep and PBA, WinMagic Security Blog, Speak, http://www.winmagic.com/blog/2014/09/17/sleep-and-pba/

[8] Microsoft, TechNet, Windows BitLocker Drive Encryption Frequently Asked Questions, March 22, 2012, https://technet.microsoft.com/en-us/library/cc766200(v=ws.10).aspx#BKMK_Sleep

[9] Travis Goodspeed and Sergey Bratus, "Emulating USB Devices with Python." http://travisgoodspeed.blogspot.de/2012/07/emulating-usb-devices-with-python.html , July 3, 2012

[10] Sergej Schumilo, Ralf Spenneberg, Hendrik Schwartke - Don't trust your USB! How to find bugs in USB device drivers, BlackHat Europe 2014, November 16, 2014, https://www.blackhat.com/docs/eu-14/materials/eu-14-Schumilo-Dont-Trust-Your-USB-How-To-Find-Bugs-In-USB-Device-Drivers-wp.pdf

[11] Andy Davis, NCC Group Plc, umap – The USB host security assessment tool, https://github.com/nccgroup/umap

[12] Microsoft, Forcing a System Crash from the Keyboard, April 1, 2015, https://msdn.microsoft.com/en-us/library/windows/hardware/ff545499(v=vs.85).aspx