Western Digital Corporation

SanDisk X600 SED Security Assessment

April 29, 2019

Prepared For:
Brian Mastenbrook | *Senior Director, Product Security Engineering, Western Digital*
Brian.Mastenbrook@wdc.com

Prepared By:
Paul Kehrer | *Principal Security Engineer, Trail of Bits*
paul.kehrer@trailofbits.com

Will Song | *Security Engineer, Trail of Bits*
will.song@trailofbits.com

Table of Contents

Executive Summary

Summary of TCG Opal and ATA security modes

SanDisk X600 SED Threat Model

Technical description of the issues

Description of the remediation

- TCG activated unlocked range vulnerability
- TCG to ATA cross mode vulnerability
- ATA Maximum capability mode Master password issue

Actions taken to validate the fix

- TCG activated unlocked range vulnerability
    - Limitations of PIN_KEK ANON remediation
- TCG to ATA cross mode vulnerability
- ATA Maximum capability mode Master password issue

Recommendations

- 1. Transforming password to AES key is done with SHA256

About Trail of Bits

Executive Summary

From April 8th to April 26th 2019 Trail of Bits conducted an analysis of the SanDisk X600 SED drive firmware source code to determine if Western Digital's proposed modifications resolved the set of cryptographic key management issues disclosed by Radboud University researchers. Radboud University contacted Western Digital in December 2018 to disclose multiple vulnerabilities discovered during their research. Western Digital developed a set of fixes and engaged Trail of Bits to validate their remediation for the protection of data at rest on the drive.

We have determined that the changes resolve the following documented issues:

- When an unlocked range was present on disk the key hierarchy contained a linkage between a KEK encrypted under an empty password and an intermediate encrypting key that allowed locked range decryption without the correct user password.
- TCG Activated and ATA security mode used the same raw PIN_KEK when initialized. When combined with the empty password-encrypted KEK from the previous vulnerability, this allowed decryption of a drive in ATA security mode if the drive was switched from TCG to ATA mode.
- With ATA security enabled the Master password remained linked to the data encryption key (DEK) when the drive was switched into Maximum capability mode.

For each of the issues Trail of Bits reviewed the original design, documentation of the proposed fix, and the concrete implementation of that fix to confirm that the vulnerability in question had been resolved. All three vulnerabilities listed above have been resolved by the changes that Western Digital has made to their design and firmware implementation.

Further details on the exact nature of the vulnerabilities and their respective resolutions are provided below.

Summary of TCG Opal and ATA security modes

The SanDisk X600 SED hard drive supports full disk encryption via the Trusted Computing Group (TCG) Opal specification (version 2.01)[1] along with the older but still widely used ATA security feature set. A complete review of the Opal feature set is out of the scope of this engagement. Instead, the specific areas of examination for this audit were the protection and derivation of the keys used to encrypt the drive, as well as the method of binding the user password to the data-encryption keys.

This drive has several modes of operation that are of interest: a drive may be considered to be in a TCG activated or deactivated state; an activated drive has multiple ranges of encrypted data with configurable levels of access control; and a TCG deactivated drive can still be encrypted with a User (and Master) password via ATA security. The set of combined modes we considered in this engagement were:

- **ATA security** with a User/Master password. This setting requires TCG to be deactivated. ATA security can be used in High capability or Maximum capability mode. When set to High capability either a User or Master password should be capable of unlocking the drive, while Maximum capability disables unlock support for the Master password and requires the User password exclusively. The Master password may still be used to erase the drive in Maximum capability mode. This feature is commonly used in enterprise deployment settings.
- **TCG activated** with locked ranges. Ranges (which correspond to contiguous regions of data on the drive) may be in a **locked** or **unlocked** state. A locked range requires a password to read/write, while an unlocked range is available at boot without a password. User passwords are configurable on a per-range basis, allowing different User passwords to decrypt different ranges. Additionally, the TCG Opal specification defines multiple levels of access control so administrator passwords may be configured that allow decryption of ranges.

Drives encrypted using a User password require the creation of a cryptographic binding between the password and the key used to encrypt the drive. In a simplified form, the drive generates a random data encryption key (DEK) and encrypts that value under the User password. In a production implementation the various features of the TCG Opal specification require the creation of a key hierarchy. The updated hierarchy Western Digital has implemented for the SanDisk X600 SED can be found in Figure 2 of this document.

[1] https://trustedcomputinggroup.org/wp-content/uploads/TCG_Storage-Opal_SSC_v2.01_rev1.00.pdf

SanDisk X600 SED Threat Model

To evaluate the security of the drive and the efficacy of the proposed remediation we need to identify the objectives and known limitations of the security design. Western Digital's original threat model for self encrypting drives can be summarized as follows:

1. Users who provide evidence of ownership of data are trusted to perform arbitrary operations on that data. A user provides evidence of ownership via password authentication.
2. Once data is unlocked via password authentication it remains unlocked until power cycle or an explicit device locking event.
3. Attackers are not able to implement side channel attacks, fault attacks, physical probing, or other physically invasive attacks.
4. Stealing a user password via social engineering or other attacks is out of scope.
5. An attacker is capable of attacks at the PCB level. An attacker may modify and replace NAND memory but is not able to modify or read internal controller memory at run-time.

Notably, this threat model assumed that the drive would remain secure against arbitrary code execution on the controller itself. This assumption was revisited after the Radboud researchers were able to load alternate firmware onto the drive that allowed them to inspect memory and issue commands to read and write at arbitrary points on the device. The threat model under which Trail of Bits audited the revised firmware adds the following statements:

1. In TCG activated mode, the attacker does not know any of the credentials for TCG Admin or User authorities.
2. In ATA security mode, the attacker does not know the ATA user password, or in High security mode, the ATA Master password. In ATA Maximum mode, the attacker is assumed to know the Master password.
3. All credentials are of sufficiently High entropy that they cannot be feasibly guessed by a computationally bounded adversary.
4. In both cases, the attacker has physical possession of the device in powered off state. The attacker is assumed to be able to run arbitrary code on the controller SoC.
5. The attacker does not replace the firmware and re-insert the drive into the authorized user's system (an "evil maid" attack).

Technical description of the issues

The SanDisk X600 SED firmware contained the following issues:

1. A vulnerability in the structure of the encryption keys allowed locked ranges to be decrypted without a password in some configurations. In TCG activated mode, if there was an unlocked range (e.g. a boot partition), then the drive maintained a key known as a $\text{PIN\_KEK}_{\text{ANON}}$. This key allowed decryption of the key that encrypted the DEK for that range. Each range had its own DEK, but all the encrypted DEKs were encrypted using the same key. This allowed any valid user password (including the empty password for $\text{PIN\_KEK}_{\text{ANON}}$) to gain access to all DEKs. If an attacker were to gain code execution on the drive this could have been used to decrypt any range, regardless of password.
2. Switching from TCG activated mode to ATA security mode allowed decryption of the drive without a password. When the drive was initialized, a $\text{PIN\_KEK}_{\text{RAW}}$ was generated for the drive. This key was shared between TCG and ATA mode. Switching from TCG activated mode to ATA security failed to clear the $\text{PIN\_KEK}_{\text{ANON}}$, which allowed recovery of the DEK.
3. Data could still be decrypted using the Master password when the drive was in ATA security Maximum capability mode. With ATA security activated, the Master password PIN_KEK was not cleared when switching to Maximum capability mode. This allowed the DEK to be recovered via the Master password even when only the user password should have been accepted.

Description of the remediation

TCG activated unlocked range vulnerability

The DEKs for locked ranges and DEKs used for unlocked ranges were previously encrypted by a shared intermediate key (the PIN_KEK). This key was encrypted with an empty password to create the $\text{PIN\_KEK}_{\text{ANON}}$. This old key hierarchy is shown in Figure 1.

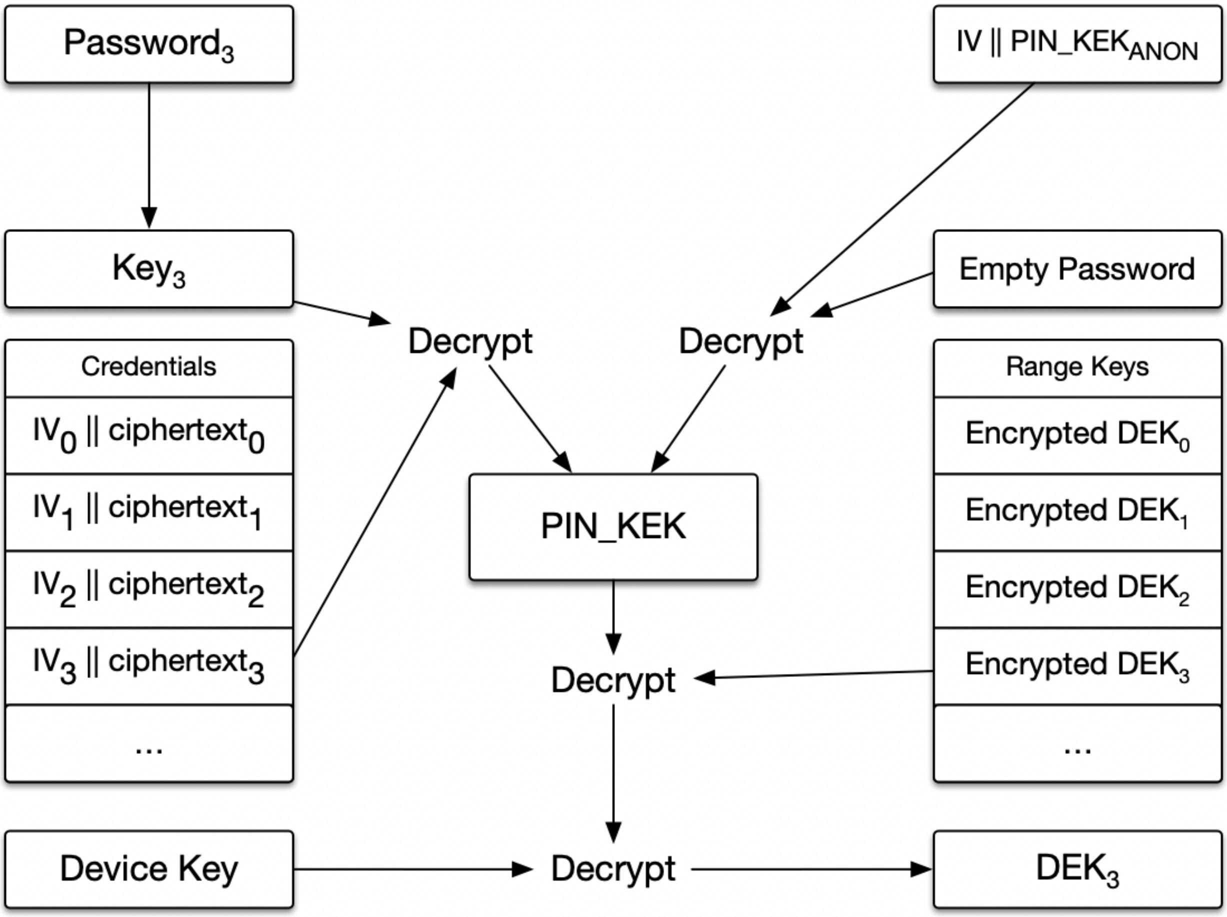

Figure 1: X600 SED (Simplified) Key Hierarchy

To fix this issue the binding between the PIN_KEK and the DEKs was removed for any ranges which do not have both read and write locking enabled. With this link removed, the $\text{PIN\_KEK}_{\text{ANON}}$ has no further utility and has been removed as well. The new hierarchy can be visualized in Figure 2.

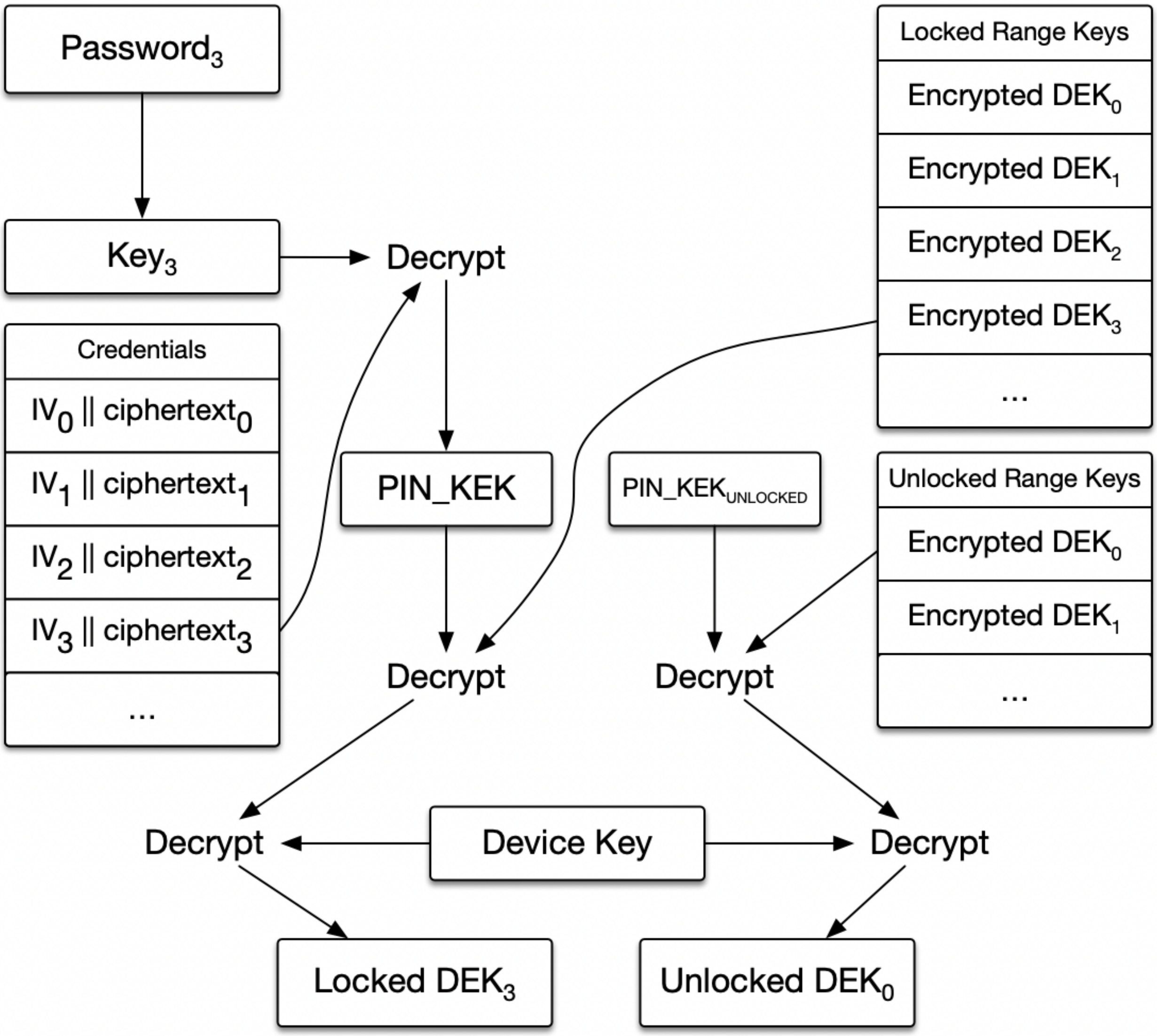

Figure 2: (Simplified) New Key Hierarchy

These changes prevent the decryption of the locked range DEKs without knowledge of any credential, ensuring a cryptographic binding between users' passwords and the decryption key. All ranges are still bound to other intermediate keys so features such as secure erasure during RMA for failure analysis remain available.

TCG to ATA cross mode vulnerability

Both TCG activated and ATA security mode originally used the same raw PIN_KEK. When switching from TCG to ATA mode this link, combined with the PIN_KEK$_{ANON}$ value that was not cleared, allowed an attacker to decrypt the intermediate key and gain access to the encrypted drive without the user password.

This has been modified to generate separate raw PIN_KEKs for each mode. This change, along with the TCG activated key hierarchy changes detailed below, resolves the design issue.

ATA Maximum capability mode Master password issue

Previously, the Master password PIN_KEK was not cleared when switching to Maximum capability mode.

To prevent unauthorized decryption of the drive using the Master password in ATA security's Maximum capability mode, the $\text{PIN\_KEK}_{\text{MASTER}}$ is now encrypted using a SHA256 hash of the user password as the key, stored in the $\text{PIN\_KEK}_{\text{ANON}}$ slot, and then $\text{PIN\_KEK}_{\text{MASTER}}$ is zeroed. This prevents decryption of the drive using the Master password, but allows restoration of that decryption capability when switching from Maximum capability back to High capability mode.

Actions taken to validate the fix

Trail of Bits reviewed the architectural documentation (including the original and revised design) and the firmware source code itself to validate that the problems enumerated above have been fully remediated.

TCG activated unlocked range vulnerability

The vulnerability in TCG activated mode was due to the binding between the PIN_KEK$_{ANON}$ and DEKs. The proposed fix removes the requirement for a PIN_KEK$_{ANON}$, so it should be impossible to recover PIN_KEK without a correct user password. This binding removal occurs on existing deployed drives when the firmware is upgraded without requiring a reformat.

During SATA initialization a function to modify the key hierarchy is invoked. Trail of Bits confirmed that the implementation of the key hierarchy modification matches the design in this call chain.

During our review we found that the PIN_KEK$_{ANON}$ is still generated at device manufacturing time. This makes the code path consistent for both new device setup and firmware upgrade (where existing devices already have PIN_KEK$_{ANON}$ and need to be migrated to the new KEK model without reformatting). However, the generated key is removed as part of a code path is executed at the factory before any drives are shipped so new drives will not have PIN_KEK$_{ANON}$.

Limitations of PIN_KEK$_{ANON}$ remediation

The PIN_KEK$_{ANON}$ remediation prevents decryption of arbitrary locked ranges without a password, but it does not attempt to address the case of multiple locked ranges with different passwords. Consider the following scenario: a drive has three locked ranges encrypted under three different passwords. The specification calls for each of those ranges to be readable/writeable only when the corresponding password is provided. However, in the updated design the DEK for a given range is encrypted under a KEK shared by all locked ranges. This is, in turn, encrypted under the various user passwords. Therefore, an attacker with knowledge of one password can decrypt the KEK and then use that KEK to decrypt the DEK for a range other than the one that corresponds to the password they provided.

TCG to ATA cross mode vulnerability

The fix was implemented in the primary function responsible for handling the mode switch. Trail of Bits confirmed that the function generates a new ATA KEK and clears out the old

$\text{PIN\_KEK}_{\text{ANON}}$. Any invocation of a switch between TCG and ATA security will invoke this code and thus zero the KEK.

ATA Maximum capability mode Master password issue

To confirm that this issue was remediated, Trail of Bits examined the code looking for mode switch logic and explored the storage of the $\text{PIN\_KEK}_{\text{MASTER}}$ when switching between Maximum capability and High capability modes. When switching into Maximum capability mode the switching logic saves the $\text{PIN\_KEK}_{\text{MASTER}}$, encrypted using a key derived from the user password, to the $\text{PIN\_KEK}_{\text{ANON}}$ slot and zeroes the $\text{PIN\_KEK}_{\text{MASTER}}$ slot. This wrapping step occurs so that the Master password decryption capability can be restored when switching from Maximum capability to High capability.

These changes correctly prevent the Master password from being used to decrypt the drive when in Maximum capability mode, but allow it to be restored without resetting the Master password when switching from Maximum capability back to High capability.

Recommendations

Five informational issues relating to code quality and one low severity issue with the implementation were discovered during review of the X600 SED documentation and firmware source code. They have been reported to Western Digital so that they can improve the code and documentation quality of their product. The low severity issue is listed below.

1. Transforming password to AES key is done with SHA256

Severity: Low

Description
When switching from High capability to Maximum capability mode in ATA security the firmware needs to encrypt the Master password. This wrapped key can be decrypted and restored if the drive is switched from Maximum capability back to High capability mode. The current drive firmware uses a single round of SHA256 to derive a key from the user password. If an attacker gains access to a drive and extracts this wrapped key they can rapidly test candidate user passwords as the per key derivation cost is very low.

Recommendation
Key derivation from a user password should be performed by a password-based key derivation function (KDF). Scrypt or Argon2id are recommended, but PBKDF2 may be used as long as the number of iterations is as high as feasible.

About Trail of Bits

Since 2012, Trail of Bits has helped secure some of the world's most targeted organizations and devices. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code.

Our clientele - ranging from Facebook to DARPA - lead their industries. Their dedicated security teams come to us for our foundational tools and deep expertise in reverse engineering, cryptography, virtualization, malware behavior and software exploits. We help them assess their products or networks, and determine the modifications necessary for a secure deployment. We're especially well suited for the technology, finance and defense industries.

After solving the problem at hand, we continue to refine our work in service to the deeper issues. The knowledge we gain from each engagement and research project further hones our tools and processes, helping us extend software engineers' abilities. We believe the most meaningful security gains hide at the intersection of human intellect and computational power.