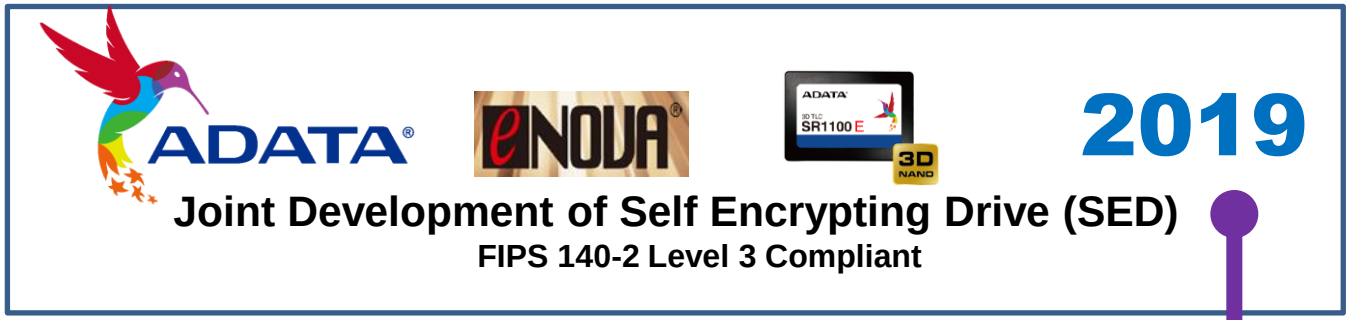
The Ending of Opal2.0 and SED SSD?

Robert Wann
President & CEO
Enova Technology Corp.
rwann@enovatech.com
www.enovatech.com

Shing Lee
Technical Director
ADATA Technology Co., Ltd.
shing_lee@adata.com
www.adata.com

Milestones of ADATA Technology



2001
Founded

2007
Start
SSD Business & Development

2012
No.1
SSD Market Share in Japan

2014
No.2
Global DRAM Module Maker

2016
No.4
Global SSD Market Share

2017
No.2
Global SSD Module Maker

2018
ADATA / JEDEC NGSFF SSD for Enterprise & Data Center

OPAL2.0 SED vs. Native SED

- OPAL2.0 SED
  - Based on Full Disk Encryption on the Global Range with self-generated Key(s)
  - Managed by Trust Commands (0x5B – 0x5F) & OPAL2.0 protocol
  - Encryption executed by drive's AES block or an external in-line crypto module
  - ATA Security Commands & OPAL2.0 protocol are mutually exclusive
  - Authentication managed by BitLocker, SecureDoc, Embassy Suite
- Native SED
  - Does not associate with any Trust Commands or OPAL2.0 protocol
  - Based on full disk encryption starting from LBA0
  - Supports various authentication protocols including ATA Security Commands
  - Encryption executed by drive's AES block or an external in-line crypto module

Authentication Methods: OPAL2.0, ATA Security Commands or FIPS Cert.?

Radboud University Advisory on SSD: CVE-2018-12037 & 12038

- No cryptographic binding between User's PIN & Encryption Key
  - OPAL2.0 self-generated Key(s) associated with respective LBA ranges.
  - User's PINs under LockingSP to lock/unlock the specific encrypted LBA range.
  - Lack of crypto binding under OPAL2.0 isn't necessarily vulnerable if both the drive firmware and Templates/Tables are encrypted.
- Reverse engineering of drive firmware
  - How to prevent that practice? An encrypted form of firmware, write protected memory space with a MAC, HMAC with a shared key, or RSA, ECC DSA?
  - Should OPAL Core Specification be included?
- Hot-plug attack – attacker removed the authenticated drive while maintained its power
- Using standard ATA Security Commands

Radboud University Advisory on SSD: CVE-2018-12037 & 12038

- Drive firmware reverse engineering is the primary cause
- Weakness in using ATA security commands
- Consider how the key(s) life cycle should be managed
  - Enhance the quality of the RNG and entropy for internally generated key(s);
  - Create a crypto binding to the generated key(s); or
  - Externally seeded in ciphertext so customers would have a complete visibility over key management
- Is cleartext user's PIN the only solution that can be deployed?
- Is OPAL2.0 SED the only solution?

Mitigations

- Secure your firmware & create a secure pathway for firmware update are critical; IoT devices may follow the same suit.
- Adopt FIPS 140-2 cert. RSA2048, DSA, ECDSA, CMAC and/or HMAC to authenticate both host and storage device.
- Choose FIPS 140-2 certified single chip crypto module to replace drive controllers' crypto functions as most of those were made without security in mind;
- Enhance OPAL2.0 with encrypted templates/tables.
- Avoid using standard ATA security commands.

Radboud University Advisory on SSD: A Brief Summary

"Hardware encryption has, at best, security guarantees similar to those of software encryption. However, in practice, they often fall short. Users should not rely solely on hardware encryption offered by SSDs for data confidentiality. As such, we recommend hardware encryption users to employ also a software full-disk encryption solution, preferably an open-source and audited one."

Do you agree?


ADATA
Flash Memory Summit
ADATA
INDUSTRIAL
Innovating the Future
VISIT US AT #714
AUGUST 6-8, 2019 | SANTA CLARA CONVENTION CENTER, CA, U.S.A.
ADATA
2.5 Inch SED SSD
SR1100E
128GB、256GB、512GB
ADATA
SR1100E
3D NAND
FIPS VALIDATED 140-2
eNOVA
FIPS 140-2 Level 3
& Level 2 Certified
X-Wall MX+

Thank You!

Questions & Follow-up:

Robert Wann
rwann@enovatech.com
www.enovatech.com

Shing Lee
shing_lee@adata.com
www.adata.com