The Use Of Encryption For Sanitization: A Case Study

Robin England
Research & Development Team Lead
Why Sanitize?

- **Protect Sensitive Data**
  - Government, Military secrets, Corporate IP, Client database

- **Avoid Data Breach**
  - Medical records / social security numbers / financial records

- **Citizens’ Right To Be Forgotten**
  - Social media posts, chat-rooms, photos

- **General Data Protection Regulation (GDPR)**
  - Know exactly where specific data is located
  - ..and be able to securely and **demonstrably** eradicate all copies of that data on demand
Sanitization (NIST Purge) & Erasure Verification

- **NIST 800-88 r1**
  - Replaced DoD standard
  - Defines 3 sanitization levels: Clear, **Purge**, Destroy
- **Purge:**
  - Hinder subsequent attempts to recover purged data
  - Be media-agnostic
  - Allow re-use of the media

- **Erasure Verification:**
  - Can any purged user data be recovered – even at the deepest “bit-level” of the physical media?

Includes reading ALL blocks, processing the physical data against controller-specific elements (e.g. ECC, XOR, bit / byte-striping) and searching for test byte patterns.
Purge Sanitization Methods (closed-source 3rd party SSD design)

Flash Block Erase – all NAND cells programmed to set level
- Not optimal for Flash -
  - drives which store firmware metadata
  - Some areas of NAND may not be completely erased (e.g. if defective)
  - Can only be done by controller (we do not have direct access to Flash)

CryptoErase – utilizes hardware encryption (shred DEK (Data Encryption Key))
- Thorough, includes hidden, active and blocks marked “bad”, defective blocks
- Very fast – no need to update every NAND block
- Can be done both outside and inside the drive..

Q: What are the potential drawbacks of using SSD hardware encryption inside the drive alone?
Typical Hardware Encryption Implementation (closed-source 3rd party SSD design)

- Encryption may get switched off or fails
- Not possible to CryptoErase individual files
- Exposed encryption key
- Weak key
- Non-encrypting drive deployed in error
- Key NOT changed by CryptoErase

Physical NAND Flash Memory

Solid-State (NAND Flash) Drive

UNENCRYPTED DATA PATH

ENCRYPTED DATA PATH

CONTROLLER

Crypto-engine and Key
Case Study – Fabric-Attached Storage (FAS) ONTAP Secure-Purge

**ONTAP Secure-Purge function:-**

- Meets 800-88 r1 purge sanitization guidelines
- Non-disruptive
- Ensures that “scrubbed” deleted data will not be recoverable at physical level
- Allows scrubbing of individual deleted files
- Remediates data “spillage” / data contamination
- Utilizes cryptographic erase
  - Encryption managed outside the drive and optionally enabled inside FIPS-140 certified encrypting drive hardware
  - Key-management and block-level encryption
Case Study - NetApp FAS ONTAP Secure-Purge

- Scenario:-
  - Need to selectively delete and purge a specific data set / file from an encrypted volume on a Flash array…

- ONTAP Secure Purge overview:-
  1. Delete the target data / set file from volume encrypted with DEK 1
  2. Create a new encrypted volume with new encryption DEK 2
  3. Copy only blocks belonging to active files / data sets to new volume
  4. Destroy DEK 1
Case Study - NetApp FAS ONTAP Secure-Purge

Challenges

- Scrub Selected Data
- Modify Existing Ontrack WAFL Tools
- Apply Encryption Keys To Data Blocks
- Ensure Compliance with NIST.SP.800-88r1
- Create Test Data Sets
- Search For Scrubbed Data In All Regions of Media
- Validate Integrity Of Active Data
- Encryption Key Verification

Flash Memory Summit 2019
Santa Clara, CA
Conclusions

- Use of 3rd party closed-source SSD hardware encryption carries with it some risks - external encryption is better

- NetApp’s secure-purge process had wiped the encryption key from the system and the scrubbed data was not recoverable

- The data sanitization process used was effective; NetApp’s software was functioning properly, and Ontrack was able to verify the results independently

- The Secure-Purge function meets the needs of those who require secure non-disruptive deletion of individual files
Thank You!

Please visit us at booth #126