Sanitization: Product Requirements and Legal Requirements

Paul Suhler

Principal Engineer, SSD Standards, KIOXIA

Chair, IEEE Security in Storage Working Group

Abstract

Operators of data storage systems are legally obligated to protect customer data and can be subject to significant penalties for data breaches. This presentation will explore existing and upcoming standards to show the best practices for sanitizing customer data.

Legal Environment

- US Federal Trade Commission (FTC) has jurisdiction over data breaches.
- US Health Insurance Portability and Accountability Act of 1996 (HIPAA) has civil penalties (up to $50k) and criminal penalties.
- Most or all US states have data protection laws.
- EU General Data Protection Regulation (GDPR) applies to personal data of EU citizens, regardless of the location of the organization holding the data.
  - Largest fine: €746 million (Amazon, 2021)
- Other nations also have data protection laws.
- Liability may exist in perpetuity.

- This list is not exhaustive. Consult your attorney for the latest regulations.

Avoiding Data Breaches

- Organizations must ensure that user data does not escape their control.
- Data breach: User data is accessible to an unauthorized entity.
  - Device stolen or disposed of without removing user data.
  - Attacker who has gained entry to the organization's system.
  - An authorized user of the system who accesses another user's data.
- Customers must establish policies and ensure that devices they purchase comply.
  - Devices must be sanitized before leaving the owner's control.
  - This includes transporting, repurposing, discarding devices.
  - Sanitization must be documented.

Sanitization: One Tool for Data Protection

- Sanitization: Eradication of all user data from a storage device.
- Recovery of user data must be infeasible.
  - Different methods of sanitization are resistant to different levels of attacks See next slide.
- Devices implement commands to sanitize user data.
- Media such as tape cartridges may require degaussing.

Sanitization Methods

- Different methods provide different levels of protection.

- **Clear**: Device remains usable, and user data cannot be read from the device.
- **Purge**: Device remains usable, but user data cannot be recovered from media – even if the device were to be disassembled and the media read at a low level (“advanced laboratory techniques”).
- **Destruct**: Device is destroyed and data cannot be recovered from the remains of the media.

- Source: IEEE Std 2883™–2022.

Verifying Results of Sanitization

- Verification: Read device to ensure that user data does not remain.
- Block Erase and Crypto Erase can leave media error correction codes invalid.
- Read commands will fail (“media error”) until new data is written.
- Workarounds:
  - NVM Express devices have a mechanism to read media and return data without reporting errors.
  - Devices perform “additional media modification” to make media readable. Slow process.
- Verification cannot check deallocated media.

Customer Concerns with Sanitization

- Is the storage device sanitization firmware buggy?
- Has an attacker compromised the firmware?
- Are there bugs in the software tool that issues the sanitization command?
- Did the technician correctly use the software tool?

- Without confidence in the entire process, the customer may decide to destroy the device, rather than risk a breach.

Thank you!

the Future of Memory and Storage