STORAGE DEVELOPER CONFERENCE
SDC 21
BY Developers FOR Developers

Virtual Conference
September 28-29, 2021

A SNIA Event

Sanitization

Forensic-proofing Your Data Deletion

Presented by:

Eric A. Hibbard, CISSP, CIPP/US, CISA

Director, Product Planning – Storage Networking & Security, Samsung Semiconductor, Inc.

About the Speaker

Eric Hibbard
CISSP-ISSAP, ISSMP, ISSEP, CIPP/US, CIPT, CDPSE, CISA, CCSK

eric.hibbard@samsung.com

Chair, SNIA Security Technical Work Group
Chair, INCITS TC Cybersecurity and Privacy
Chair, IEEE Computer Society, Cybersecurity & Privacy Standards Committee (CPSC)
Co-Chair, Cloud Security Alliance (CSA) – International Standardization Council (ISC)
Member, American Bar Association – Science & Technology (SciTech) Law Council
Member, American Bar Association – Cybersecurity Legal Task Force
Co-Chair, American Bar Association – SciTech Law – Internet of Things (IoT) Committee
ISO Editor: ISO/IEC 27040, ISO/IEC 27050 (multi-part), ISO/IEC 17788, ISO/IEC 22123 (multi-part), ISO/IEC 20648
IEEE Editor: IEEE Std 1619 (XTS-AES)

Abstract

This session outlines the various forms of sanitization and methods used (e.g., clear, purge, and destruct).

Details are provided on representative storage to help explore what needs to be done, what can go wrong, and identify additional measures that may be needed to protect an organization.

Information is provided on the state of sanitization standards and practices.

Overview

Data Lifecycle Management (DLM)

Data destruction/disposal is typically the last phase of DLM.

Necessary to avoid data breaches and to meet compliance obligations.

Destroying Data

- Data destruction is non-trivial:
  - All copies must be located (e.g., backups, images of files, temp copies)
  - Data storage technologies are designed to guard against data loss
  - There may be specific compliance obligations (e.g., record keeping)
  - Advanced forensic tools exist to recover data

- The method of “destroying” data is normally selected based on the:
  - underlying sensitivity of the data being destroyed, or
  - potential harm they could cause if they are recovered or inadvertently disclosed.

Confusing Language

- Data deletion
- Secure data deletion
- Data shredding
- Data wiping
- Data overwriting
- Data erasure
- Data clearing
- Data destruction
- Data sanitization

NOTE: Most of these are poorly and inconsistently defined and/or do not ensure the elimination of data.

Sanitization Defined

- Sanitization: process or method to render access to target data on storage infeasible for a given level of effort

- Wherefores and Provisos:
  - Access can mean the data no longer exists, the storage devices/media no longer exist, or there is something that permanently prevents access to the data
  - Target data refers to data stored and can also include metadata associated with the data
  - Infeasible for a given level of effort can mean computationally infeasible or the level of effort makes it near impossible or too complicated to be done; this language acknowledges that adjustments may be needed in the future

Forensic Data Recovery

- Application aware (email, chat, etc.)
- Finding and retrieving lost or deleted files
- Metadata review and extraction
- Easily recover digital pieces of data/evidence from sources like cloud services, smartphones, IoT devices, computers, etc.
- Capture the contents of RAM and make on-screen acquisitions

- Correct sanitization should render these tools useless

Forms of Sanitization

- ***Data sanitization:*** focused on all instances of stored data, wherever the data resides. Aligned with DLM Destroy.

- ***Storage sanitization:*** focused on data stored on ICT infrastructure that uses non-volatile storage
  - ***Logical sanitization:*** focused on data stored on logical/virtual storage
  - ***Media sanitization:*** focused on data stored on storage devices or storage media

Common Aspect of Storage Sanitization

- Identification of the form of storage involved: logical/virtual storage or media-aligned (media sanitization)
- Selecting the sanitization method that is appropriate for the type of storage and the data sensitivity
- Executing one or more of the selected storage sanitization techniques
- Verifying the results of the storage sanitization to determine the level of residual risk
- Producing evidence of the storage sanitization action that has been taken to meets compliance obligations (proof of sanitization)

Storage Sanitization

Background

- Current published standards:
  - ISO/IEC 27040:2015, *Information technology—Security techniques—Storage security*
  - NIST SP 800-88 Revision 1, *Media Sanitization*

- Draft standards:
  - Draft IEEE Std 2883, *Standard for Sanitizing Storage*
  - ISO/IEC WD 27040.3 (2nd Ed.), *Information technology—Security techniques—Storage security*

Storage Sanitization Methods

- **Clear**: sanitize using *logical techniques* on user data on all addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user
- **Purge**: sanitize using *logical techniques or physical techniques* that make recovery of target data infeasible using state of the art laboratory techniques, but which preserves the storage media and the storage device in a potentially reusable state
- **Destruct**: sanitize using *physical techniques* that make recovery of target data infeasible using state of the art laboratory techniques and results in the subsequent inability to use the storage

Clear Sanitization Method

- Applicable to both logical storage and media-based storage
- Clear forms:
  - Overwriting all addressable locations; it is not applicable to storage media that do not permit data to be erased or changed after data are written
  - Security erase unit, format unit, block erase, overwrite data erase, etc. commands

Purge Sanitization Method

- Applicable to both logical storage and media-based storage
- Purge forms:
  - Cryptographic erase, sanitize block erase, sanitize overwrite, etc. commands
  - Media-based Cryptographic erase
  - Degauss* magnetic storage media

* Degaussing of HDD storage devices generally results in rendering the storage device permanently inoperable (i.e., not purge).

Degauss

- Renders magnetically stored data unreadable by applying a strong magnetic field to the storage media with an organizationally approved field strength
- Degaussing applies to some magnetic storage media. It is not applicable to storage devices that contain non-magnetic storage media (e.g., paper, SSD, or the non-magnetic components in an SSHD).
- Degaussing may be useable as a Destruct sanitization method if the field strength is sufficient to remove manufactured features, (e.g., servo tracks), that are required to access the media and the device is incapable to replacing those manufactured features.

Cryptographic Erase

- Purge sanitization method in which the encryption key for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible
- Without the encryption key used to encrypt the target data, the data are unrecoverable
- ISO/IEC 27040 pre-conditions for cryptographic erase:
  - encryption of all data intended for cryptographic erase prior to recording on the storage;
  - the strength of the cryptographic algorithm (including mode of operation) used to encrypt the target data is at least 128 bits;
  - the level of entropy of the encryption key used to encrypt the target data is at least 128 bits; and
  - all copies of the encryption keys used to encrypt the target data are sanitized; if the target data's encryption keys are, themselves, encrypted with one or more wrapping keys, it is acceptable to perform cryptographic erase by sanitizing a corresponding wrapping key.

Cryptographic Erase (cont.)

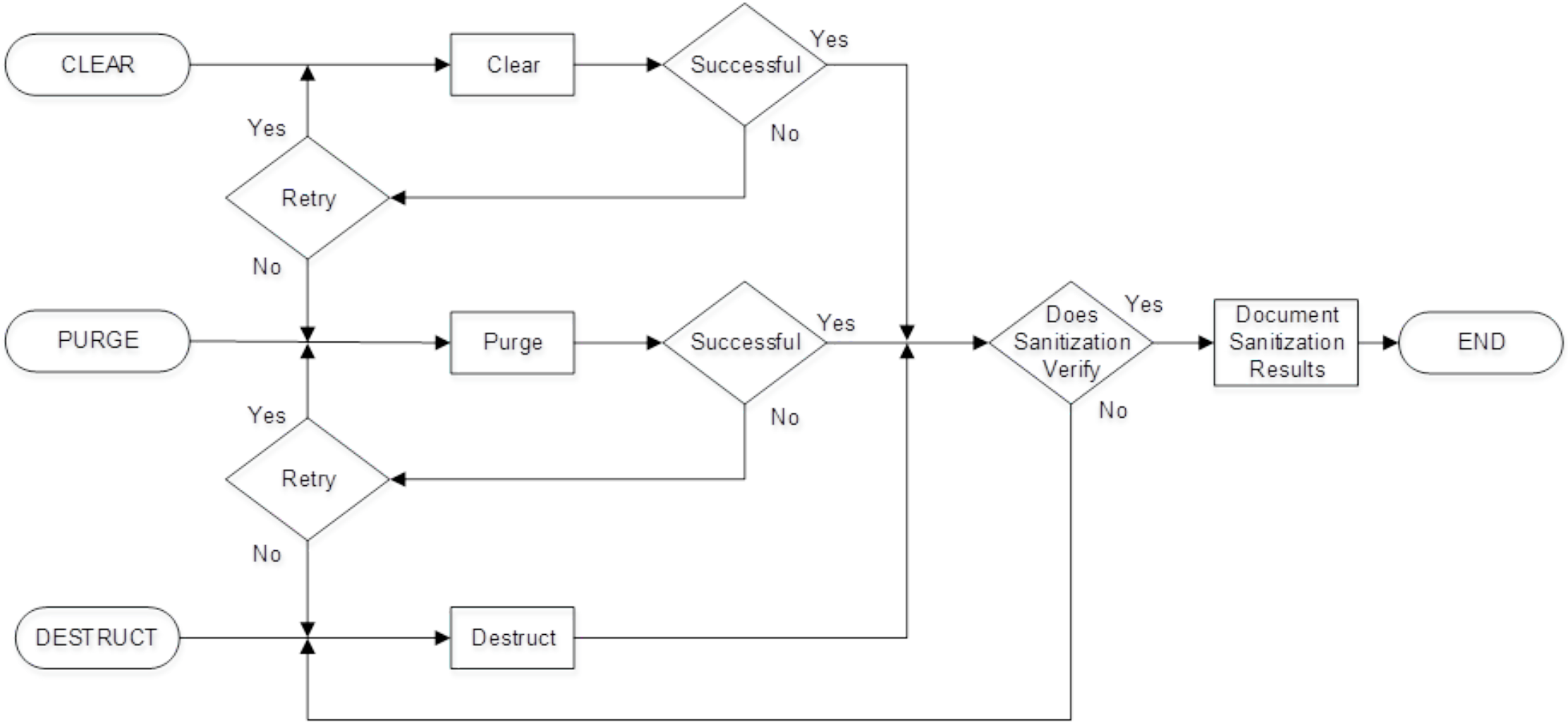
- The level of effort needed to decrypt this data without the encryption key is the lesser of:
  - the strength of the cryptographic algorithm used to encrypt the data (including mode of operation);
  - the level of entropy of the target data's encryption.
- Sanitization may be performed with high assurance much faster than with other sanitization techniques. Cryptographic erase can be executed in seconds.
- Cryptographic erase can also be used as a supplement or in addition to other sanitization approaches.
- Some organizations perform an additional, but unneeded, sanitization using a clear method to reduce the attack surface by preventing access to the ciphertext.

Destruct Sanitization Method

- Applicable to media-based storage; not logical storage
- Destruct forms:
  - Disintegrate - destruct by separating storage medium into its component parts
  - Incinerate - destruct by burning storage medium completely
  - Melt - destruct by changing storage medium from a solid to a liquid state generally by the application of heat
  - Pulverize* - destruct by grinding storage medium to a powder or appropriately small particles
  - Shred* - destruct by cutting or tearing storage medium into small particles
- If the storage media cannot be removed, then the storage device can be subjected to the destruct technique; a storage device can contain multiple storage media.

* IEEE 2883 has identified this form of destruct as “obsolete”

Selection of Sanitization Method



Verification

- Verification of the sanitization outcomes can be an important element of a data sanitization program when a determination as to the adequacy or effectiveness of the storage sanitization is required.
- Verification differs depending on the sanitization method
  - For clear or purge, verification that a command was performed
  - For destruct, physical inspection is used to check the sanitization outcomes
- Full verification is typically recommended for clear or purge, but representative sampling may be adequate

Record Keeping

- Organizations should maintain a record of sanitization activities
  - document what storage media were sanitized
  - when and how they were sanitized
  - the final disposition of the storage media
- Proof of sanitization takes on at least two forms:
  - an audit log trail
  - a certificate of sanitization
- ISO/IEC 27040 identifies specific information that should be recorded

Factors Affecting the Ability to Sanitize

- The storage media is not identifiable.
  - For example, tape cartridges are usually are labeled with the technology and generation, but some may not be labeled.
- The organization lacks the expertise to sanitize the storage media (while leaving it usable) or to verify that sanitization was successful.
- The equipment is not working or is anticipated to not be working soon.
- The equipment or software needed to perform the operations is not available.
  - Examples include a storage device to access removable storage media, an interface for the storage device, a degausser with sufficient strength to erase newer magnetic storage media, etc.

Summary

Emerging Standards

- ISO/IEC 27040 (2nd Ed.)
  - Requires sanitization of storage prior to disposal when sensitive data were recorded on the storage
  - Requires verification of sanitization outcomes
  - Recommends proof of sanitization
- IEEE Std. 2883
  - Provides guidance and requirements for media sanitization
  - Identifies acceptable sanitization techniques for each method for various type of storage devices/media

Final Thoughts

- Sanitizing storage before disposal or repurposing ICT systems
  - Considered reasonable security
  - May be obligated under a legal, statute, or regulatory requirement
- When used correctly, cryptographic erase is a powerful tool, but there are limitations
- Some organizations only use destruct to simplify their sanitization programs
- Eco-friendly sanitization should be considered
- Adequate records may be necessary to avoid data breach protocols

Thank you for Your Time!

Please take a moment to rate this session.

Your feedback is important to us.

