Non-Physical Data Destruction for Enterprise Storage

Leader: Ke Du, Marvell

Listen to the webinar recording:
https://inemi.webex.com/inemi/lsr.php?RCID=9698c7464d6f44c8b2c5f16a06144a18

Call for Participation
May 18, 2020
• The life of HDDs/SSDs is about 3-5 years. Eventually all storage devices need to be decommissioned at end of life cycle.

• A common method today is physical destruction, to mitigate risk of access to the information on the storage media. Unfortunately, this renders limited value recovery from the hardware, and is also an incremental operational expense.

• The iNEMI Project on Value Recovery from Hard Disk Drives successfully explored and demonstrated techniques to drastically improve the value recovery of end of life HDDs with specific focus on the economic and technical feasibility.
Genesis for this Project

If we could mitigate the need for physical destruction, **value recovery** would increase even more, and **EOL operating expense would decrease**.

However, the need for data security sanitization for these devices is a priority which has promoted shredding and other physical destruction techniques that minimize or eliminate the ability to recover whole devices, key components and, sometimes, even basic material recovery.

This project aims to more comprehensively understand the factors driving physical data destruction and data sanitization while exploring the non-physical data destruction technologies that are available along with their ability to provide the required data sanitization needed to enable more value recovery.
Value Recovery from Used Electronics, Phase 2 (2018 – 2019)

• Demonstrated value recovery pathways necessary for an HDD circular economy

• Developed decision-making tools for data wiping, life cycle analysis and logistics assessments, economic return on HDD resale, systems dynamics models for HDD stocks and flows for large-volume users of HDDs necessary to assess the sustainability of specific pathways

• Identify barriers to reuse and develop a strategy to remove them
Problem Statement

• Need to address the technology gaps identified from Value Recovery Phase 2 Project
  • The current data wiping technology needs further improvement to assure data privacy
  • Unable to electronically wipe data from failed devices (data is still on the media)
  • Minimize e-waste from data centers
Data Sanitization Standard - NIST

- Data Sanitization is a process to render access to target data on the media infeasible for a given level of recovery effort.
- NIST Special Publication 800-88R1 is widely used guideline for the data sanitization.
  - It defined three level of data erasure: Destroy, Purge and Clear where destroy is the highest level of data sanitization.
  - Destroy is an option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media.

<table>
<thead>
<tr>
<th>Erasure</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear</td>
<td>Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques.</td>
<td>Overwrite. Or resetting the device to factory state if rewriting is not supported.</td>
</tr>
<tr>
<td>Purge</td>
<td>Applies physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques.</td>
<td>Overwrite, block erase, and Cryptographic Erase, using dedicated, standardized device sanitize commands that bypass the typical read/write commands.</td>
</tr>
<tr>
<td>Destroy</td>
<td>Target data retrieval is infeasible using state of the art laboratory techniques. The media cannot be reused as originally intended.</td>
<td>Disintegrate, Pulverize, Melt, and Incinerate, Shred.</td>
</tr>
</tbody>
</table>
The overwrite, block erase methods have inherent issues such as implementation difficulties and operation efficiency. The existing Cryptographic Erase (CE) is promising if implemented correctly. All these methods require working devices. However, the decommission process also needs to deal with drives that have failed.

When using CE with current Self Encryption Drive (SEDs), NIST800-88R1 requires that all encryptions keys, including the wrapping keys, be sanitized. These keys cannot be erased if a device fails. This means the device (media) needs to be physically shredded (SSD/HDD) or degaussed (HDD) if devices fail at decommission.

The physical destruction of the SSD has additional concern since the die size can be very small. The shredding may not be effective or difficult to verify.
New methodologies, such as new Cryptographic Erase (CE) technology in Self Encryption Drive (SED) are emerging to make the data sanitization process automatic and effective, regardless of device working conditions. A new CE, for example, has the following benefits when used in enterprise data applications:

- Meets NIST800-88R1 data sanitization standards up to purge level sanitization requirement
- Automatic data sanitization (decommission, repurpose, disposal, etc.)
- Simple implementation in SED design, and can be as extension of Trusted Computing Group (TCG) standard
- Effective regardless of devices working conditions (functional or non-functional)
- Effective for HDDs (and SSDs)
Scope of Work

For spinning hard drives and solid-state drives used in public and private data centers or data servers, investigate the root cause(s) that are driving physical destruction of these devices and what could be done to move to more non-physical data destruction/erasure that would promote more reuse and cost reduction while still providing the required data security.
Project Goals

• Identify policy, standards, regulations, guidelines and customer requirements that are driving data destruction decisions at data centers

• Understand the risk assessments that are being made, both real and perceived risks, and available mitigation strategies

• Identify and verify “data erasure solutions” that conform to the NIST guidelines for NIST Clear and Purge level sanitization

• Demonstrate feasibility and effectiveness of non-physical destruction, ideally with multiple stakeholders/partners/sites relative to the needs of the data centers
### IS / IS NOT Analysis

<table>
<thead>
<tr>
<th>This Project <strong>IS:</strong></th>
<th>This Project <strong>IS NOT:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Spinning Media HD; Solid State Drives</td>
<td>For use primarily as Consumer, Mobile ICT or Persistent Memory Devices; or other parts of the system that could include persistent data that could be identifiable to a customer on a non-HDD or SSD (such as adapters that might have a cache or system data)</td>
</tr>
<tr>
<td>Non-governmental data (classified or unclassified)</td>
<td>Classified governmental data</td>
</tr>
<tr>
<td>Identification of policy, related standards, regulations, guidelines, customer requirement that are driving data center decisions</td>
<td>Biased towards specific suppliers, geographies, or market segments</td>
</tr>
<tr>
<td>Understanding and addressing the risk assessments that are being made which includes both the Real Risks and Perceived Risks of the data centers</td>
<td>Not physically stealing data devices (though may prevent access if device is stolen)</td>
</tr>
<tr>
<td>Customer responsibility for data erasure</td>
<td>Standards Development</td>
</tr>
<tr>
<td>Creation of case studies with/by data centers and/or other key stakeholders about reuse of drives that have been erased for sale or internal reuse.</td>
<td>Holistic Data Security; Chain of Custody and/or “Bad” internal players</td>
</tr>
<tr>
<td>Identification and verification of data security erasure solutions</td>
<td>Physical Data Destruction (i.e. degaussing, shredding, incinerating, punching etc.)</td>
</tr>
<tr>
<td>Conformance to NIST guidelines (Purge and Clear levels), ISO 27040:2015</td>
<td>Repeat of prior or existing work</td>
</tr>
<tr>
<td>Public and Private Data Centers (And Data Servers)</td>
<td></td>
</tr>
</tbody>
</table>
Task 1 – Identify policy, standards, regulations, guidelines, customer requirement, etc. that are driving data destruction decisions at data centers and what security protocols that data sanitization providers need to meet.

Task 2 – Understand the risk assessments that are being made, including both real and perceived risks and what mitigation strategies are available.

Task 3 – Identify and verify “data erasure solutions” that, at a minimum, conform to the NIST guidelines for Clear and ideally, NIST Purge.

Task 4 – Conduct one or more “pilot” tests that demonstrate feasibility and effectiveness of non-physical destruction, ideally with multiple stakeholders/partners/sites relative to the needs of the data center that could ideally be used to move more storage devices into reuse.

Task 5 – Provide recommendations for improvements to data security requirements (such as NIST guidelines or HIPAA or GDPR requirements etc.) and to improve erasure technologies.
Schedule

• Call for Participation Webinars:
  • Monday, May 18th 11 am – Noon ET
  • Monday, May 18th 9 pm – 10 pm ET

• Initial Sign up ends June 29th

• Project Kickoff Plan
  • Week of July 13th

• Duration (Approximately 12 months)
  • Start in July 2020 and present findings by end of July 2021
Steps for Joining

- Details, including the SOW and Project Statement, can be found on the project website: https://community.inemi.org/non_physical_data_destruct

- iNEMI Members:
  - Download the Project Statement and statement of work from project website
  - sign the Project Statement and return to iNEMI

- Non-members:
  - This is a fast turn project
  - Non-members join for a fee of $7500
  - Request, sign and return the MOU to iNEMI
  - Contact Mark Schaffer, marks@inemi.org for more details and for the MOU