SNIA STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Sanitization or Anti-forensics?

IEEE 2883 and digital forensics

Presented by Richard Austin MS, CISSP-Retired
Raustin@ieee.org

A SNIA Event

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

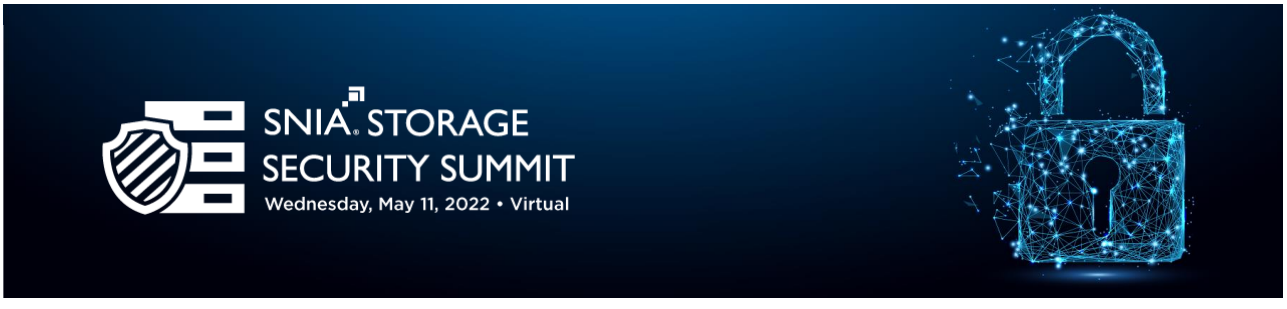
Abstract

Sanitization is a critical process in data life cycle management with the goal of assuring that information is removed from devices prior to their reuse or discard. Sanitization has implications for the practice of digital forensics where the goal is to retrieve all remaining information from storage devices. This session will briefly review sanitization as envisioned in IEEE 2883 and some potential impacts on the practice of digital forensics.

Based on that, the presentation is broken down into two sections:

- Sanitization as a normal part of the data life cycle with the intent of assuring that no unauthorized disclosure of information occurs when storage is repurposed or discarded.
- The potential impacts of sanitization on the practice of digital forensics.

SNIA STORAGE SECURITY SUMMIT



What is sanitization?

And what does IEEE 2883 have to say about it?

We have a problem!

- Our society generates and stores data at a prodigious rate.
- Storage devices are repurposed, sold on the used market, fail or become technologically obsolete.
- How do we make sure that the data on those devices is no longer accessible?

What is sanitization?

- Sanitization is the process we go through when repurposing or discarding storage to assure that its previous contents are removed.
  - Prevents unauthorized disclosure of information.
- Formally, it's defined as "render access to target data infeasible for a given level of effort" (ISO/IEC 27040).
- Sanitization is such an important process that the IEEE Computer Society's Security in Storage Working Group (SISWG) developed a standard, IEEE 2883, to guide organizations in effectively sanitizing storage.

But what is level of effort?

- Level of effort is a rather amorphous term that basically represents how hard an adversary will work to recover the data.
  - $L_e \approx f(V_a, C_a)$ or the level of effort an adversary will apply depends on the value of the data to the adversary and the capability of the adversary.
- Some examples of adversaries and their capabilities:
  - A curious employee with an undelete utility.
  - A competitor with access to commercial forensic tools.
  - A technically sophisticated adversary with access to tools commonly found in a well-equipped university research (or forensic) lab.
  - A well funded nation state intelligence service performing economic espionage.
- Obviously, it's much easier to foil the curious employee than a nation state intelligence service which is why there are different sanitization methods.

Three methods

- The three general sanitization methods are:
  - Clear – sanitize using logical techniques on user data in all user addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user.
    - Non-invasive implies you're not going to disassemble the device to get access to things not visible through the normal host interface.
  - Purge – sanitize using logical or physical techniques that make recovery of target data infeasible using state of the art laboratory techniques, and preserves the storage media and 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 device.
- Clear offers least resistance while purge and destruct offer more.

State of the art laboratory techniques

- A difficult term to define as its open-ended.
  - Basically, it's anything an adversary can come up with to access data on storage.
  - Not restricted to the normal mode of access through the host interface.
    - May include disassembling the device to access internal components.
    - May include replacing the device firmware.
    - …
- The type of thing a group of PhD's and talented engineers might develop when given a healthy budget and lots of equipment.

Clear

- The simplest of sanitization methods.
- The simplest clear technique is to write zeroes (or any other value) to all user addressable locations on a device.
  - Clear only affects user addressable portions of the media
  - Does not affect overprovisioned space, spared blocks, HPA, DCO, etc.
    - This means that even if you write 0's to every block that is addressable through the host interface, there may be data left in these other areas that wasn't touched and a sufficiently adept adversary might be able to retrieve it.
  - Writing to every addressable location does increase wear on SSD's so beware of doing multiple overwrite passes!
    - A single pass of zeroes is usually sufficient.
    - Depending on the drive technology, there are alternatives to overwrite for accomplishing a clear that do not cause wear on the device. See IEEE 2883 for details.

Purge

- Purge methods affect both the user addressable and non user-addressable portions of the device.
- Purge methods make recovery of data infeasible even when using state of the art laboratory techniques.
- Purge methods leave the device in a potentially reusable state.
  - In some cases, there may be additional operations which must be performed before the device can be reused.
- An example of a purge technique is cryptographic erase where all data on the drive is encrypted and the sanitization process is to delete all copies of the encryption keys.

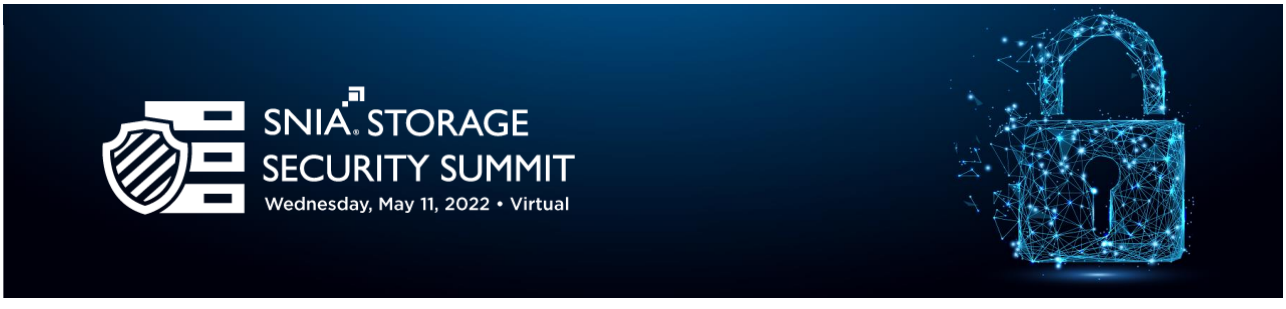
Destruct

- Destruct methods use physical techniques that make recovery of data infeasible using state of the art laboratory techniques *but* render the device unusable.
  - An example of a destruct method would be to physically shred the device.
- Destruct may be the only option in the case of failed devices but more environmentally friendly methods should be used whenever possible.

Choosing a sanitization method

- Choosing a sanitization method is a risk-based decision.
  - In other words, it will depend on:
    - the value of the information;
    - the threat environment the organization faces;
    - the regulatory environment of the organization;
    - the risk tolerance of the organization.
- The process for choosing a sanitization method will usually be formalized in a security policy.

SNIA STORAGE SECURITY SUMMIT

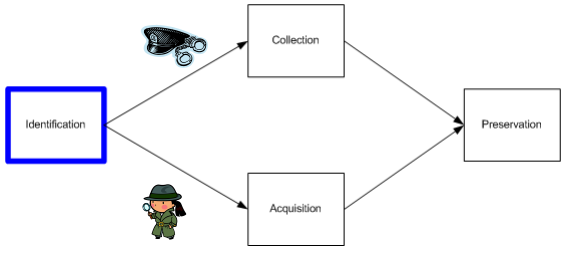


Is 2883 the end of forensics as we know it?

What is digital forensics?

- "Forensics" comes from the Latin *forensis* meaning having to do with courts or public discussion.
- Process for identifying, acquiring, preserving and analyzing data of potential evidentiary value.
  - One important source is data on storage.

What does a digital investigation look like?



Intent of IEEE 2883

- The intent of IEEE 2883 is to guide organizations in effectively sanitizing storage.
  - It provides extensive guidance on the sanitization commands available in the newer storage devices and maps them to the three sanitization methods.
  - Organizations must implement the guidance in 2883 to effectively sanitize storage.
    - Since the publication of NIST 800-88 in 2006, one would have expected most entities, whether individuals or organizations, to use basic sanitization hygiene before selling used equipment to the public.
    - However, continuing studies show that devices are routinely offered for sale with their contents either intact or easily retrievable.
    - The forensic community should continue to be aware that entities' implementation of 2883 may be neither complete nor error free.

Dependency on HW Implementation of Standards

- The sanitization commands recommended in IEEE 2883 are specified in various standards.
  - Devices do not execute standards; they execute implementations of standards.
  - As we've seen before, such implementations are not necessarily complete or error free.
- One would expect the forensics community to investigate the implementations of these commands across manufacturers to assess their adequacy.

Threat Models

- Developers of standards, consciously or unconsciously, use a threat model which represents adversary capabilities and therefore what must be countered.
- Sometimes that threat model might not be truly representative of reality.
- For example, a sanitize command might mark all data blocks as invalid meaning that they cannot be read until they are rewritten.
  - This is effective against attempts to read those blocks through the host interface.
  - However, a well funded, capable adversary might develop a custom storage controller that would ignore the invalid markings and read the blocks anyway.
    - A custom storage controller is an example of a “state of the art laboratory technique”.
    - This possibility was not part of the threat model used.
    - Use of a custom controller is described in https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf
    - More information about such exploits can be found in Ross Anderson’s book “Security Engineering” (now in its 3rd edition).
- Forensic practitioners should evaluate the threat model used by standard developers to identify where the developer might have underestimated their capability.

Not just disks!

- And, of course, digital forensics is not just about data on disks!
- There are many other sources of useful information available:
  - Memory;
  - Network traffic flows or the traffic itself;
  - Various types of logs;
  - Any any other sources of relevant information in an infrastructure.
- These other sources are beyond the purview of 2883.

Not the end

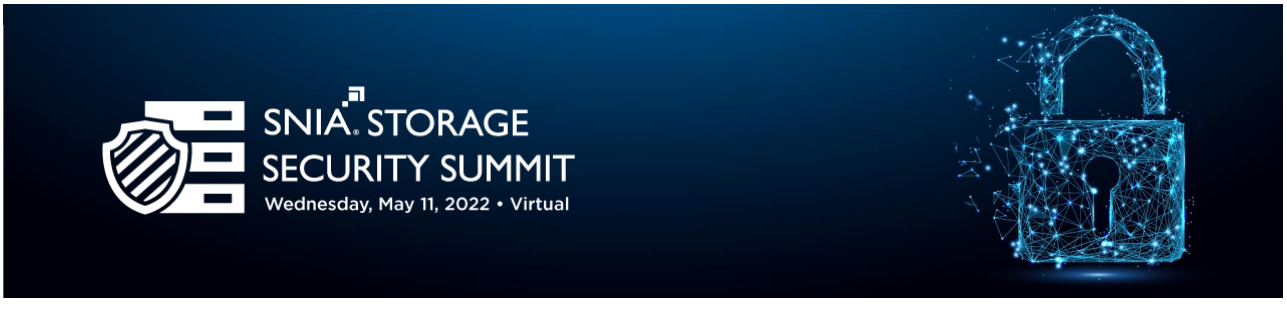
- While it's true that a well implemented sanitization program based on IEEE 2883 should result in less data available to be recovered on sanitized media, I expect digital forensics to continue to be useful for a long time to come.
  - Most implementers of IEEE 2883 will be organizations seeking to reuse storage devices internally or sell them on the used market.
    - Intent is to avoid unauthorized disclosure of information.
  - Entities may face challenges in using the guidance in IEEE 2883 to conceal evidence of their activities.
    - The guidance is not necessarily trivial to implement. For example, issuing some of the device sanitization commands may require booting up under a different operating system which takes time.

Sanitization or Anti-forensics?

- Forensics is about retrieving all the relevant information remaining on a device while sanitization is about removing all information from a device so there is definitely a tension between the two.
- The answer depends on why you use the sanitization.
  - Sanitization is a legitimate process used to prepare media for reuse or discard.
  - Anti-forensics connotes an attempt to conceal evidence of wrongdoing or culpability.

THANKS FOR ATTENDING!!!

SNIA STORAGE SECURITY SUMMIT



Please take a moment to rate this session.

Your feedback is important to us.