Sanitization of Solid State Disks (SSDs)

ICRS Conference
November 13, 2013
Solid State Disk (SSD)
Benefits of SSDs

• Speed – much faster than HDDs
• Low power consumption
• Durability – more shock resistant than HDDs
• Smaller footprint/less weight
SSD market is growing

Growth of tablets and other mobile devices

<table>
<thead>
<tr>
<th>Device Type</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>PC (Desk-Based and Notebook)</td>
<td>341,273</td>
<td>303,100</td>
<td>281,568</td>
</tr>
<tr>
<td>Ultramobile</td>
<td>9,787</td>
<td>18,598</td>
<td>39,896</td>
</tr>
<tr>
<td>Tablet</td>
<td>120,203</td>
<td>184,431</td>
<td>263,229</td>
</tr>
<tr>
<td>Mobile Phone</td>
<td>1,746,177</td>
<td>1,810,304</td>
<td>1,905,030</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2,217,440</strong></td>
<td><strong>2,316,433</strong></td>
<td><strong>2,489,723</strong></td>
</tr>
</tbody>
</table>

Source: Gartner (October 2013)
SSD market is growing

Growing in the PC market (both consumer and enterprise markets)

Source: IHS Inc., April 2013
Reuse/recycling challenges exist

SSDs are now commonplace and present unique resale and retirement challenges because sanitization techniques for HDDs have not been proven effective for SSDs

• NO direct access to disk sectors and
• NOT STANDARDIZED (like HDDs have been), each manufacturer implements proprietary control systems
Reuse/recycling challenges exist

- SSDs are problematic in different ways:
  - Identification
  - Erasure
  - Non-standardization

“Both revolutionary and evolutionary changes make sanitization more difficult”

-NIST SP 800-88 Rev 1
Problem of identification

- Many different types of SSDs on the market
  - SSDs can resemble other computer components
    - SSD vs HDD or Hybrid
    - Can look like an adapter card, memory, etc
  - SSDs can reside in many types of interfaces
    - SATA, mSATA, PCI Express, Mini PCIe, M.2, etc

Copyright 2014
Cascade Asset Management
Sanitization challenges

Effective sanitization requires

• Identification of the storage device media type (Flash/hard disk/hybrid...)

• Applying the appropriate sanitization method for the specific media

• Verification that sanitization was successful
Sanitization challenges

Smart phones/tablets often utilize built-in Unit Erase commands for sanitization, however...

• Support varies among vendors
• Salability requires Operating Systems on devices to remain intact while other data are sanitized
• Models and firmware can change often
• Specialized software is required in some cases
Sanitization challenges

• Software overwriting of PC/laptop SSDs isn’t always successful due to firmware issues
  – Flash translation layer hides data from OS
    • Un-provisioned space
    • Data are copied and moved (and controlled by the drive)
Sanitization challenges

- SSD manufacturers implement firmware differently and it’s sometimes buggy
  - This creates issues for drive erasure as sanitization programs try to utilize firmware commands
  - FAST research paper from researchers at SDSU found that Secure Erase functions were effective in many drives but not all
  - Each model of SSD would need to be evaluated independently to verify effectiveness of sanitization
Sanitization solutions

• Crypto-erase – encrypting the drive and then removing the encryption key
  – Extremely fast
  – Encryption has shown vulnerabilities over time
  – Encryption can be implemented poorly
  – Data remains on the drive although unreadable without key

• Degaussing is ineffective
Sanitization solutions

• Some sanitization software providers are marketing SSD sanitization capabilities
  – Building in capabilities to access un-provisioned areas on at least some models/types of drives
  – Often combining methods of erasure to deal with problems and inconsistencies of firmware/FTL issues
    • Crypto-erase
    • Secure Erase
    • Overwrites (multiple wipes)
Sanitization solutions

- Challenged with verification limitations of crypto-erase and overwriting, sanitization program developers are working to shift the burden of proof:
  - Industry pressure to prove verification at the sector level but it’s very difficult to prove crypto or overwrite success/failure with SSD architecture
  - Sanitization companies are instead giving their solutions to 3rd party forensic testing...“Prove us wrong”
Theory vs. Practicality?

- Research shows data remanence from some SSDs and other flash memory even after Secure Erase has been run.
- Practicality says data recovery is unlikely, especially when data removal tools have been applied (crypto, SE, overwrites).
Destructive solutions

• Destructive solutions are working to meet smaller particle needs
  – Disintegrators/Pulverisers/Media shredders
  – Hard drive crushers with SSD inserts
What we’ve learned...

Verification methods are key to sanitization efficacy – three key verification areas:

• **Verification of sanitization** – investigating devices to ensure target data has been effectively sanitized

• **Verification of personnel** – ensuring operator competency to identify devices and sanitize devices

• **Process verification** – verifying that sanitization processes are effective when applied to different types of SSD devices
What we’ve learned...

• Each device type needs independent evaluation – 3rd party validation should be part of the evaluation process

• Inventory and control of devices throughout the process is important – chain of custody and physical control is essential

• Keeping up with hardware and industry changes is important – use available resources to stay on top of industry changes
Resources

• NAID – National Association of Information Destruction www.naidonline.org
• SDSU Non-Volatile Systems Laboratory nvsl.ucsd.edu
• Storage and Destruction Business Magazine www.sdbmagazine.com
Thank you!

Contact Information:
TJ Barelmann, CSDS – Director of Operations
Cascade Asset Management
tj@cascade-assets.com
608-280-1840
@TJBarelmann
www.linkedin.com/in/tjbarelmann/