Challenges and Designs for Secure Deletion in Storage Systems

Wei-Chen Wang¹, Chien-Chung Ho², Yu-Ming Chang³ and Yuan-Hao Chang⁴

¹ National Taiwan University, Taiwan
² National Chung Cheng University, Taiwan
³ Wolley Inc., Taiwan
⁴ Academia Sinica, Taiwan
• **Introduction of Storage Devices and Secure Deletion**

• **Background and Conventional Secure Deletion Techniques**

• **Advanced Secure Deletion Optimization Techniques**

• **Conclusion**
In recent years, diverse applications (e.g., big data applications) keep generating more data than before.

The tremendous needs on performance and storage capacity:
- Hard disk drive (HDD)
- Solid-state drive (SSD) or NAND flash memory

Size of Global NAND Flash Market, in USD billion

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>32.1</td>
<td>35.5</td>
<td>39.2</td>
<td>42.8</td>
<td>46.8</td>
<td>51.5</td>
<td>56.5</td>
<td>61.8</td>
<td>67.5</td>
<td>73.7</td>
<td>80.3</td>
</tr>
</tbody>
</table>

*Forecast
Why Secure Deletion on Storage Systems?

- Nowadays, data security has risen to be one of the most critical concerns of computer professionals
  - E.g., Sanitize command of NVMe
- To protect sensitive data
  - Bank’s data and accounts
  - Enterprise’s secret data
  - User’s web browsing history
  - Anyone’s temporary files
- More and more enterprise services start to distribute their data on the cloud
  - Cache Sensitive user data on local disks for the purposes of achieving better performance

The idea of “secure deletion” is proposed to meet the needs of completely removing the sensitive data from the storage devices physically
Agenda

• Introduction of Storage Devices and Secure Deletion

• Background and Conventional Secure Deletion Techniques

• Advanced Secure Deletion Optimization Techniques

• Conclusion
Secure Deletion Challenges on HDD

- **CMR technology has run up against the superparamagnetic limit**
  - SMR technology that overlaps the neighboring tracks is proposed to reduce the effective track width without reducing the write head size.

- **CMR HDDs could achieve secure deletion by overwriting all the file content with random data**
  - However, this method **cannot** be directly adopted on SMR HDDs.

- **Conventional magnetic recording (CMR)**

- **Shingled magnetic recording (SMR)**
Secure Deletion Challenges on NAND Flash

- NAND Flash memory is an out-place-update device
  - It may produce **several versions** which are hidden from users

- The **erase operation** is the only way to achieve secure deletion for general NAND flash
  - It may induce **large number of live-page copying and long secure deletion response time**

FTL: Flash translation layer

Delete LBA “0x04f“

Free Block

FTL: Flash translation layer
Main Idea:
- To achieve the secure deletion by sanitizing encryption key

Solution Steps:
- Encrypt each data node with a unique key
- Collect the keys in a (dense) key storage area (KSA)
- Periodically purge KSA to remove deleted keys
Overwriting-based Technique - Scrubbing

Due to the drawbacks for secure deletion in NAND flash, an overwriting-based operation called *scrubbing* is proposed.

**Scrubbing:**
- Works by re-charging the page to turn all the 1s into 0s
- **Advantage:**
  - Per-page secure deletion and efficiency
- **Disadvantages:**
  - The scrubbed page still cannot be used until it is erased
  - It results in scrubbing disturbance and has the possibility of introducing data errors

Table:

<table>
<thead>
<tr>
<th>Page 1</th>
<th>Page 2</th>
<th>Page 3</th>
<th>Page 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page 5</td>
<td>Page 6</td>
<td>Page 7</td>
<td>Page 8</td>
</tr>
<tr>
<td>Page 9</td>
<td>Page 10</td>
<td>Page 11</td>
<td>Page 12</td>
</tr>
<tr>
<td>Page 13</td>
<td>Page 14</td>
<td>Page 15</td>
<td>Page 16</td>
</tr>
</tbody>
</table>

Agenda

• Introduction of Storage Devices and Secure Deletion

• Background and Conventional Secure Deletion Techniques

• Advanced Secure Deletion Optimization Techniques

• Conclusion
ErasuCrypto: A Light-weight Secure Data Deletion Scheme for Solid State Drives

- **Main Idea:**
  - To smartly combine erasure-based and encryption-based approaches

- **Goal:**
  - To minimize the secure deletion cost: \((\# Mgr + k \times \# Era)\)

---

**Typical encryption-based technique**

- **Original blocks:**
  - \(<A1,K1>\), \(<A2,K2>\), \(<A3,K3>\), \(<A4,K4>\), \(<A5,K5>\), \(<A6,K6>\), \(<A7,K7>\), \(<A8,K8>\)

- **Key block:**
  - K1~K8

- **Active blocks:**
  - \(<A3,A7>\), \(<B1,C1>\), \(<B7,C7>\)

---

**ErasuCrypto Technique**

- **Original blocks:**
  - \(<B1,K1>\), \(<B2,K2>\), \(<B3,K3>\), \(<B4,K4>\), \(<B5,K5>\), \(<B6,K6>\), \(<B7,K7>\), \(<B8,K8>\)

- **Key block:**
  - K1~K8

- **Active blocks:**
  - \(<A3,A7>\), \(<C1>\), \(<C2>\), \(<C4>\), \(<B1>\), \(<B2>\), \(<B4>\), \(<B5>\), \(<B6>\), \(<B7>\), \(<B8>\)

---

- **Page states before secure deletion**
  - 1 erasure

- **Page states after cryptography-based secure deletion**
  - 1 erasure + 1 migration
  - 14 migrations
Scrubbing-aware Secure Deletion for 3D NAND Flash

- **Main Idea:**
  - To smartly combine erasure-based and overwriting-based approaches

- **Goal:**
  - To minimize the secure deletion execution time:

\[
ET_{sd} = t_e + N_{vp}^{sd} \times (t_r + t_w)
\]

\[
ET_{scr} = N_{sp} \times t_s \times f\left(\frac{N_{asp}}{2 \times N_{sp}}\right) + N_{vp}^{scr} \times (t_r + t_w).
\]
Achieving Fast Sanitization with Zero Live Data Copy for MLC Flash Memory

Main Idea:
- To achieve an extremely high efficiency *overwriting-based* approach

Approach:
- Exploit the low-overhead *one-shot sanitization*
- Overlap the threshold voltage ($V_t$) windows

Sanitize high page, then low page

Sanitize low page, then high page
Enabling File-Oriented Fast Secure Deletion on Shingled Magnetic Recording Drives

Main Idea:
- To achieve a high efficiency secure deletion technique on SMR HDDs

Motivation:
- To support secure deletion in SMR HDDs, the SMR translation layer (STL) should keep track of every data version for each LBA

Goal:
- To minimize the number of involved SMR zones for each deleted file
Agenda

• Introduction of Storage Devices and Secure Deletion
• Background and Conventional Secure Deletion Techniques
• Advanced Secure Deletion Optimization Techniques
• Conclusion
This paper evaluates the implementation challenges of secure data deletion and sanitization techniques. Meanwhile, we survey the state-of-the-art designs that have been paid to pursue better efficiency, verifiability, and portability for both HDDs and SSDs. The pros and cons on implementing “secure deletion” of different techniques are also discussed:

- Encryption-based technique
- Erasure-based technique
- Overwriting-based technique
- Mixed technique
Q&A

Thanks for your attention
References

• [1] https://www.mordorintelligence.com/industry-reports/solid-state-drive-market