intel Security

New Intel Solid State Drive Capabilities and Disk Forensics

TM

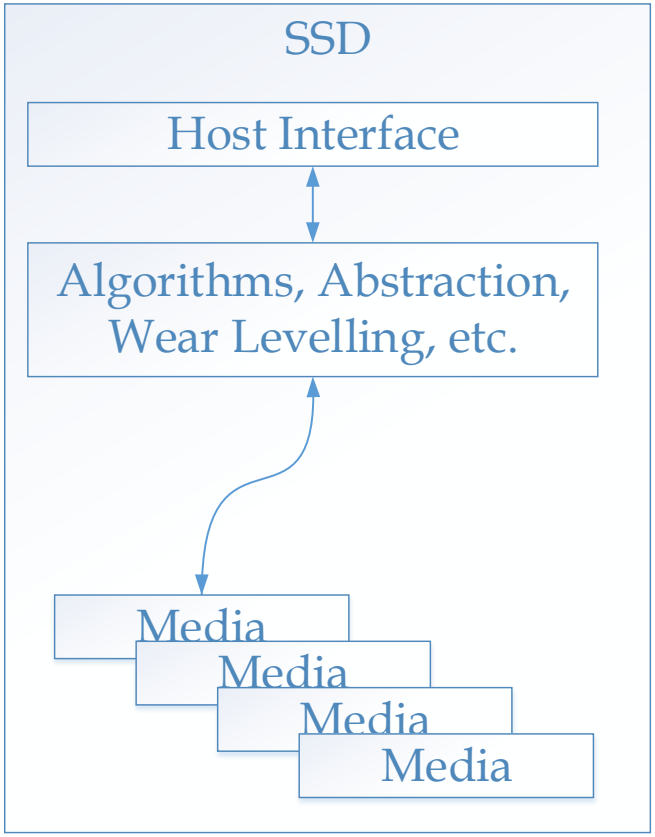
- Xiaoning Li (Intel Labs)
- Benjamin W. Boyer (Intel)

ISC 2016 Forensics Forum

Solid State Drives

Modern SSDs typically contain a layer of abstraction between the host and the backing media. There are multiple reasons for this, from wear levelling, thermal management, and performance algorithms, to abstracting away quirks of the actual storage media.

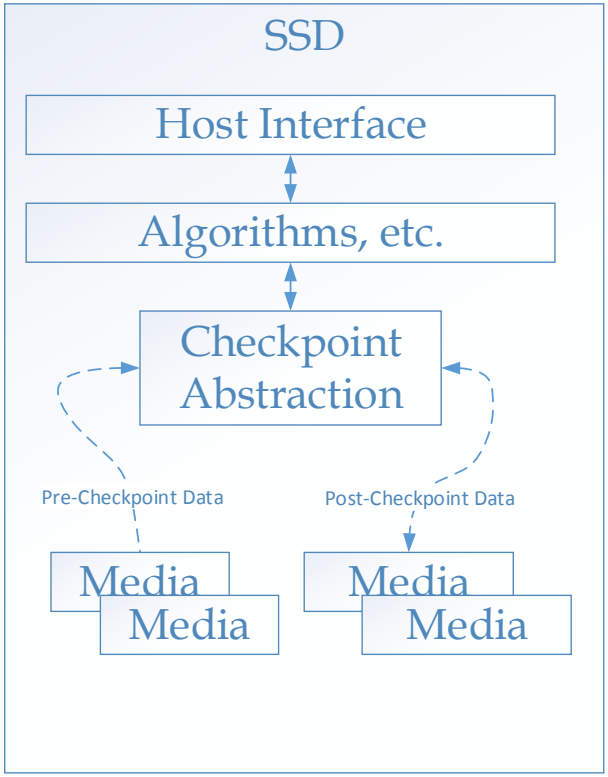
Of particular interest for this prototype is the resultant fact that a given host's logical block address (LBA) can actually be stored in *any* location in the backing media.



What if we could save a snapshot of the data in the device at an arbitrary point in time?

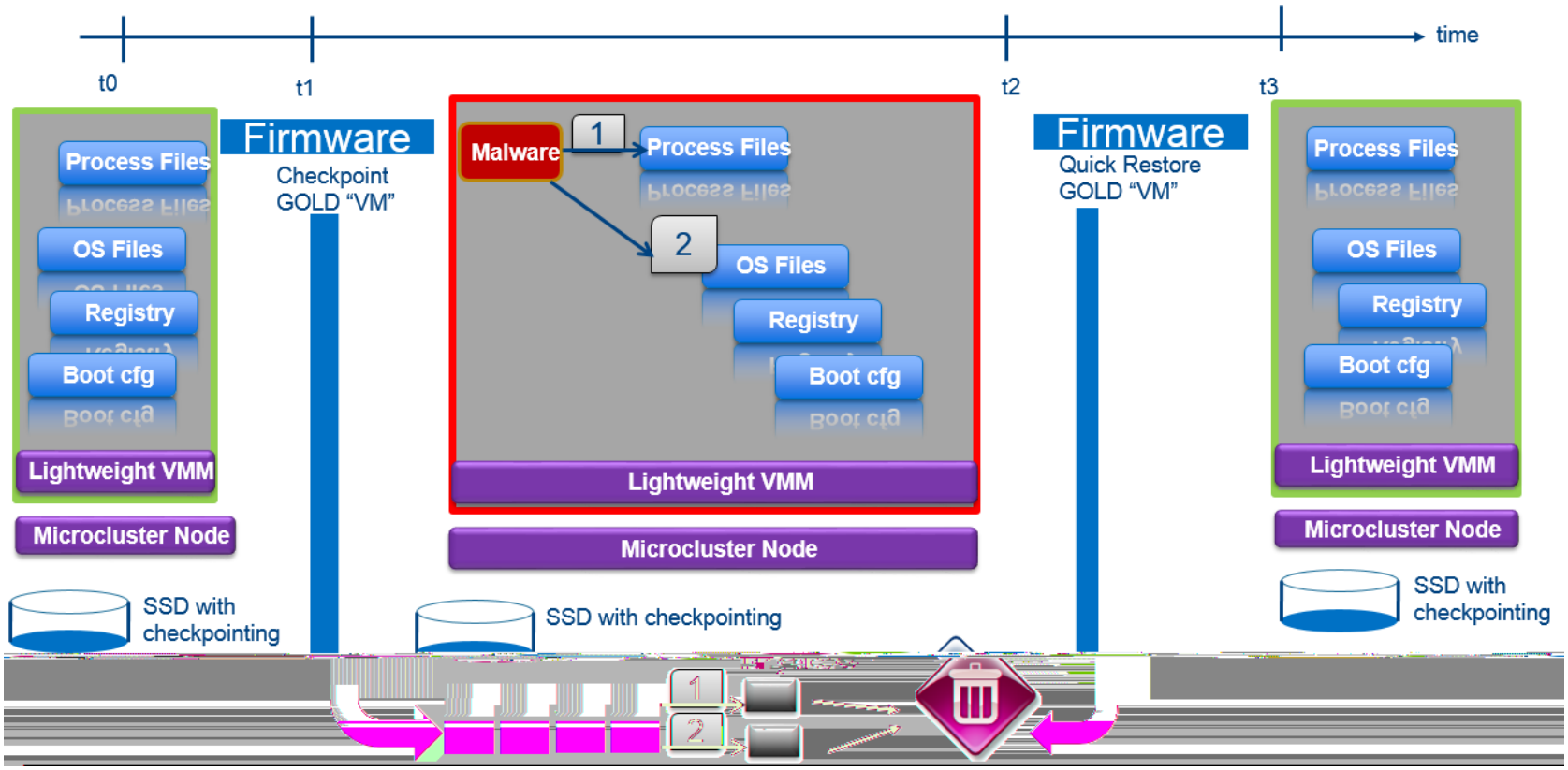
SSD Internal Checkpoint

- By leveraging the media abstraction subsystems of our SSDs, we created new functionality that allows a system to mark a checkpoint of the device contents at a given moment in time.
- Subsequent I/O operations do not overwrite the data present at time of checkpoint.
- Changes can be inspected after the fact.
- The entire change set can be quickly reverted to the checkpointed state.
- Our initial prototype shrinks the exposed LBA range by 50%, and allows indefinite overwriting of the exposed LBA range without the loss of checkpointed data.



SSD Checkpoint Usage

- Supporting checkpoint from SSD firmware.
- Rapidly recovering golden image/snapshot.

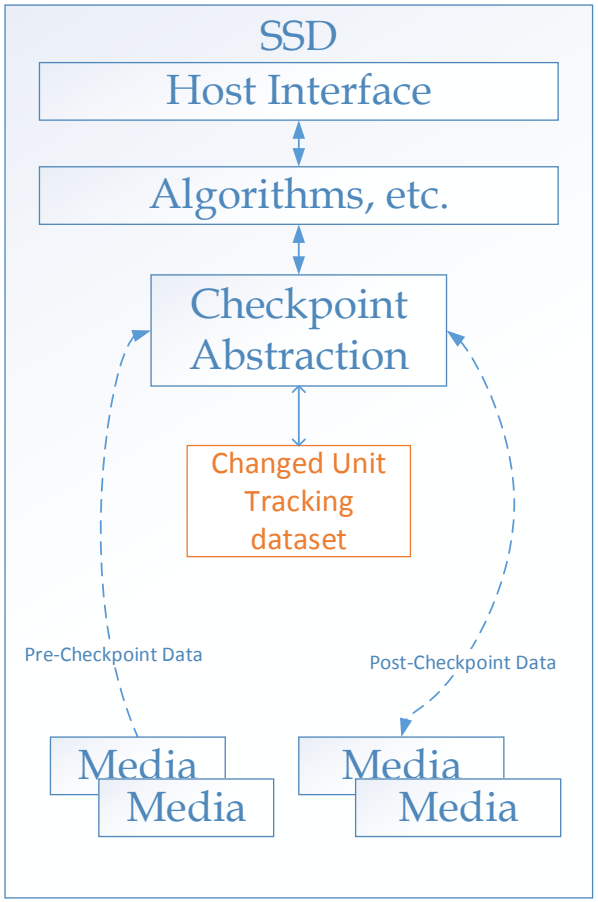


Forensics analysis cost

- Before recovering to the Pre-Checkpoint image, a full disk scan is required to detect and inspect all changes.
- After recovering to the Pre-Checkpoint image, all Post-Checkpoint disk changes disappear.
- Creates a challenge for disk forensics.

SSD ChangeLog

- By leveraging the media abstraction subsystems of our SSDs, we log all write operations.
- Changes to LBAs are abstracted aggregated at 4KB pages.
- This Changelog can be exported by a General Purpose Logging (GPL) request.

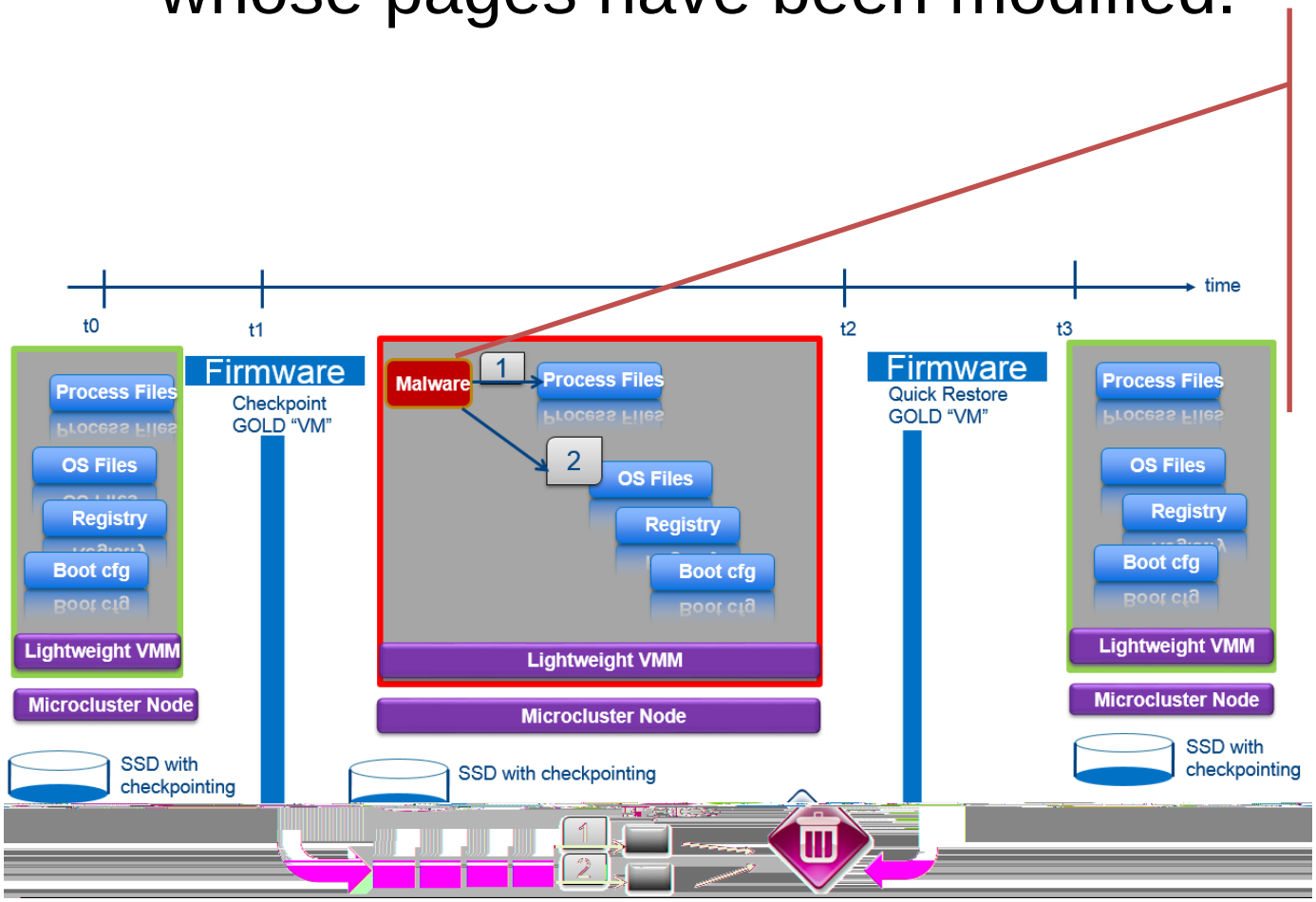


Page Info to LBA Calculation

$$LBA\ Start = Page\ Address\ * 8$$
$$LBA\ End = Page\ Address\ * 8 + 7$$

SSD ChangeLog Usage

- Inspected LBAs can be reduced to only those whose pages have been modified.



Pages
Page 1
Page …
Page N

Forensics analysis cost

- By utilizing SSD Checkpoint, we can reduce the scope of inspection from the entire disk to only the changed pages.

Summary

- SSD checkpoint creates many snapshot usages , but at a cost: additional work is required to inspect dirty LBAs.

- SSD ChangeLog significantly reduces the scope of disk forensics by constraining the LBA range to only what has changed.

Thank You!

Xiaoning.Li@intel.com


intel
Security