Apps Can Quickly Destroy Your Mobile's Flash: Why They Don't, and How to Keep It That Way

Tao Zhang¹, Aviad Zuck², Donald E. Porter¹, Dan Tsafrir²,³
SSD Lifespan Nowadays Considered Non-issue

- Flash can only endure a limited write quota
  - E.g., 3K rewrites of the entire SSD
Mobile Flash Storage: Compact SSD (with Compromises)

- Smaller
- More power efficient
- Cost less
- Lower capacity
- Limited hardware
- Worse performance (eMMC)
- Less sophisticated firmware
• Smartphones skew toward dangerous bandwidth/capacity ratio
• Easy to issue lifetime’s worth of writes
• Conventional wisdom: SSD wear-out not a problem

• Our analysis: There is cause for concern
  1. Dangerous bandwidth/capacity skew
  2. Less sophisticated devices
  3. App stores are trusted (too much)
  4. Users perceive mobile phones as safer (strict permissions, app stores)

• How bad could it be?
  – Let’s try attacking mobile devices and measure lifespan!
Threat Model

• Mobile storage device (eMMC/UFS)
• Long-term warranty (e.g., 2Y)
• Supports synchronous IO
• Code snippet can access storage space by default
  – E.g., app with no special privileges
Wear-out Attack

- Prototype Android app with less than 1K lines of code
- No special permission needed
- Stealthily rewrite small files in app’s storage space

Run as background service

Only run on charging status

Pause workload on screen lit
Phone Wear-out Experiment Results

BLU
512MB
4GB
<br><br>6 days
<br><br>Moto E
8GB
<br><br>8 days
<br><br>SMG S6
32GB
<br><br>22 days
<br><br>SMG S9
64GB
<br><br>~2 weeks
<br><br><br>Phones can be worn out in weeks!
• Mobile flash storage can be worn out quickly
• Mobile flash storage can be worn-out quickly

Why my phone is not dead (yet)?
Mobile App I/O Characterization

• Platform: Samsung S6 32GB
  – ~88 TiB estimated lifetime write
  – 2Y warranty

• Two usage scenarios
  – 27 preloaded apps (camera, etc.) + top 150 free apps from Google Play Store*

  ![App Icons]

  – I/O-intensive workloads (FTP server, file copies, backup/restore)

* 23 apps excluded due to various reasons, details in paper
Initial conclusions

• Most apps don’t consume dangerous levels of write bandwidth
  – Most apps are not used most of the time
• Minority of apps are write-intensive
  – Lets look more closely at these “troublemakers”
Write-heavy Apps/Workloads

- Apps issue bursts of I/O
Can apps prematurely wear-out your phone?

- Reasonable app usage won’t shorten device lifetime
  - Most write-heavy usage scenarios not long-term/frequently used
- Extreme use cases **CAN** prematurely wear-out phone (but not likely)
Most apps cause little to no background I/O activities
• Mobile flash storage can be worn-out quickly
  – Wear-out level evaluation
  – Smartphone storage wear-out experiments

• Mobile flash storage is safe with benign apps under reasonable usage
  – Reasonable app usage won’t shorten device lifetime
  – Most apps cause little to no background I/O activities
  – Extreme use cases CAN prematurely wear-out your phone

More details in the paper.
• Mobile flash storage can be worn-out quickly
  – Wear-out level evaluation
  – Smartphone storage wear-out experiments
• Mobile flash storage is safe with benign apps under reasonable usage
  – Reasonable length of app usage is not long enough to shorten lifetime
  – Most apps cause little to no background I/O activities
  – Extreme use cases CAN prematurely wear-out your phone

Should we stop worrying about mobile flash lifespan?
OS Wear Management *is* Necessary

- Potential wear-out attack
- User may playing Final Fantasy for more than 9 hours daily
- Buggy app can unintentionally kill your phone as well
OS-level Wear Management

• Monitor and measure app-specific I/O behavior
  – Extend diskstats accordingly

• Per-app I/O rate limiting mechanism
  – cgroups v2 (Linux kernel 4.5 or newer)
  – Prototype implemented on Samsung S6 (Android 6.0.1) & Linux kernel 3.10.101.

• Let the user choose!
  – Prompt user whether to rate-limit suspicious app
Wear Management Policy

- Apps tend to issue bursty I/O
  - Allocate write (lifetime) slack quota to accommodate bursts

- Denial-of-Service attack on slack quota
  - Quota & threshold with finer granularity (daily)

- Foreground vs. background
  - Stricter quota & threshold on background apps (i.e., hourly)

More details in the paper
Evaluation (Write-intensive Apps)

- Video shooting with camera (foreground)
- Bursts are permitted
- ~1.2 hours daily usage without intervention

- Google Hangouts receiving messages every 5s (background)
- ~300 KiB/s background workload

Benign apps run with no/minimum disruption
Evaluation (Wear-out attack)

- Malicious wear-out attack in background
- \(~80\text{MiB/s}\) maximum throughput

Phone protection kicks in within 30s
Conclusion

• Mobile flash storage is still in danger
  – App with no special perm can doom storage in days/weeks

• App I/O characterization
  – Mobile flash storage is safe with benign apps under reasonable usage
  – Extreme usage scenarios can still prematurely exhaust storage lifespan

• Prototype of flash wear management mechanism
  – Effectively identify & rate-limit malicious apps
  – Little to no disturbance on benign apps and user experience

• Flash storage lifespan as depletable resource needs to be managed
  – Embedded devices with flash storage (IoT devices, medical devices, etc.)

Aviad Zuck
aviadzuc@cs.Technion.ac.il
Backup slides
Flash Internals

- Floating gate (flash cell)
  - Program (inject electrons)
  - Erase (eject electrons)
  - Electrons trapped in insulating oxide (worn out)
SLC ⇚ MLC ⇚ TLC: Evolution or Degeneration?

- Higher density (lower cost)
- Poorer performance
- Easier to wear-out
  - SLC: up to 100K P/E cycles
  - MLC: 3K ~ 10K P/E cycles
  - TLC: < 1000 P/E cycles
- “...global shipment share of client-grade SSDs using TLC Flash will exceed 75% by in 2017.” [DRAMeXchange]

(Source: EE Times)
How to Evaluate Wear-out Level

- Built-in Wear-out Indicators
  - eMMC [JESD84-B51] Extended CSD register
  - UFS [JESD220C] Device Health Descriptor
  - Value from 1 to 11

<table>
<thead>
<tr>
<th>Value</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life Consumed</td>
<td>0%</td>
<td>10%</td>
<td>20%</td>
<td>30%</td>
<td>40%</td>
<td>50%</td>
<td>60%</td>
<td>70%</td>
<td>80%</td>
<td>90%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Worn out
eMMC Flash Chips Can Wear-out in Days

- ~23 TiB total write, ~7 days at 40 MiB/s
- ~8 TiB total write, ~6 days at 20 MiB/s
Can apps prematurely wear-out your phone?

<table>
<thead>
<tr>
<th>App</th>
<th>Avg. Throughput</th>
<th>Daily Usage Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB Copy</td>
<td>29.74 MiB/s</td>
<td>1.18 hours</td>
</tr>
<tr>
<td>Restore (local)</td>
<td>23.29 MiB/s</td>
<td>1.51 hours</td>
</tr>
<tr>
<td>FTP</td>
<td>6.39 MiB/s</td>
<td>5.50 hours</td>
</tr>
<tr>
<td>Daily Horoscope</td>
<td>4.98 MiB/s</td>
<td>7.05 hours</td>
</tr>
<tr>
<td>Camera</td>
<td>4.26 MiB/s</td>
<td>8.24 hours</td>
</tr>
<tr>
<td>Final Fantasy</td>
<td>3.84 MiB/s</td>
<td>9.15 hours</td>
</tr>
<tr>
<td>Backup (local)</td>
<td>2.30 MiB/s</td>
<td>15.25 hours</td>
</tr>
</tbody>
</table>

- Most write-heavy usage scenarios are neither long-term operations nor frequently used
- Reasonable length of app usage is not long enough to shorten lifetime
• Video shooting with \(~7\text{MiB/s}\) write activity
• \(~1.2\text{ hours}\) daily usage without intervention
• May exceed, for short time
• Google Hangouts receiving messages (per 5s) in background
• \(~300\) KiB/s background workload

Benign apps run with no/minimum disruption