Apps Can Quickly Destroy Your Mobile's Flash:

Why They Don't, and How to Keep It That Way

Tao Zhang[1], **Aviad Zuck[2]**, Donald E. Porter[1], Dan Tsafrir[2,3]

1 THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

2 TECHNION Israel Institute of Technology

3 vmware

We Expect Improvements Over Time

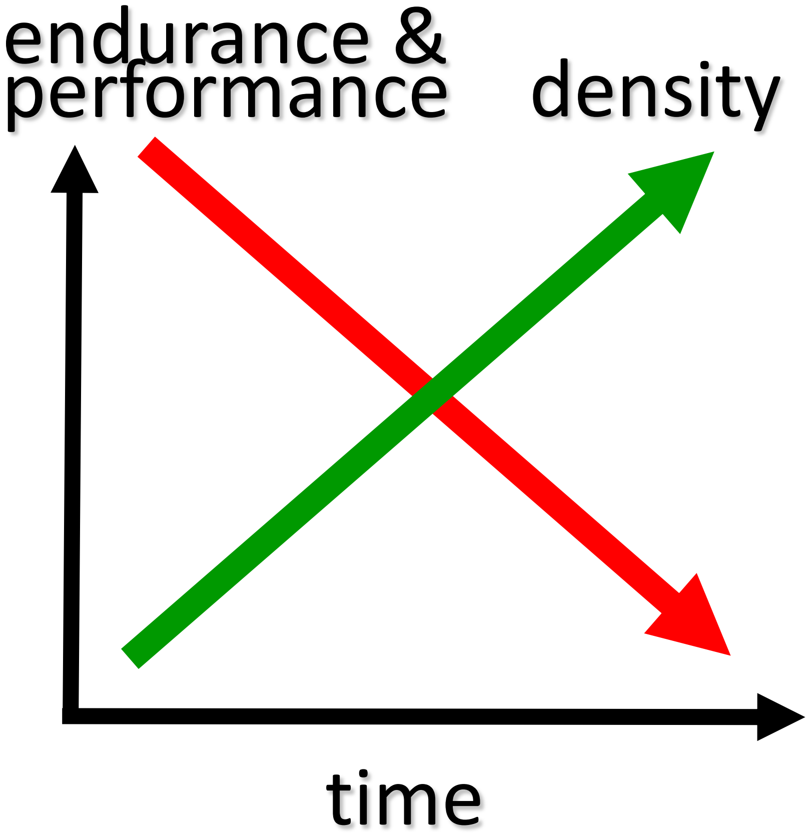
Samsung S1
(2010)

a decade later

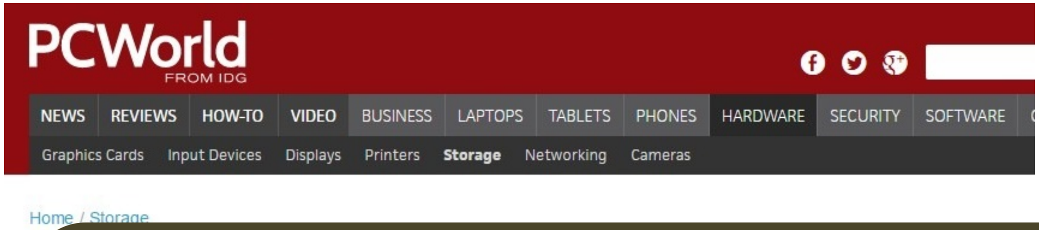
Samsung S10
(2019)

Flash Evolution

- Higher density (lower cost)
  - Smaller cells (1x nm)
  - More bits per cell
- Easier to wear out
  - QLC flash can't reliably store data after < 1K write cycles
- Poorer performance



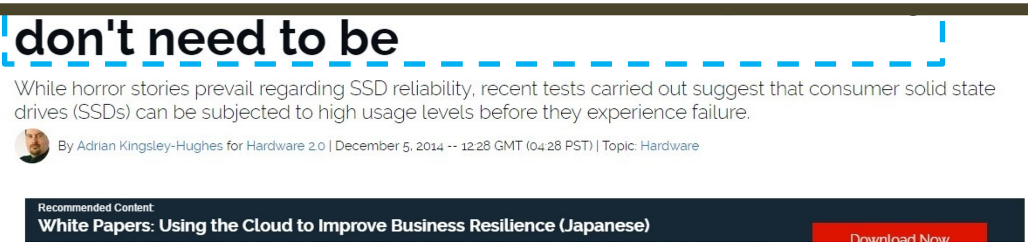
Problem #1: Many People Think SSD Endurance is a Non-issue



Modern SSDs can last a lifetime

By Mihăiță Bamburic | Published 2 years ago

misconception also extends to operating systems designers



don't need to be

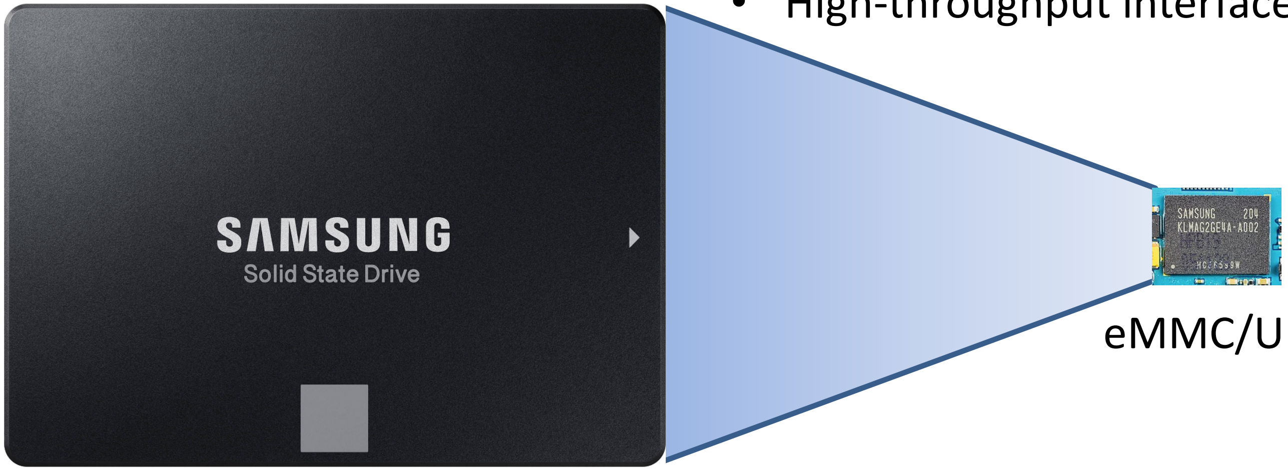
While horror stories prevail regarding SSD reliability, recent tests carried out suggest that consumer solid state drives (SSDs) can be subjected to high usage levels before they experience failure.

By Adrian Kingsley-Hughes for Hardware 2.0 | December 5, 2014 -- 12:28 GMT (04:28 PST) | Topic: Hardware

Recommended Content:
White Papers: Using the Cloud to Improve Business Resilience (Japanese)

Problem #2: Compact SSD (with Compromises)

- Smaller form factor
- More power efficient
- Cost less
- High-throughput interfaces



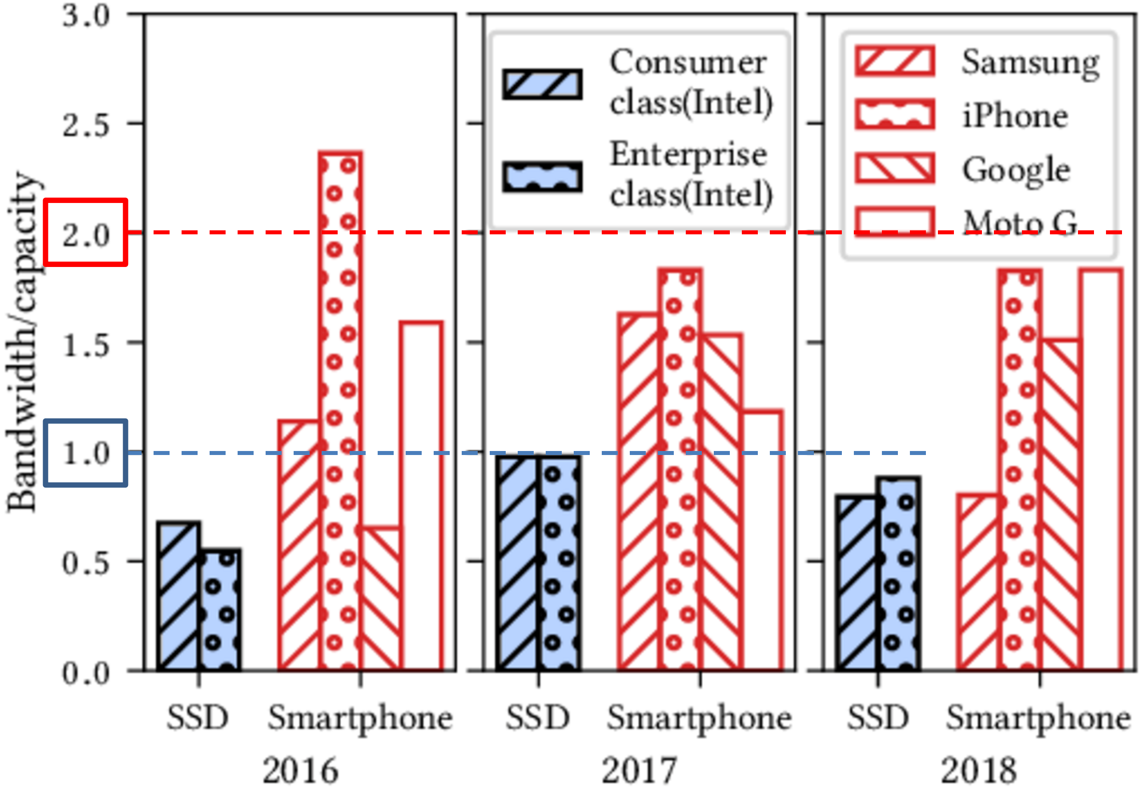
eMMC/UFS

- Lower capacity
- Limited hardware
- Less sophisticated firmware
- No replacement!

Write Bandwidth/Capacity Ratio

Intel Pro 7600p

$\frac{1.6\ GB/s}{2TB}$=0.79



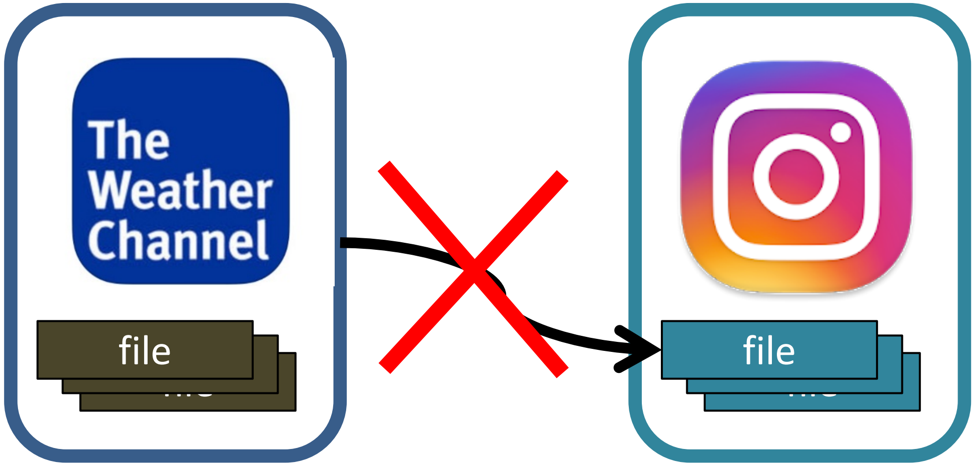
Moto G6

$\frac{117\ MB/s}{64GB}$=1.83

- Smartphones skew toward dangerous bandwidth/capacity ratio
- Easy to issue lifetime's worth of writes

Problem #3: False Sense of Security

- Tighter security models

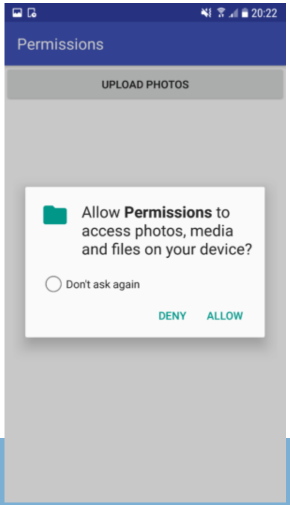


Problem #3: False Sense of Security

- Misplaced trust in app marketplaces
  - "In September alone, researchers uncovered 172 infected apps with over 335 million installs on the Play Store"
    thenextweb.com, Oct 1 2019
- Users carelessly grant permissions

Google Play

App Store


20:22

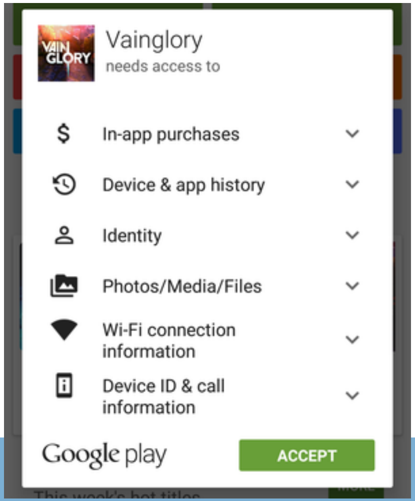
Permissions

UPLOAD PHOTOS

Allow **Permissions** to access photos, media and files on your device?

○ Don't ask again

DENY ALLOW


Vainglory
needs access to

$ In-app purchases

Device & app history

Identity

Photos/Media/Files

Wi-Fi connection information

Device ID & call information

Google play ACCEPT

- Conventional wisdom: SSD wear-out not a problem
- Our analysis: There is cause for concern, especially for mobile storage:
  1. Dangerous bandwidth/capacity skew
  2. Less sophisticated devices
  3. Users perceive mobile phones as safer (strict permissions, app stores)

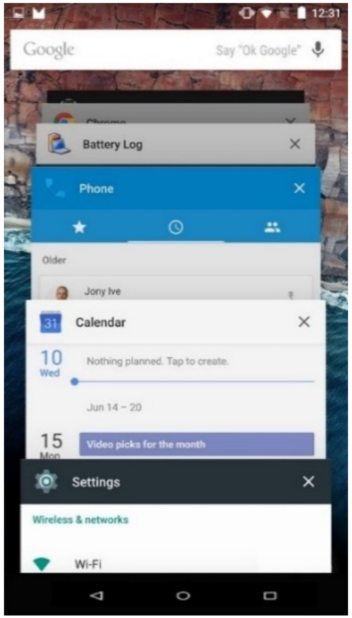
- **How bad could it be?**
  - Let's try attacking mobile devices and measure lifespan!

Threat Model

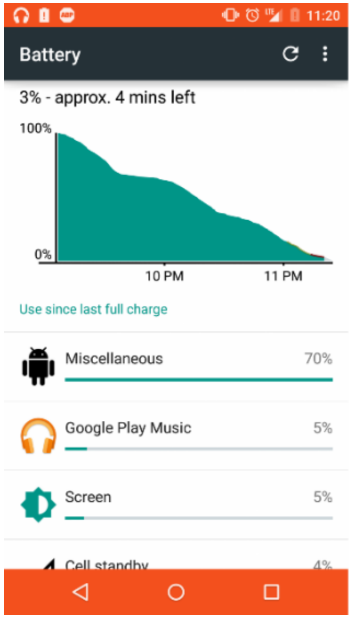
- Mobile storage device (eMMC/UFS)
- Long-term warranty (e.g., 2Y)
- Supports synchronous IO
- Code snippet can access storage space by default
  - Granted by default to all apps
  - E.g., app requires no special privileges

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
- Current OSs provide no protection/warning



Run as background service

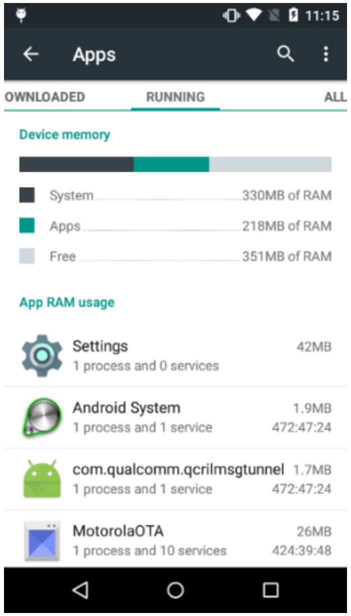


3% - approx. 4 mins left

Use since last full charge

Miscellaneous	70%
Google Play Music	5%
Screen	5%
Cell standby	4%

Only run on charging status



Device memory

■	System	330MB of RAM
🟩	Apps	218MB of RAM
□	Free	351MB of RAM

App RAM usage

Settings 1 process and 0 services	42MB
Android System 1 process and 1 service	1.9MB 472:47:24
com.qualcomm.qcrilmsgtunnel 1 process and 1 service	1.7MB 472:47:24
MotorolaOTA 1 process and 10 services	26MB 424:39:48

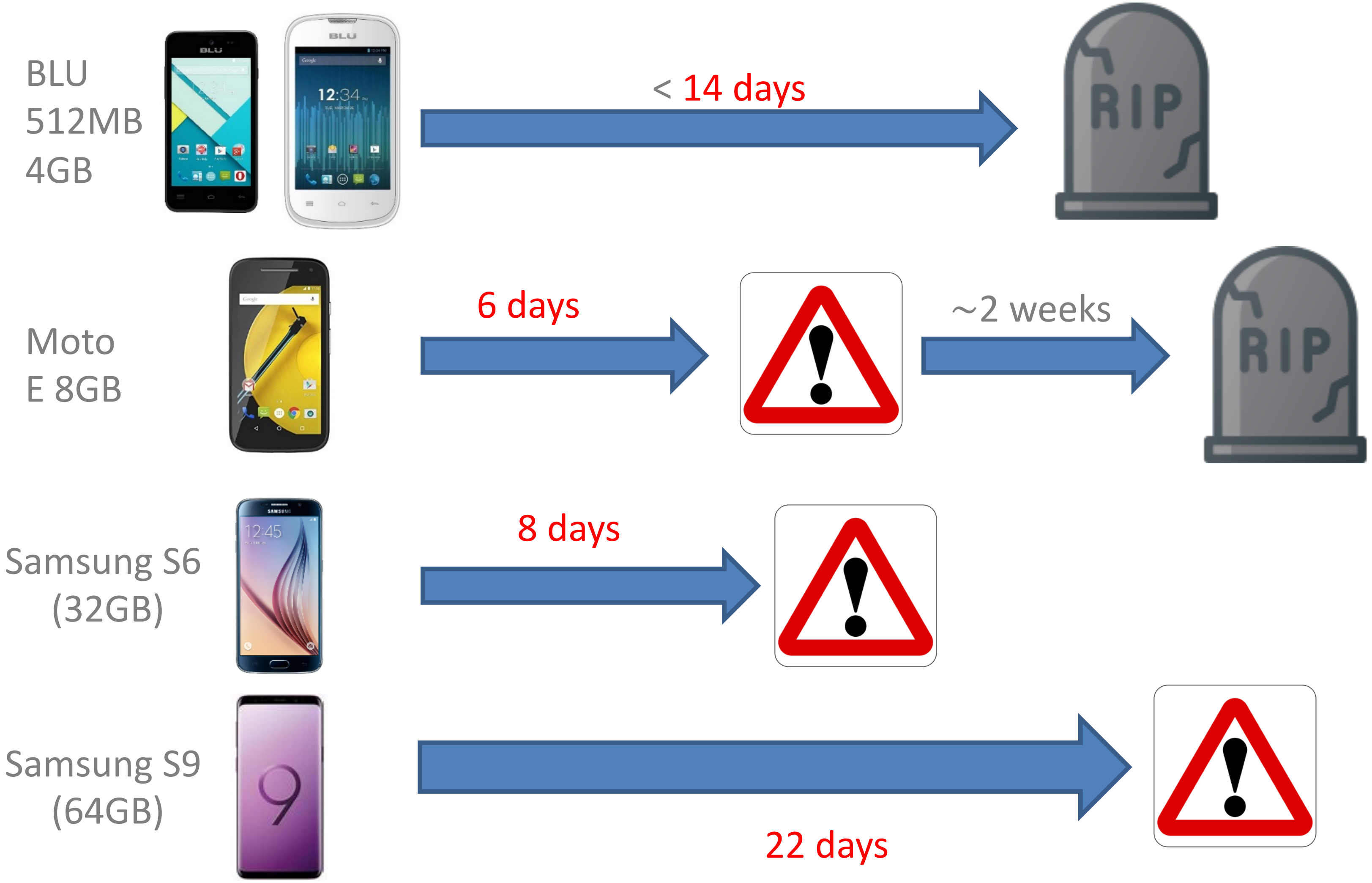
Pause workload on screen lit

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

Value	1	2	3	4	5	6	7	8	9	10	11
Life Consumed	0% ~ 10%	10% ~ 20%	20% ~ 30%	30% ~ 40%	40% ~ 50%	50% ~ 60%	60% ~ 70%	70% ~ 80%	80% ~ 90%	90% ~ 100%	Worn out

Phone Wear-out Experiment Results



BLU 512MB 4GB

< 14 days

Moto E 8GB

6 days

~2 weeks

Samsung S6 (32GB)

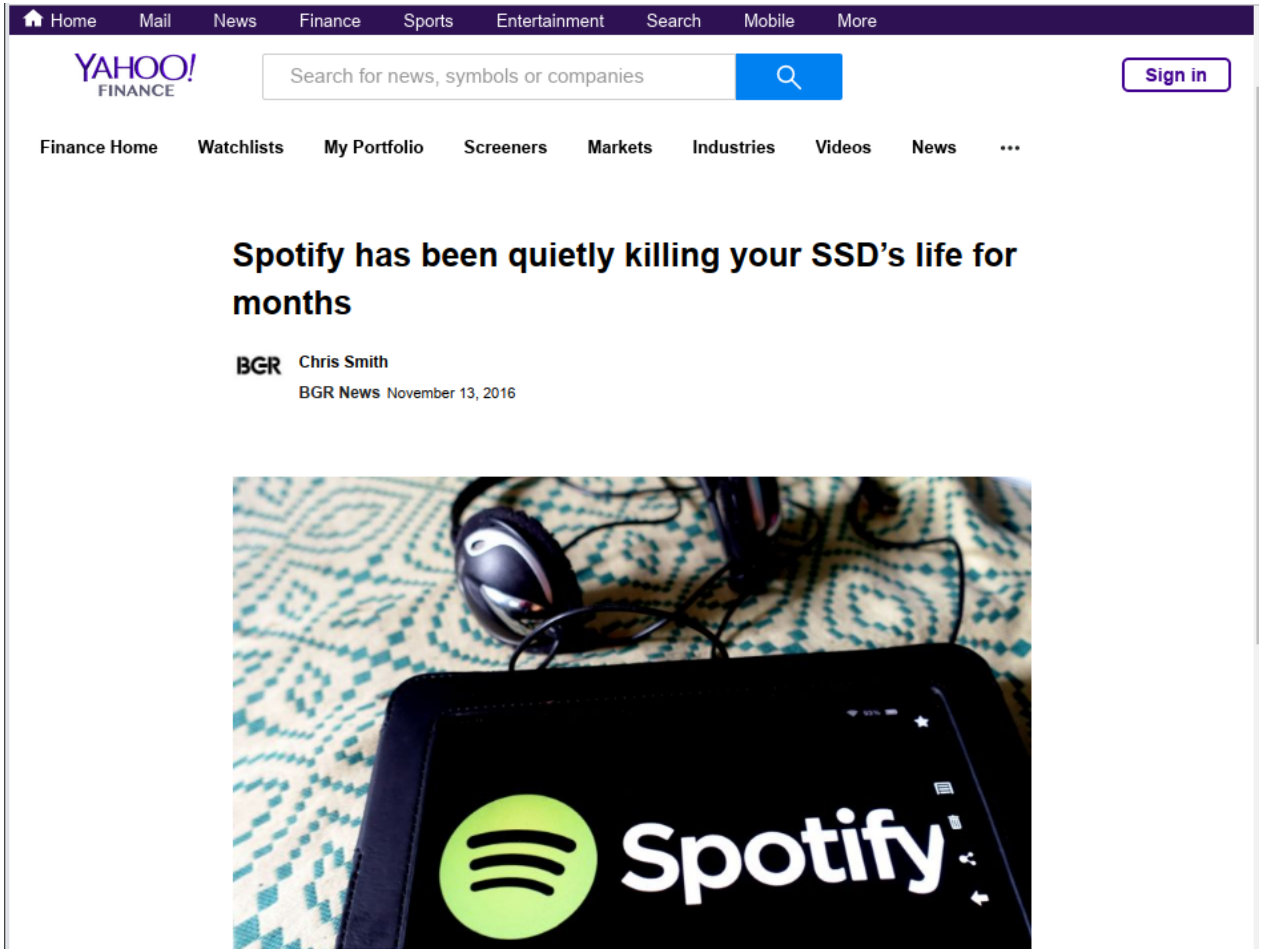
8 days

Samsung S9 (64GB)

22 days

Phones can be worn out in weeks!

Buggy Apps Can Also Kill SSDs



Spotify has been quietly killing your SSD's life for months

BGR Chris Smith

BGR News November 13, 2016

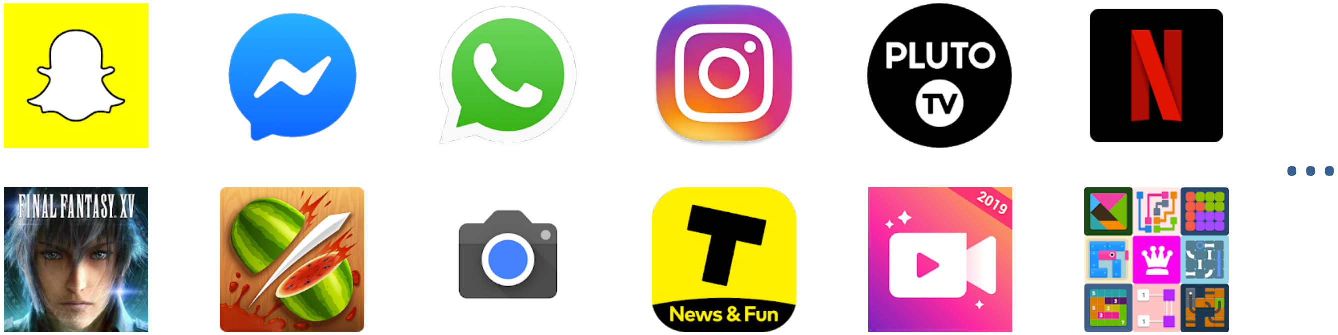
- Mobile flash storage can be worn out quickly

- 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
- 1st characterization of mobile app I/O behavior:
  - Top 150 free apps from Google Play Store*
  - 27 preloaded apps (camera, etc.)
  - I/O-intensive workloads (FTP server, file copies, backup/restore)

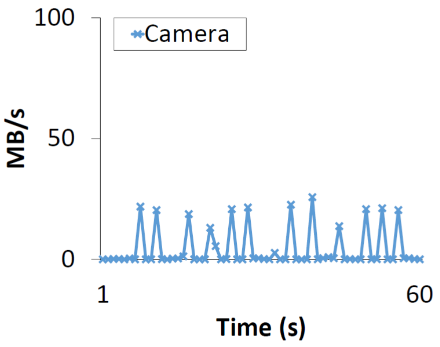


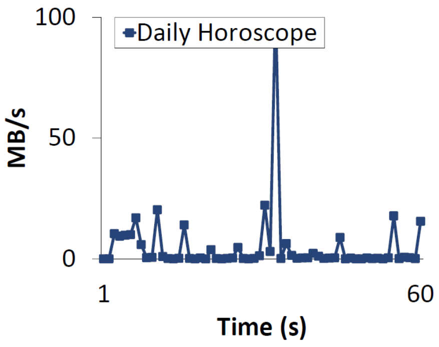
* 23 apps excluded due to various reasons, details in paper

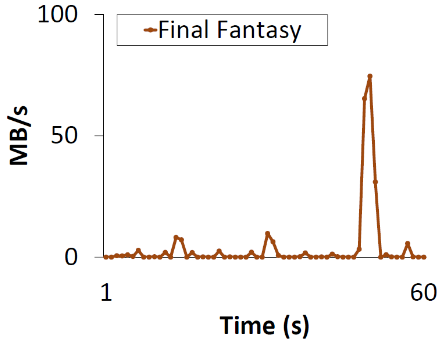
Initial conclusions

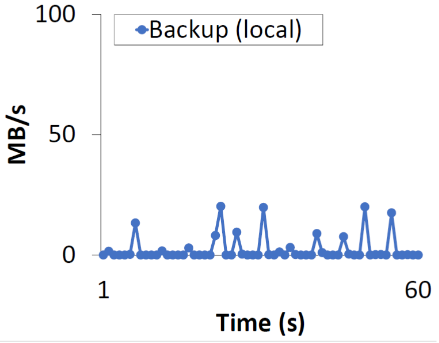
- Most apps don’t consume dangerous levels of write bandwidth
  - Most apps are not used most of the time
- Minority of apps are write-intensive
  - Lets look more closely at these “troublemakers”

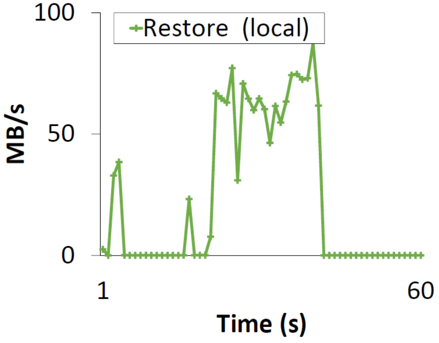
Write-heavy Apps/Workloads

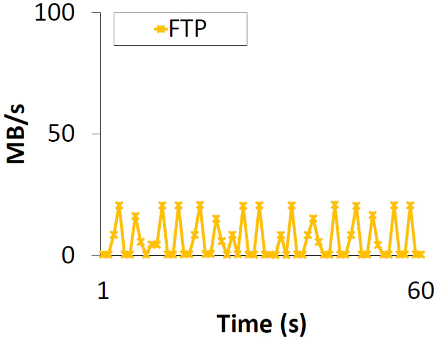


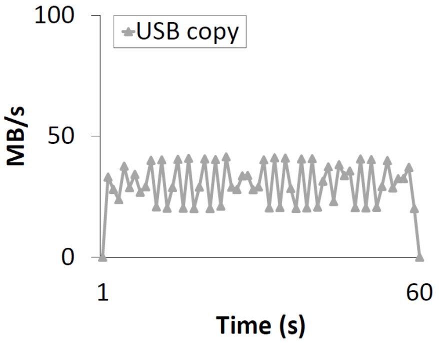












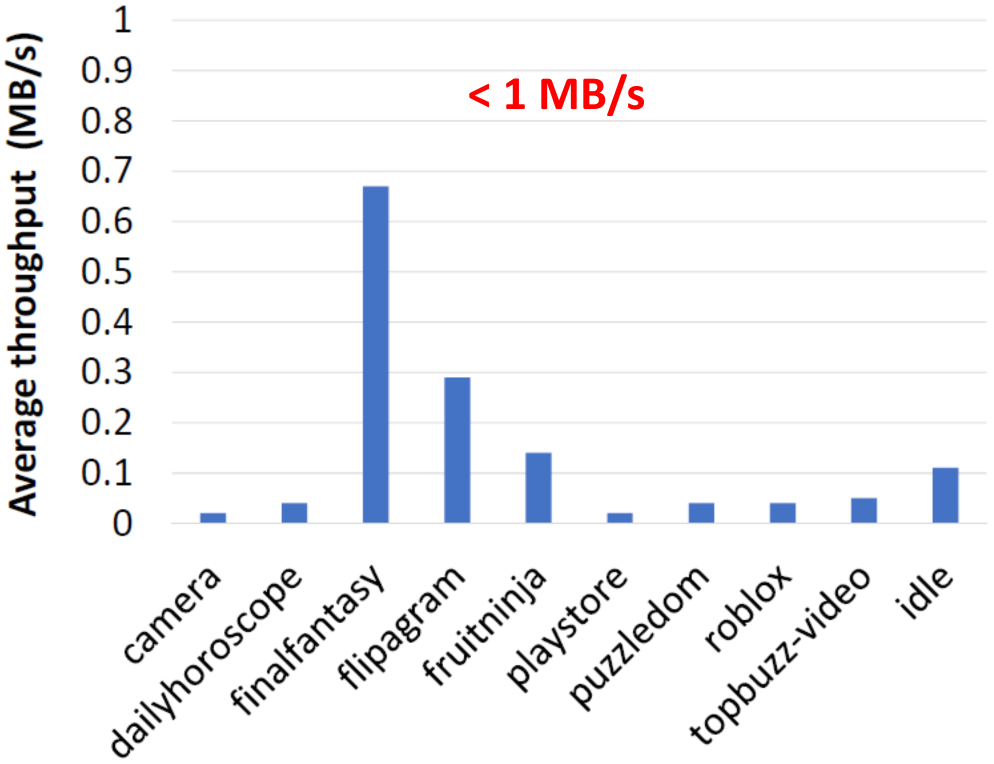
- Apps issue bursts of I/O

Can apps prematurely wear-out your phone?

app	avg. throughput (MiB/s)	required daily usage (hours)
USB copy	29.74	1.18
FTP	6.39	5.50
Camera	4.26	8.24
Backup (local)	2.3	15.25
Restore (local)	23.29	1.51
Daily Horoscope	4.98	7.05
Final Fantasy	3.84	9.15

- 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)

App Background I/O Characterization



- Most apps cause little to no background I/O activities

Interim Summary: device killers

- Buggy apps (unintentionally)
- Wear-out attack (intentionally)
- App users (unintentionally)

Impact Beyond Phones

Same storage devices used in TVs, medical devices, wearables, IoT, GPS, smart home devices, cars…

OS-level Wear Management

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

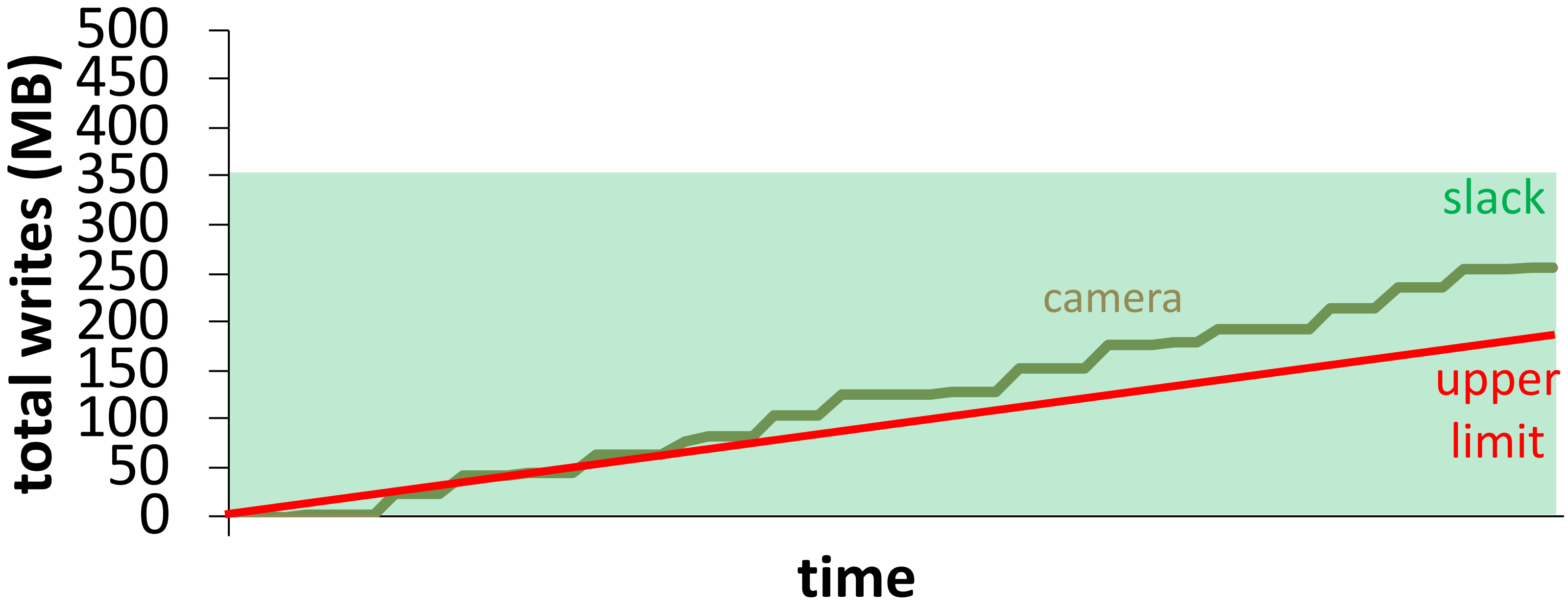
- **Let the user choose whether app behavior is normal!**

- But help users make informed decision

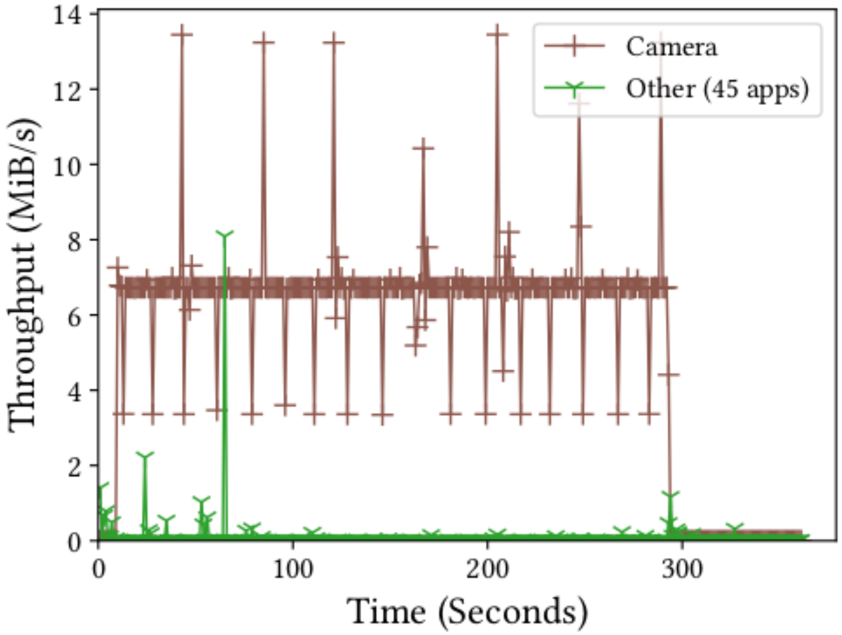
Write Quota Regulation

- Upper limit (per-second) on I/O writes
- Appropriate 50% of lifetime writes as slack (daily)
    - Accommodates write bursts of benign apps
    - Stricter quota & threshold on background apps (i.e., hourly)

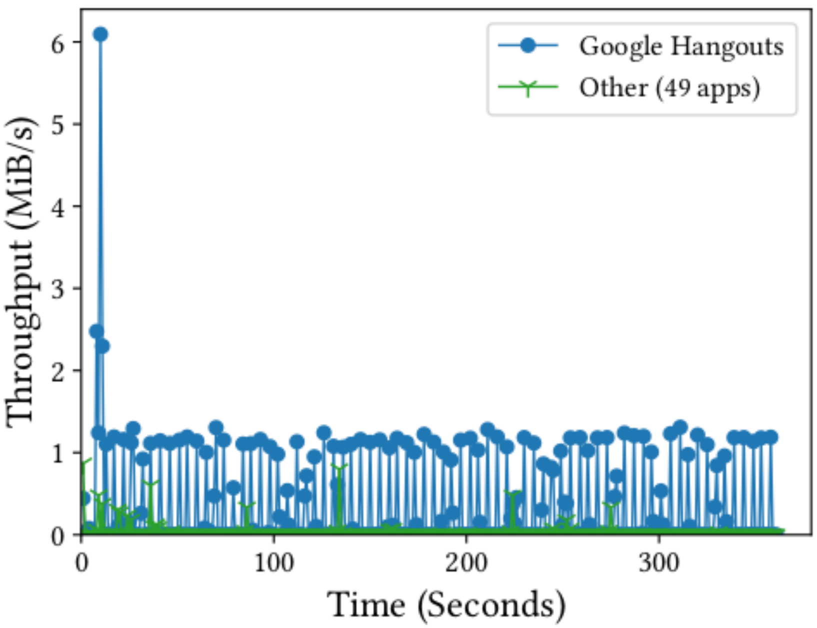
- More details in the paper



Evaluation (Write-intensive Apps)



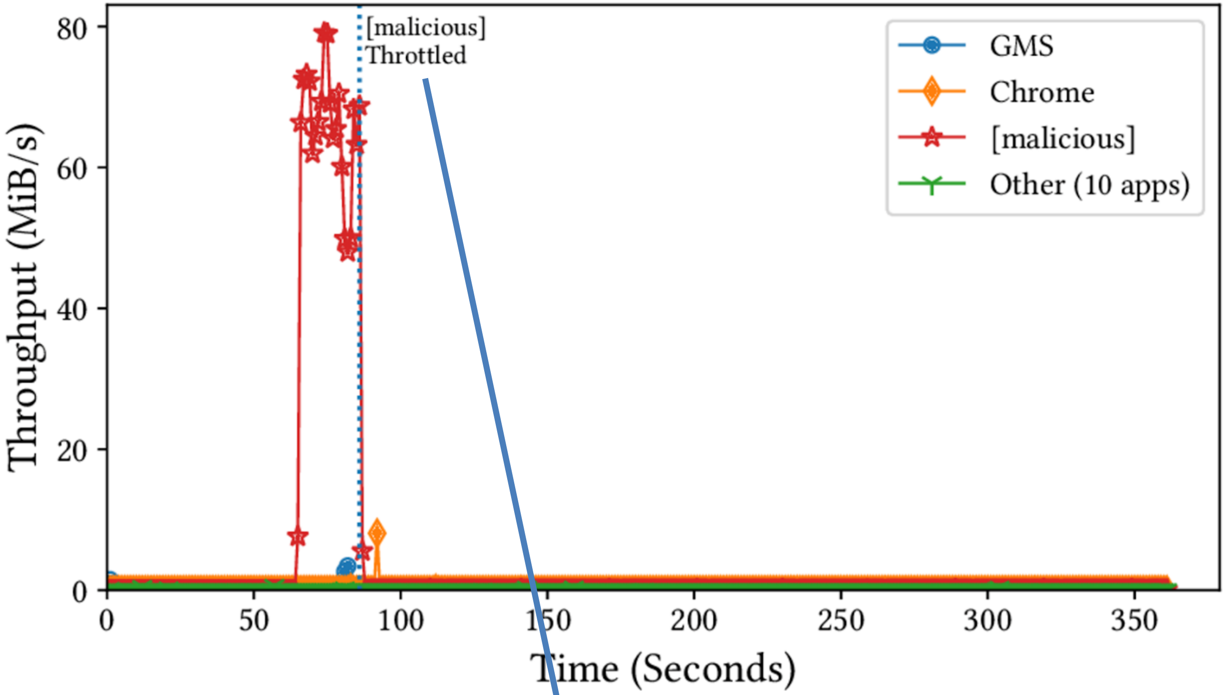
- Video shooting with camera (foreground)
- Bursts are permitted
- ~1.2 hours daily usage without intervention



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

Benign apps run with no/minimum disruption

Evaluation (Wear-out attack)



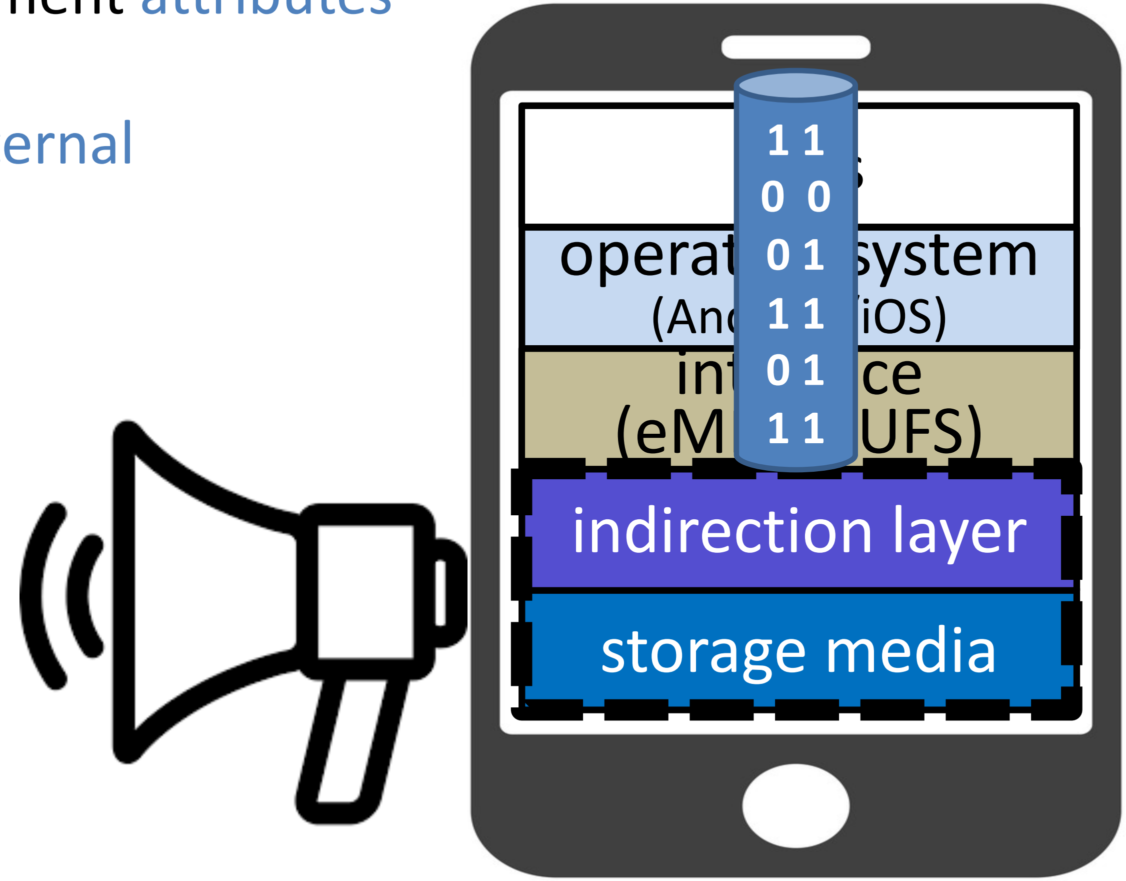
- Malicious wear-out attack in background
- ~80MiB/s maximum throughput

Phone protection kicks in within 30s

Done, But Not Over

- Firmware can amplify write I/O
- Effective wear management attributes app I/O to flash writes
- Need to understand internal firmware behavior

80x



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

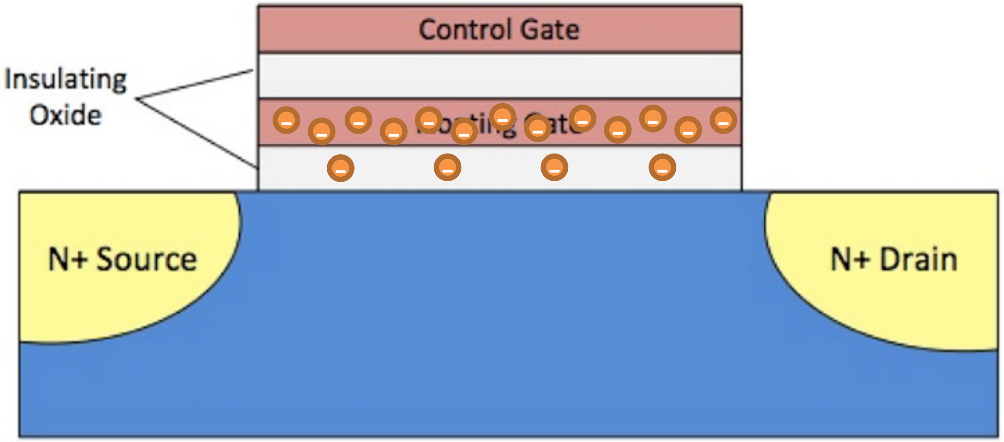
- Flash storage lifespan as depletable resource needs to be managed
  - Embedded devices with flash storage (IoT devices, medical devices, etc.)

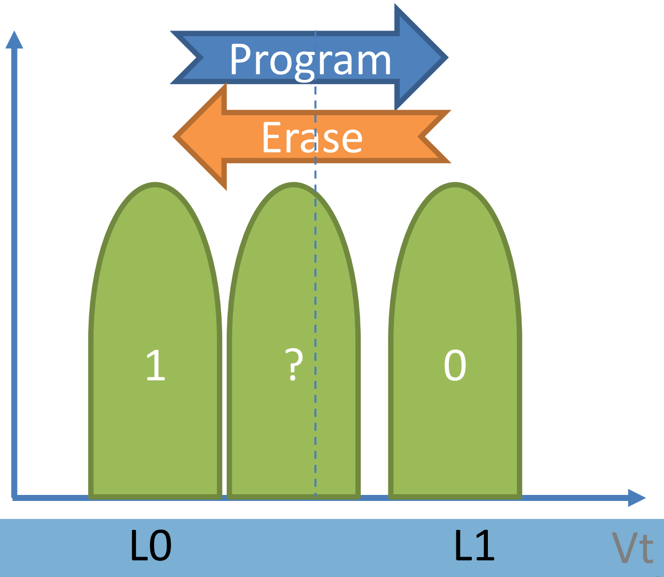
Aviad Zuck
aviadzuc@cs.technion.ac.il

Backup slides

Flash Internals

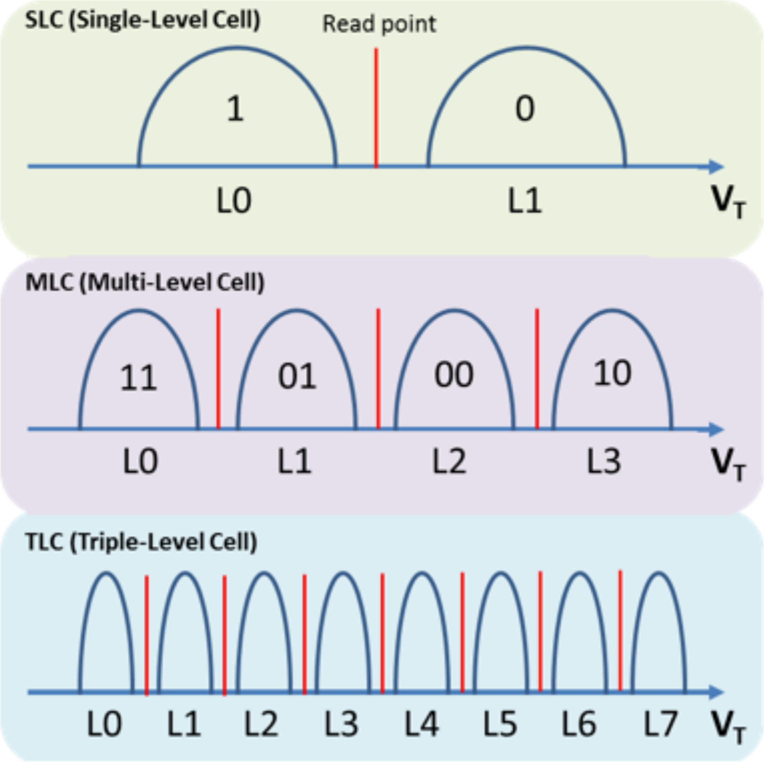
- Floating gate (flash cell)
  - Program (inject electrons)
  - Erase (eject electrons)
  - Electrons trapped in insulating oxide (worn out)





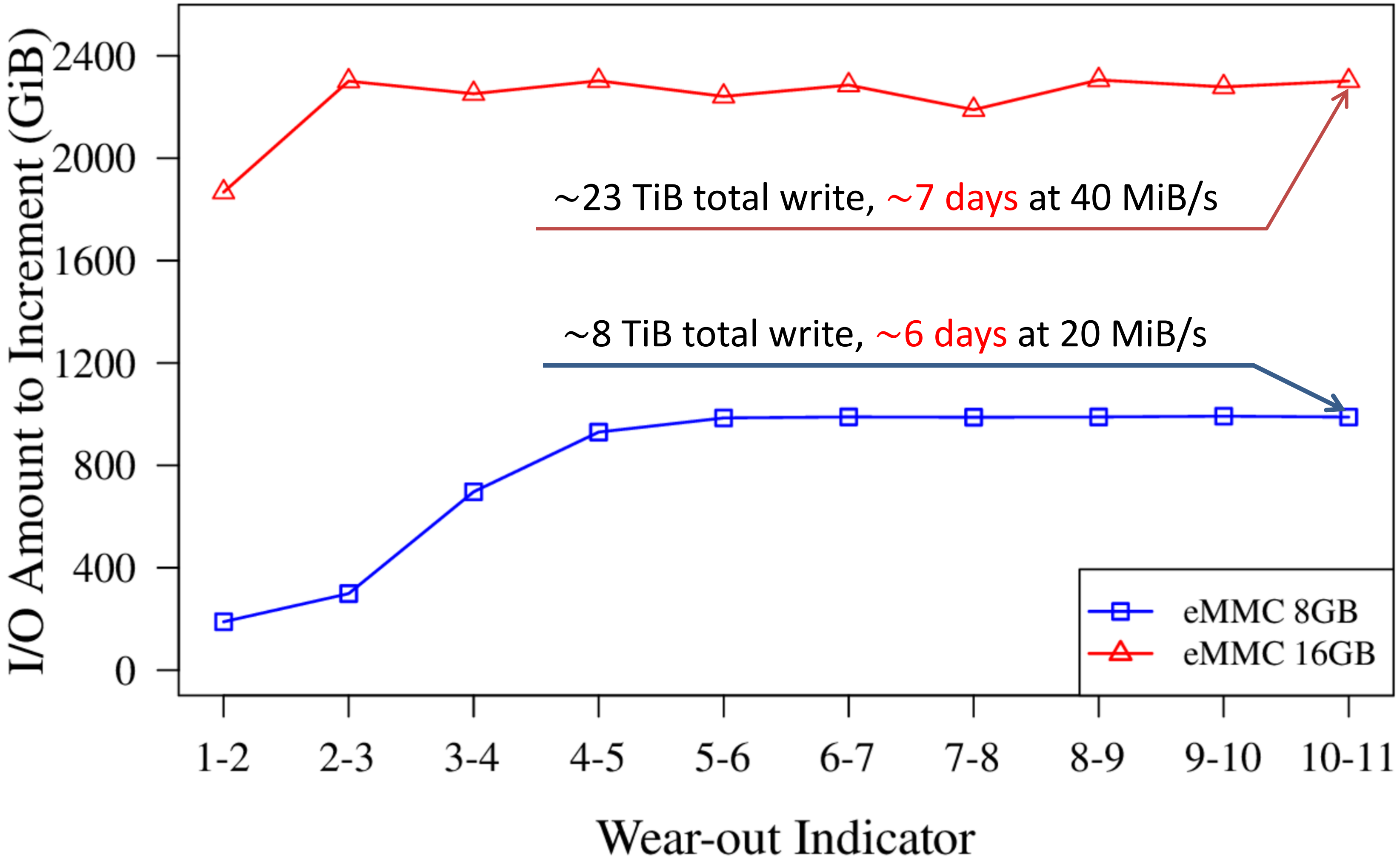
SLC ⇨ MLC ⇨ TLC: Evolution or Degeneration?

- 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)

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