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]

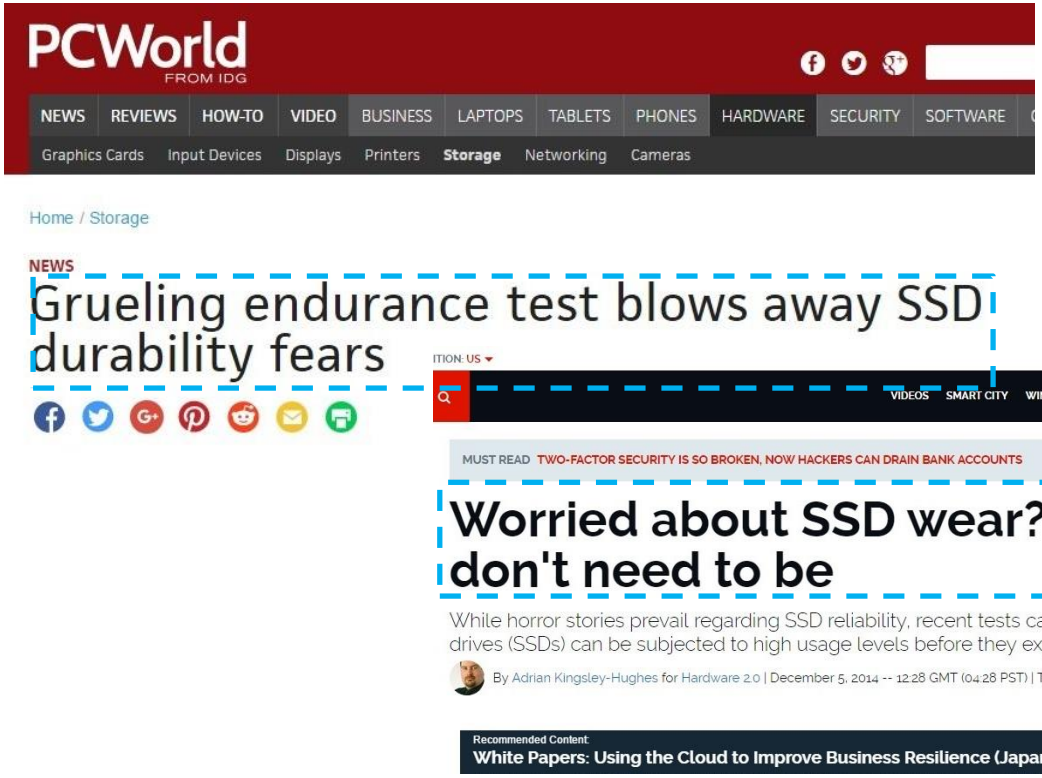
1 THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

2 TECHNION Israel Institute of Technology

3 vmware®

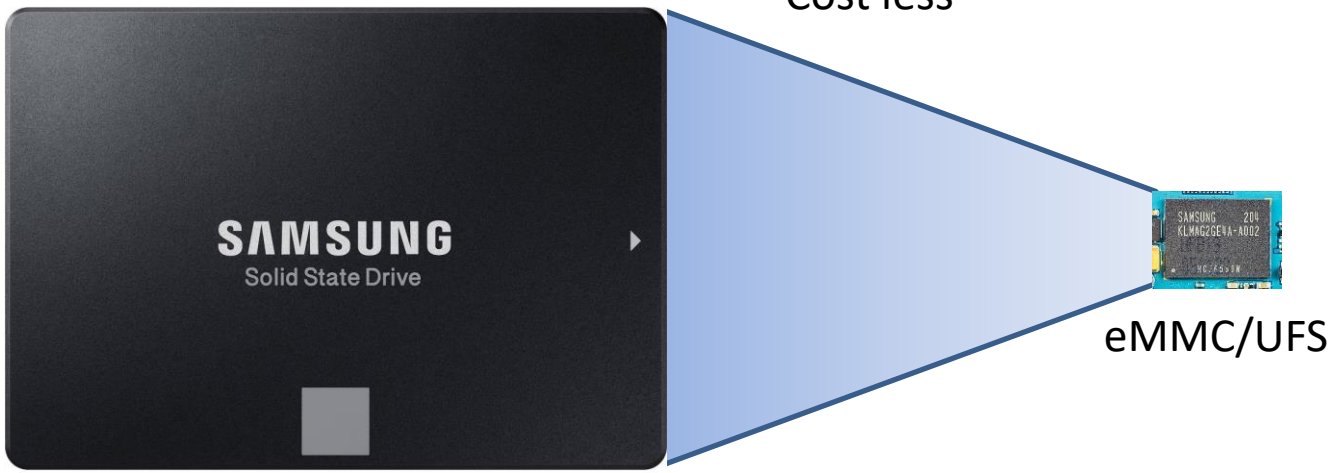
SSD Lifespan Nowadays Considered Non-issue

- Flash can only endure a limited write quota
  - E.g., 3K rewrites of the entire SSD



Mobile Flash Storage: Compact SSD (with Compromises)

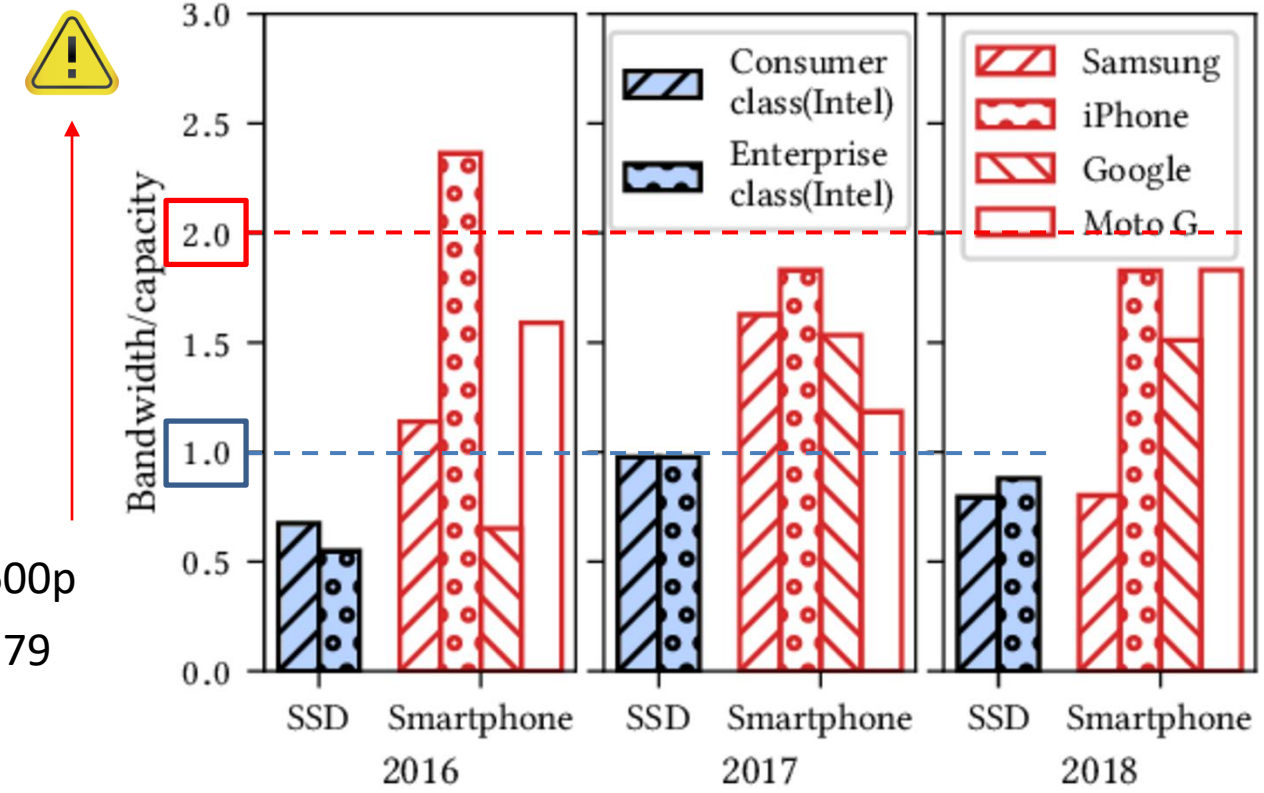
- Smaller
- More power efficient
- Cost less



eMMC/UFS

- Lower capacity
- Limited hardware
- Worse performance (eMMC)
- Less sophisticated firmware

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

- 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)

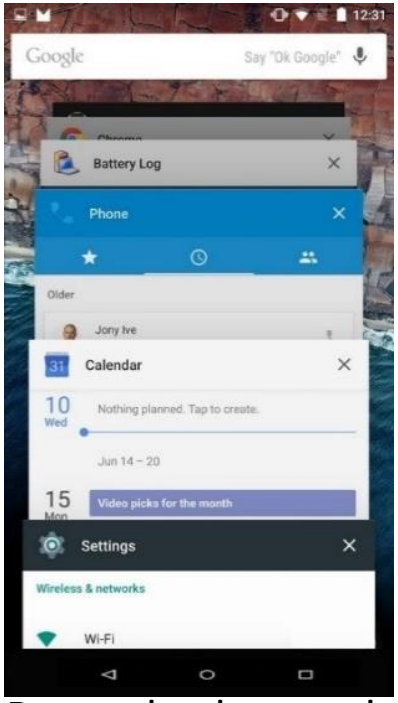
- **How bad could it be?**
  – Let's try attacking mobile devices and measure lifespan!

Threat Model

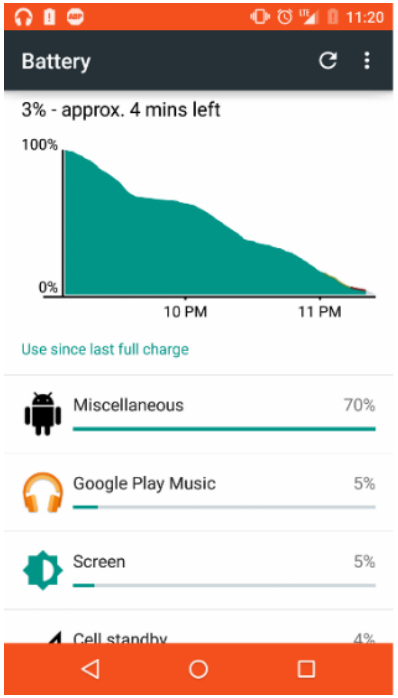
- Mobile storage device (eMMC/UFS)
- Long-term warranty (e.g., 2Y)
- Supports synchronous IO
- Code snippet can access storage space by default
  - E.g., app with no special privileges

Wear-out Attack

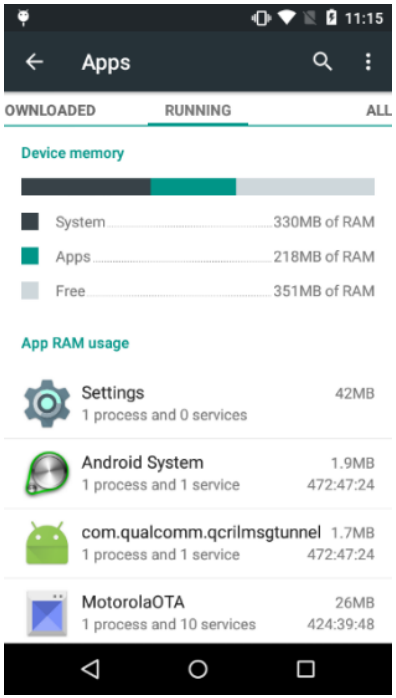
- Prototype Android app with less than 1K lines of code
- No special permission needed
- Stealthily rewrite small files in app's storage space



Run as background service



Only run on charging status



Pause workload on screen lit

Phone Wear-out Experiment Results

BLU
512MB
4GB

< 14 days

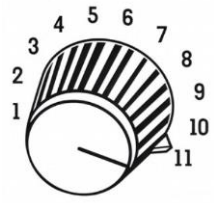
Moto
E 8GB

6 days

~2 weeks

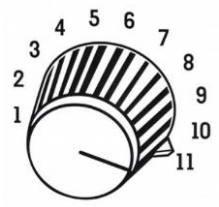
SMG S6
32GB

8 days



SMG S9
64GB

22 days



Phones can be worn out in weeks!

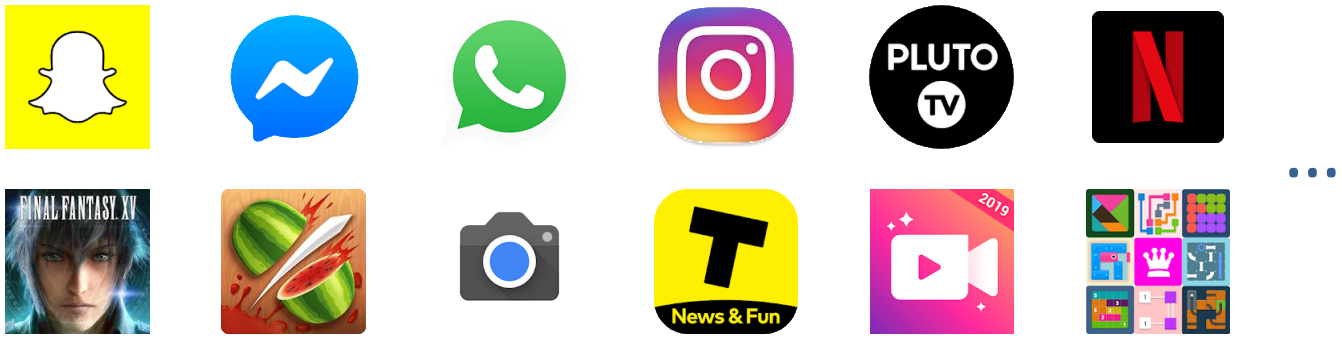
- Mobile flash storage can be worn out quickly

- 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*



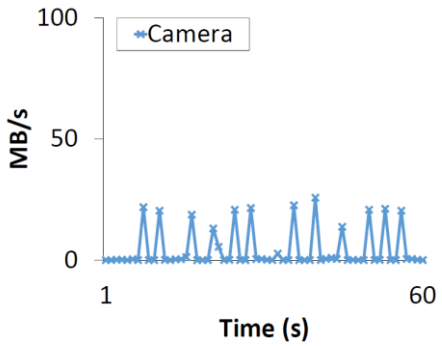
  - I/O-intensive workloads (FTP server, file copies, backup/restore)

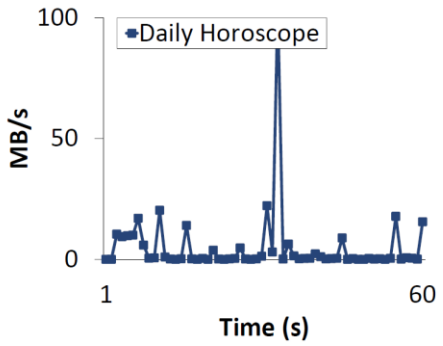
* 23 apps excluded due to various reasons, details in paper

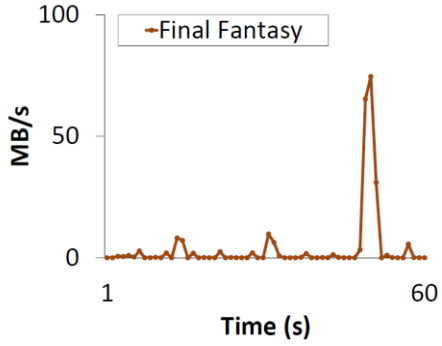
Initial conclusions

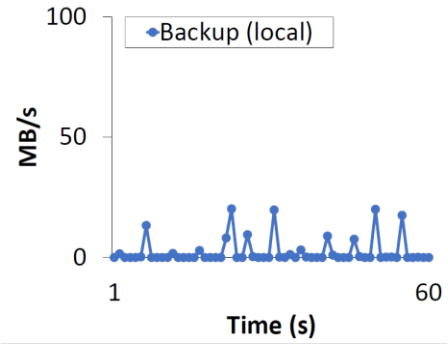
- Most apps don't consume dangerous levels of write bandwidth
  - Most apps are not used most of the time
- Minority of apps are write-intensive
  - Lets look more closely at these "troublemakers"

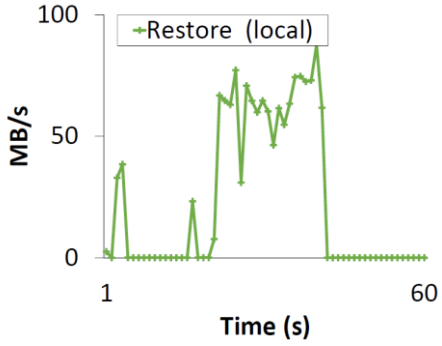
Write-heavy Apps/Workloads

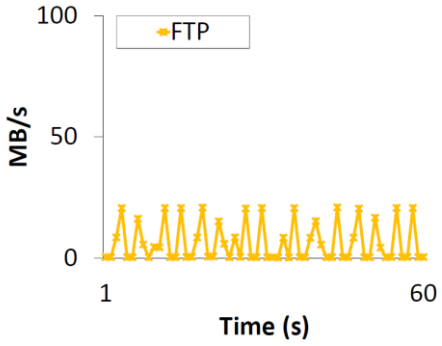


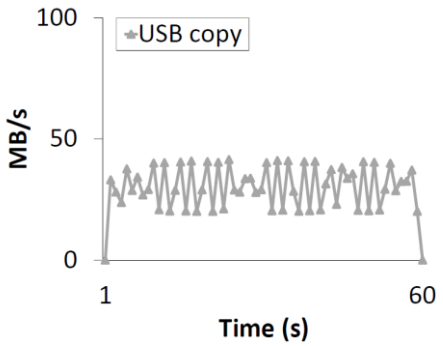






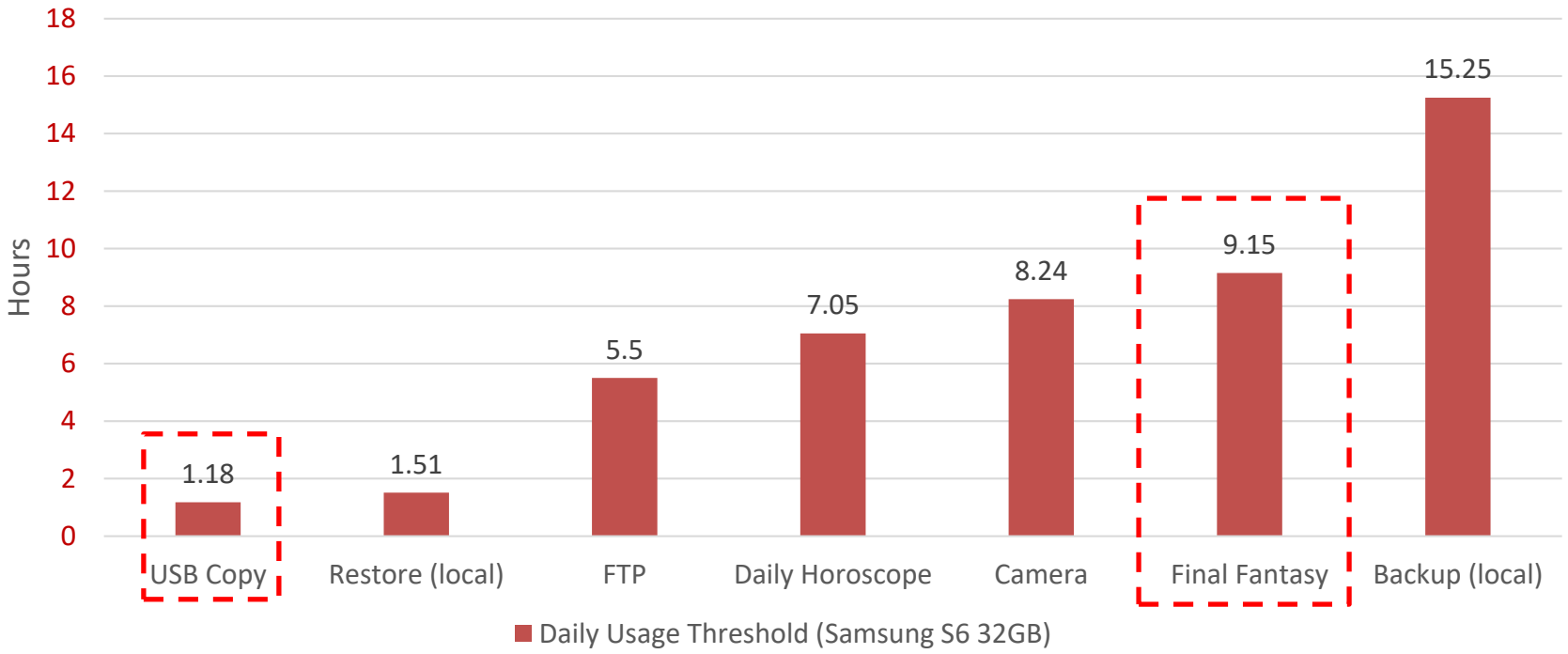






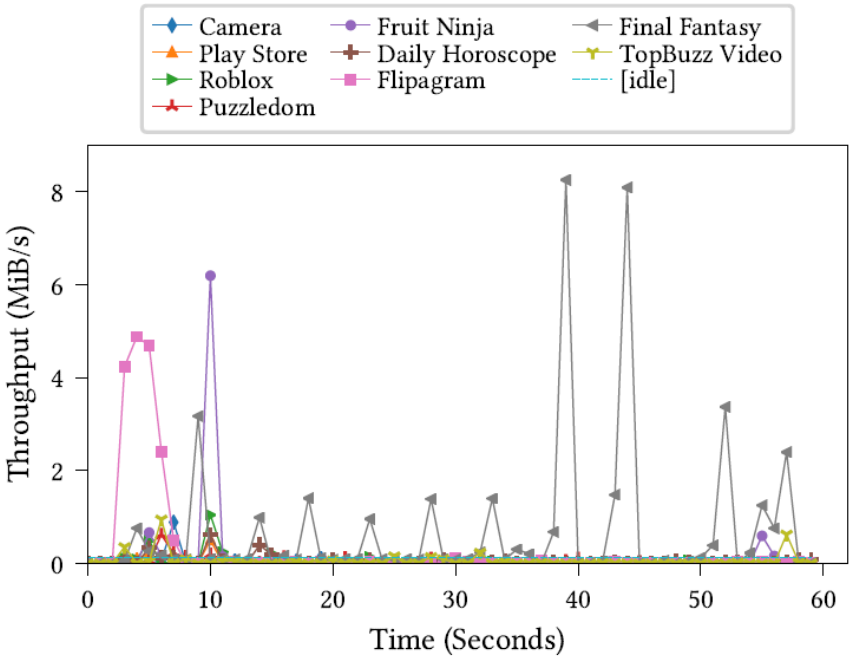
- Apps issue bursts of I/O

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)

App Background I/O Characterization



App	Avg (MB/s)
camera	0.02
dailyhoroscope	0.04
finalfantasy	0.67
flipagram	0.29
fruitninja	0.14
playstore	0.02
puzzledom	0.04
roblox	0.04
topbuzz-video	0.05
idle	0.11

< 1 MB/s

- 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

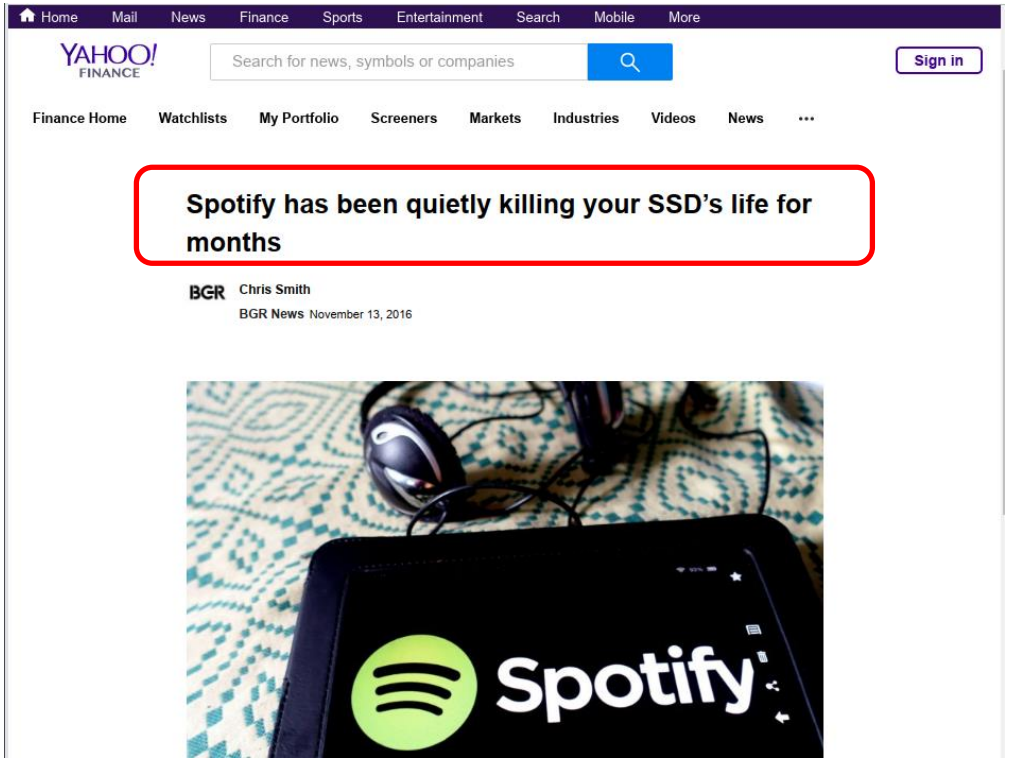
More details in the paper.

- 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



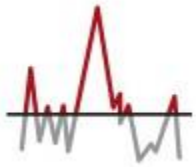
OS-level Wear Management

- 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



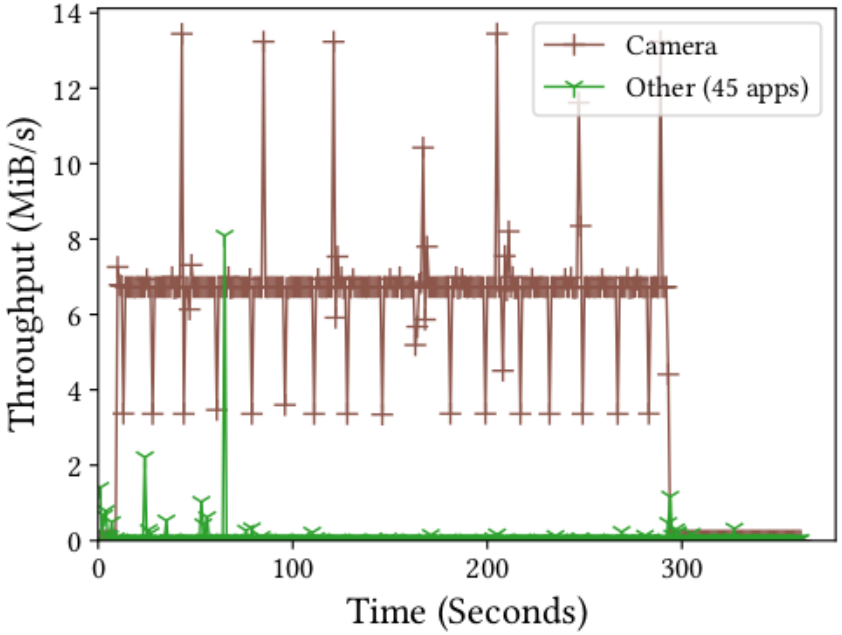
- Apps tend to issue bursty I/O
  - Allocate write (lifetime) slack quota to accommodate bursts

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

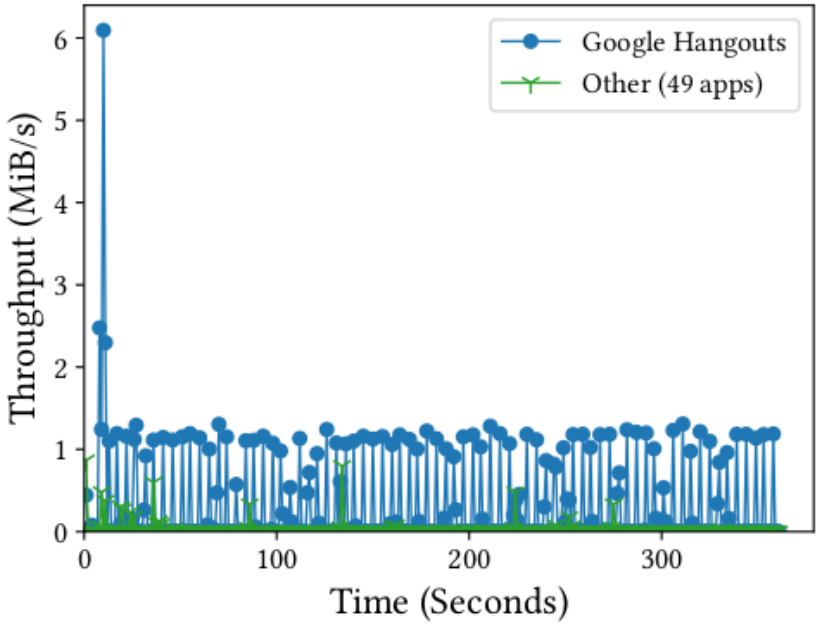
- Foreground vs. background
  - Stricter quota & threshold on background apps (i.e., hourly)

More details in the paper

Evaluation (Write-intensive Apps)



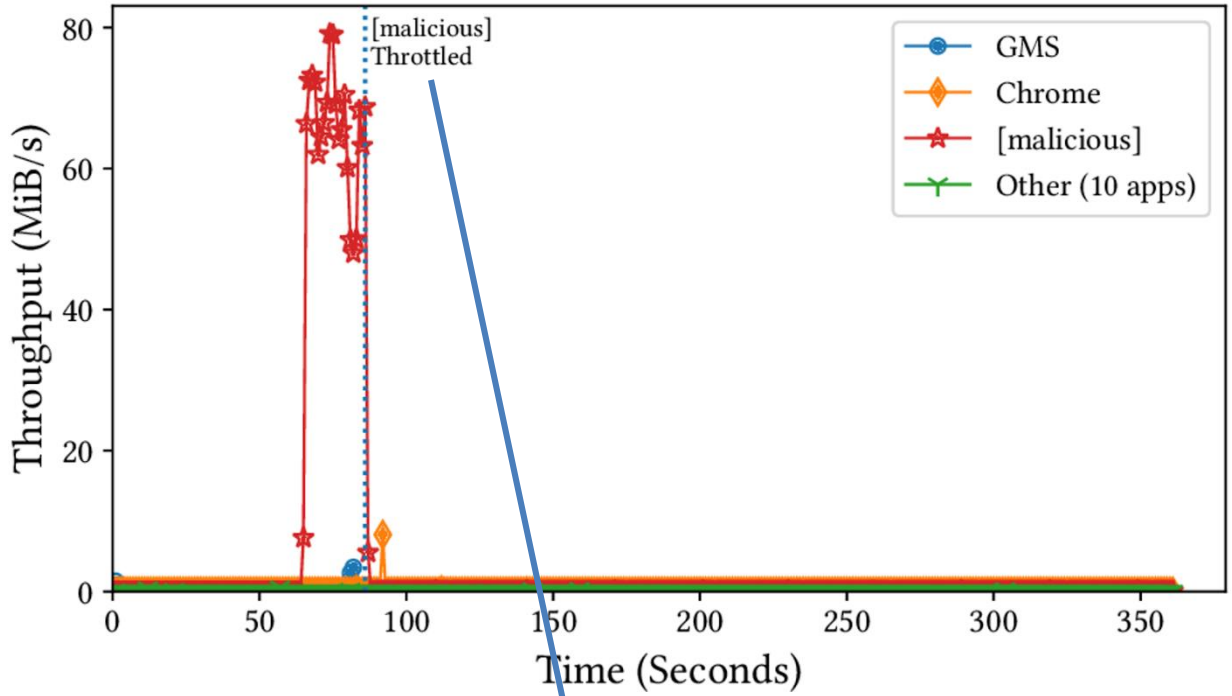
- Video shooting with camera (foreground)
- Bursts are permitted
- ~1.2 hours daily usage without intervention



- 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
- ~80MiB/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

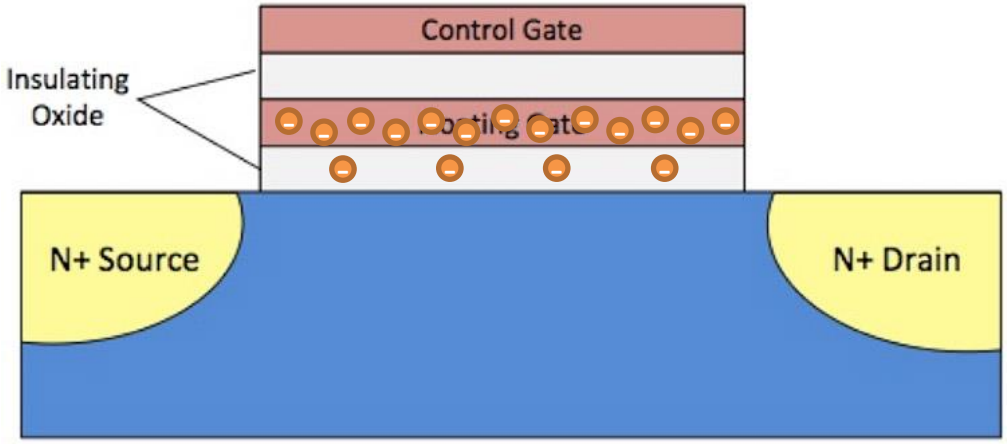
- Flash storage lifespan as depletable resource needs to be managed
  - Embedded devices with flash storage (IoT devices, medical devices, etc.)

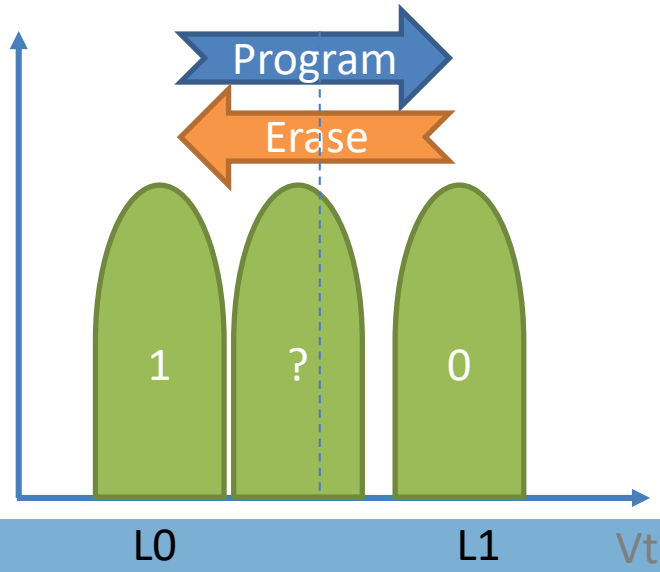
Aviad Zuck
aviadzuc@cs.Technion.ac.il

Backup slides

Flash Internals

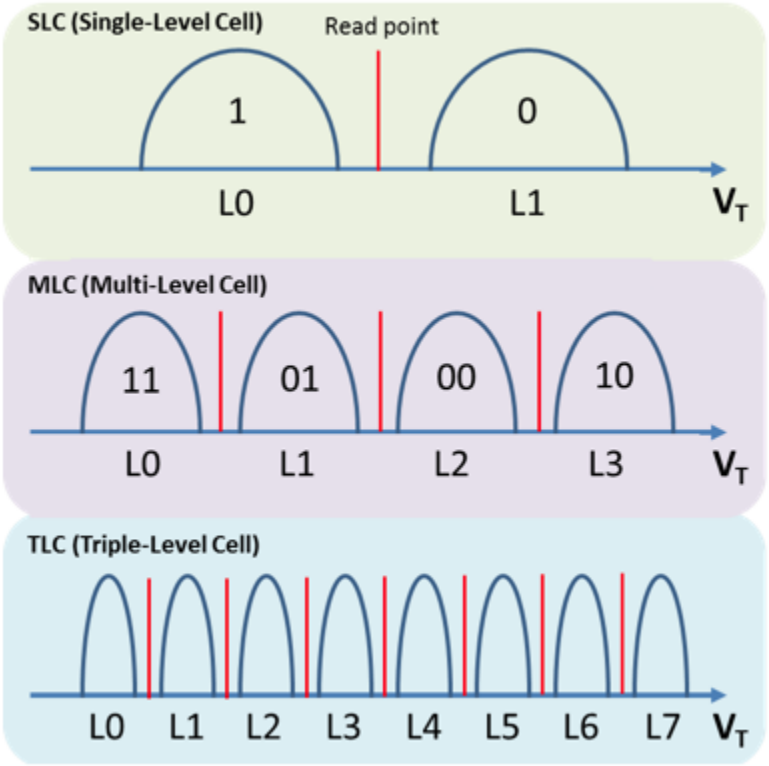
- Floating gate (flash cell)
  - Program (inject electrons)
  - Erase (eject electrons)
  - Electrons trapped in insulating oxide (worn out)





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]



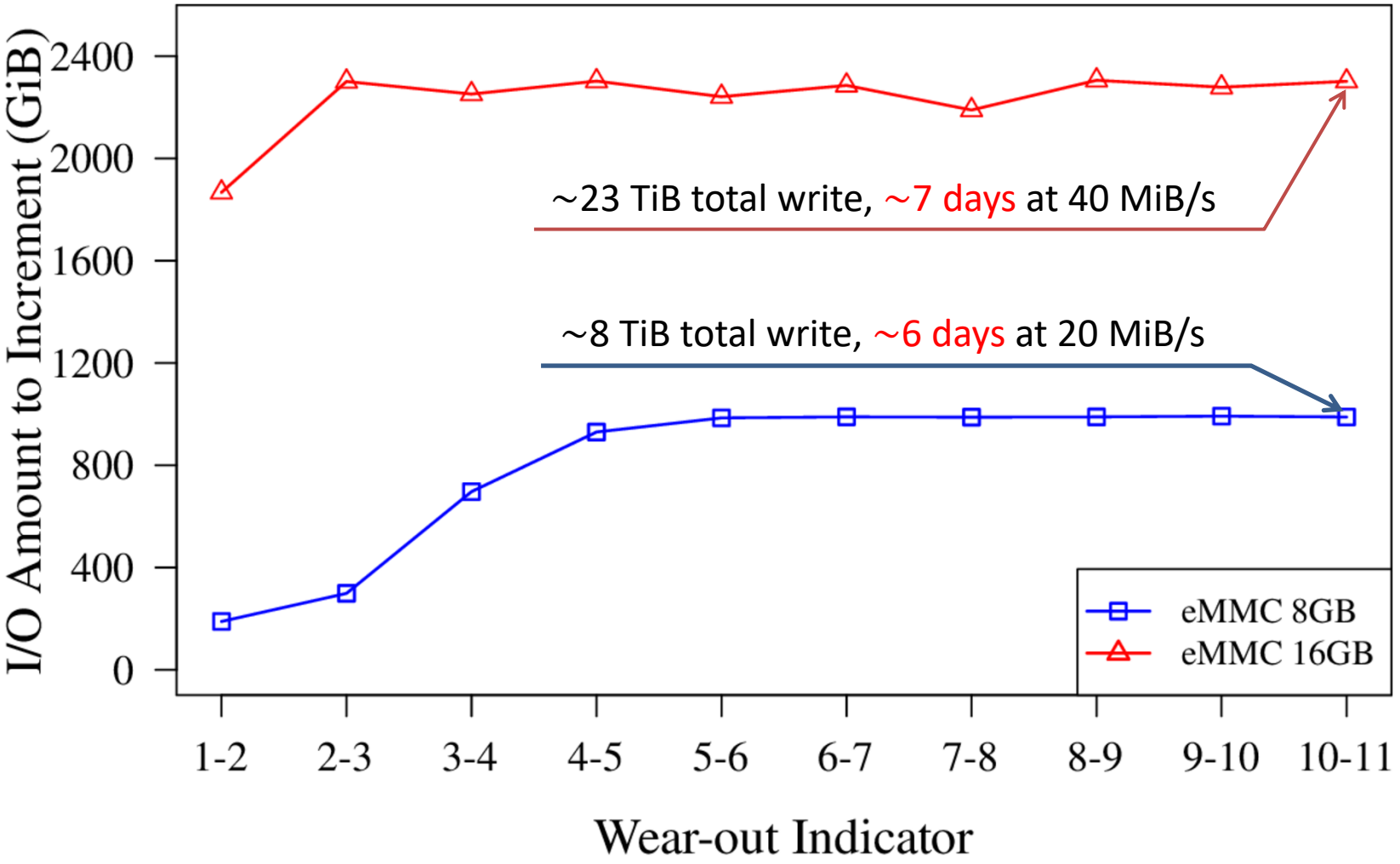
(Source: EE Times)

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`

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

eMMC Flash Chips Can Wear-out in Days

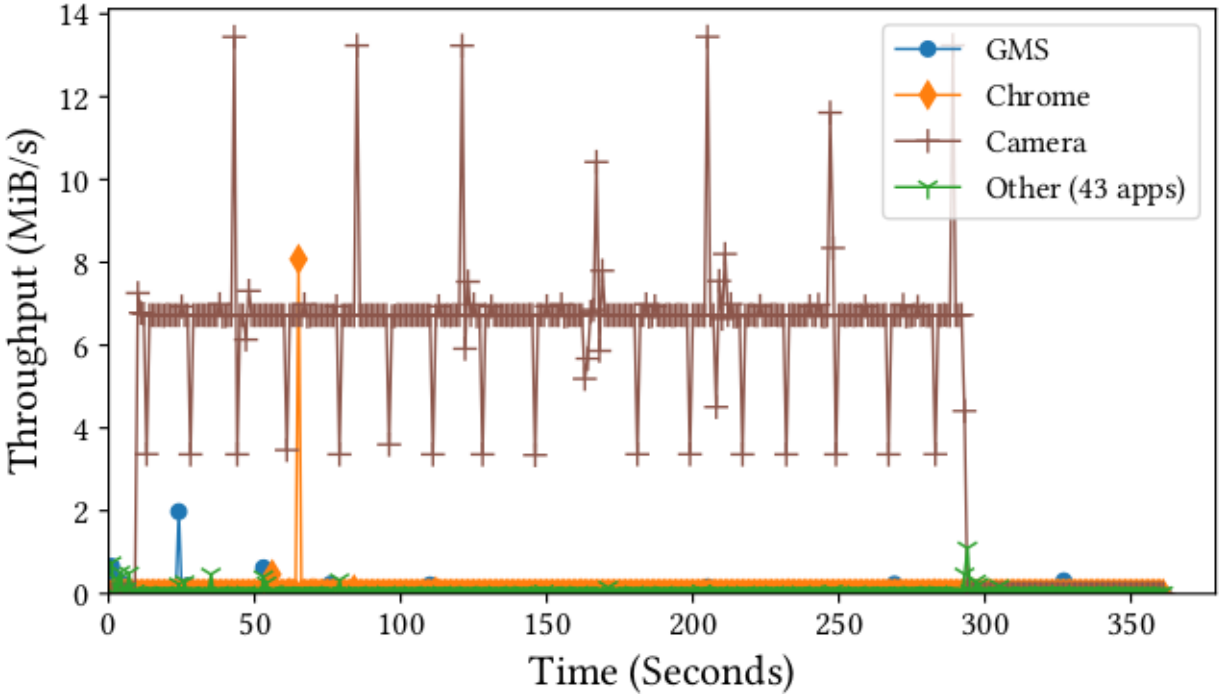


Can apps prematurely wear-out your phone?

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

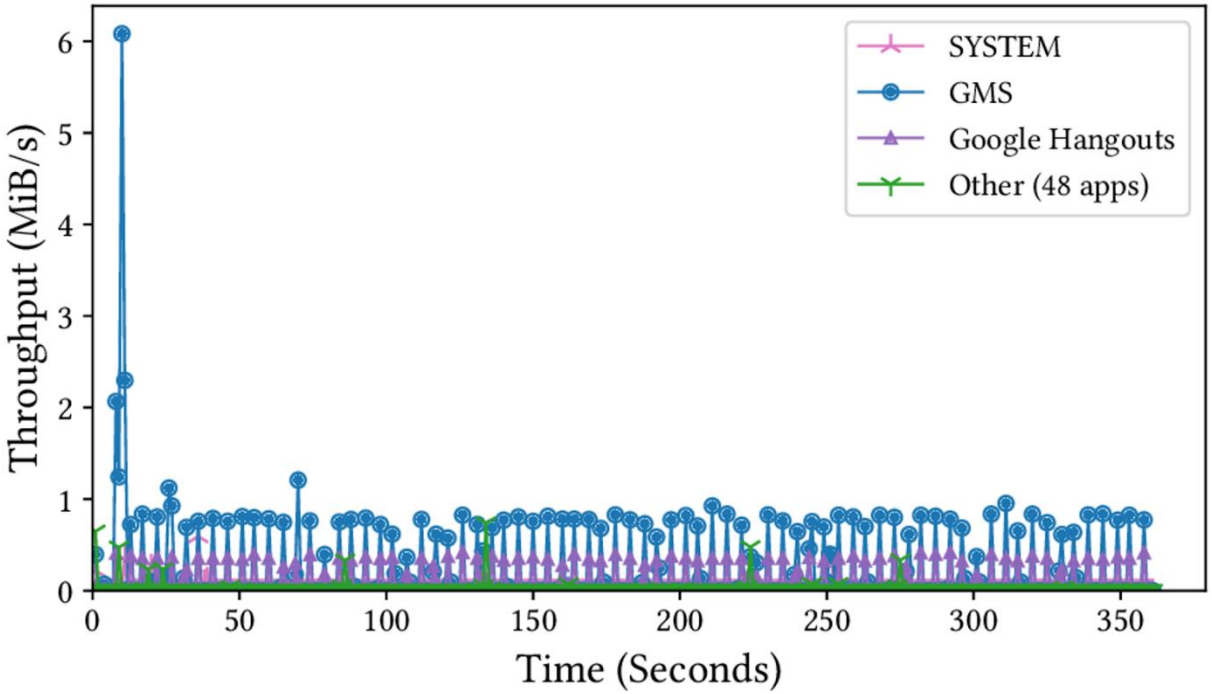
- Most write-heavy usage scenarios are neither long-term operations nor frequently used
- Reasonable length of app usage is not long enough to shorten lifetime

Evaluation (Foreground)



- Video shooting with ~7MiB/s write activity
- ~1.2 hours daily usage without intervention
- May exceed , for short time

Evaluation (Background)



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

Benign apps run with no/minimum disruption