GANGRENE: Exploring the Mortality of Flash Memory

Robert Templeman

Naval Surface Warfare Center, Crane Division

Indiana University

Apu Kapadia

Indiana University





Flash memory is ubiquitous



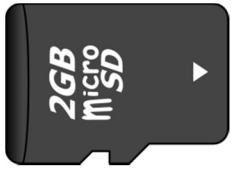




http://www.flickr.com/photos/sucello/6220857499/



http://www.clker.com/cliparts/1/a/c/c/1197098931277351227PanamaG_Playstation_3.svg.hi.png





http://www.flickr.com/photos/intel_italia/6150057911/sizes/l/in/photostream/

Flash memory is ubiquitous



http://www.rugged.com/sites/default/files/product/img/e112.jpg



http://www.engineerlive.com/media/images/large/large_Logix_Family.jpg



http://images.nitrobahn.com.s3.amazonaws.com/wp-content/uploads/2010/08/Harman-Infotainment-for-Fiat-Chrysler.jpg

51227PanamaG_Playstation_3.svg.hi.png

Flash memory is fast, rugged, and cheap



Crucial M4 - Solid state drive - internal - 128 GB - 2.5" - Serial ...

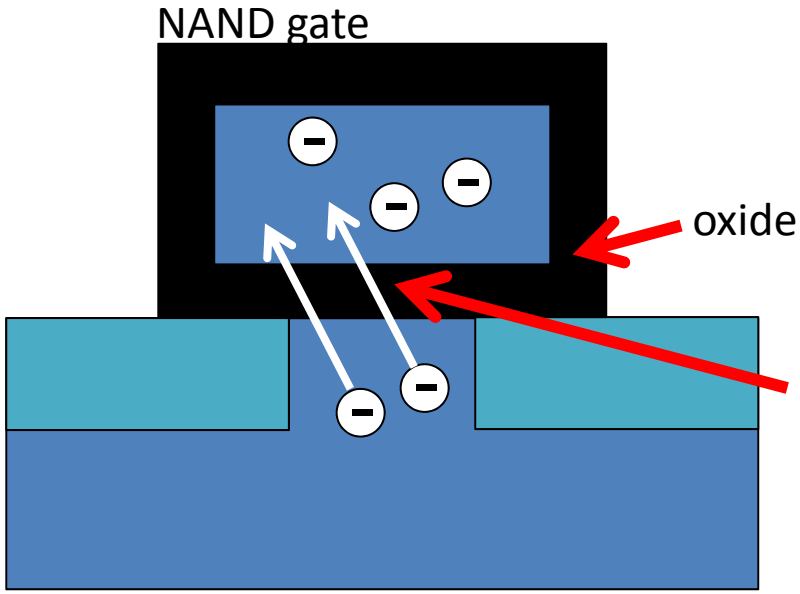
$110 from 192 stores

Internal - 128 GB - Crucial - SATA - Solid State

★★★★½ 218 reviews

…but flash memory has a weakness

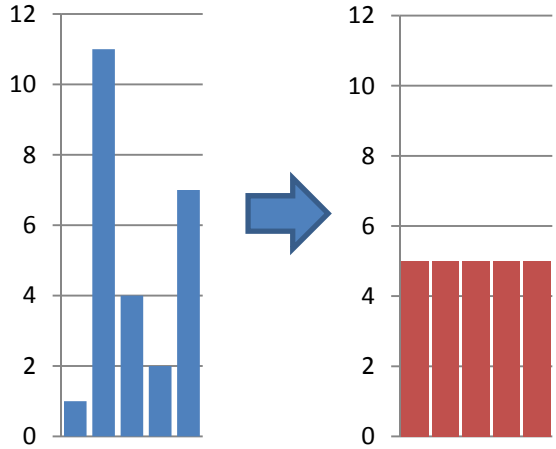
finite write endurance



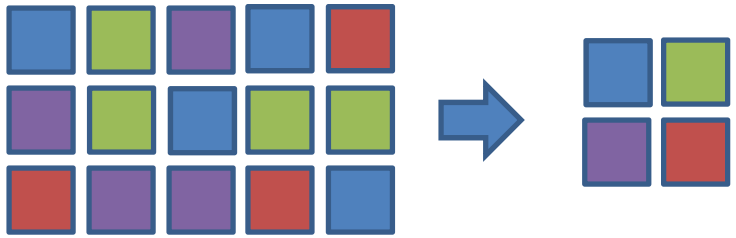
Architecture	Endurance (PE cycles)
SLC	~100,000
MLC	~10,000
TLC	<1,000

"depletable storage" – *both capacity and write endurance are limited constraints, Prabhakaran (HOTSTORAGE 2010)*

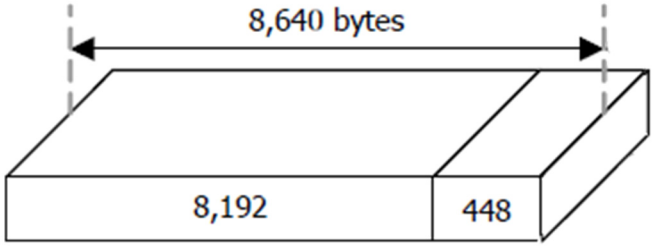
Various strategies are used to increase flash endurance



wear-leveling

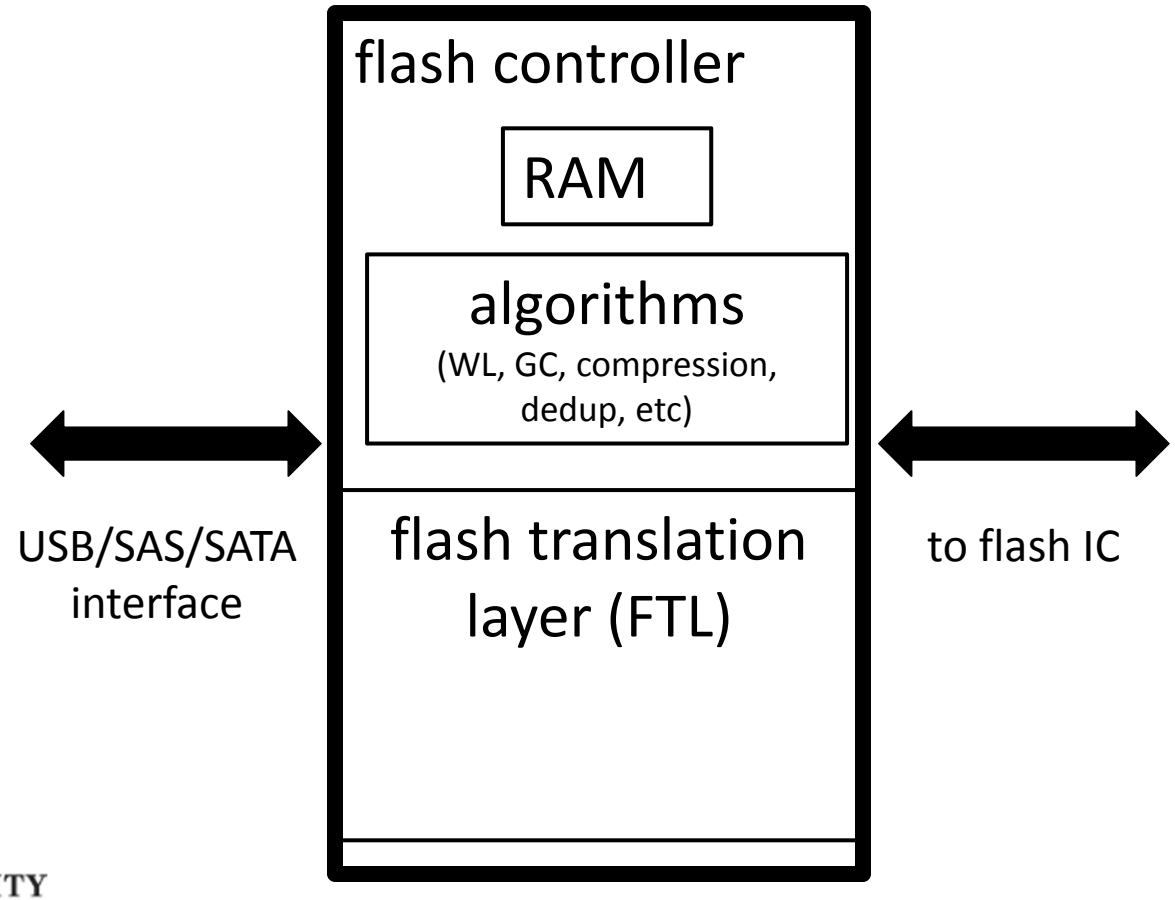


deduplication



error correction codes

Flash controllers employ these strategies and manage flash



Flash memory is generally tested under “normal” use

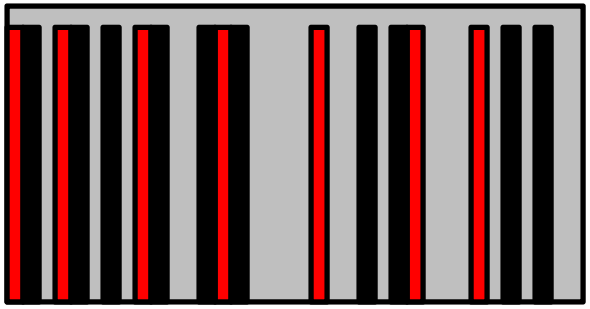


http://www.jokes4oldfolks.com/2011_11_01_archive.html

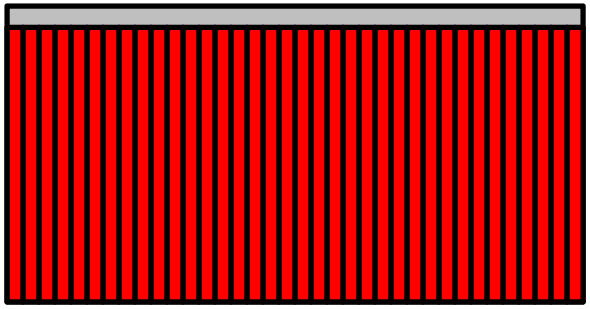
vs



http://image.mustang50magazine.com/f/eventcoverage/m5lp_1001_2009_mustang_week/31020948+w200/m5lp_1001_10_+2009_mustang_week+drifting.jpg



READ
WRITE



GANGRENE seeks to induce premature death of flash

Goals:

- maximally accelerate wear
- attack with no a priori knowledge
- passively evade detection

What is the meaning of LIFE?

$$LIFE = \frac{C \times E_{max}}{A}$$

$LIFE$ – device life expressed in GB written

C – published device capacity in GB

E_{max} – rated PE cycles (vendor provided)

A – acceleration factor ($LIFE$ is reduced for A > 1)

What is the meaning of LIFE?

Example

2GB device with endurance rating of 3,000 cycles dies after 600 GB are written:

$$A = \frac{C \times E_{max}}{LIFE} = \frac{2\ \text{GB} \times 3{,}000}{600\ \text{GB}} = 10$$

This device experienced a 10x acceleration in degradation

We implemented GANGRENE

GANGRENE in C

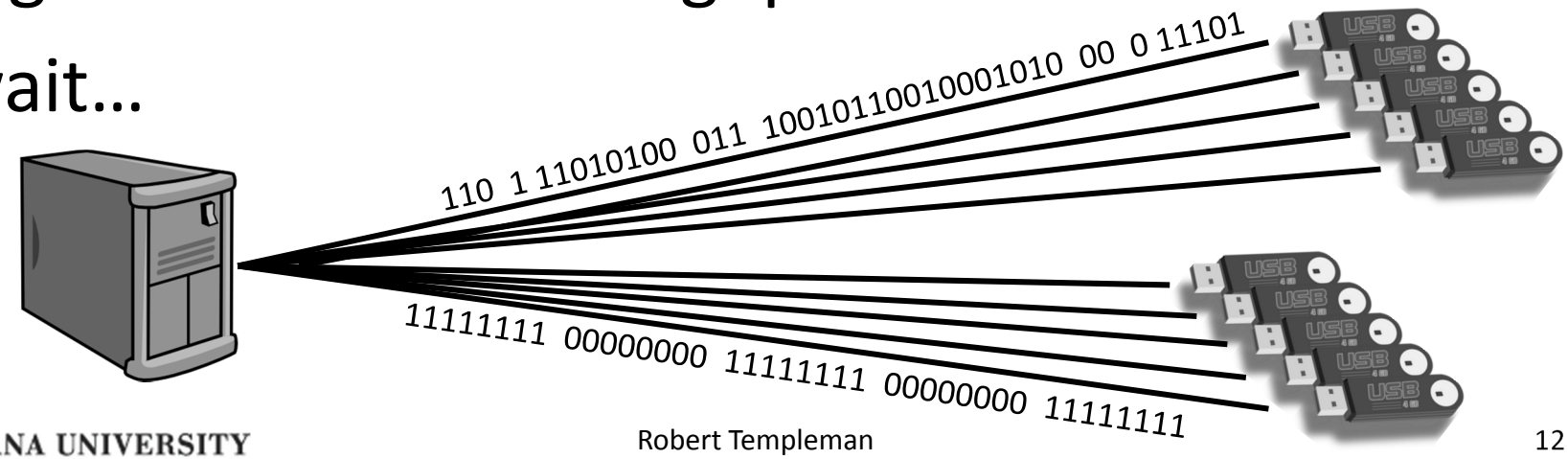
maximize write activity

vary file size

vary file contents

log and monitor throughput

wait…



For our random protocol we observed a mean acceleration of 15.94

Drive #	C (GB)	E_{max}	$LIFE$ (GB)	A
1	2	3,000	204.6	29.33
2	2	3,000	414.9	14.46
3	2	3,000	450.2	13.33
4	2	3,000	627.1	9.57
5	2	3,000	461.5	13.00

$$\mu_A = 15.94$$
$$\sigma_A = 7.71$$

These drives failed in 14-29 days

These results are 'out of the box' (no tuning)

For our test drives we observed a mean acceleration of 15.94

Drive #	$LIFE$ (GB)	C(GB)	E_{max}	A

no failures from the deterministic protocol drives after 6 months!

still going…

What is death like?

- denial to write
- failure may preserve existing data
- failure is not always permanent
- failure occurs with no warning

What about other flash devices?



What about other flash devices?





What about other flash devices?





http://www.flickr.com/photos/sucello/6220857499/



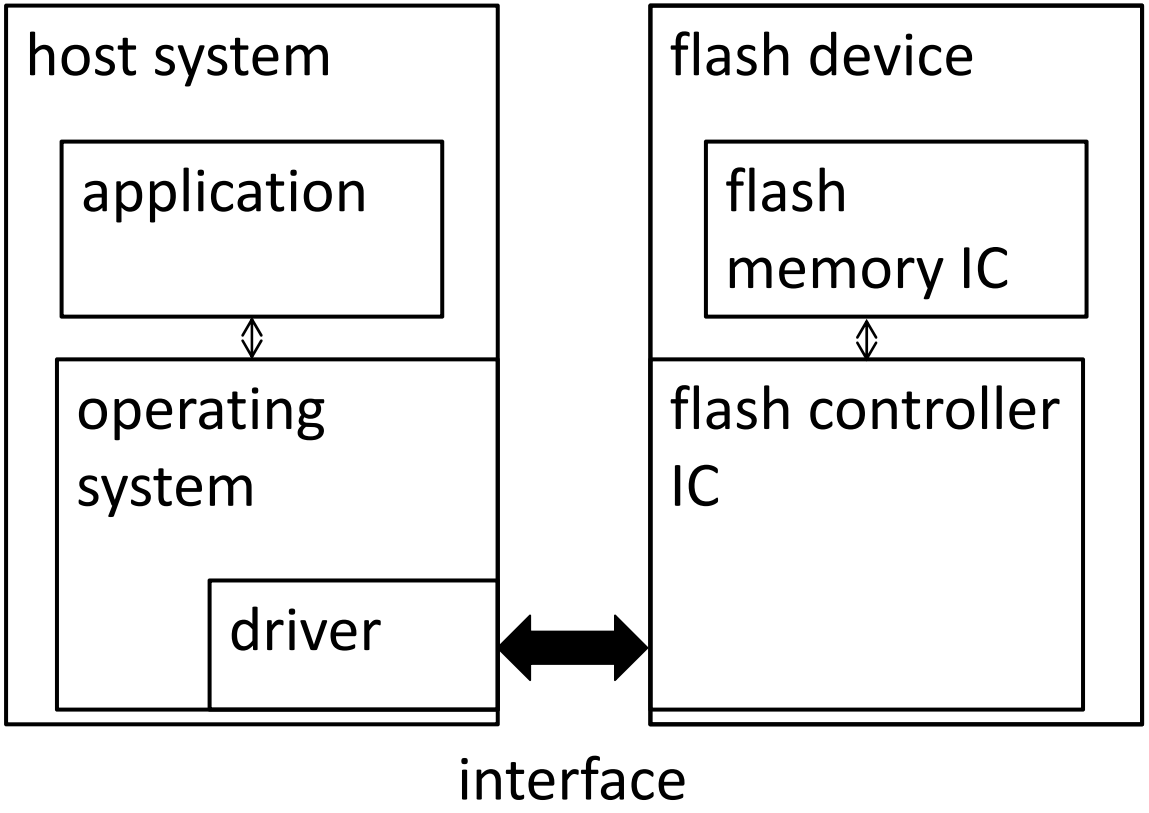


http://www.flickr.com/photos/intel_de/5567056659/

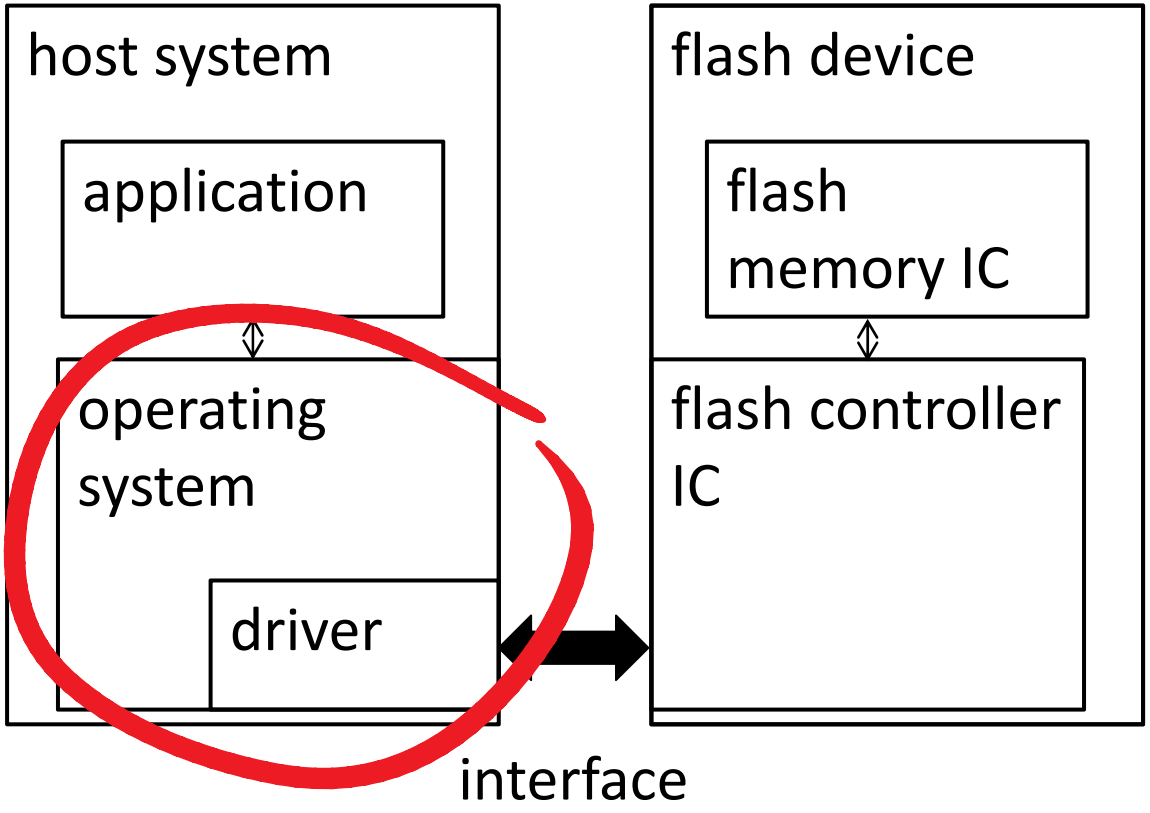
Can GANGRENE do better?

- we still know very little about flash vulnerability
- can A be increased?
- more testing is necessary

How can we defend against GANGRENE?



How can we defend against GANGRENE?

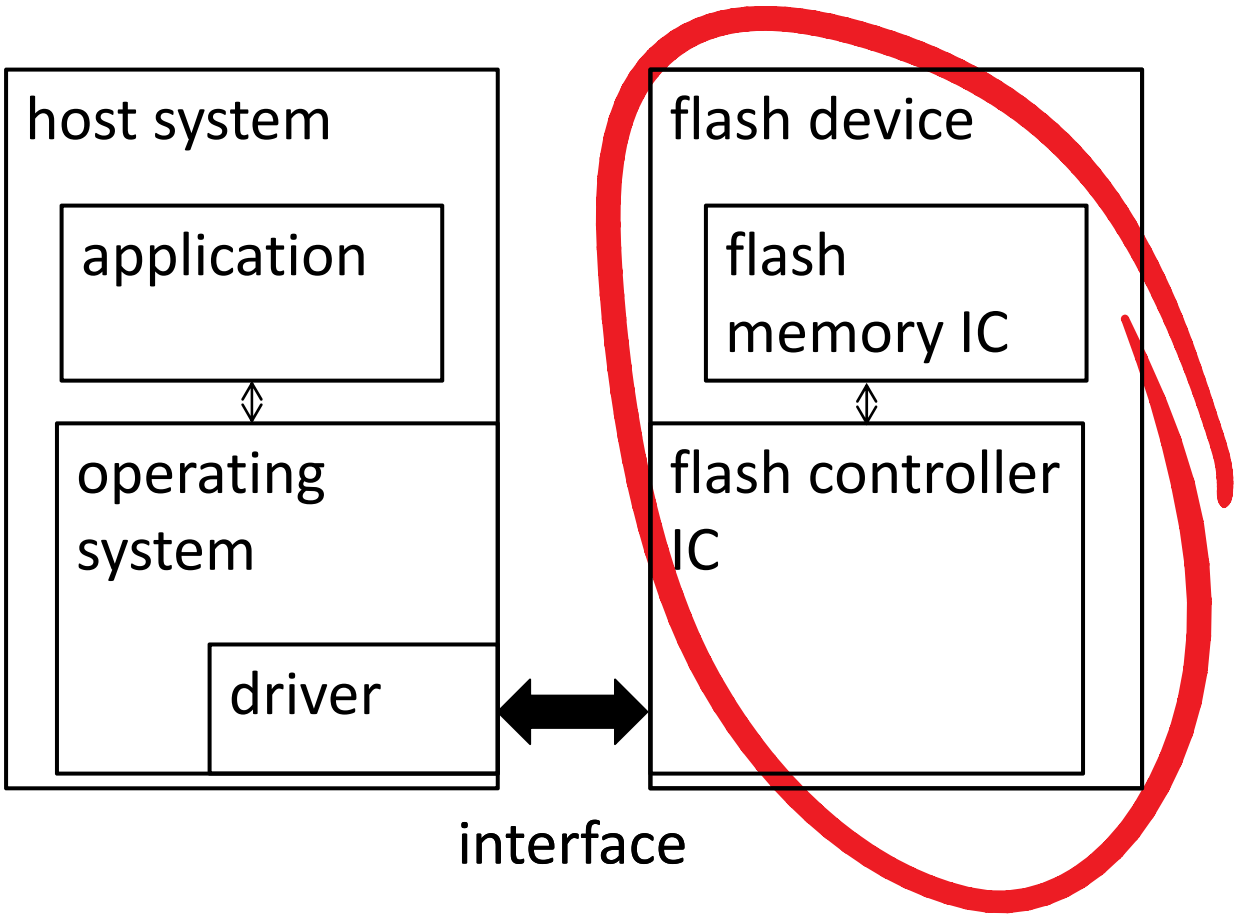


monitor I/O use

display

detect

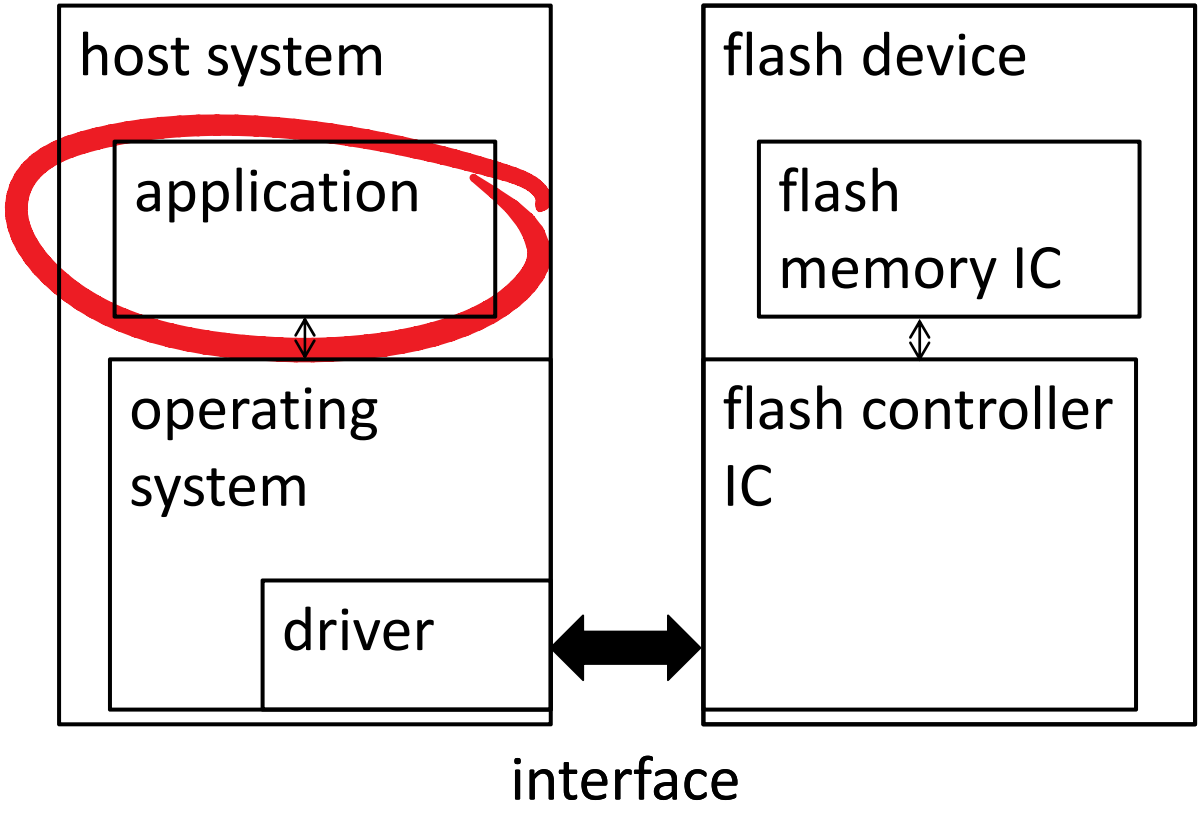
How can we defend against GANGRENE?



visibility of wear

fine-grained write control

How can we defend against GANGRENE?



don‘t be write promiscuous

More work is needed to bolster flash devices against malicious use

- we rely on many devices that use flash memory
- our results show that failure occurs completely and without warning
- are SSDs and mobile devices vulnerable to GANGRENE?