FlashGuard: Leveraging Intrinsic Flash Properties to Defend Against Encryption Ransomware

Jian Huang [†, ‡]

Jun Xu   Xinyu Xing   Peng Liu   Moinuddin K. Qureshi [†]

[†] Georgia Institute of Technology

[‡] ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

PennState

May 12, 2017

WannaCry

Ransomware Attack

May 12, 2017

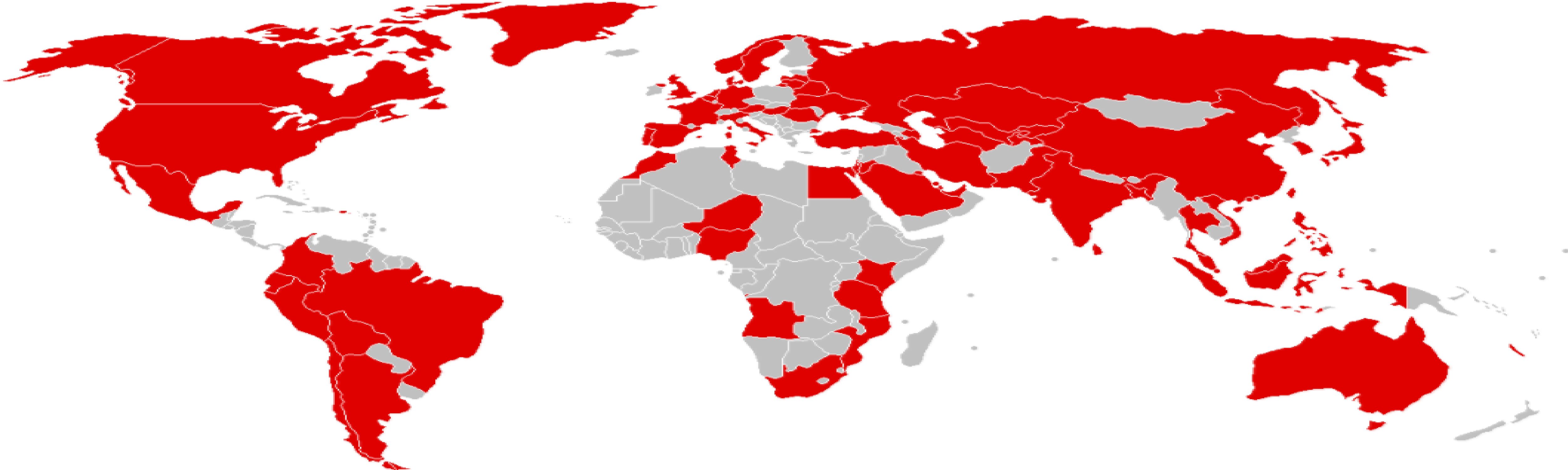
WannaCry

Ransomware Attack

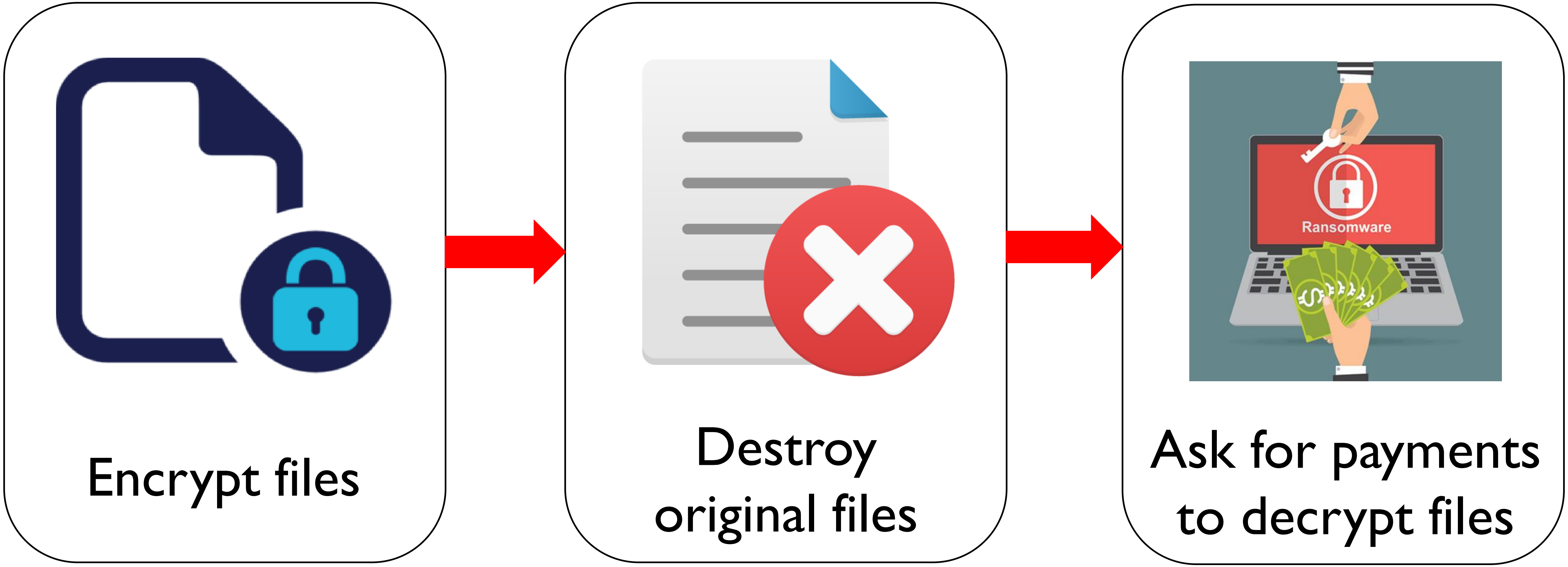
230,000+ computers

150+ countries

$300-$600 per ransom



What Is Encryption Ransomware?

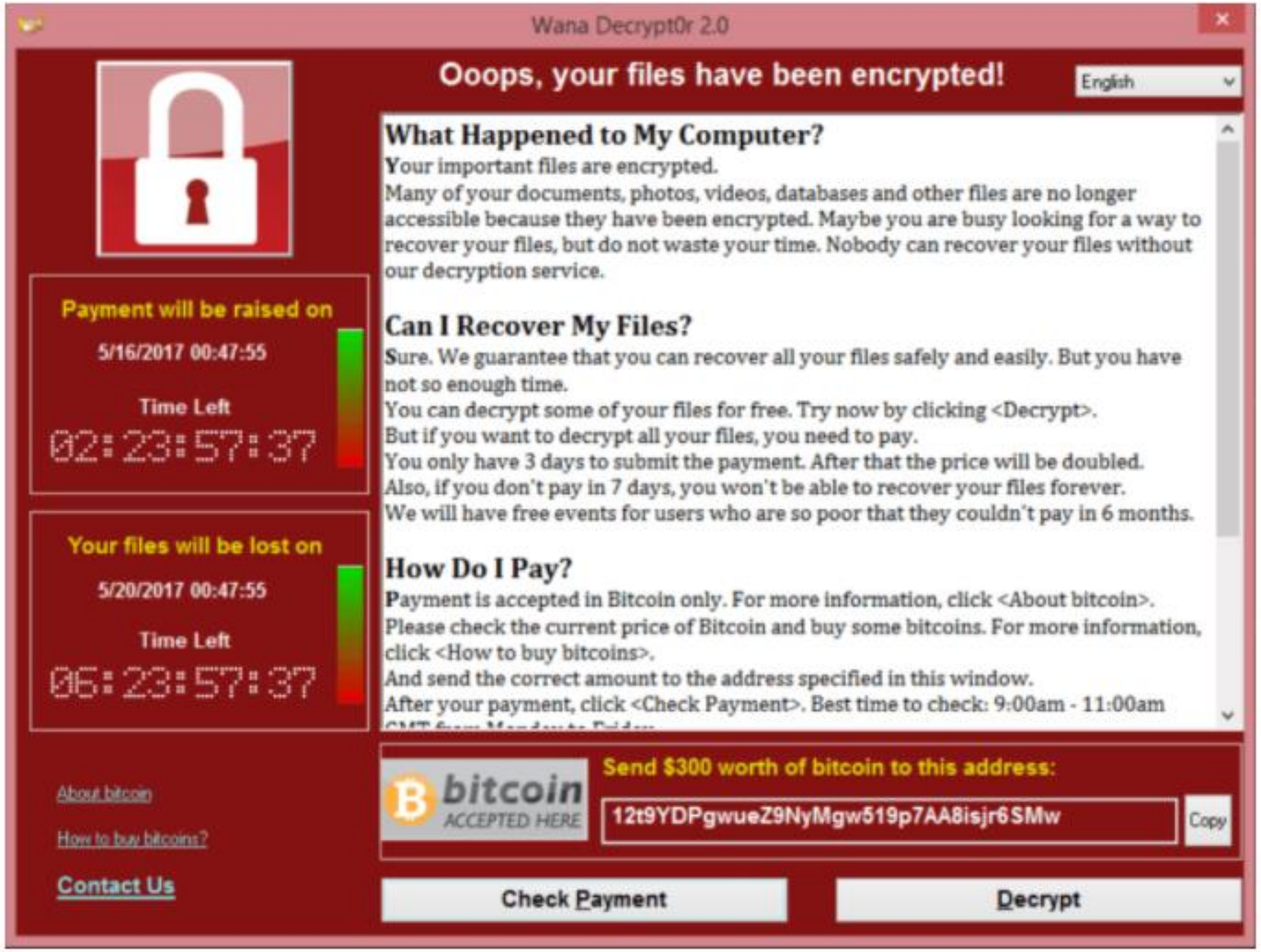


Encrypt files

Destroy original files

Ask for payments to decrypt files

What Is Encryption Ransomware?



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

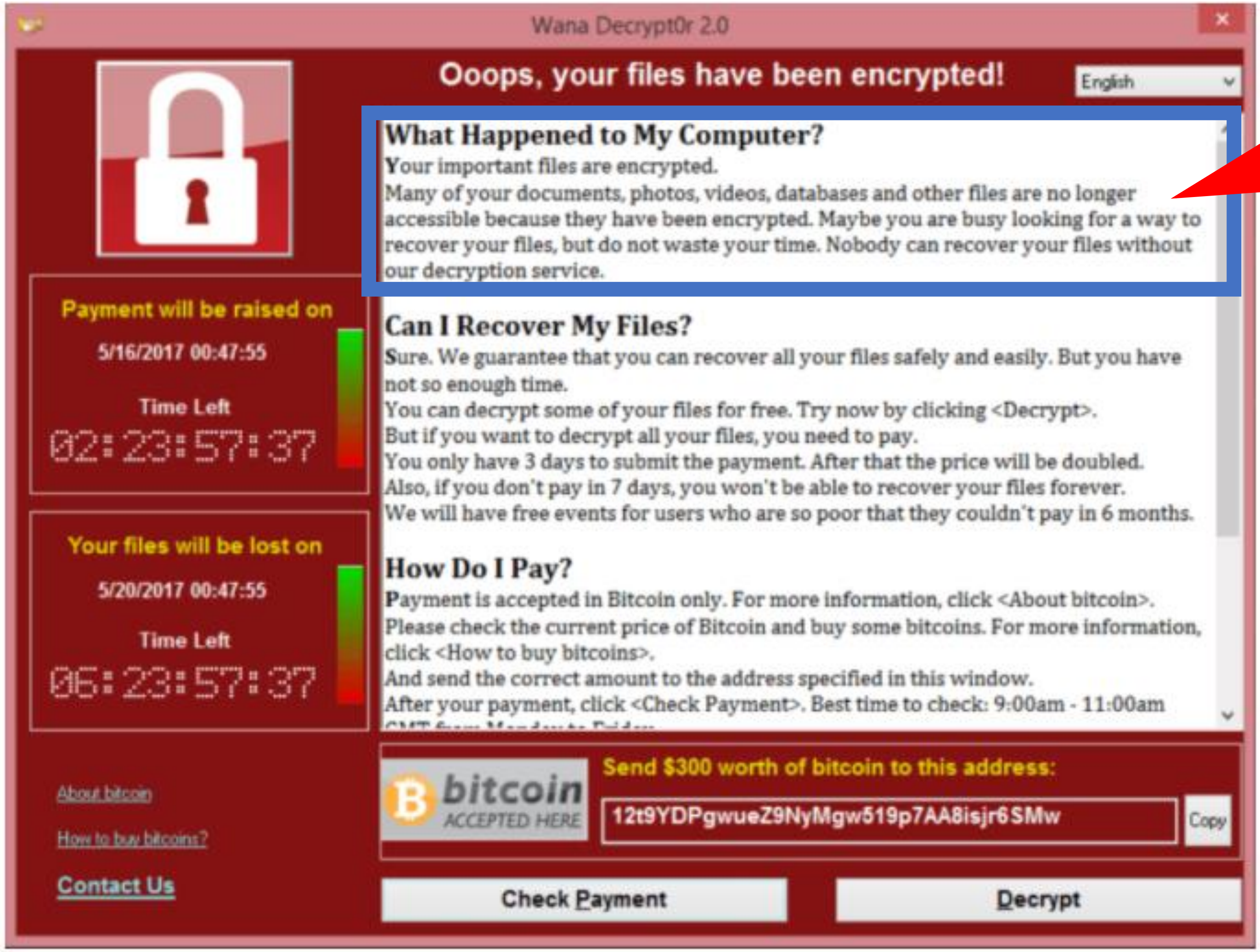
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

What Is Encryption Ransomware?



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

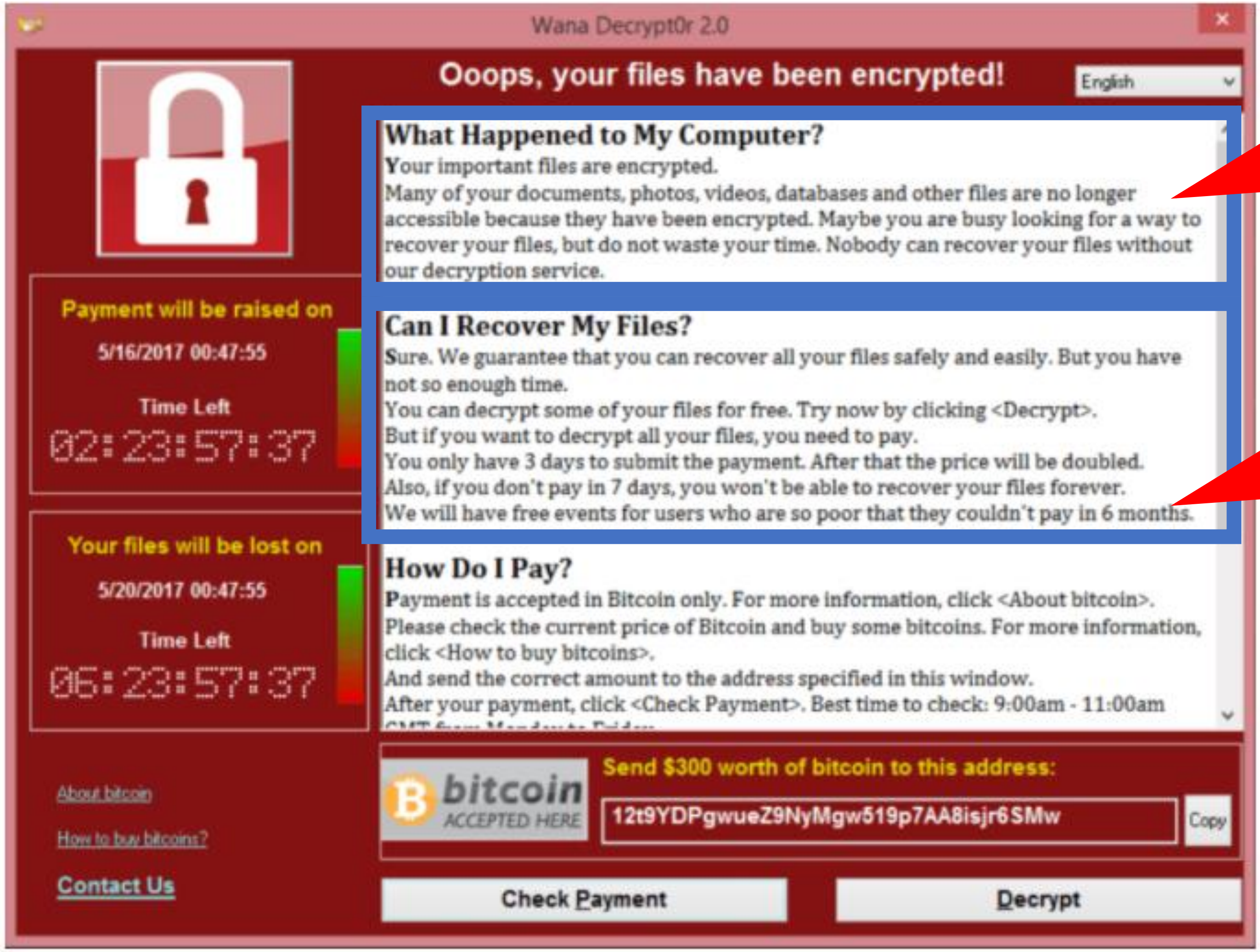
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

A ransom notification: users files have been encrypted

What Is Encryption Ransomware?



Ooops, your files have been encrypted!

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

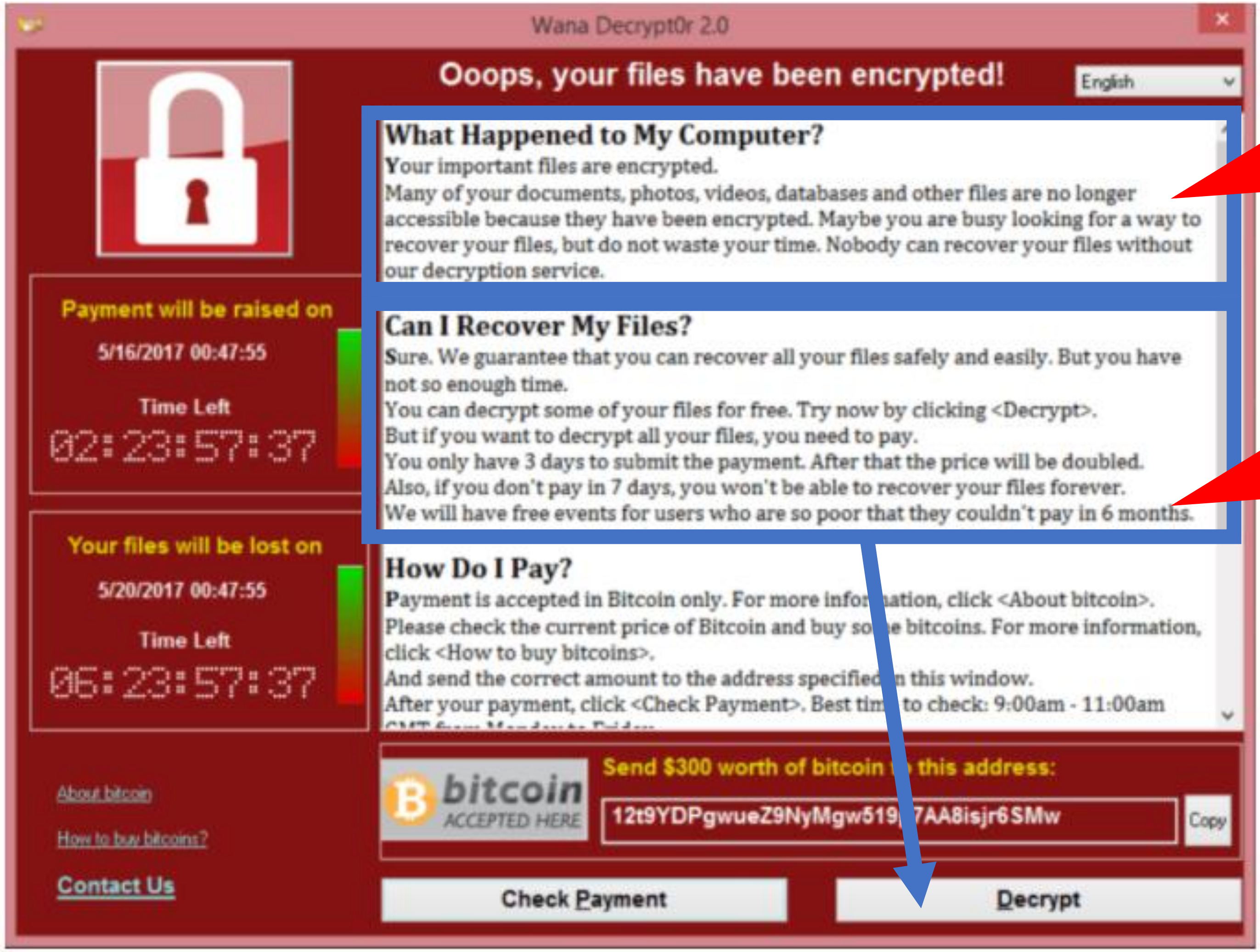
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

A ransom notification: users files have been encrypted

Pay ransom to recover user files

What Is Encryption Ransomware?



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Payment will be raised on

5/16/2017 00:47:55

Time Left

02:23:57:37

Your files will be lost on

5/20/2017 00:47:55

Time Left

06:23:57:37

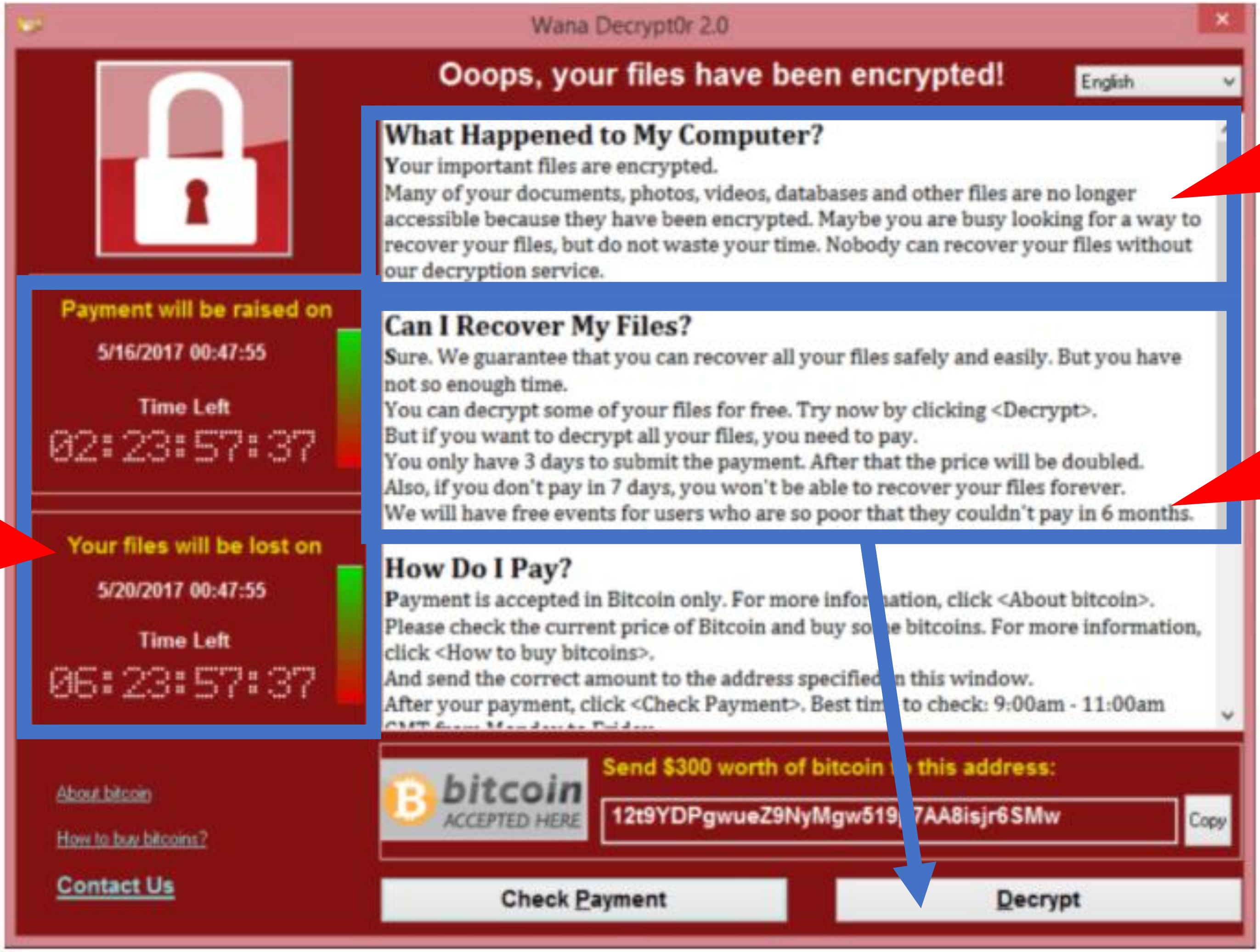
Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

A ransom notification: users files have been encrypted

Pay ransom to recover user files

What Is Encryption Ransomware?



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

A ransom notification: users files have been encrypted

Pay ransom to recover user files

More ransom required if the payment is delayed

Characteristics of Encryption Ransomware

Family	#Samples
Petya	14
CTB-Locker	119
Jigsaw	5
Mobef	7
Maktub	10
Stampado	42
Cerber	29
Locky	344
7ev3n	16
TeslaCrypt	75
HydraCrypt	13
CryptoFortree	4
CrytoWall	799
Total	1477

Characteristics of Encryption Ransomware

Family	#Samples
Petya	14
CTB-Locker	119
Jigsaw	5
Mobef	7
Maktub	10
Stampado	42
Cerber	29
Locky	344
7ev3n	16
TeslaCrypt	75
HydraCrypt	13
CryptoFortree	4
CrytoWall	799
Total	1477

How long does it take for ransomware to finish the attack?

Characteristics of Encryption Ransomware

Family	#Samples	Attack Time (minutes)
Petya	14	2
CTB-Locker	119	14
Jigsaw	5	16
Mobef	7	16
Maktub	10	22
Stampado	42	27
Cerber	29	37
Locky	344	43
7ev3n	16	44
TeslaCrypt	75	44
HydraCrypt	13	70
CryptoFortree	4	75
CrytoWall	799	75
Total	1477	

Ask for ransom quickly

Characteristics of Encryption Ransomware

Family	#Samples	Attack Time (minutes)	Backup Spoliation
Petya	14	2	✗
CTB-Locker	119	14	✗
Jigsaw	5	16	✗
Mobef	7	16	✗
Maktub	10	22	✓
Stampado	42	27	✗
Cerber	29	37	✓
Locky	344	43	✓
7ev3n	16	44	✓
TeslaCrypt	75	44	✓
HydraCrypt	13	70	✓
CryptoFortree	4	75	✓
CrytoWall	799	75	✓
Total	1477		

Characteristics of Encryption Ransomware

Family	#Samples	Backup Spoliation
Petya	14	✗
CTB-Locker	119	✗
Jigsaw	5	✗
Mobef	7	✗
Maktub	10	✓
Stampado	42	✗
Cerber	29	✓
Locky	344	✓
7ev3n	16	✓
TeslaCrypt	75	✓
HydraCrypt	13	✓
CryptoFortree	4	✓
CrytoWall	799	✓
Total	1477	

Many ransomware attempt to delete backup files

(and bypass User Access Control)

Why Existing Solutions Are Not Good Enough?

Malware detection

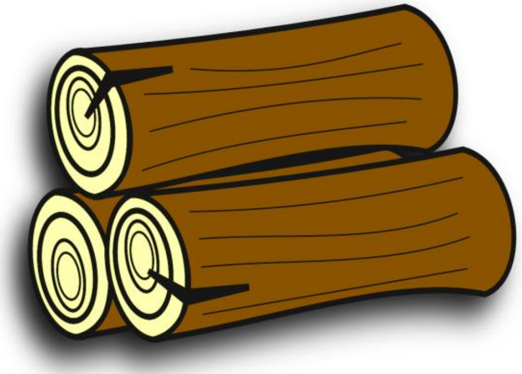
Why Existing Solutions Are Not Good Enough?

Malware detection

Damage has already happened when ransomware is detected

Why Existing Solutions Are Not Good Enough?

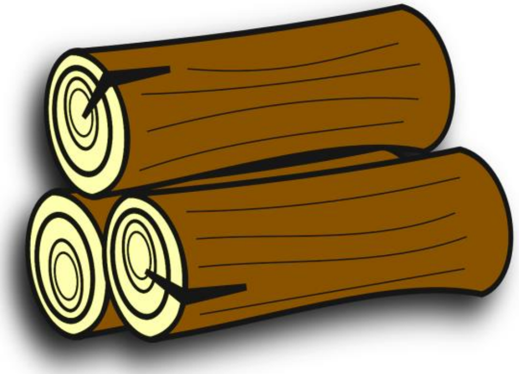
Malware detection



Journaling &
log-structured FS

Why Existing Solutions Are Not Good Enough?

Malware detection

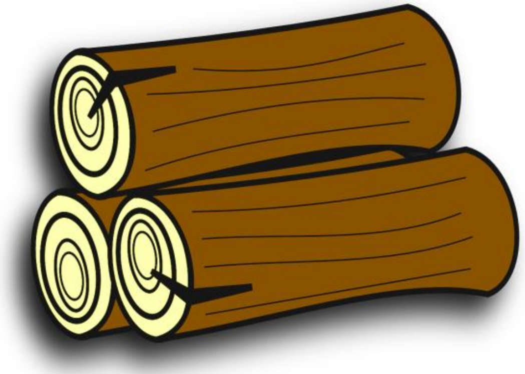


Journaling &
log-structured FS

Ransomware with kernel privilege can destroy data backups

Why Existing Solutions Are Not Good Enough?

Malware detection

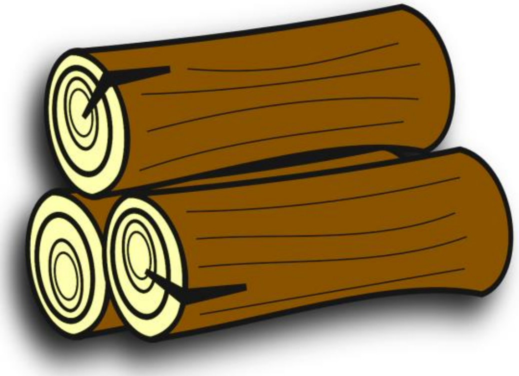


Journaling & log-structured FS

Networked & Cloud Storage

Why Existing Solutions Are Not Good Enough?

Malware detection

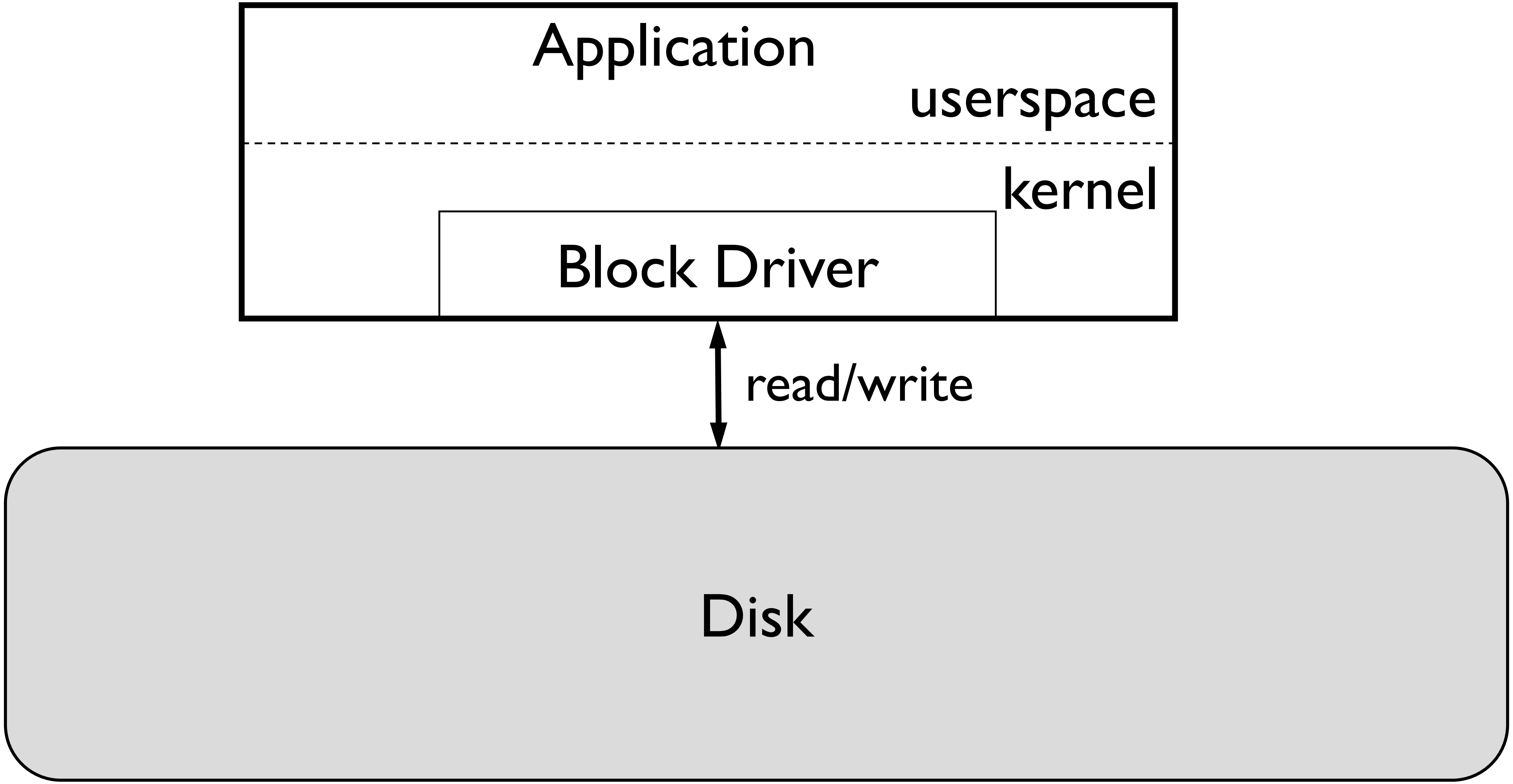


Journaling & log-structured FS

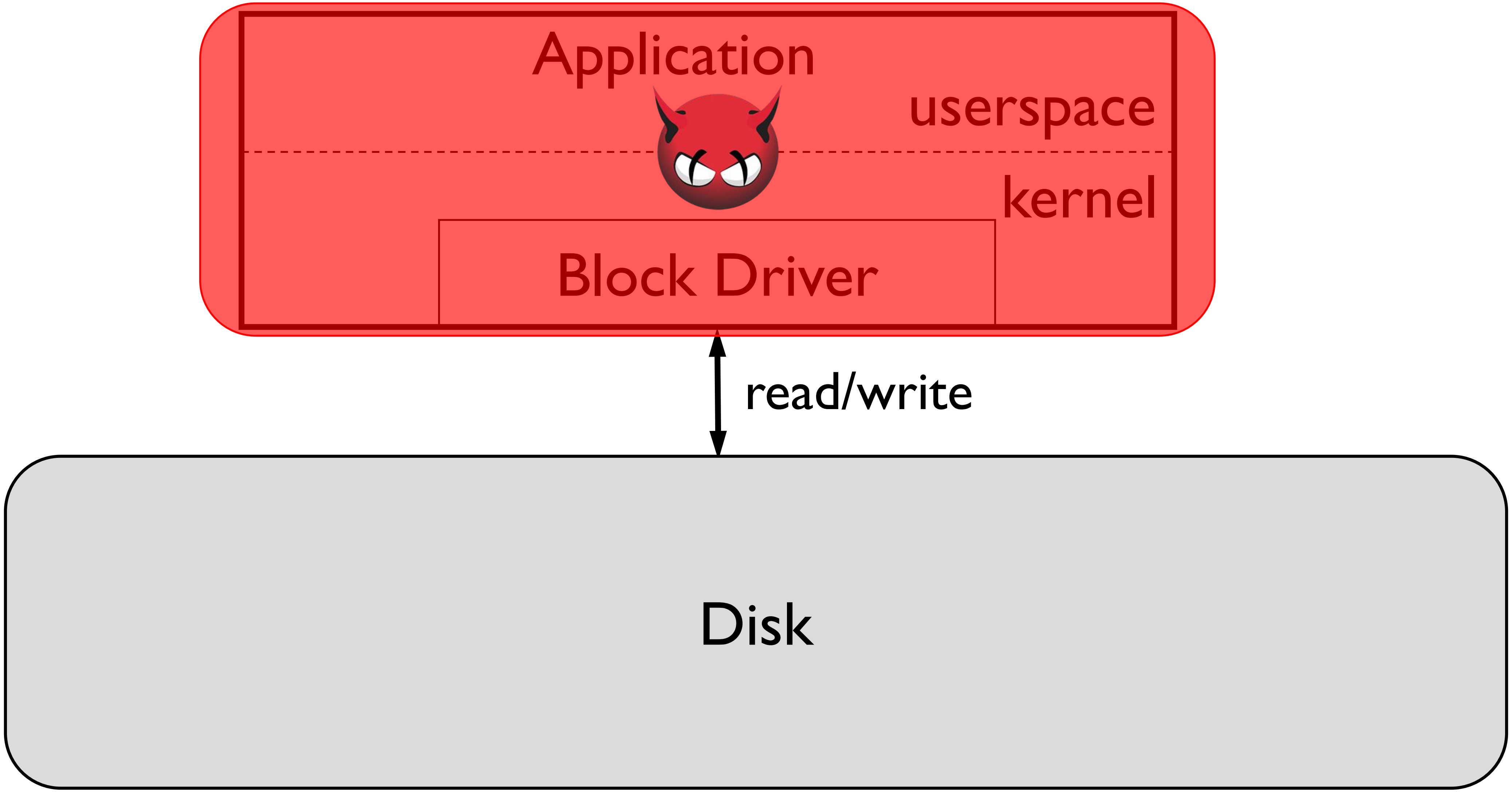
Networked & Cloud Storage

Increased storage cost & can be stopped by ransomware

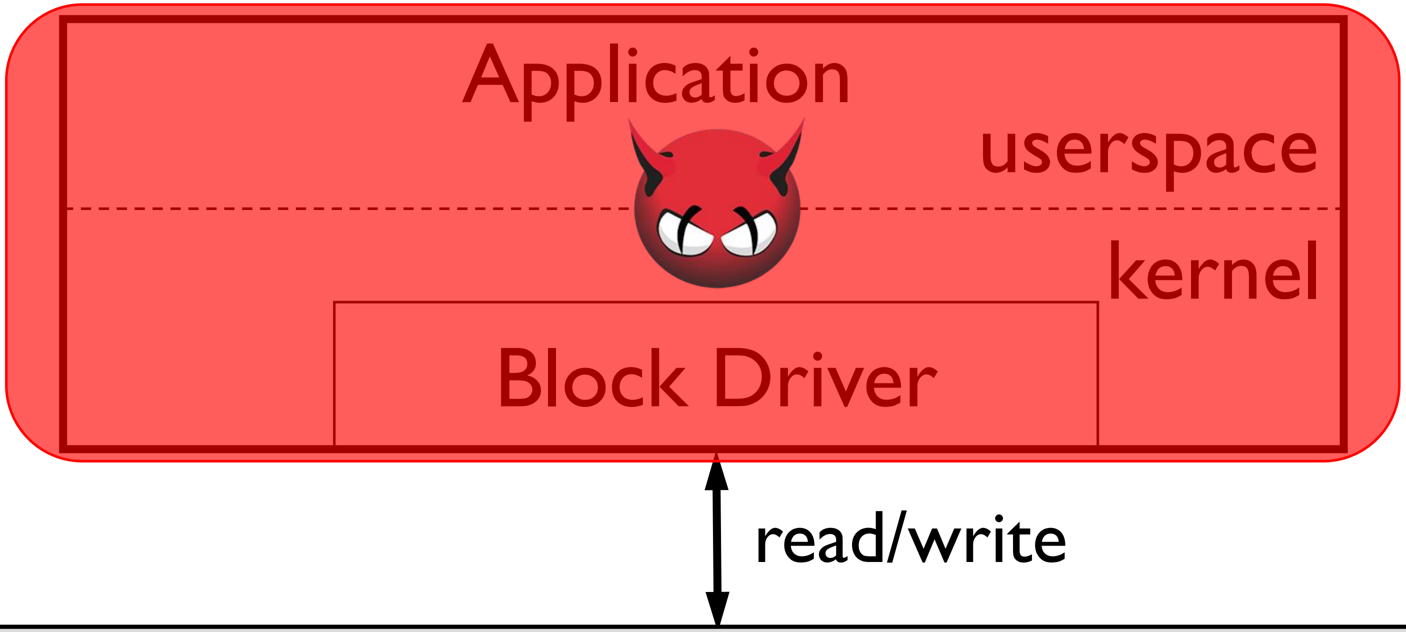
Threat Model of Encryption Ransomware



Threat Model of Encryption Ransomware

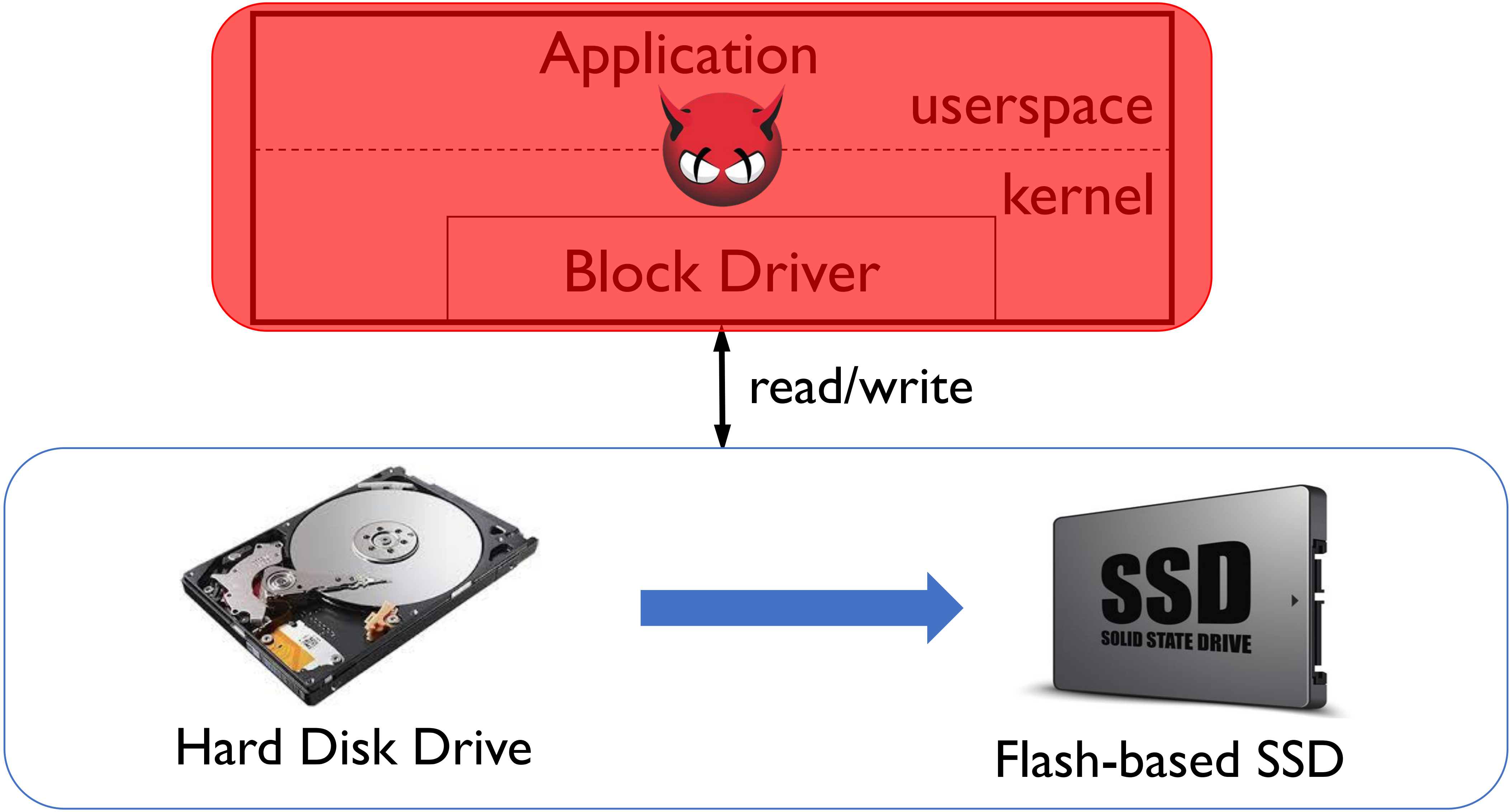


Threat Model of Encryption Ransomware



Our Goal: defend against encryption ransomware *without relying on software-based solutions & without explicit data backups*

Threat Model of Encryption Ransomware



Application

userspace

kernel

Block Driver

read/write

Hard Disk Drive

Flash-based SSD

Flash Performs Better Than Hard Disk Drive

No Seek Latency

40x lower latency

Flash Performs Better Than Hard Disk Drive

No Seek Latency

40x lower latency

Increased Parallelism

Dozens of parallel chips

Flash Performs Better Than Hard Disk Drive

No Seek Latency

40x lower latency

Increased Parallelism

Dozens of parallel chips

Became Commodity

Less than $0.2/GB

Flash Performs Better Than Hard Disk Drive

No Seek Latency

40x lower latency

Increased Parallelism

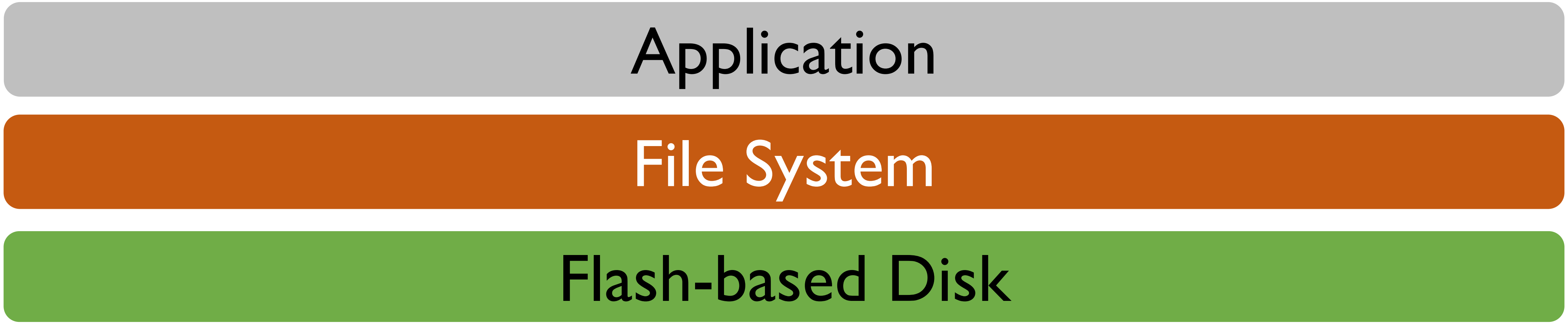
Dozens of parallel chips

Became Commodity

Less than $0.2/GB

Significant improvements on Flash

How Flash Is Used Today?

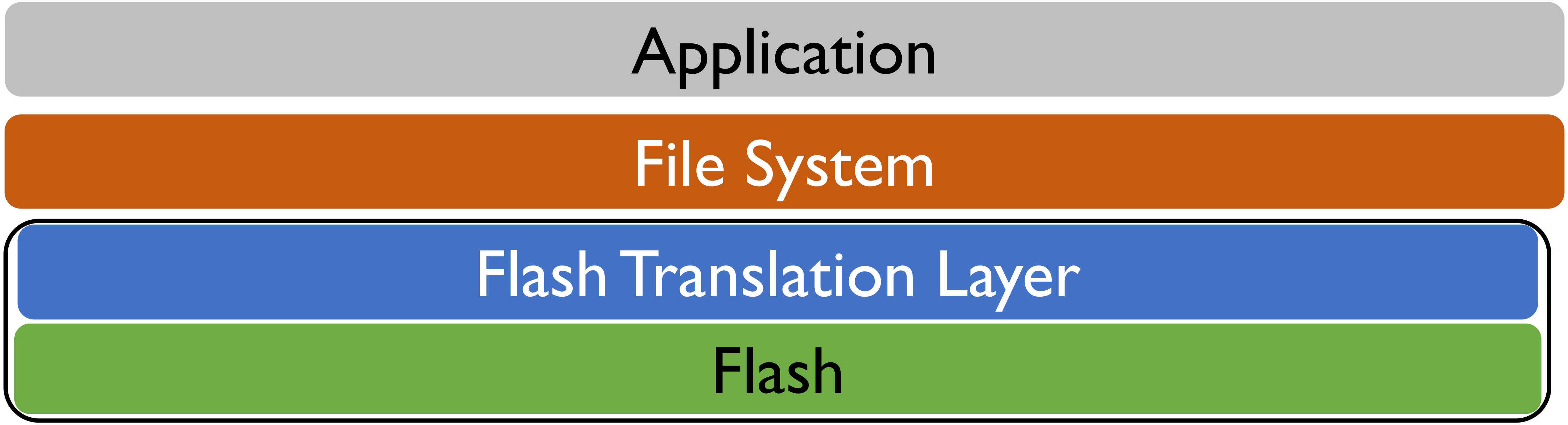


Application

File System

Flash-based Disk

How Flash Is Used Today?



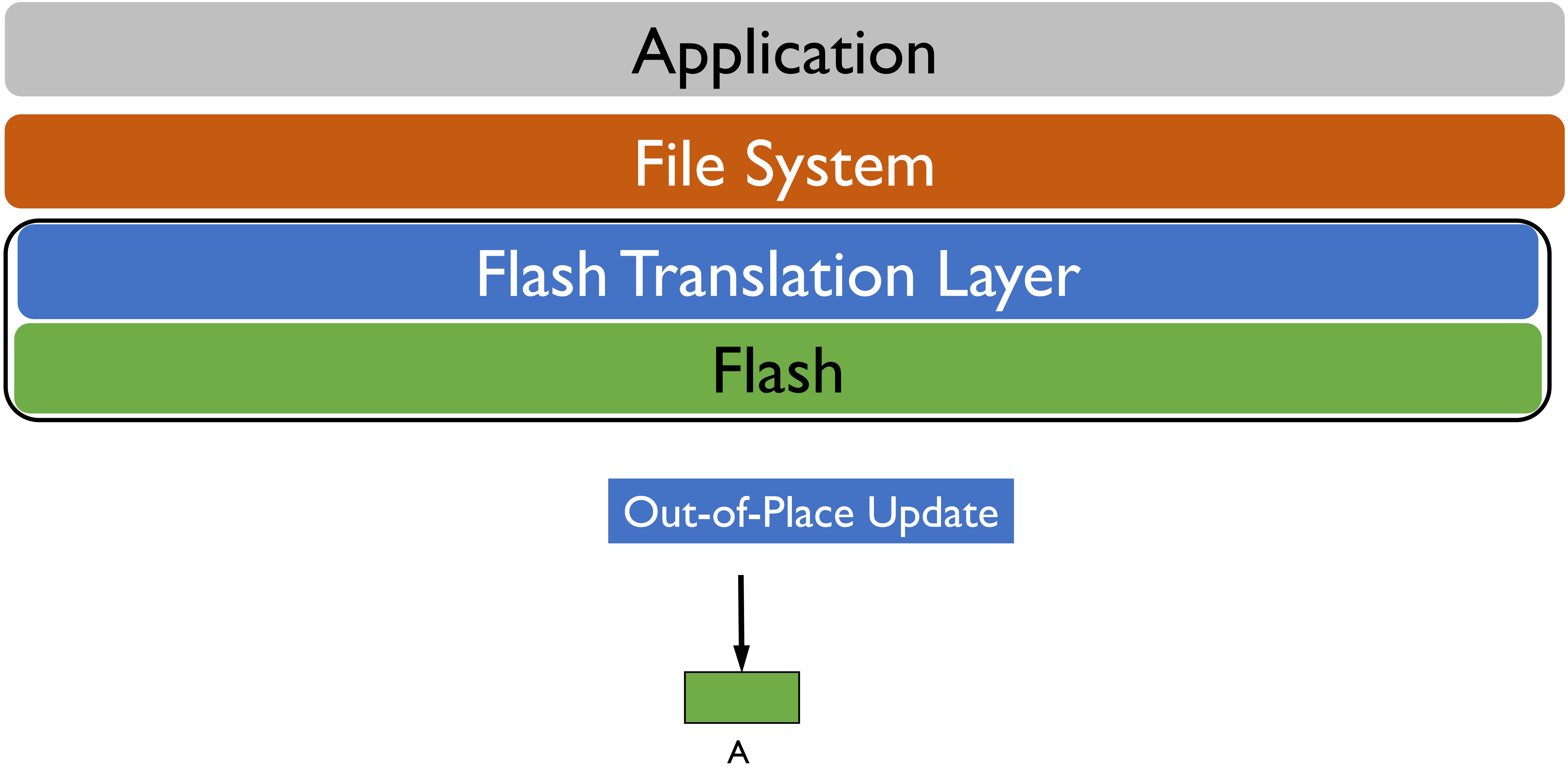
Application

File System

Flash Translation Layer

Flash

How Flash Is Used Today?



Application

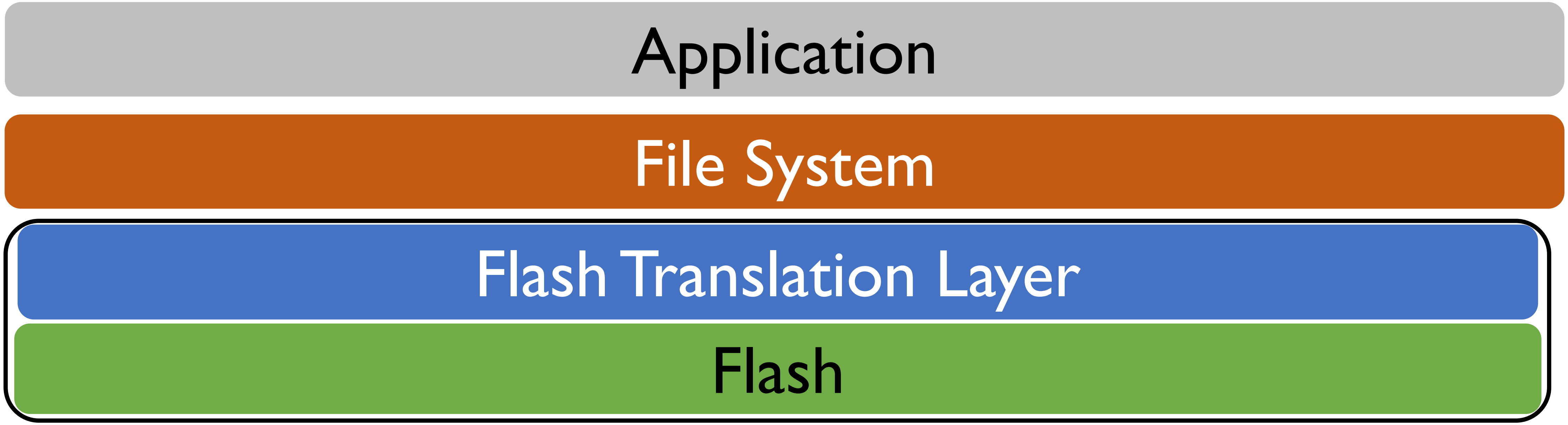
File System

Flash Translation Layer

Flash

Out-of-Place Update

How Flash Is Used Today?



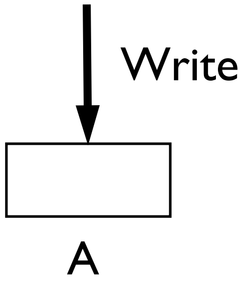
Application

File System

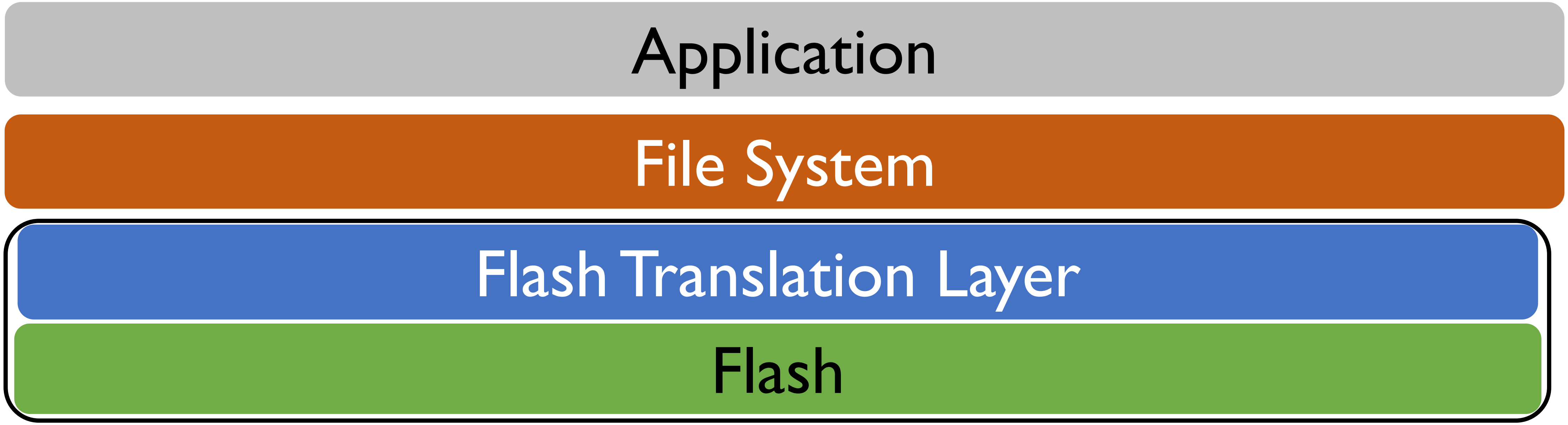
Flash Translation Layer

Flash

Out-of-Place Update



How Flash Is Used Today?



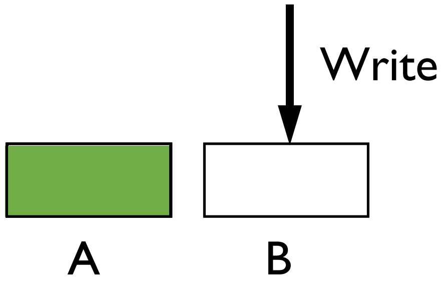
Application

File System

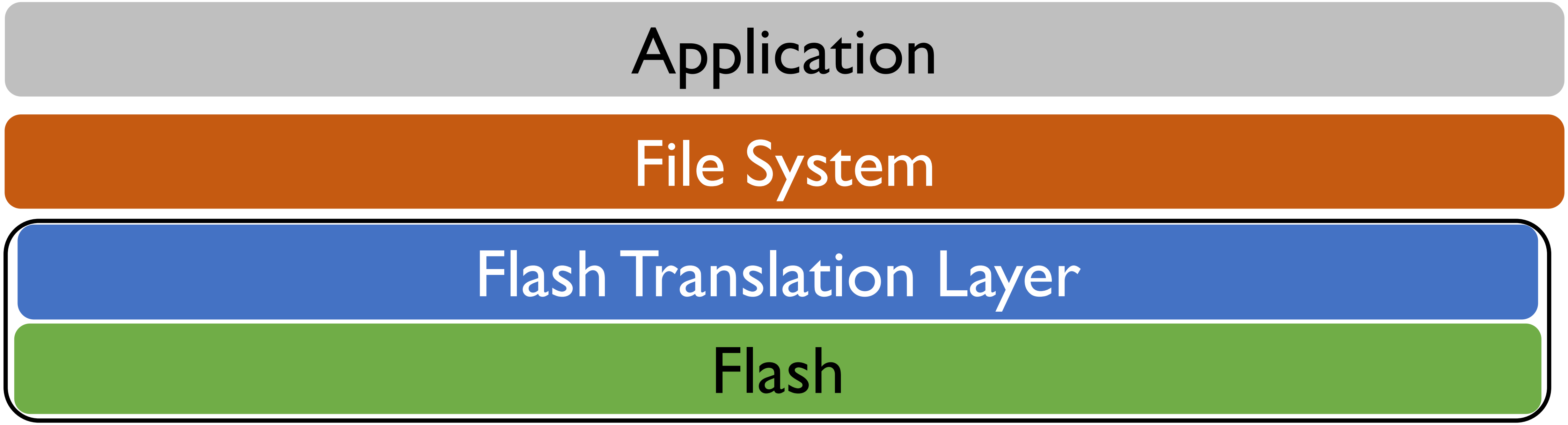
Flash Translation Layer

Flash

Out-of-Place Update



How Flash Is Used Today?

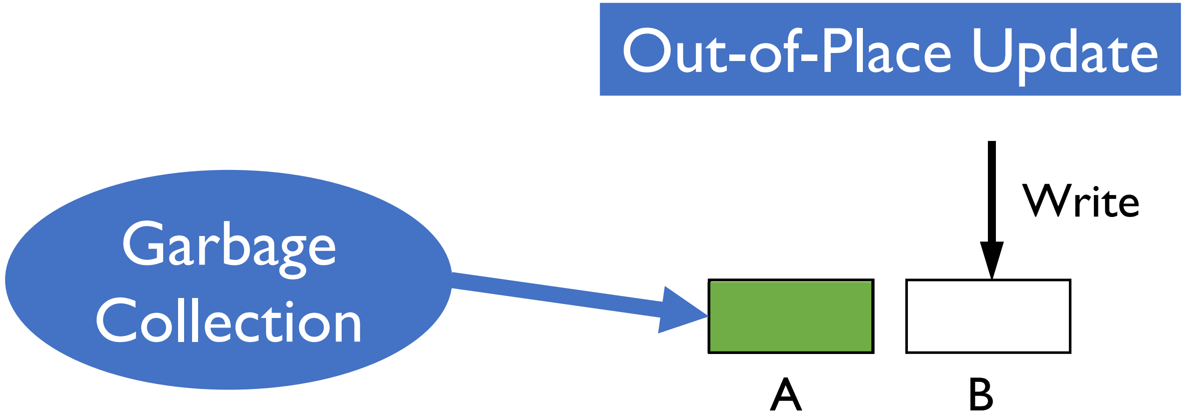


Application

File System

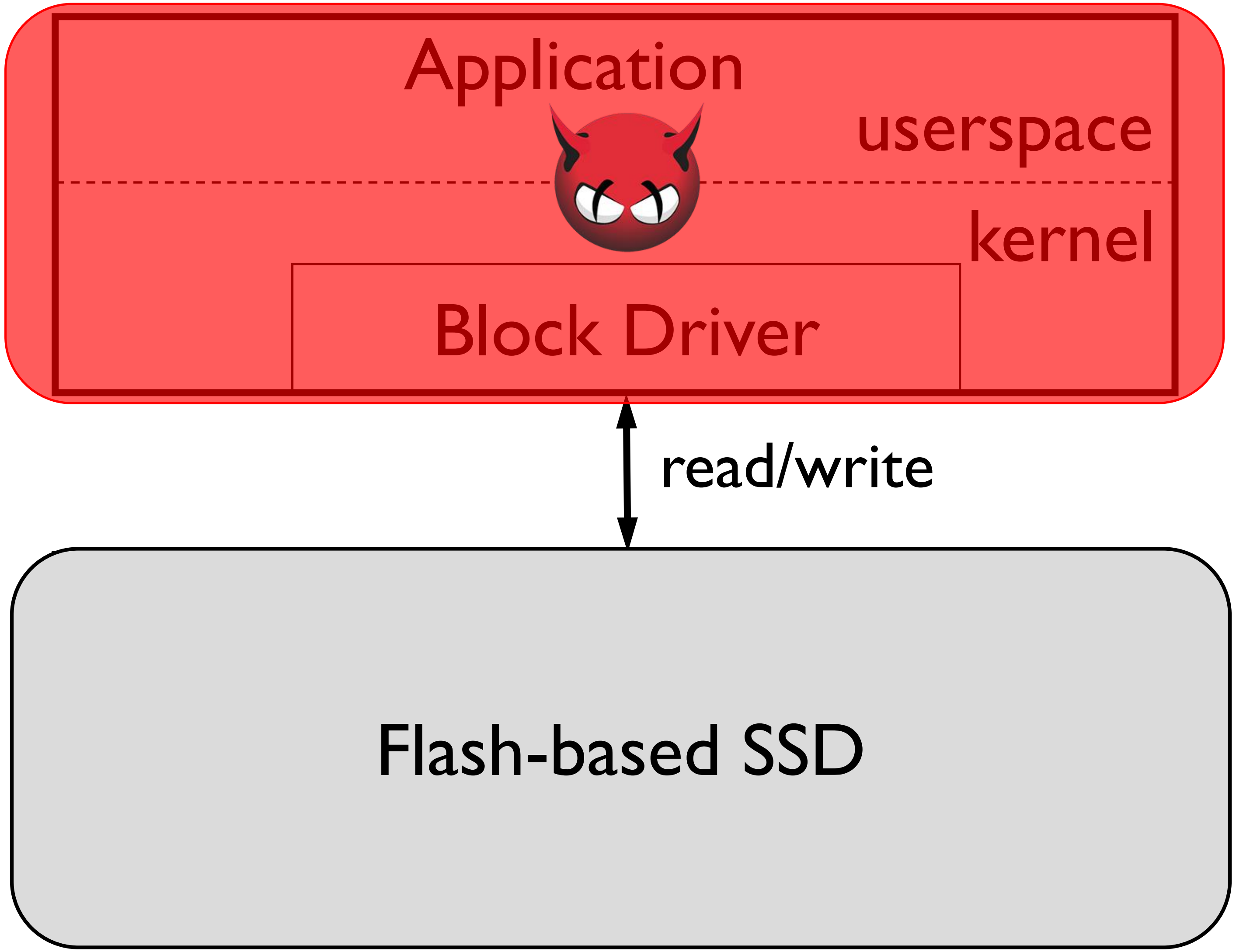
Flash Translation Layer

Flash

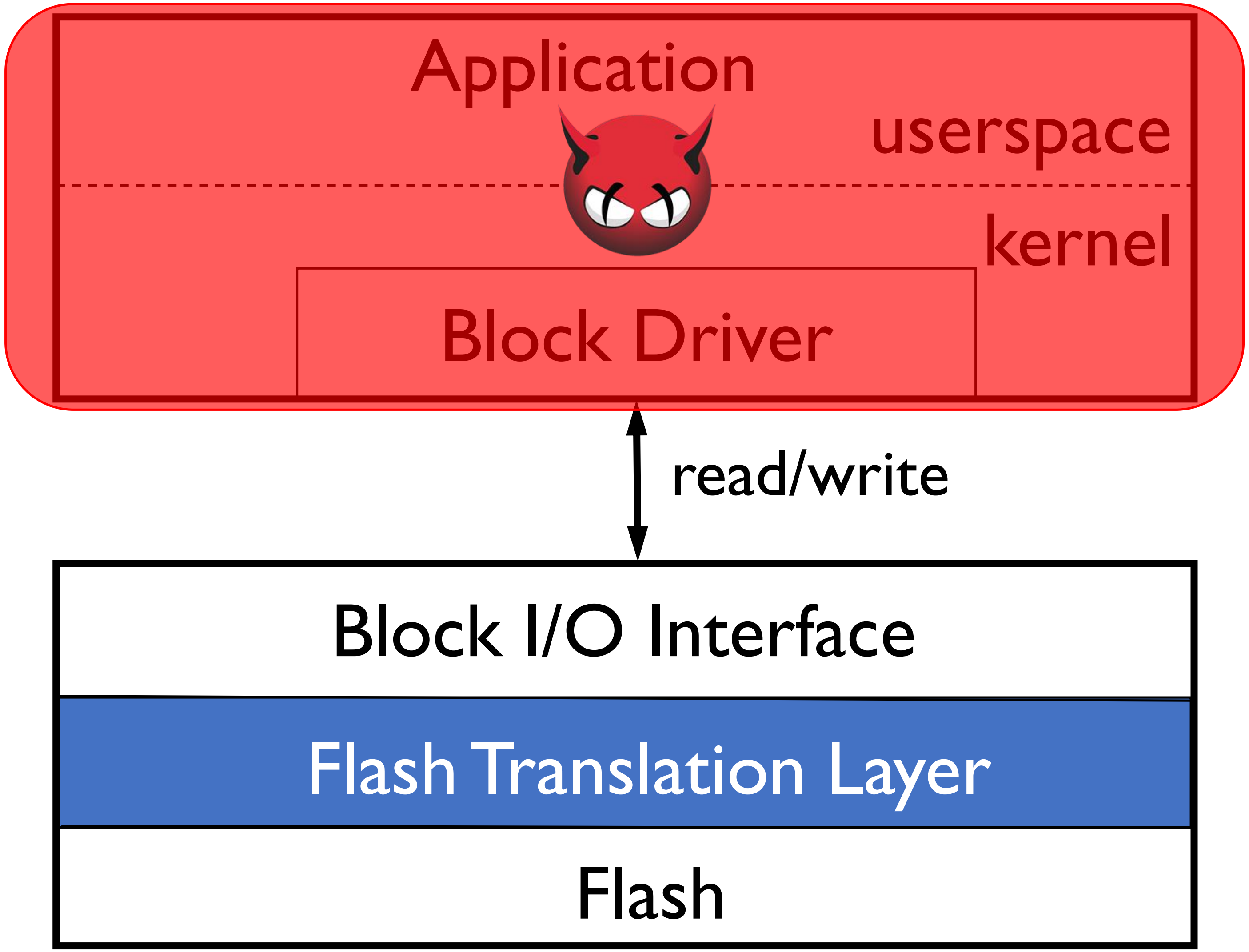


Out-of-Place Update

FlashGuard: Leveraging Intrinsic Flash Properties

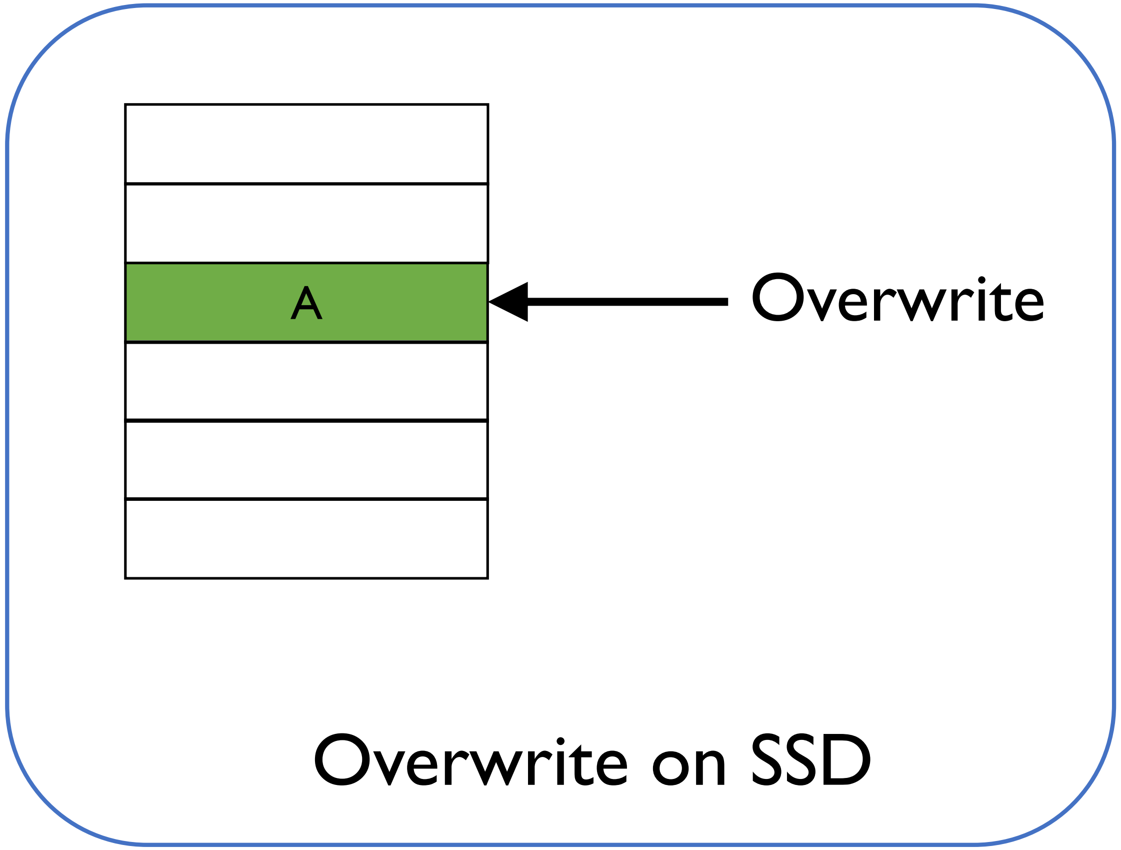


FlashGuard: Leveraging Intrinsic Flash Properties



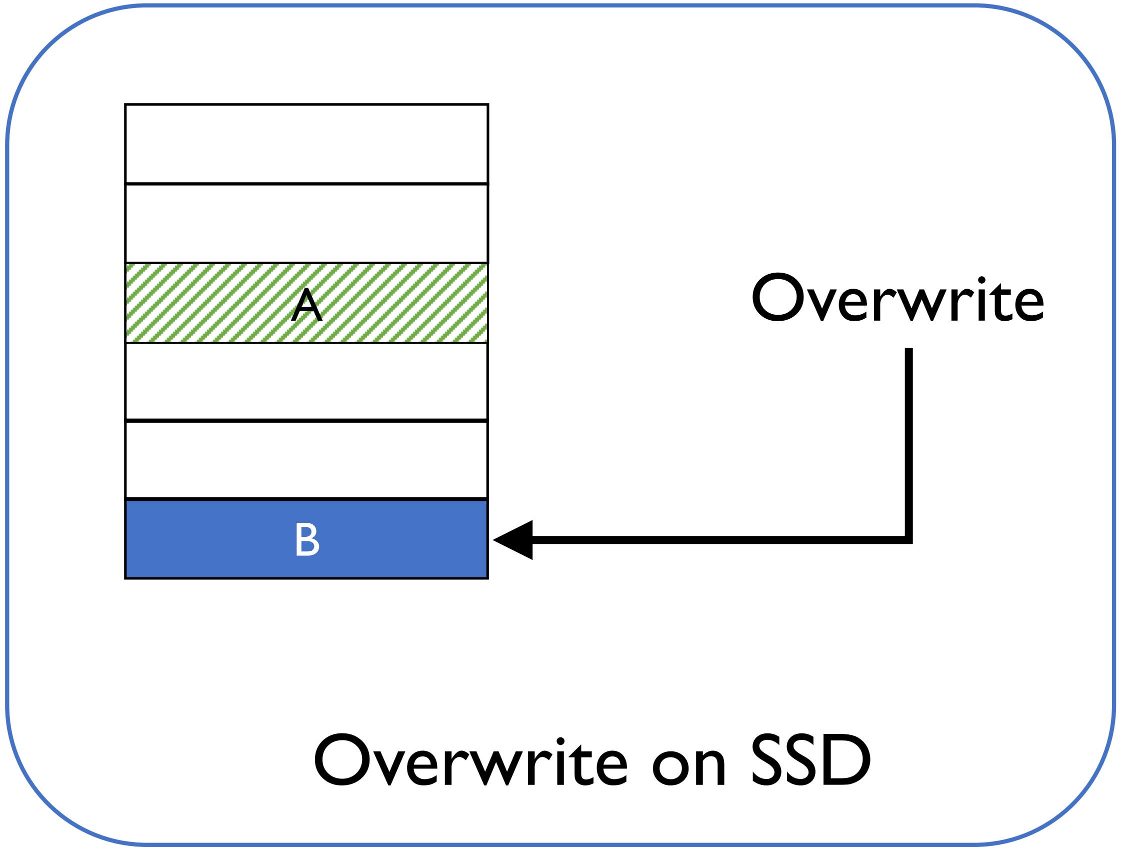
Retaining Data in SSDs without Hardware Modification

Overwrite a block



Retaining Data in SSDs without Hardware Modification

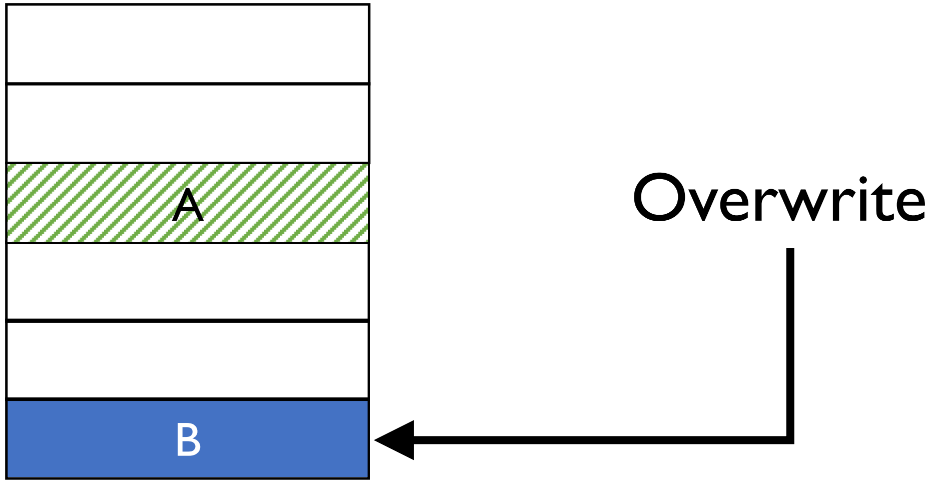
Overwrite a block



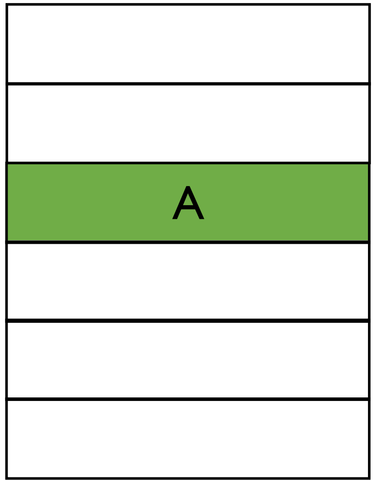
Overwrite on SSD

Retaining Data in SSDs without Hardware Modification

Overwrite a block



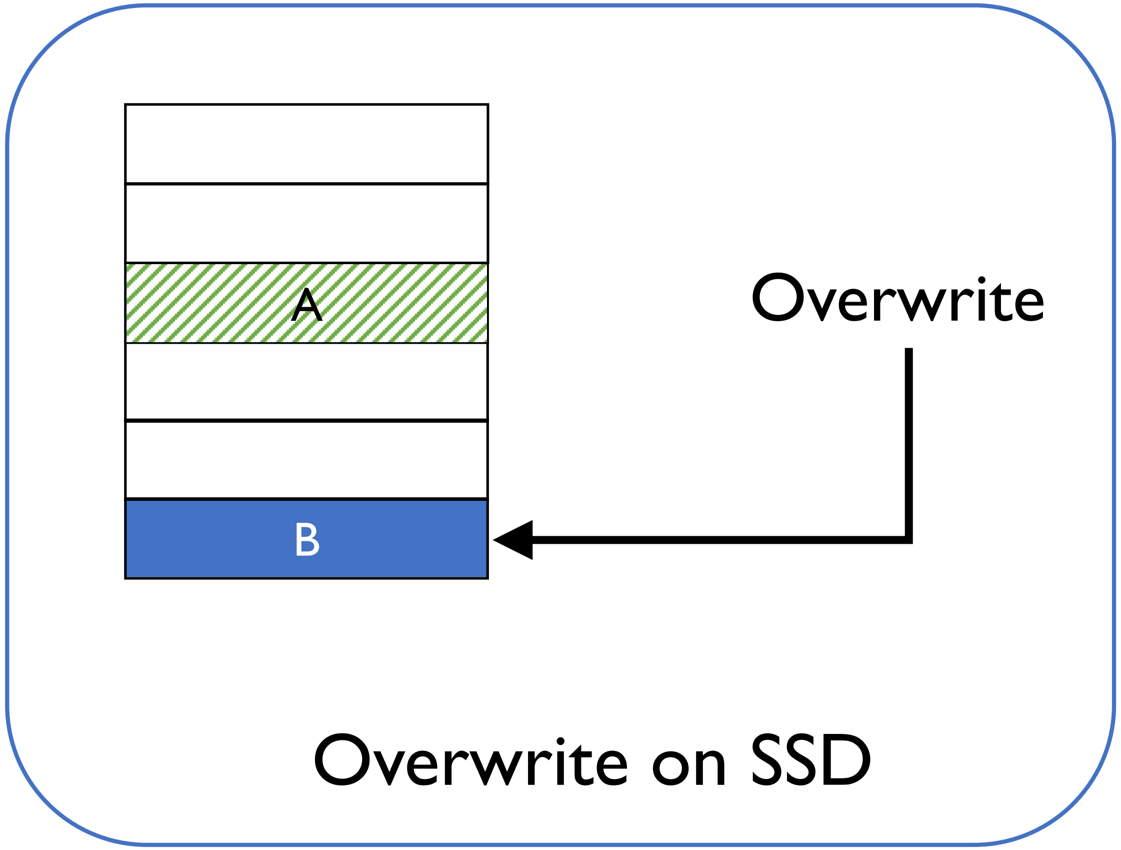
Overwrite on SSD

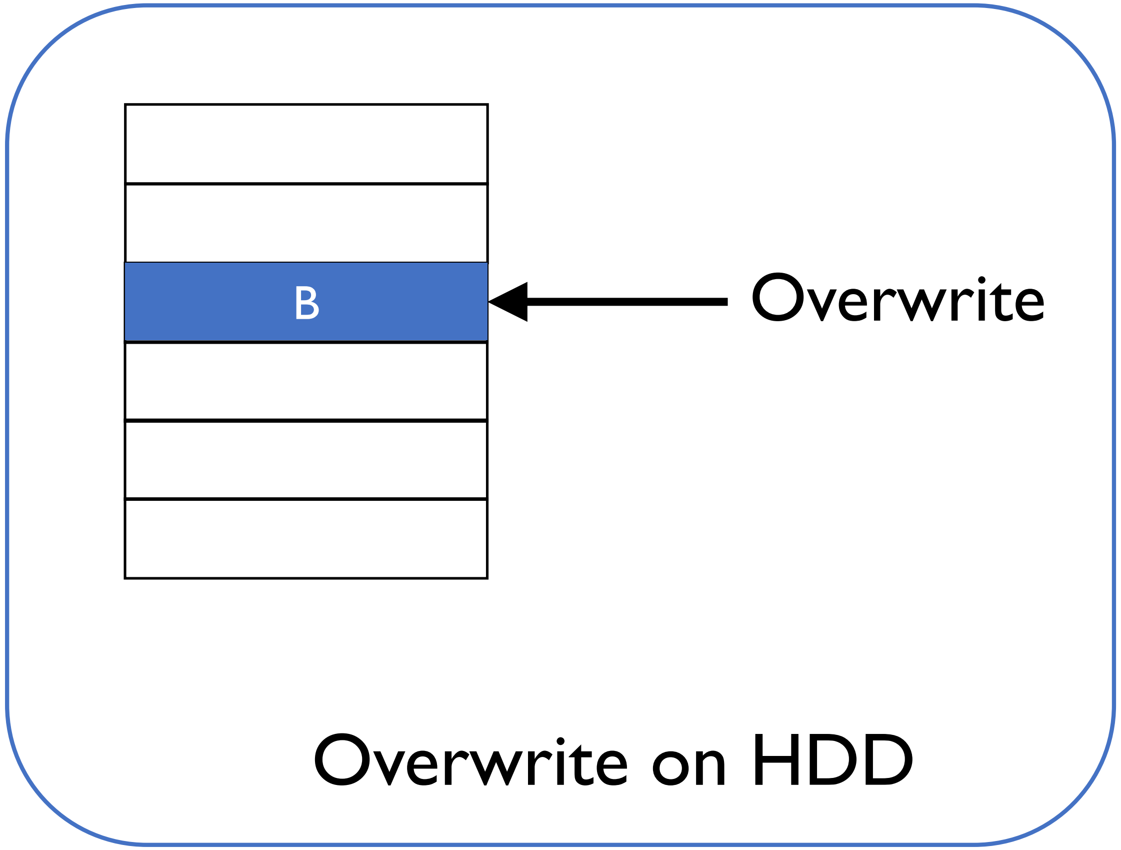


Overwrite on HDD

Retaining Data in SSDs without Hardware Modification

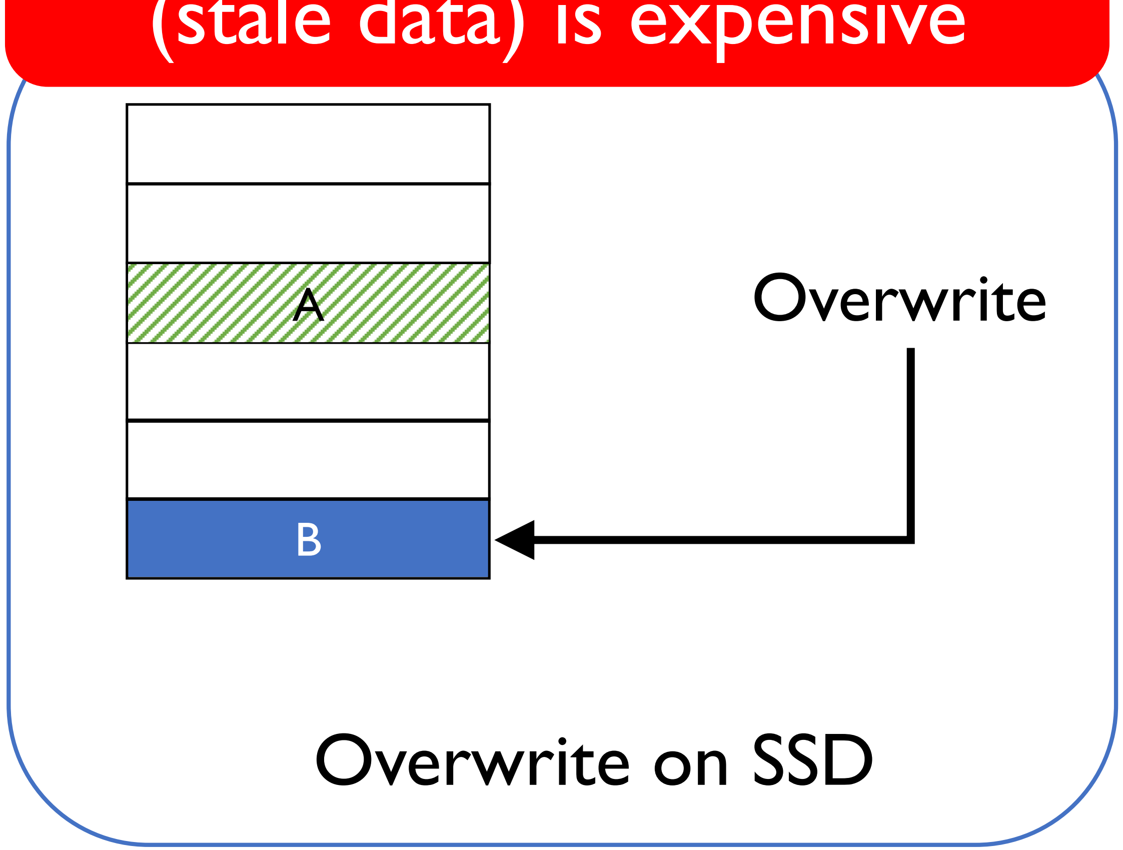
Overwrite a block

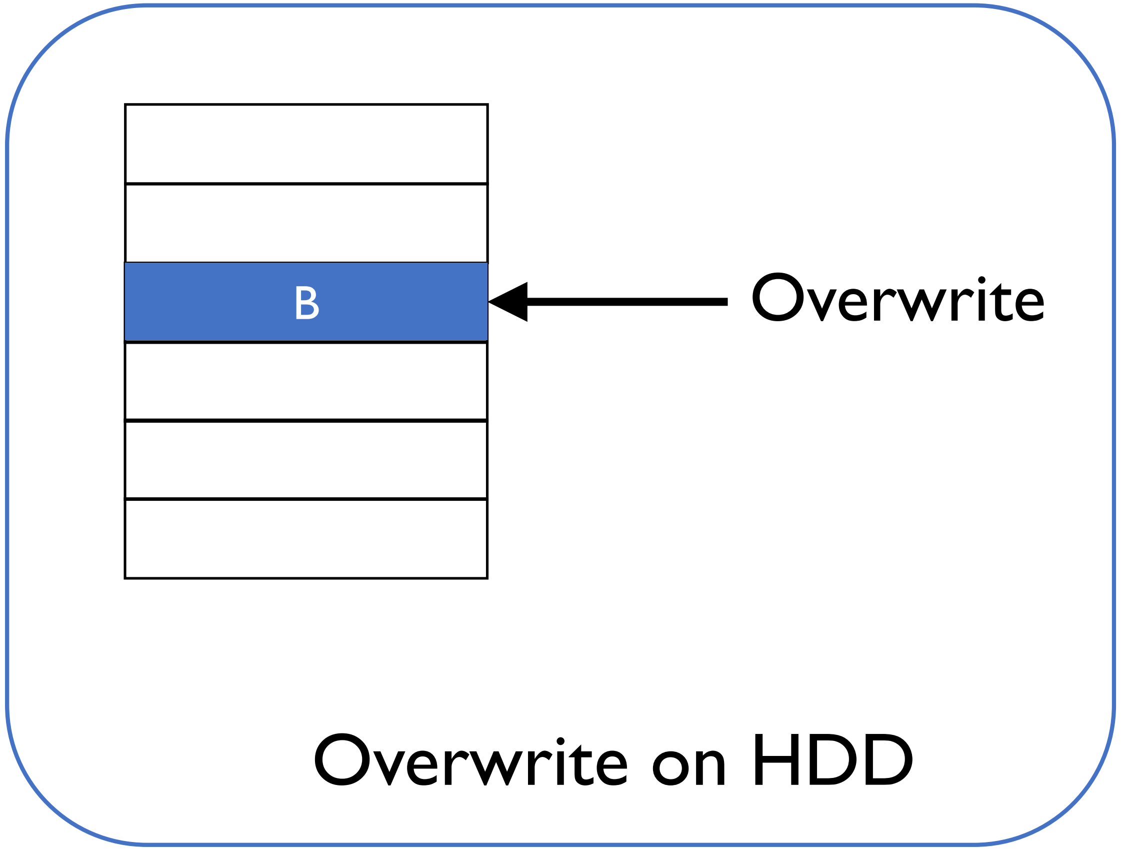




Retaining Data in SSDs without Hardware Modification

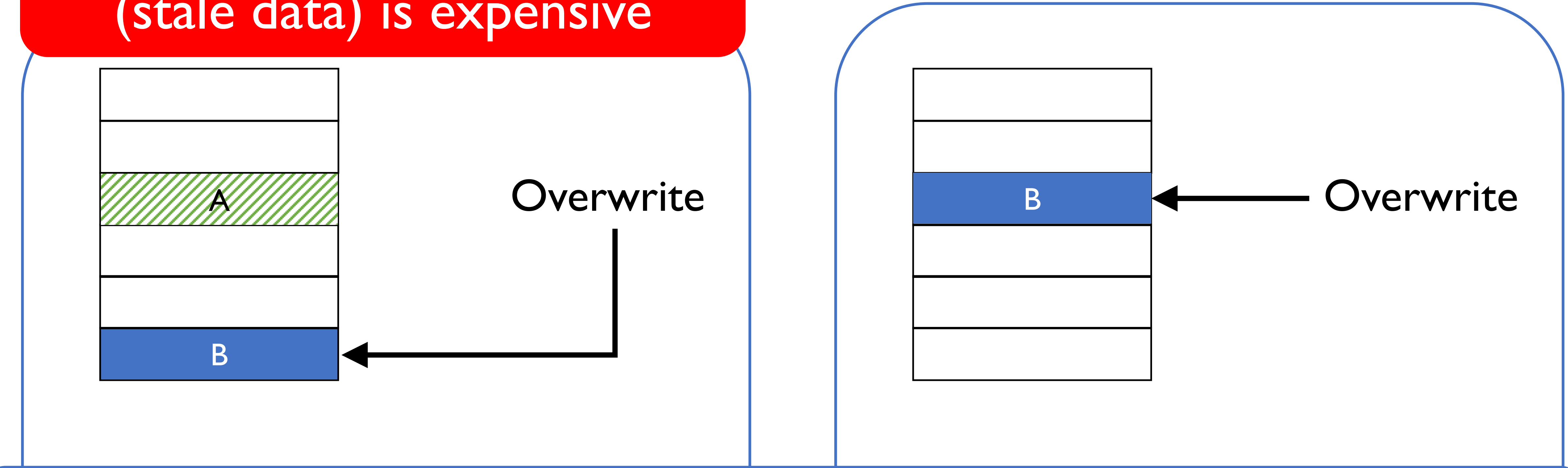
Retaining all the invalid pages (stale data) is expensive





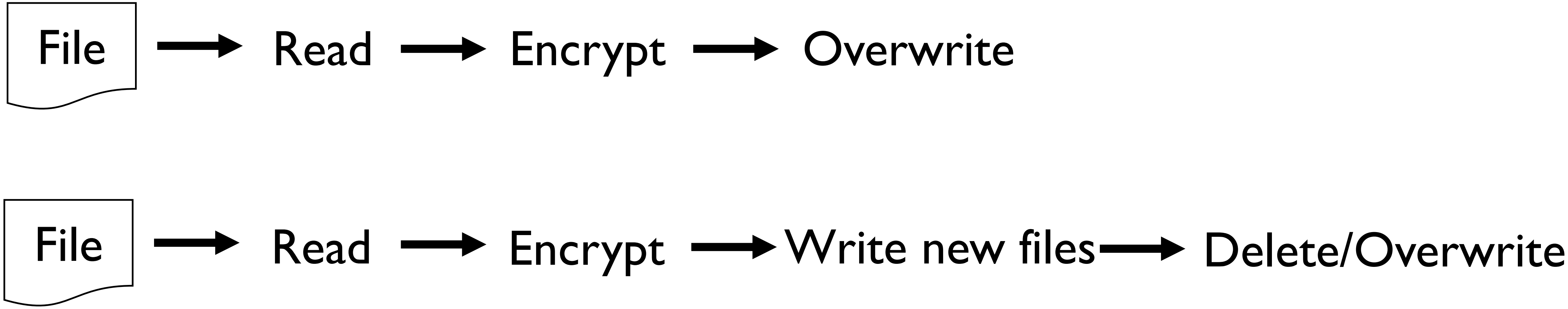
Retaining Data in SSDs without Hardware Modification

Retaining all the invalid pages (stale data) is expensive



Only retain the invalid pages caused by encryption ransomware

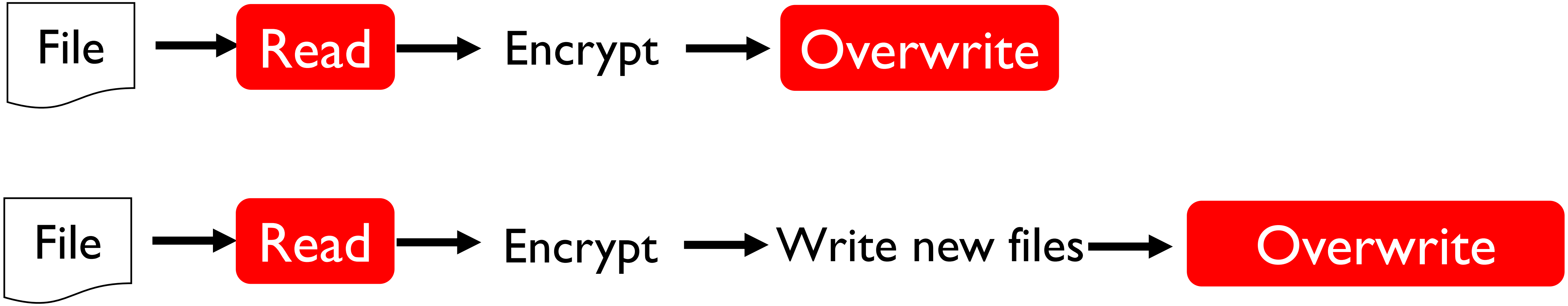
FlashGuard: A Ransomware-Aware SSD



File → Read → Encrypt → Overwrite

File → Read → Encrypt → Write new files → Delete/Overwrite

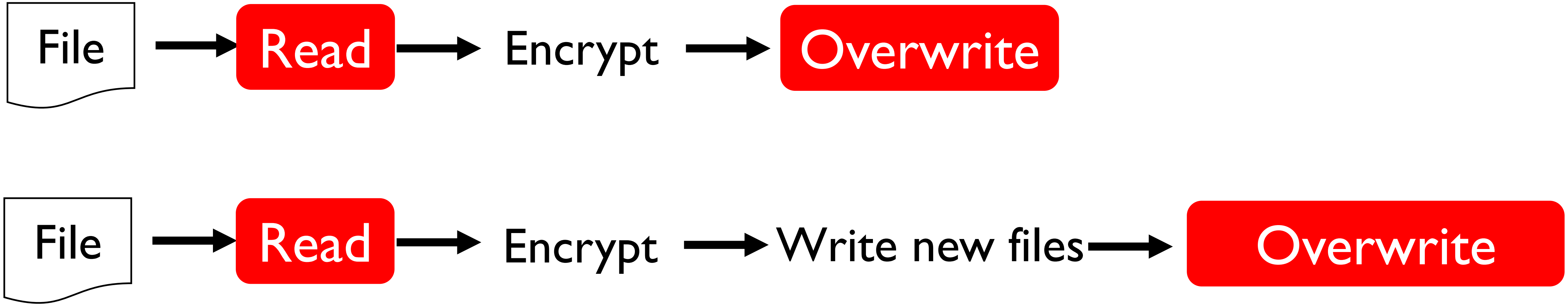
FlashGuard: A Ransomware-Aware SSD



File → Read → Encrypt → Overwrite

File → Read → Encrypt → Write new files → Overwrite

FlashGuard: A Ransomware-Aware SSD

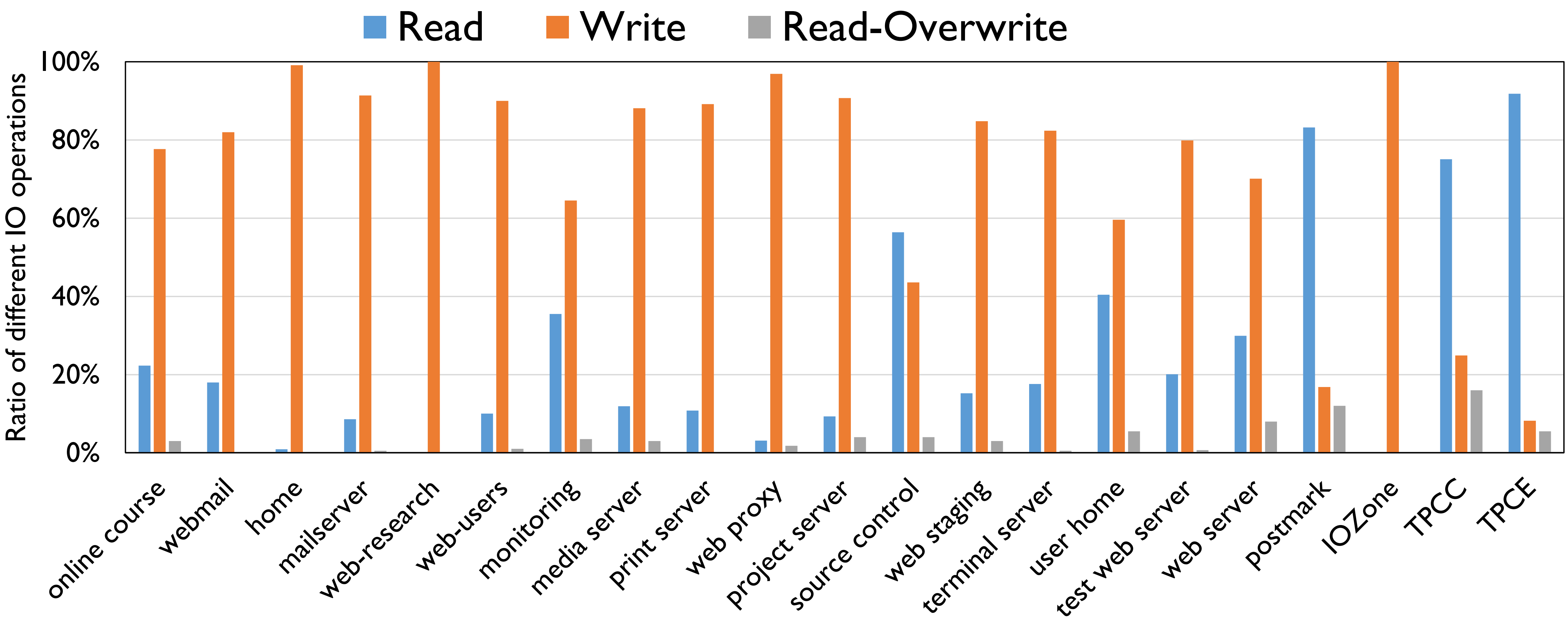


File → Read → Encrypt → Overwrite

File → Read → Encrypt → Write new files → Overwrite

FlashGuard only retains invalid pages that have been read for a certain period of time

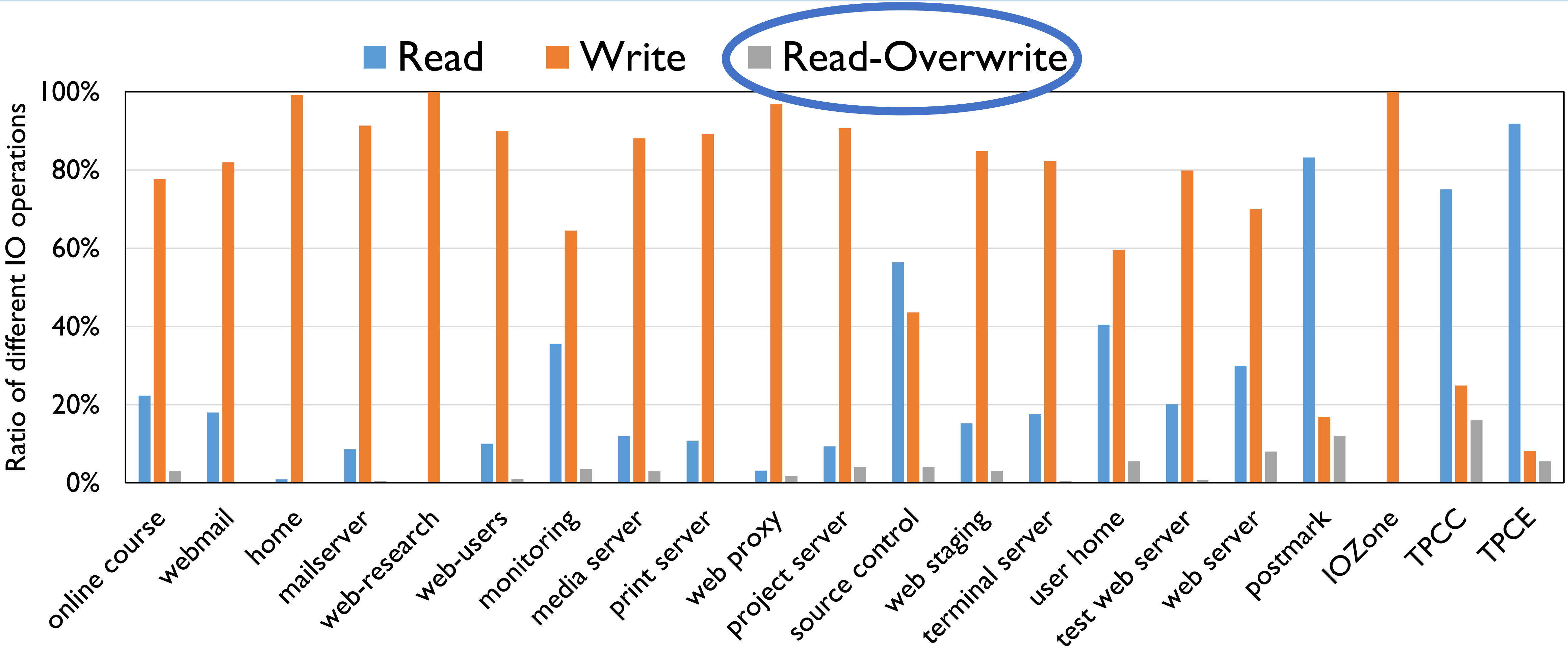
FlashGuard: A Ransomware-Aware SSD



University computers (20 days)

Enterprise servers (6-10 days)

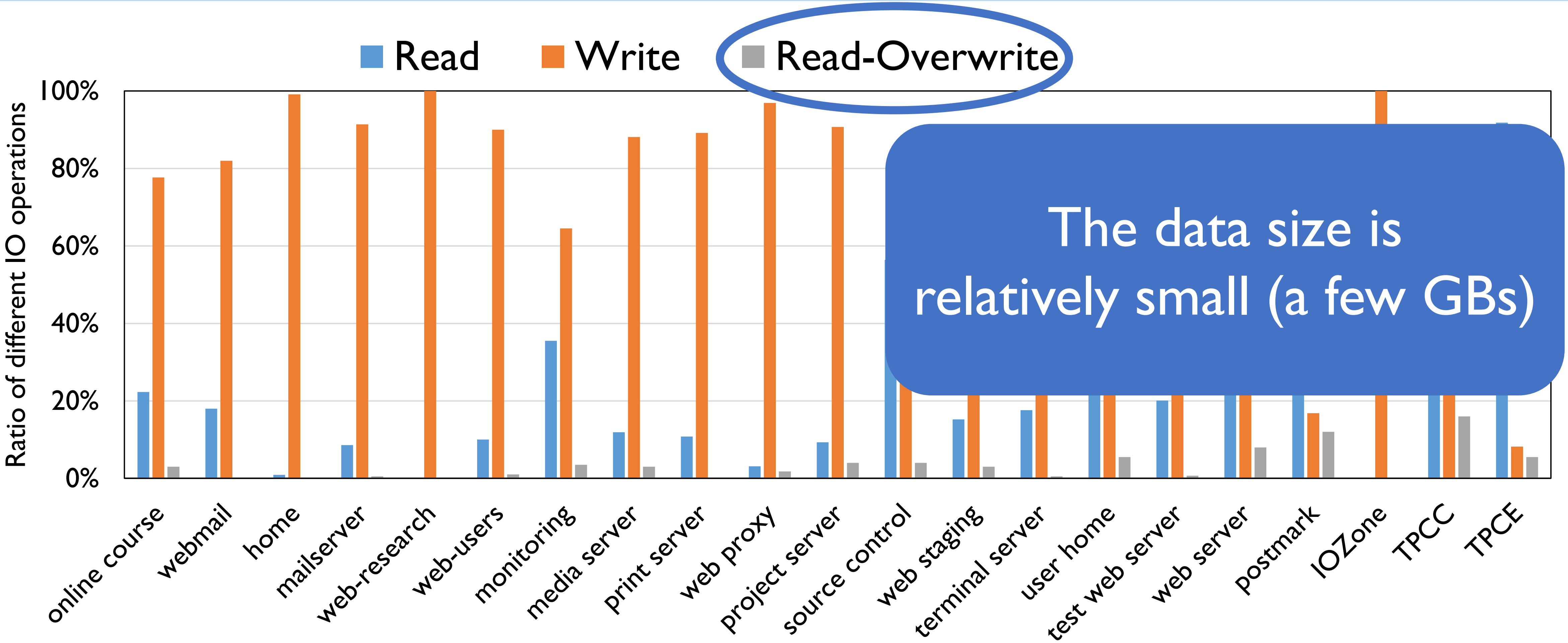
FlashGuard: A Ransomware-Aware SSD



University computers (20 days)

Enterprise servers (6-10 days)

FlashGuard: A Ransomware-Aware SSD

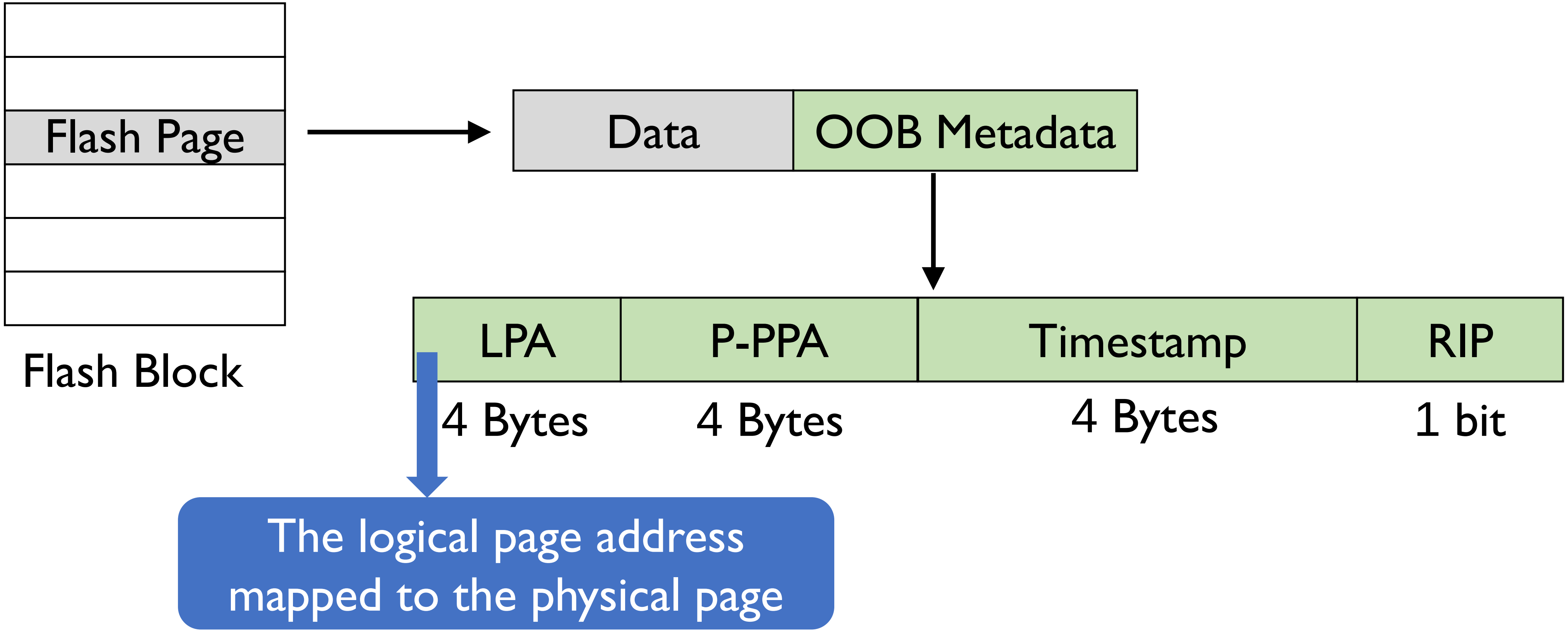


The data size is relatively small (a few GBs)

University computers (20 days)

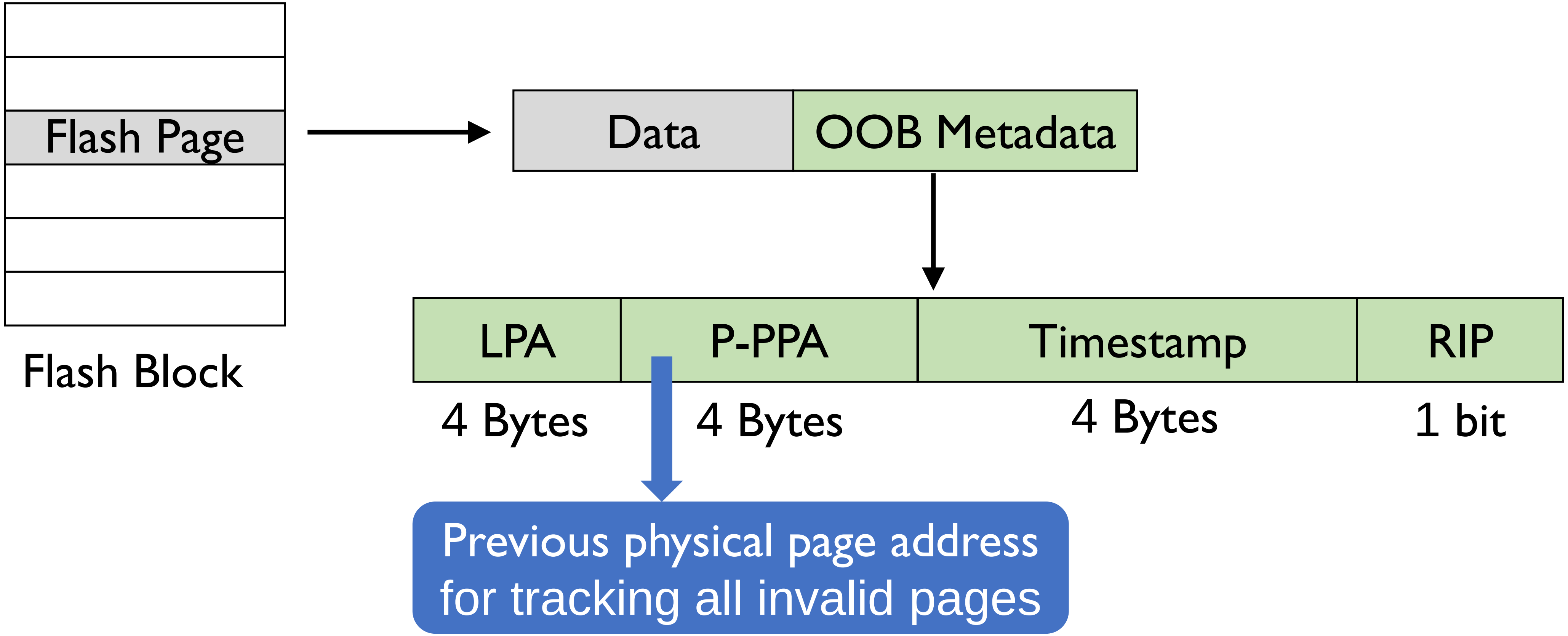
Enterprise servers (6-10 days)

Tracking Invalid Data with Out-of-Band Metadata



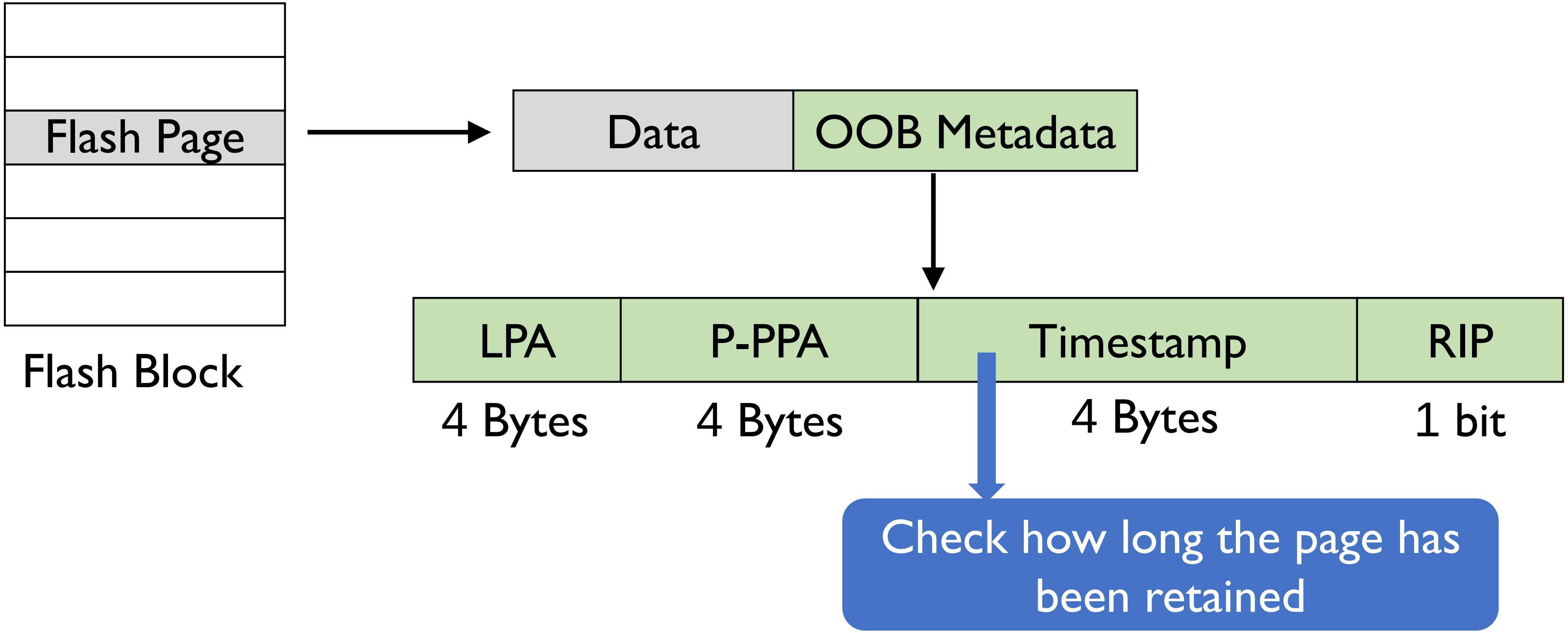
The logical page address mapped to the physical page

Tracking Invalid Data with Out-of-Band Metadata



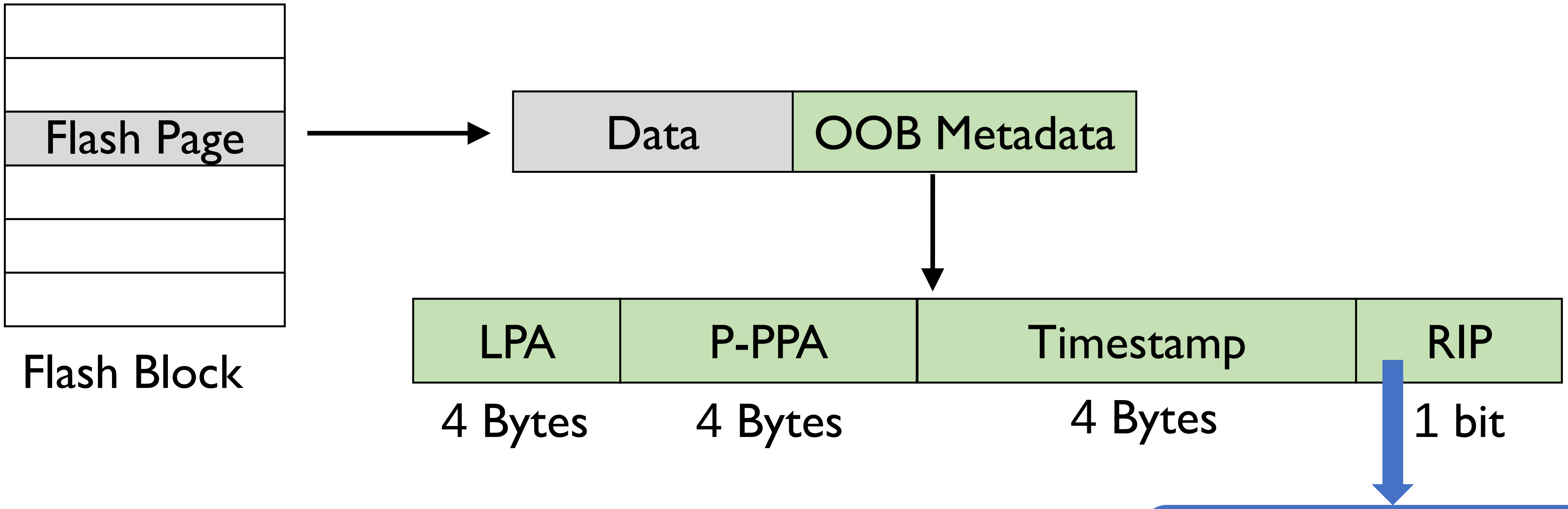
Previous physical page address for tracking all invalid pages

Tracking Invalid Data with Out-of-Band Metadata



Check how long the page has been retained

Tracking Invalid Data with Out-of-Band Metadata

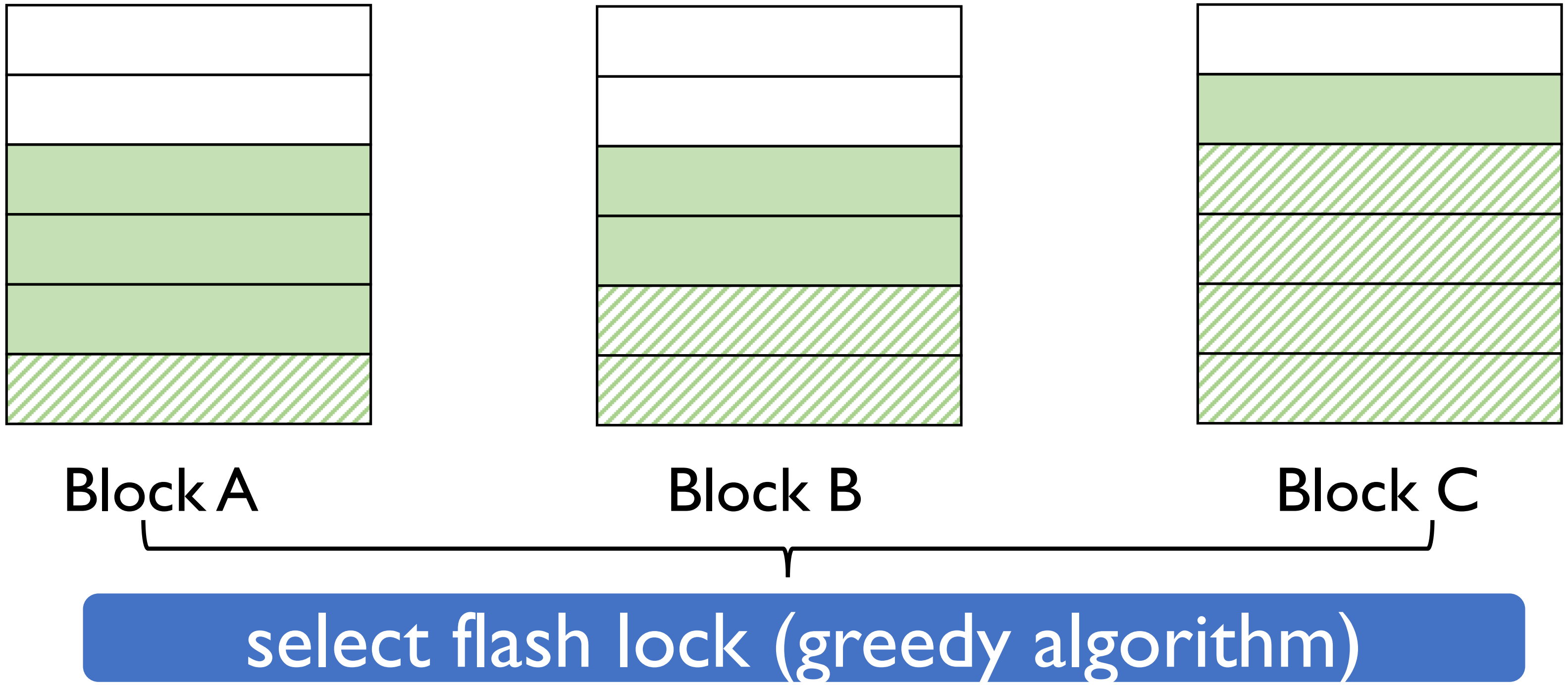


LPA	P-PPA	Timestamp	RIP
4 Bytes	4 Bytes	4 Bytes	1 bit

Identify whether this page is a retained invalid page

Ransomware-Award Garbage Collection in FlashGuard

□ valid page 🟩 invalid page ▨ retained invalid page



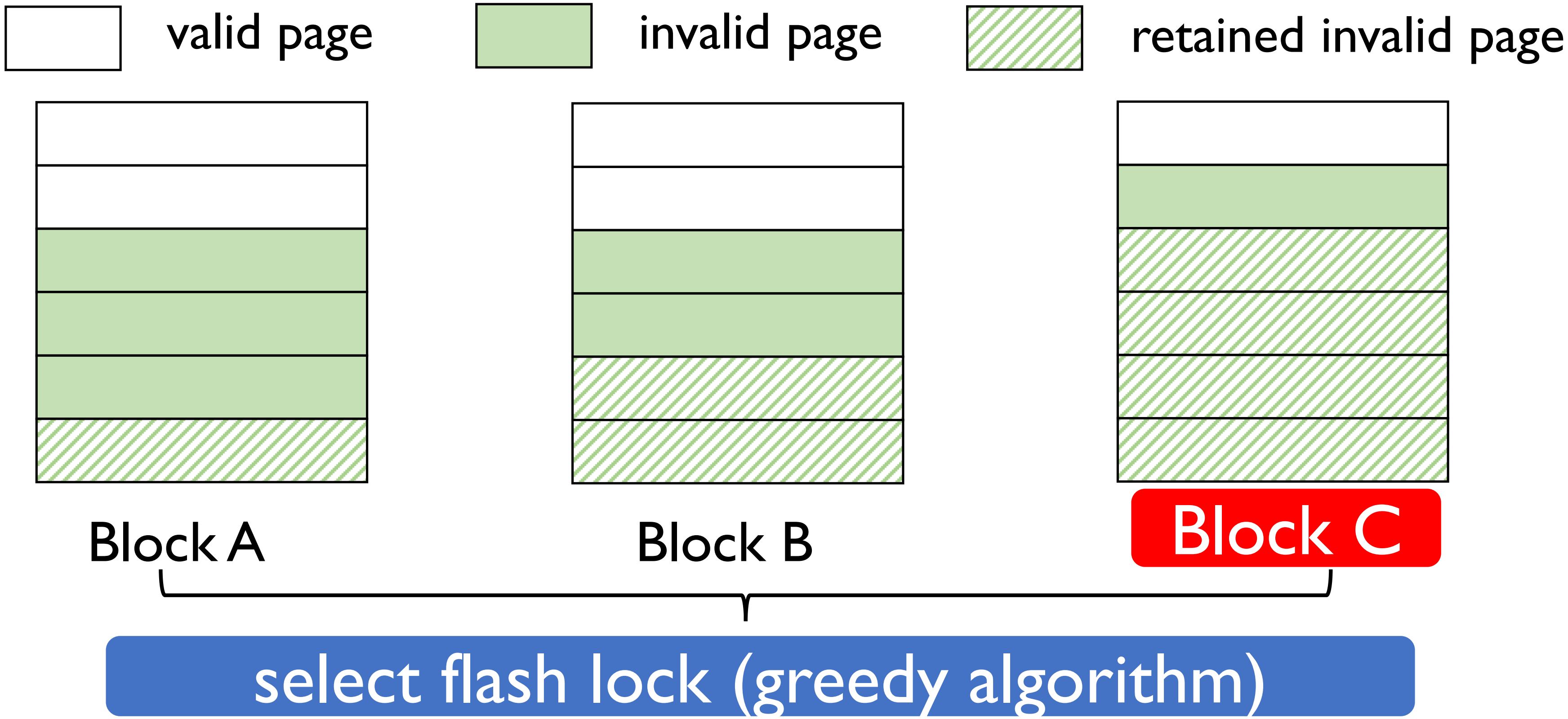
Block A

Block B

Block C

select flash lock (greedy algorithm)

Ransomware-Award Garbage Collection in FlashGuard



□ valid page

🟩 invalid page

▨ retained invalid page

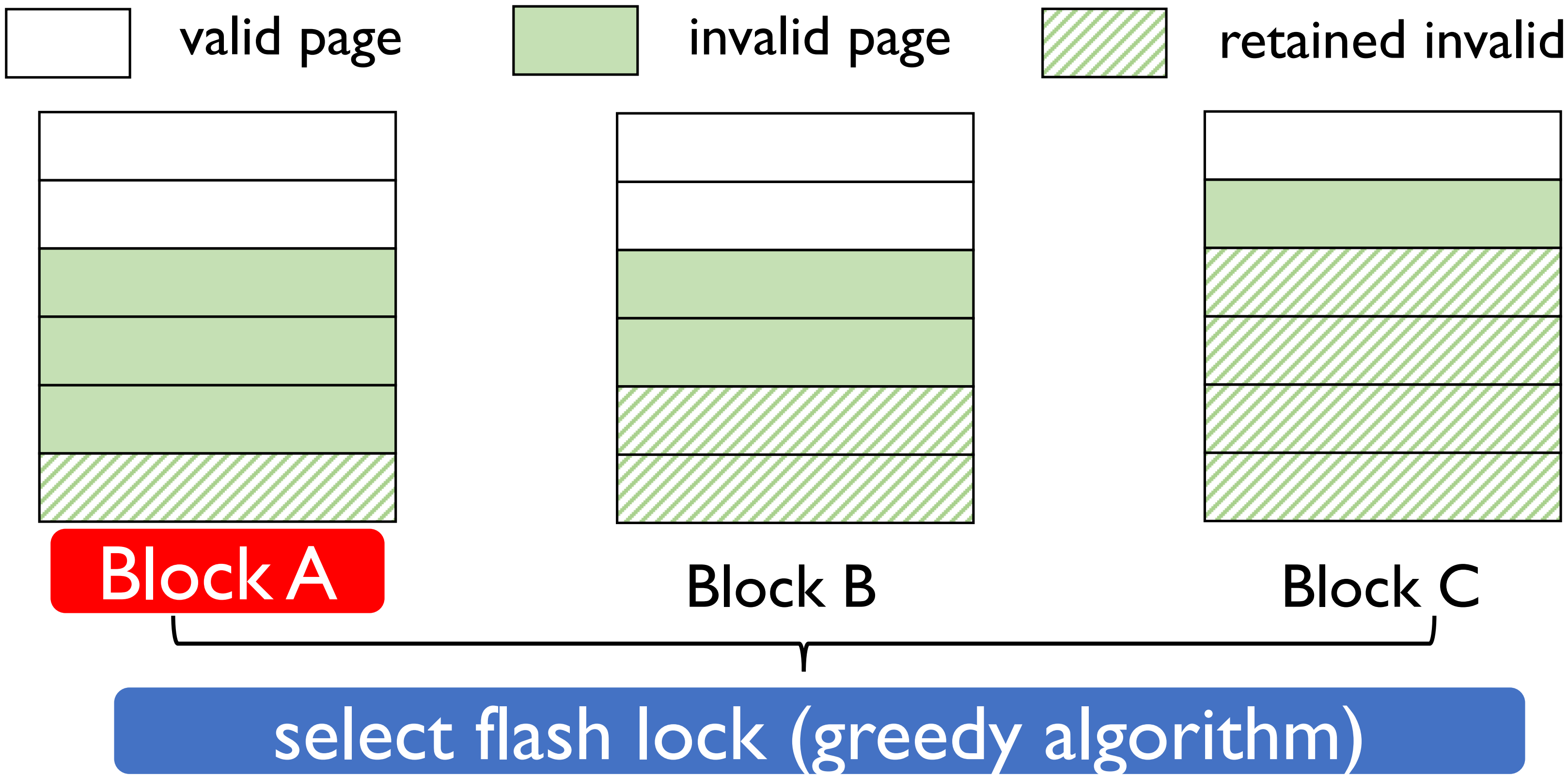
Block A

Block B

Block C

select flash lock (greedy algorithm)

Ransomware-Award Garbage Collection in FlashGuard



□ valid page

🟩 invalid page

▨ retained invalid page

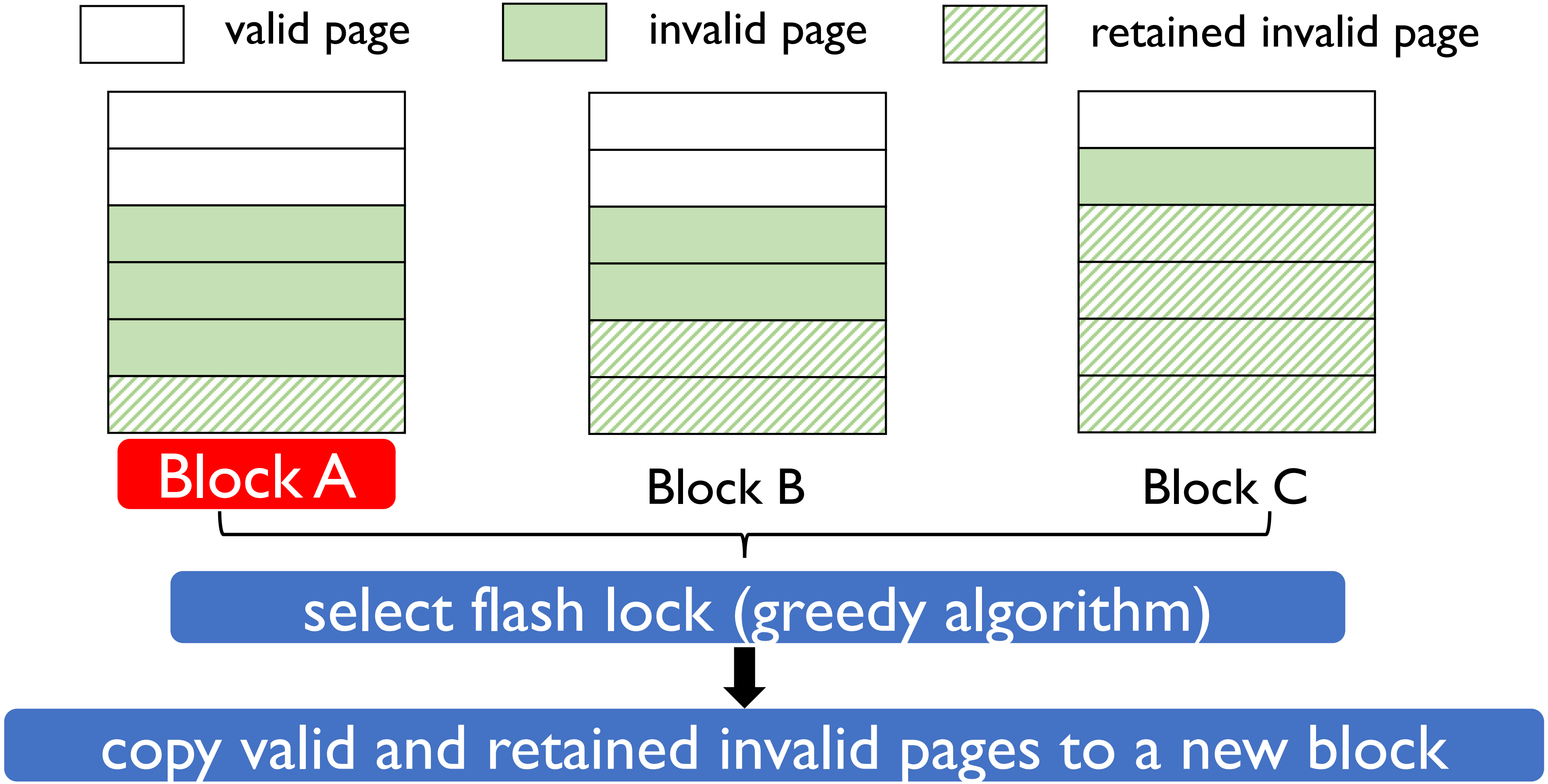
Block A

Block B

Block C

select flash lock (greedy algorithm)

Ransomware-Award Garbage Collection in FlashGuard



□ valid page

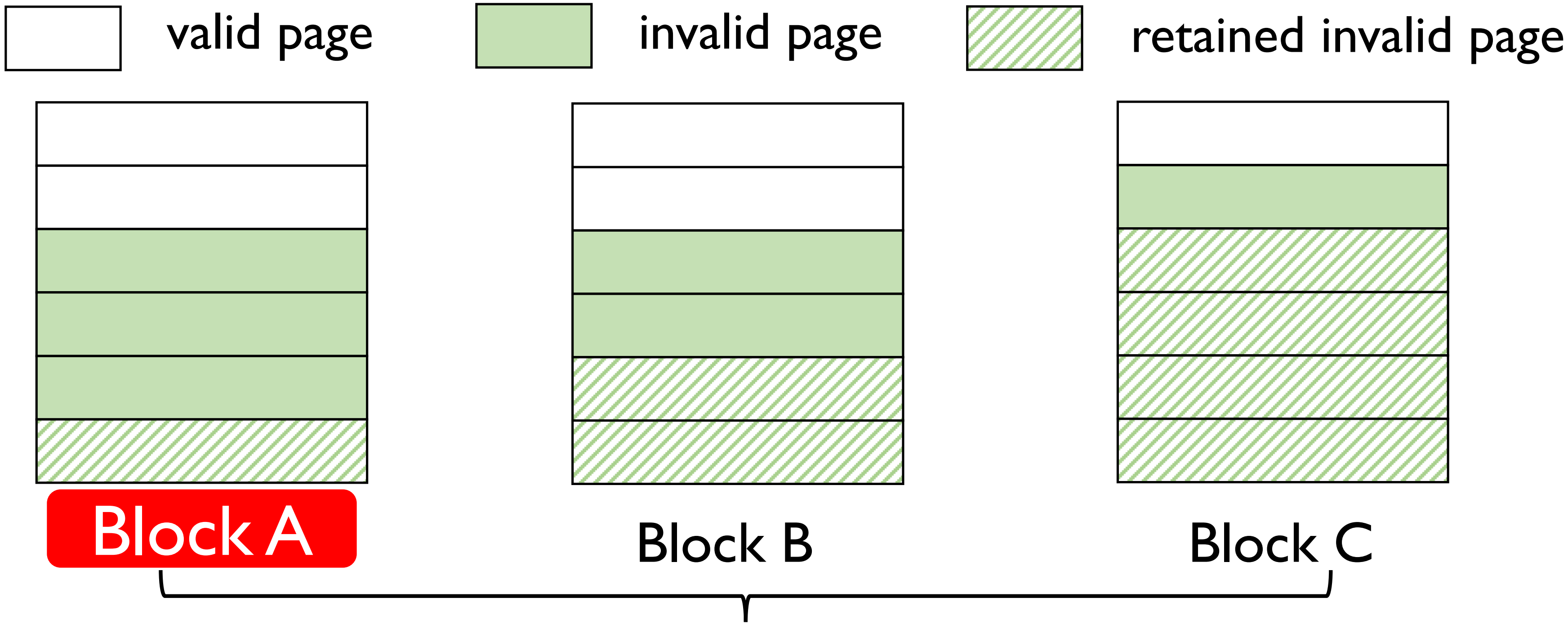
🟩 invalid page

▨ retained invalid page

select flash lock (greedy algorithm)

copy valid and retained invalid pages to a new block

Ransomware-Award Garbage Collection in FlashGuard



select flash lock (greedy algorithm)

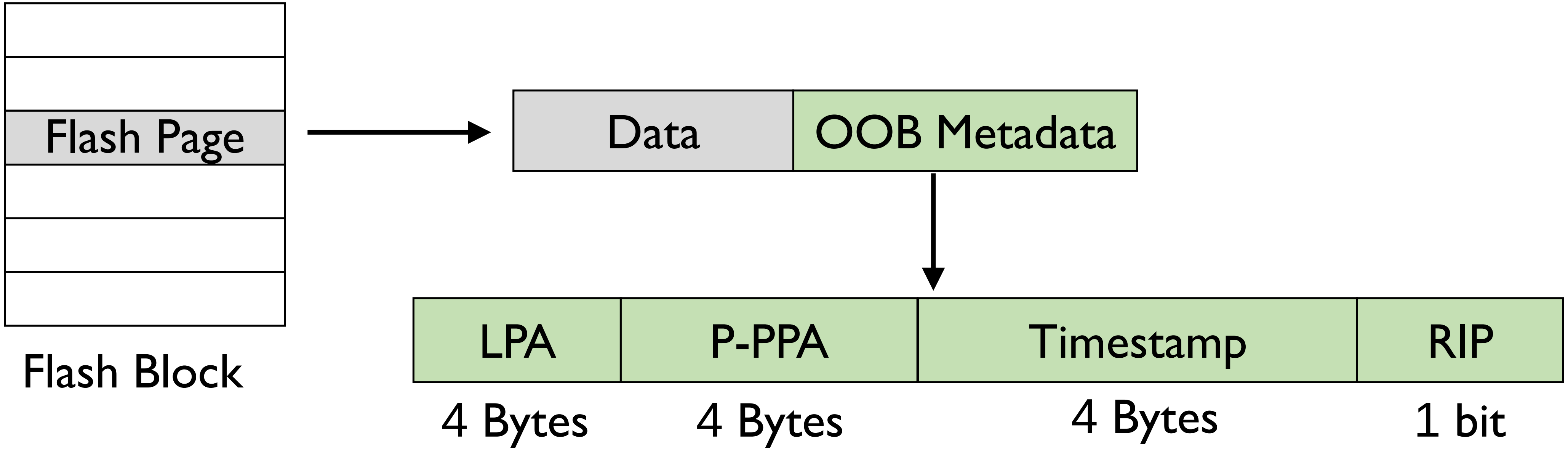
↓

copy valid and retained invalid pages to a new block

↓

erase old flash block

Data Recovery in FlashGuard



Flash Page

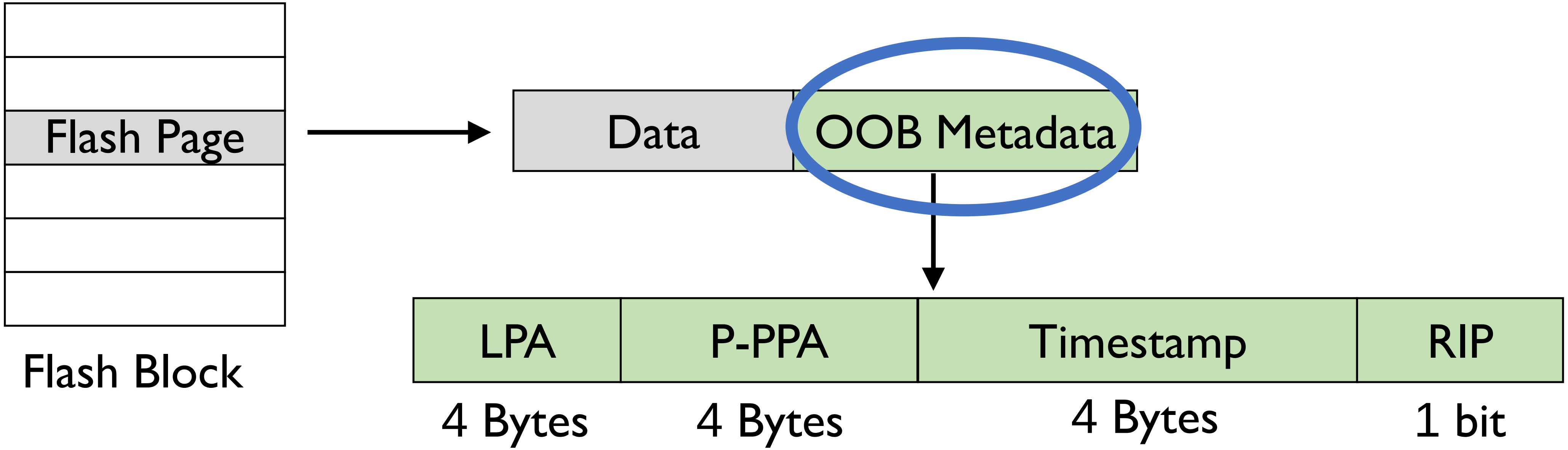
Flash Block

Data

OOB Metadata

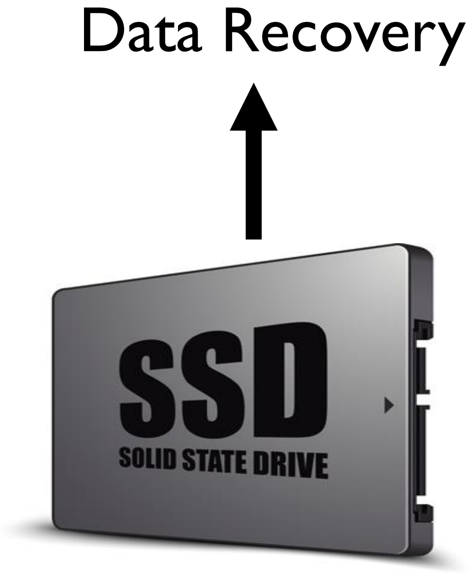
LPA	P-PPA	Timestamp	RIP
4 Bytes	4 Bytes	4 Bytes	1 bit

Data Recovery in FlashGuard



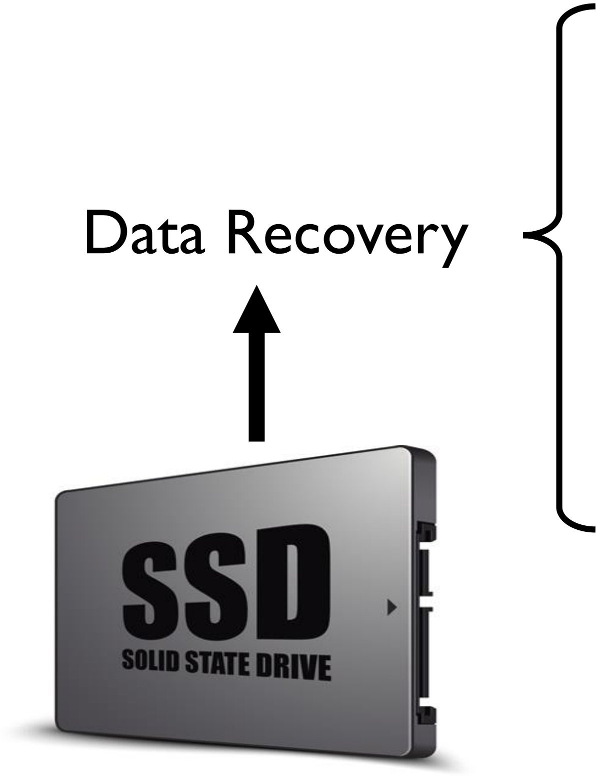
Leveraging OOB metadata to retrieve index information for recovery

Data Recovery in FlashGuard



Data Recovery

Data Recovery in FlashGuard

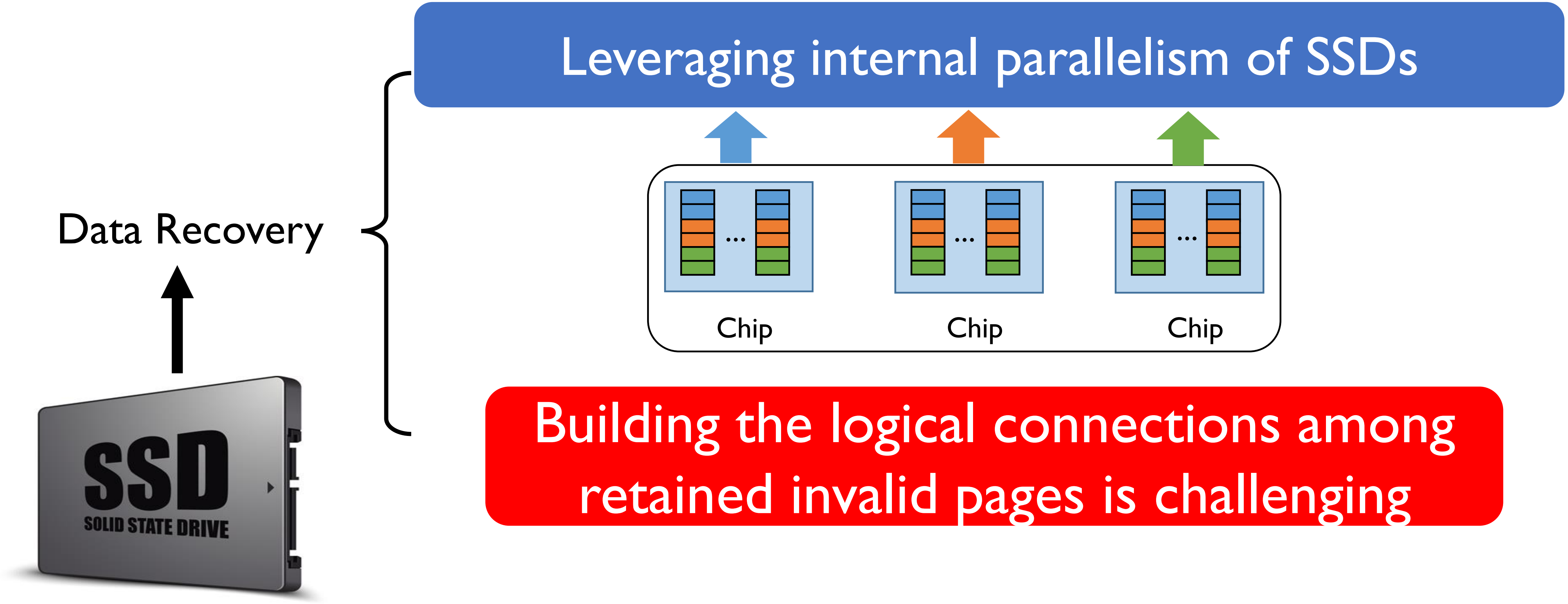


Data Recovery

Checking flash block one by one is slow

Building the logical connections among retained invalid pages is challenging

Data Recovery in FlashGuard



Leveraging internal parallelism of SSDs

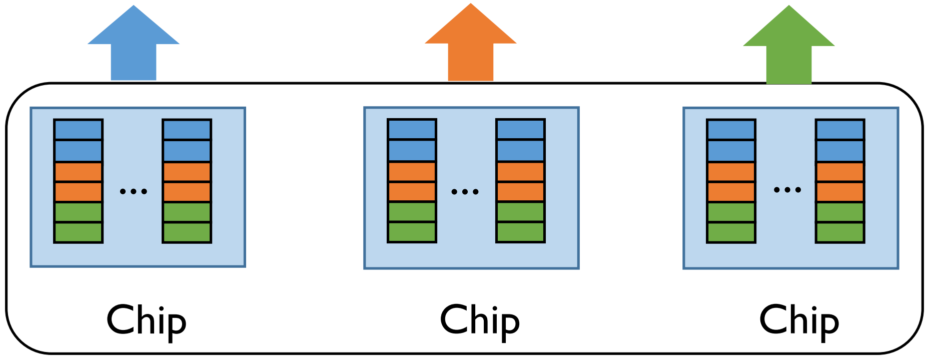
Data Recovery

Building the logical connections among retained invalid pages is challenging

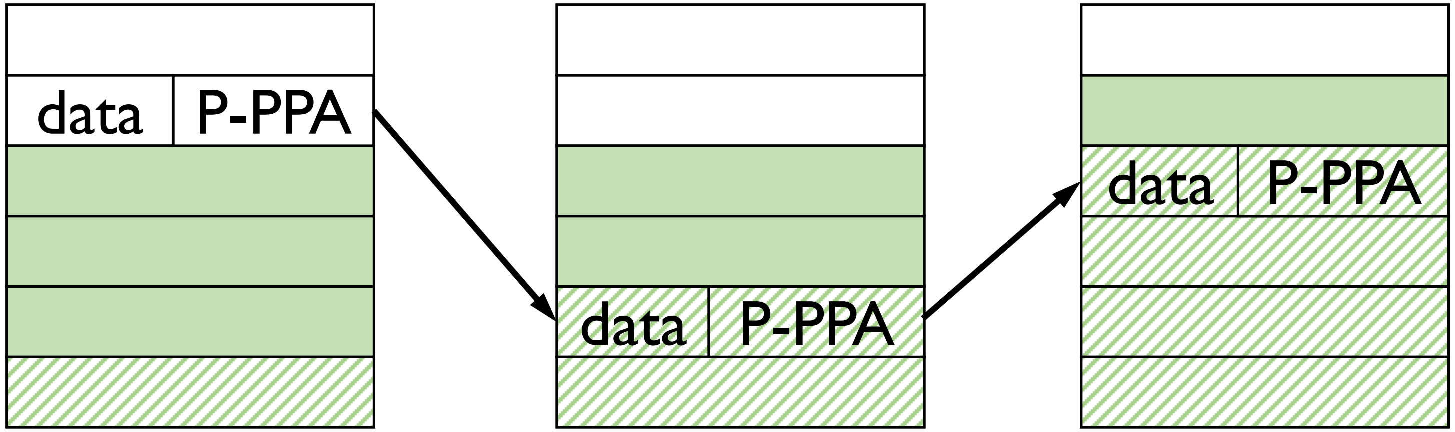
Data Recovery in FlashGuard

Data Recovery

Leveraging internal parallelism of SSDs



Leveraging previous-PPA stored in OOB metadata



FlashGuard Experimental Setup

Programmable SSD

1 TB
64 pages/block
4 KB/page
over-provisioning ratio: 15%

FlashGuard Experimental Setup

Programmable SSD

1 TB
64 pages/block
4 KB/page
over-provisioning ratio: 15%

Ransomware Samples

1,477 ransomware samples (VirusTotal)

FlashGuard Experimental Setup

Programmable SSD

1 TB
64 pages/block
4 KB/page
over-provisioning ratio: 15%

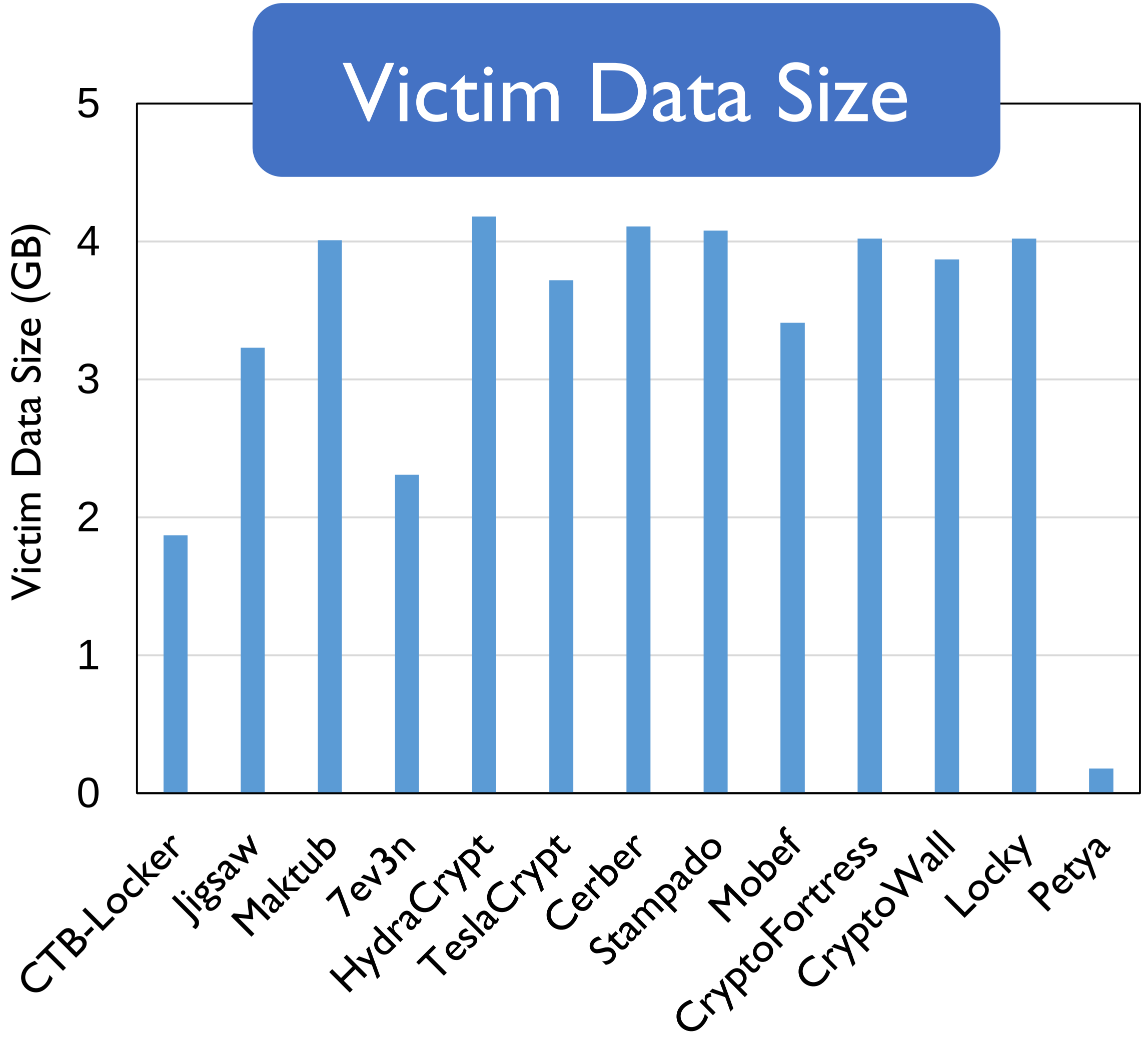
Ransomware Samples

1,477 ransomware samples (VirusTotal)

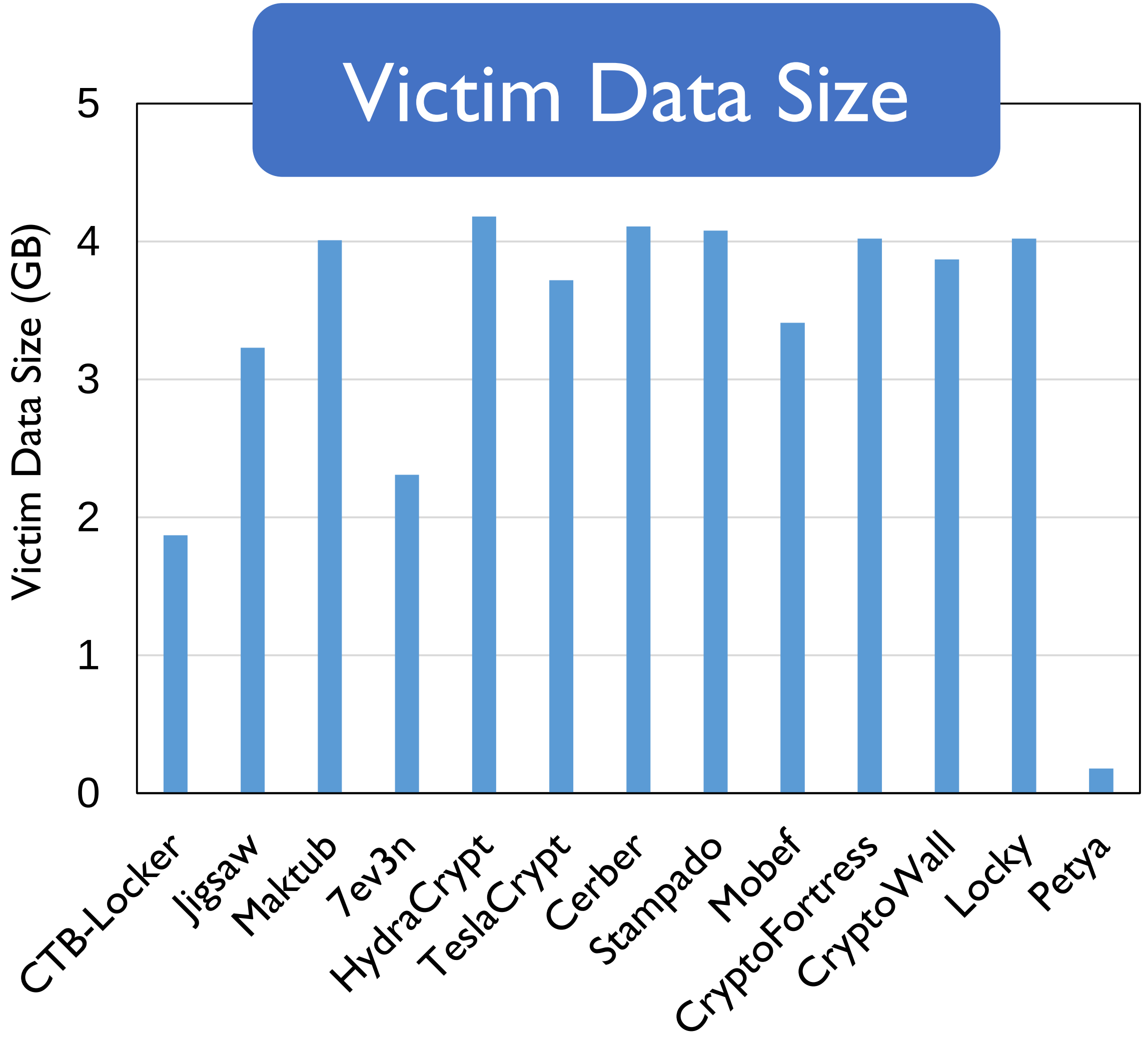
Storage Workloads

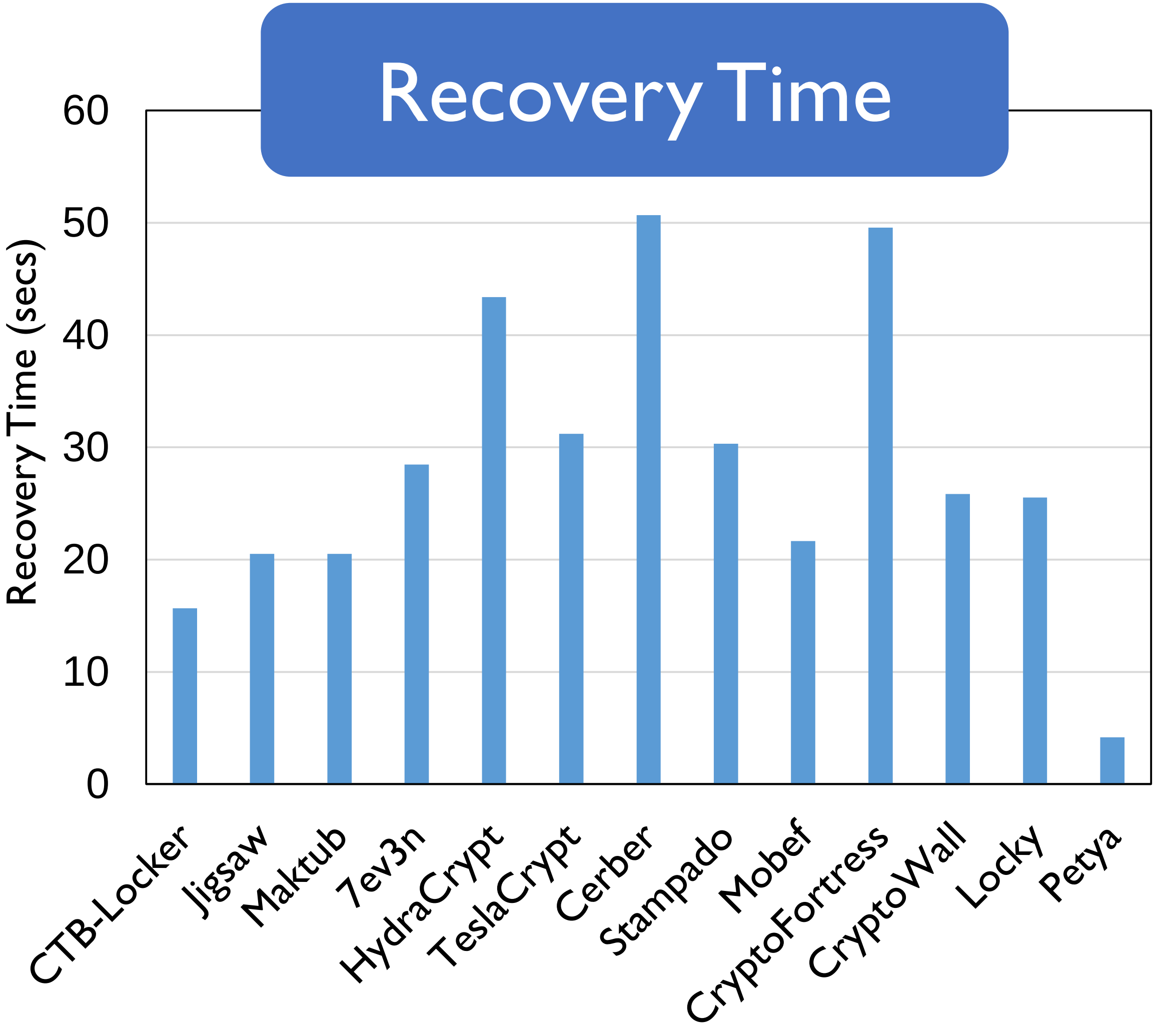
Enterprise servers (11 workloads)
University machines (6 workloads)
Storage benchmarks: IOZone/Postmark
Database workloads (TPCC/TPCE)

Recovery Time of Ransomware Samples

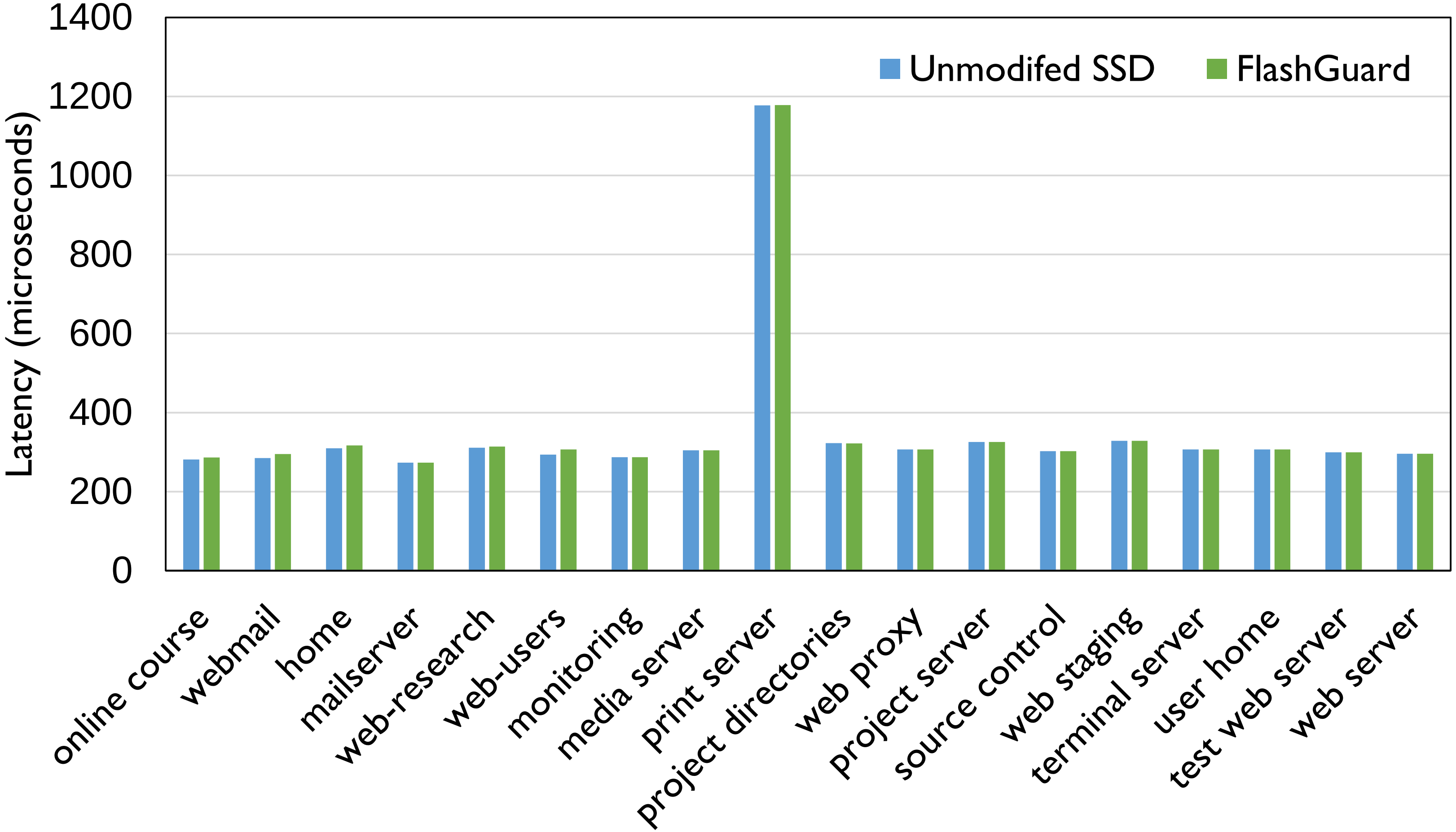


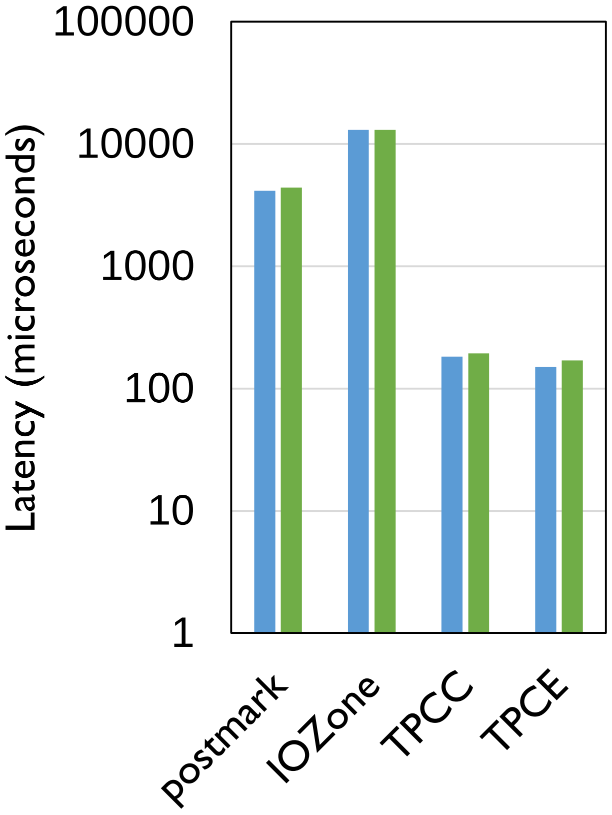
Recovery Time of Ransomware Samples





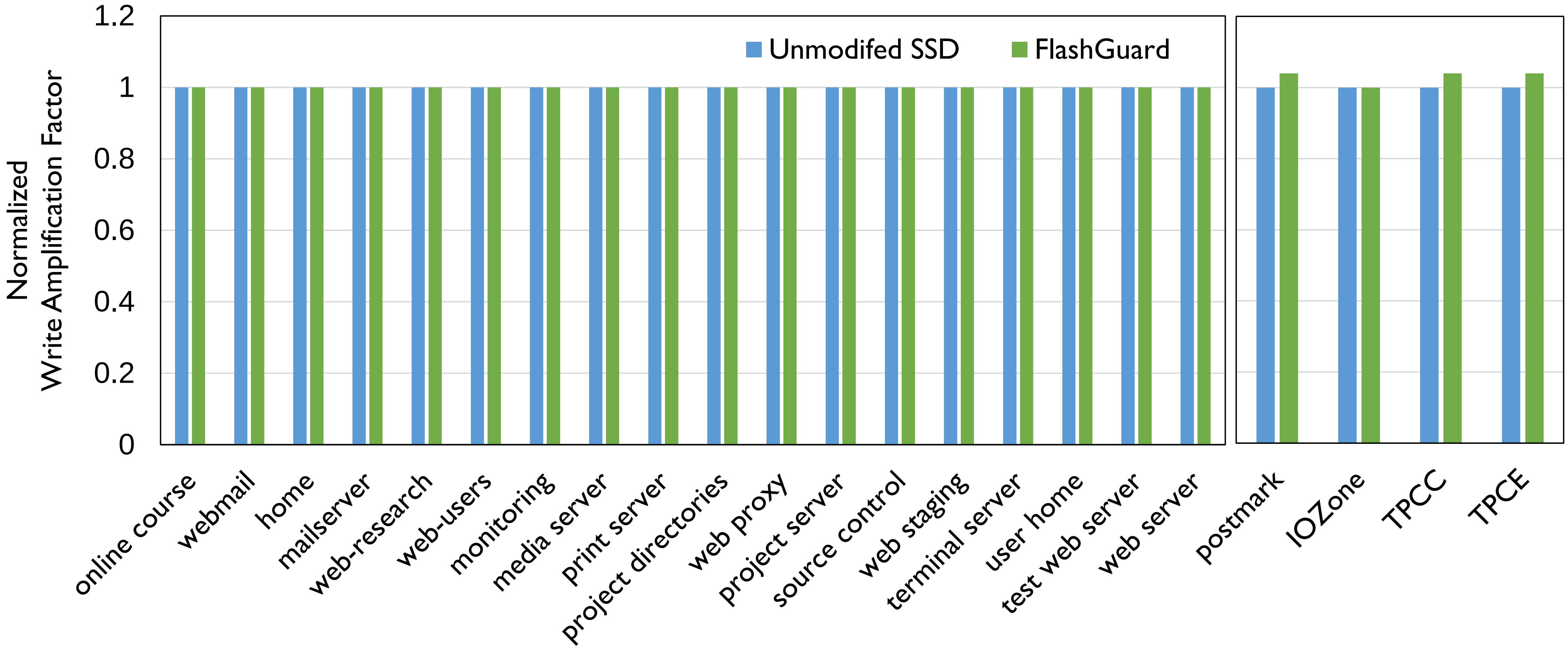
Impact on Regular Storage Operations





FlashGuard decreases the storage performance by 6% for I/O-intensive workloads

Impact on SSD Lifetime



FlashGuard increases the WAF by 4%
due to the additional page movements in GC

Potential Attacks and Future Work

GC Attack

Potential Attacks and Future Work

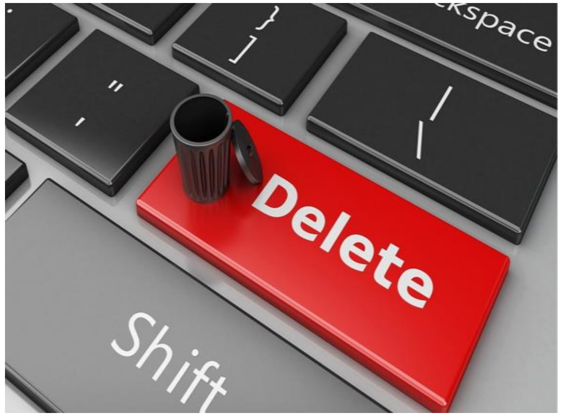
GC Attack

Timing Attack

Potential Attacks and Future Work

GC Attack

Timing Attack



Secure Deletion

FlashGuard Summary

Hardware-assisted Defense
Against Encryption Ransomware

Negligible Impact on
SSD performance & lifetime

Thanks!

Jian Huang[†] [‡]
jianh@illinois.edu

Jun Xu Xinyu Xing Peng Liu Moinuddin K. Qureshi [†]

[†] Georgia Tech

[‡] ILLINOIS
UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

PennState

Q&A