Hypervisor-based Background Encryption

Yushi　OMOTE
祐志　表

University of Tsukuba

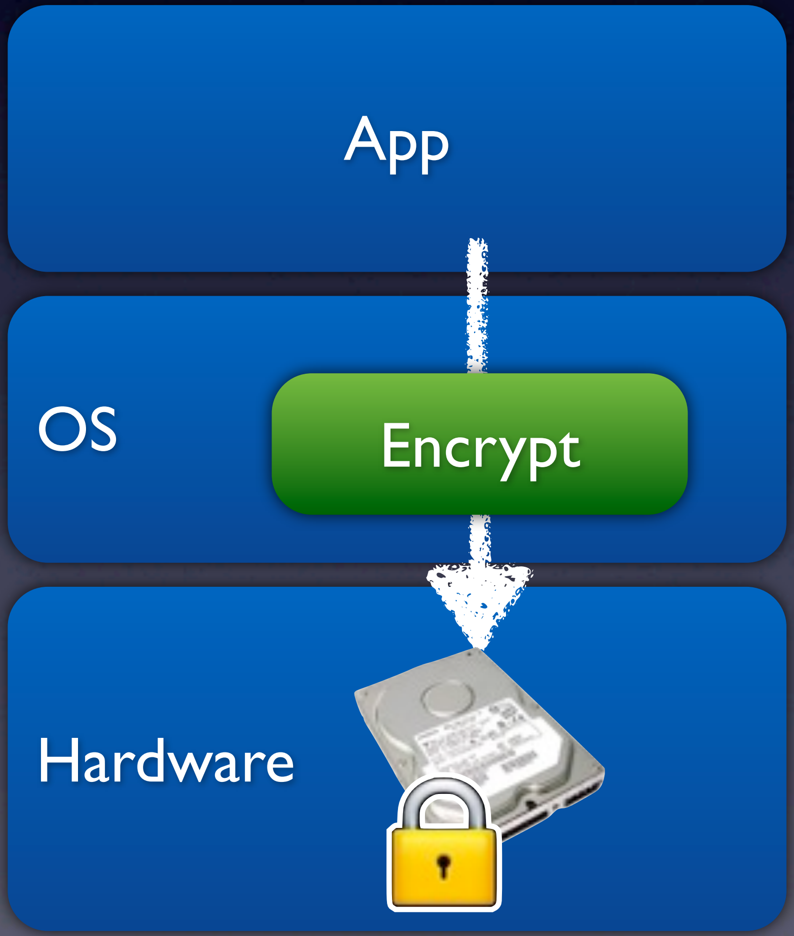
Full-Disk Encryption (FDE)

- Recent study shows 10% of laptop computers are lost or stolen every year*
- To prevent data breach, many organizations deploy FDE
- FDE encrypts and protects entire contents in hard disks

* Ponemon Institute LLC. Business risk of a lost laptop, April 2009.

OS-based FDE

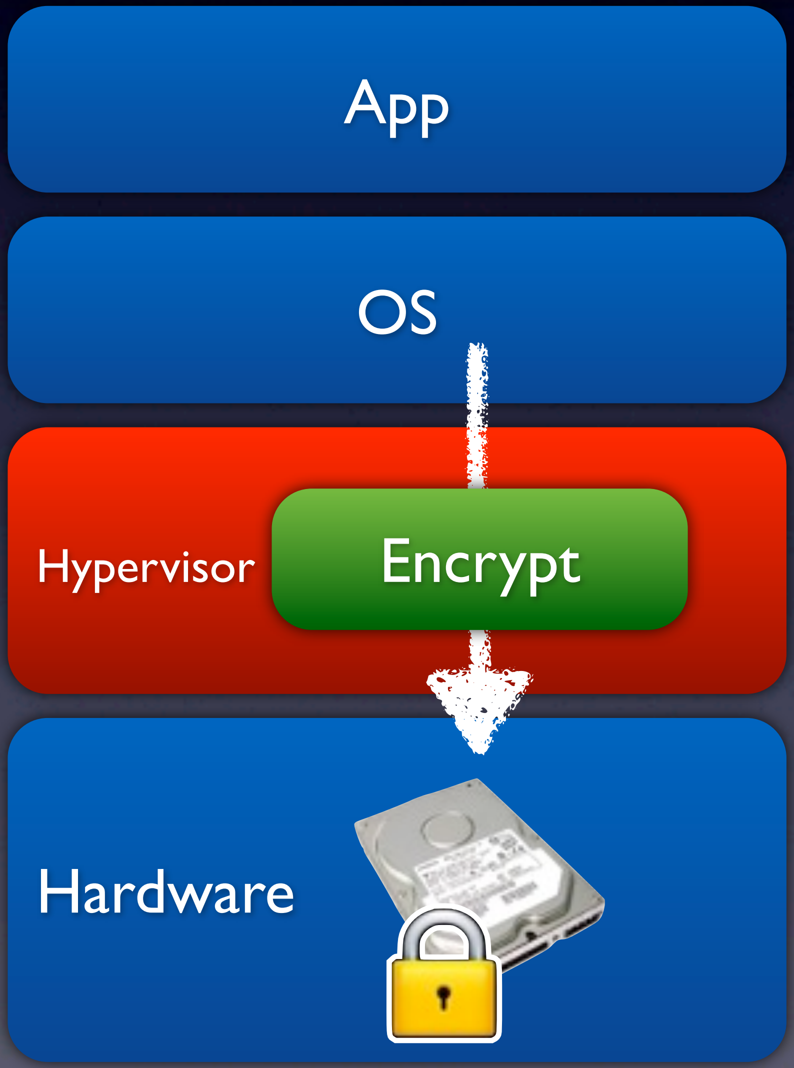
- Commonly-used approach in practice
  - Low initial deployment cost
    - Instant installation
    - Background encryption support
- Some drawbacks
  - OS vulnerability
  - OS dependency



ex) BitLocker, Endpoint Encryption, Compusec, WinMagic,...

Hypervisor-based FDE

- Secure & OS-independent approach
- However, HIGH initial deployment cost
  - Manual encryption
    - No background encryption support
  - P2V conversion
    - Put OS on hypervisor
  - Hypervisor installation
    - Host OS with configuration

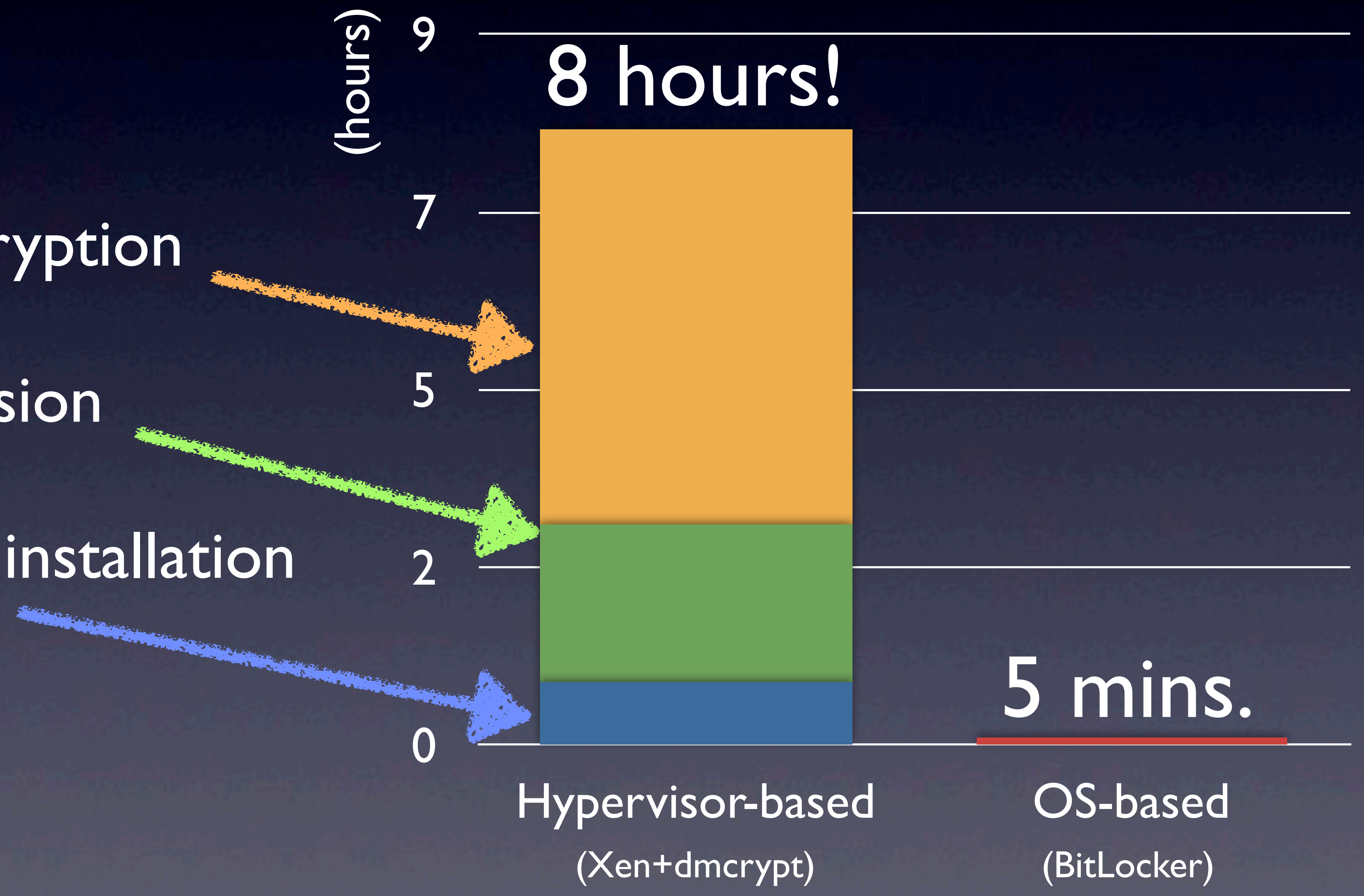


ex) Xen-based FDE [Liang'10], TcVisor [Rezaei'10], BitVisor [Shinagawa'09]...

Hypervisor-based FDE requires so much time for deployment

- Manual encryption
- P2V conversion
- Hypervisor installation

Required time before user can start using PC

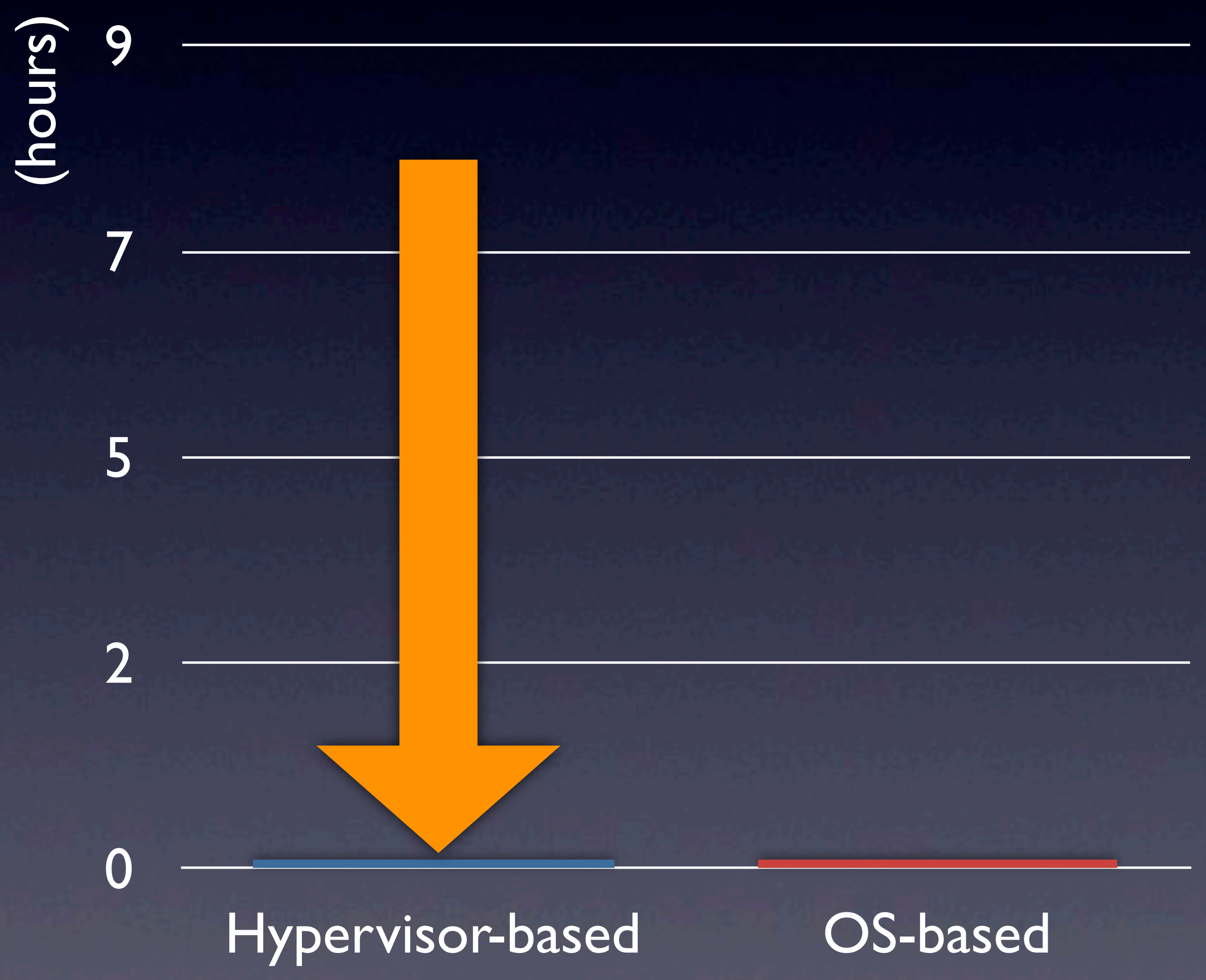


Encryption for pre-installed OS (1TB partition)

Our Goal

- ~~Manual encryption~~
- ~~P2V conversion~~
- ~~Hypervisor installation~~

Required time before user can start using PC

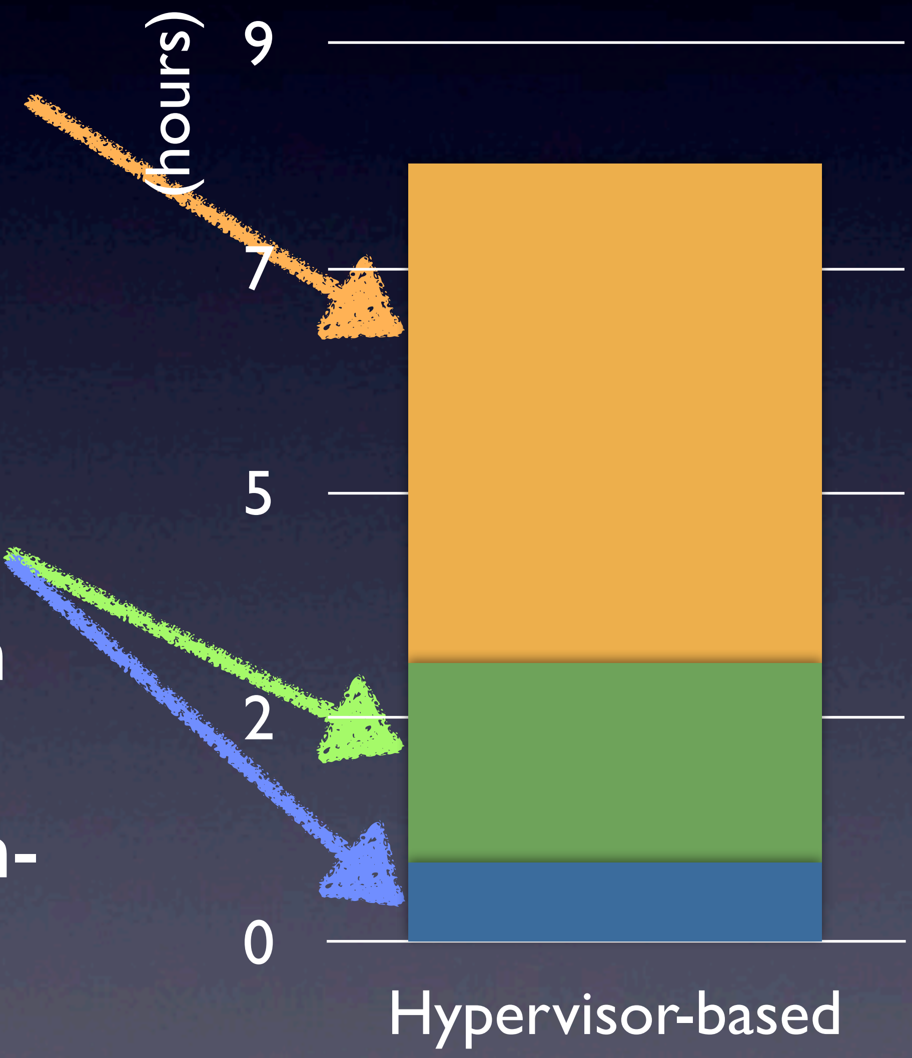


Encryption for pre-installed OS (1TB partition)

Approach

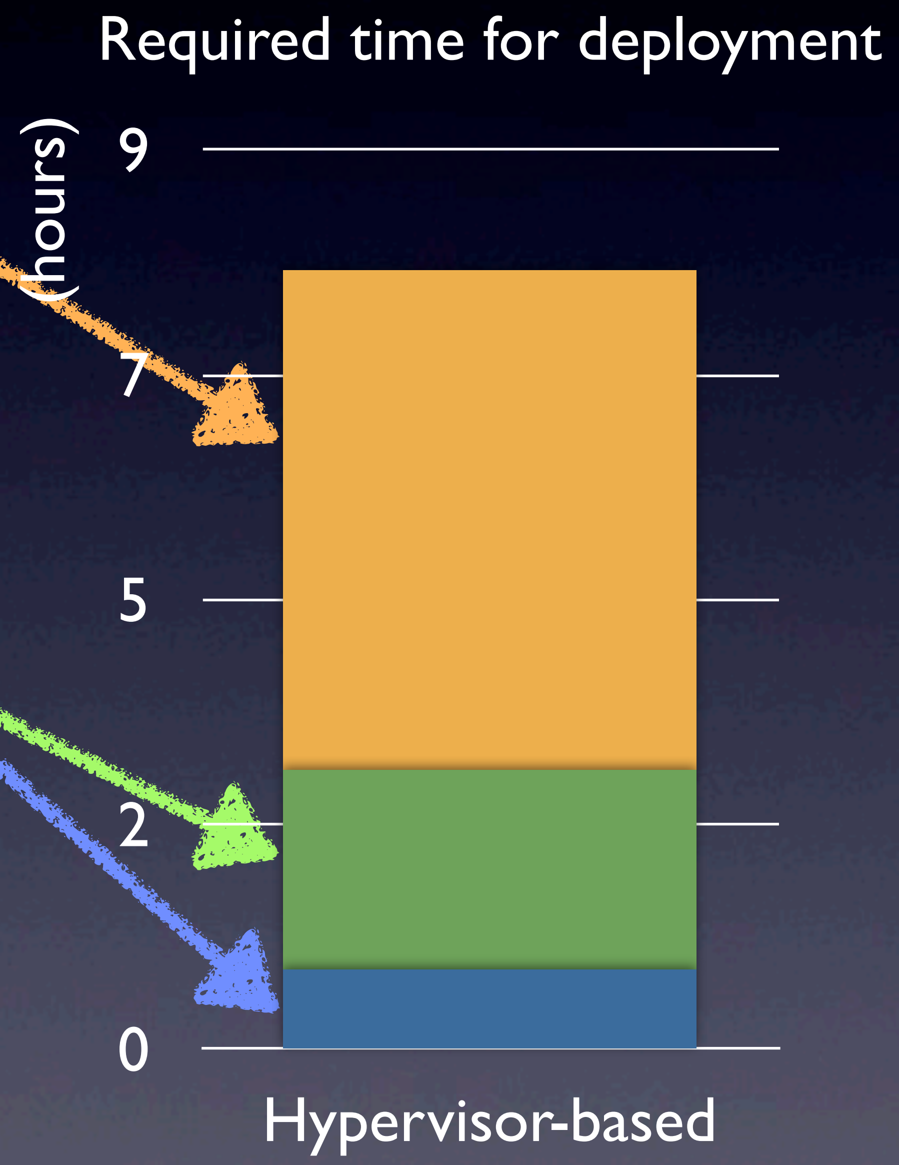
- To remove Manual encryption
  - Implement background encryption in hypervisor
- To remove P2V conversion & simplify hypervisor installation
  - Leverage Para-pass-through-based hypervisor [Shinagawa'09]

Required time for deployment



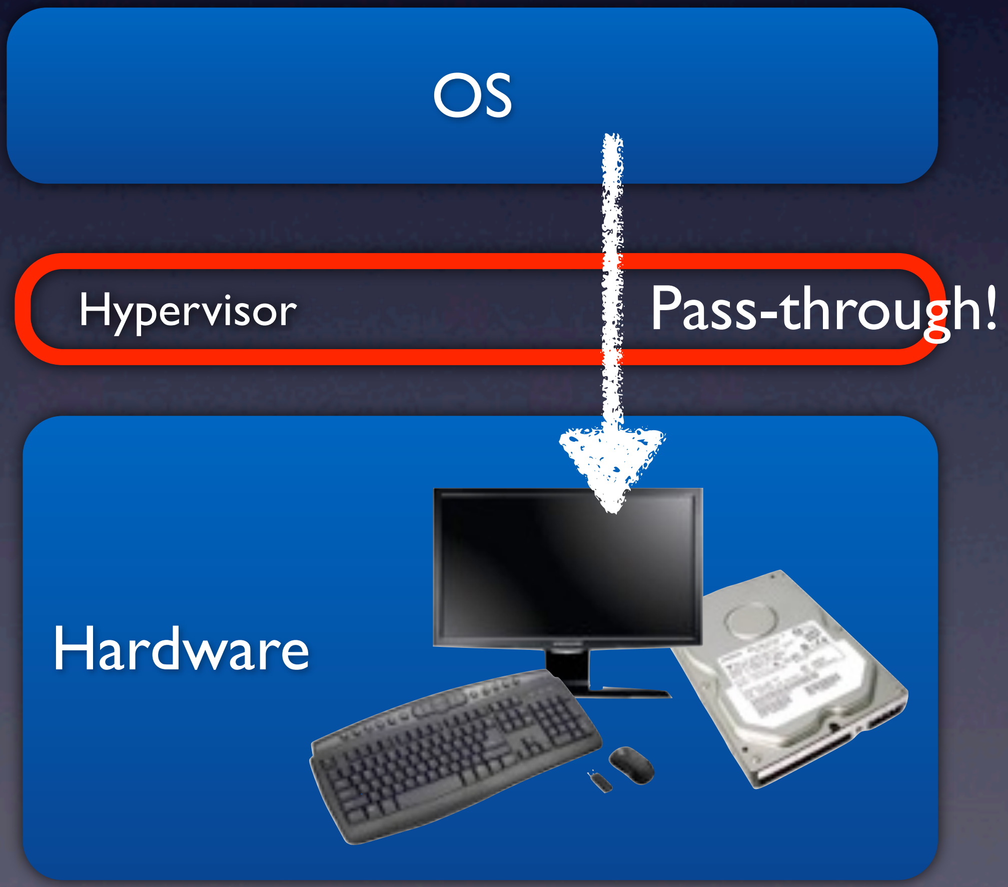
Approach

- To remove Manual encryption
  - Implement background encryption in hypervisor
- To remove P2V conversion & simplify hypervisor installation
  - Leverage Para-pass-through-based hypervisor [Shinagawa'09]



Para-pass-through-based Hypervisor (BitVisor VEE'09)

- Avoid P2V conversion
  - Most I/Os pass-through from guest OS
  - Make 'Virtual' identical to 'Physical'
- Simplify hypervisor installation
  - Guest directly handles devices
  - No host OS



OS

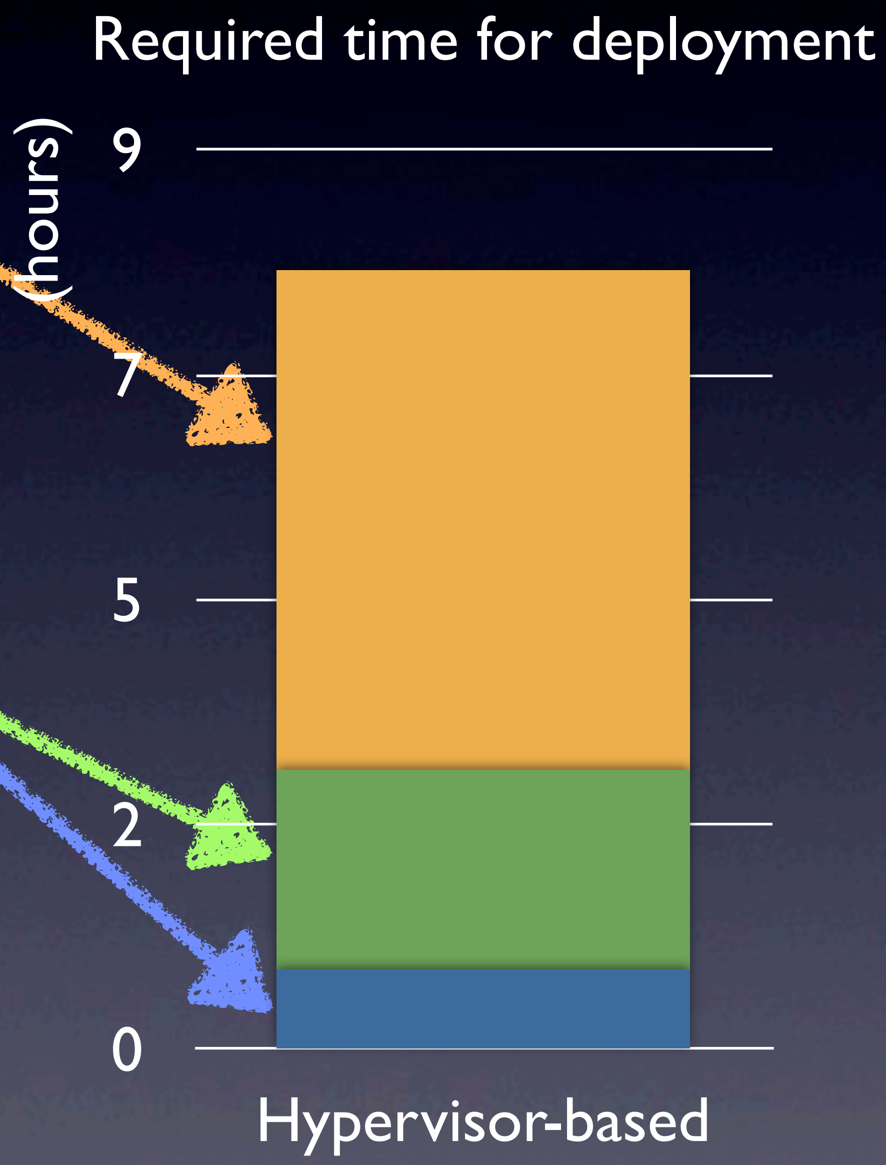
Hypervisor

Pass-through!

Hardware

Approach

- To remove Manual encryption
  - Implement background encryption in hypervisor
- To remove P2V conversion & simplify hypervisor installation
  - Leverage Para-pass-through-based hypervisor [Shinagawa'09]

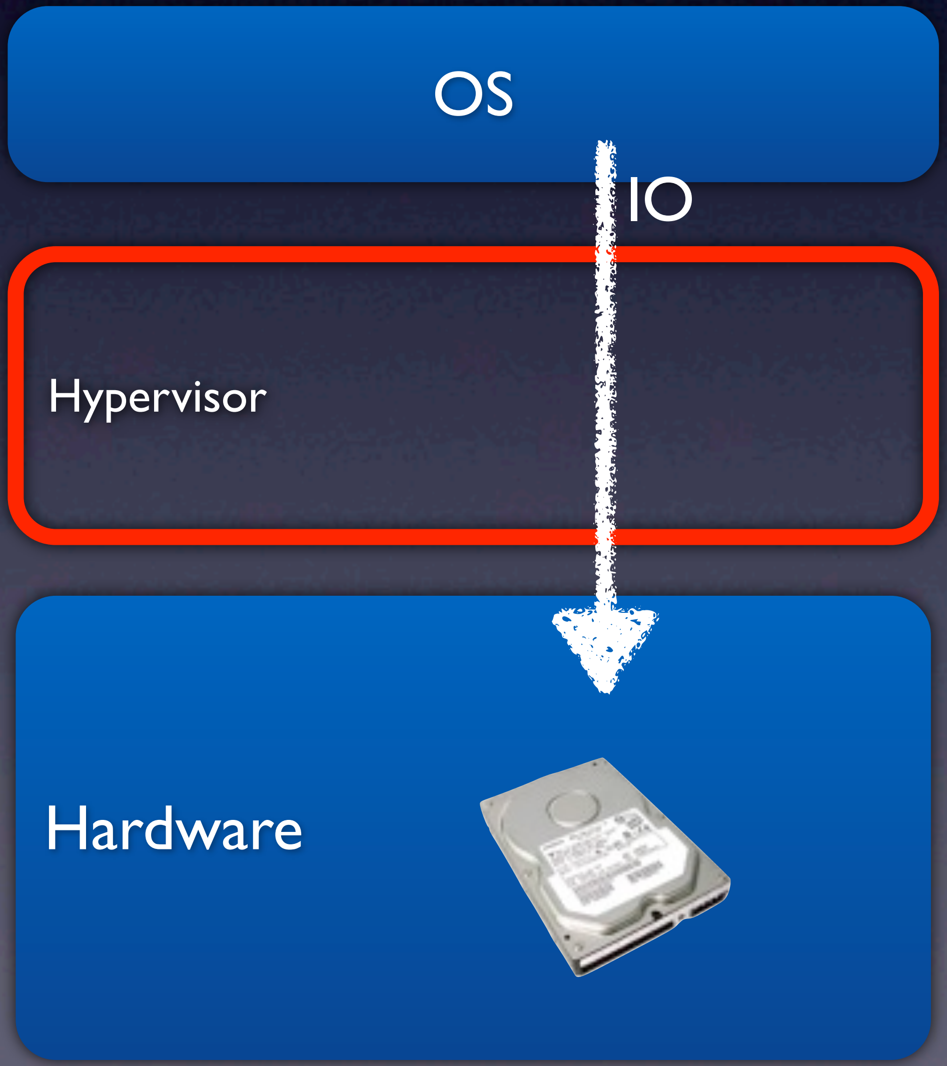


Encryption for pre-installed OS (500GB partition)

Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS

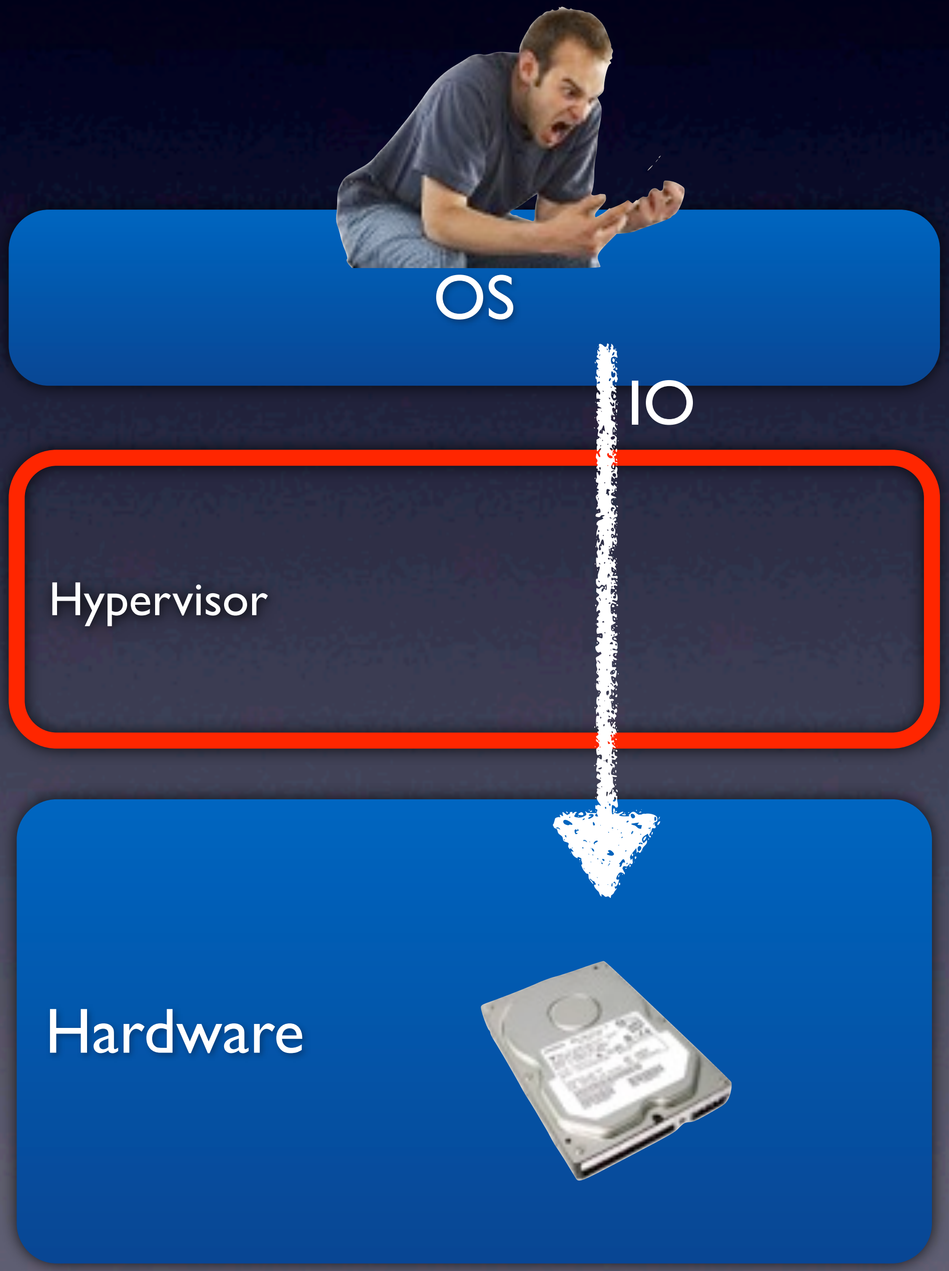
- Guest performance
- IO intermixture
- Read/write timing



Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS

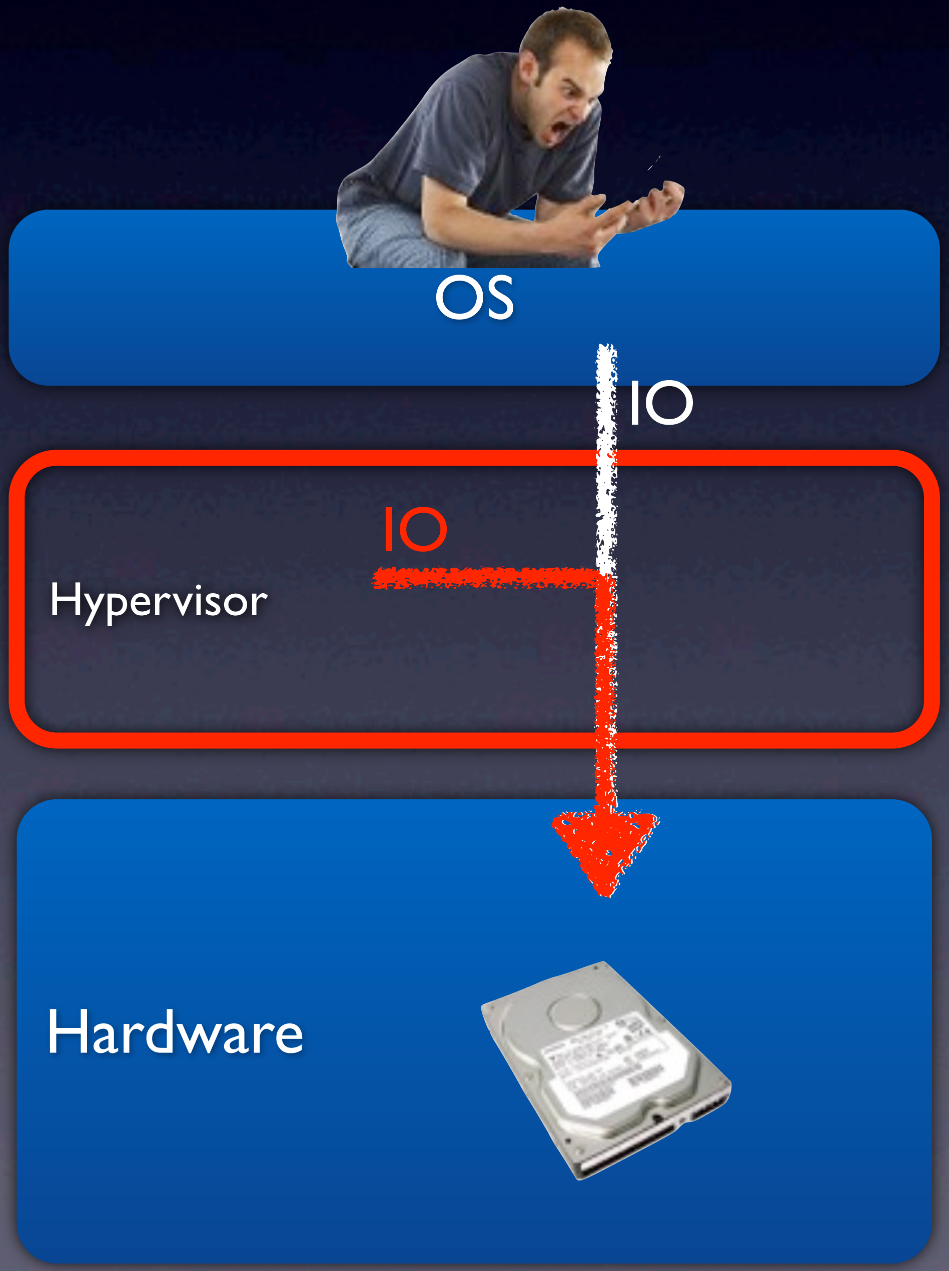
- Guest performance
- IO intermixture
- Read/write timing



Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS

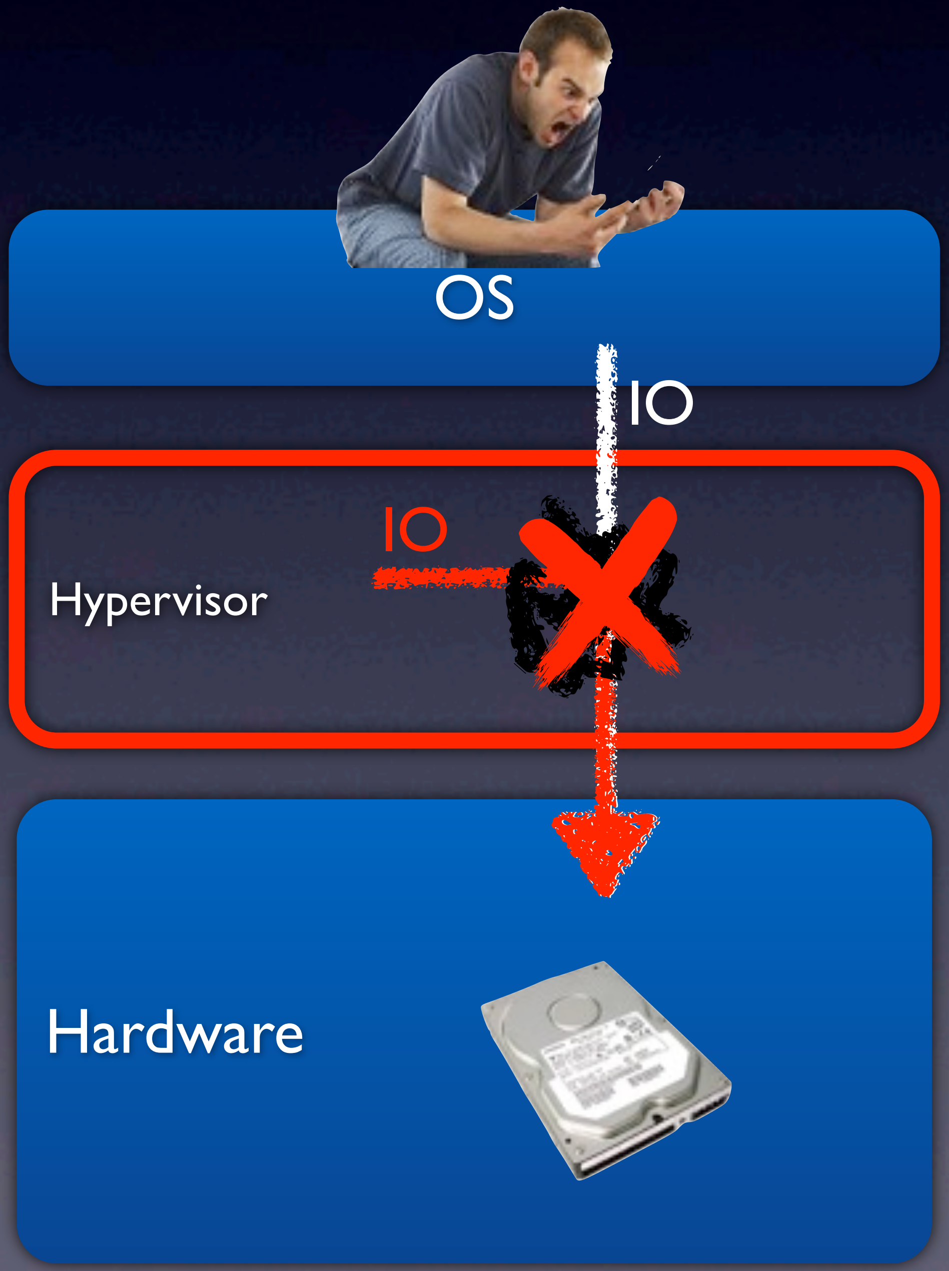
- Guest performance
- IO intermixture
- Read/write timing



Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS

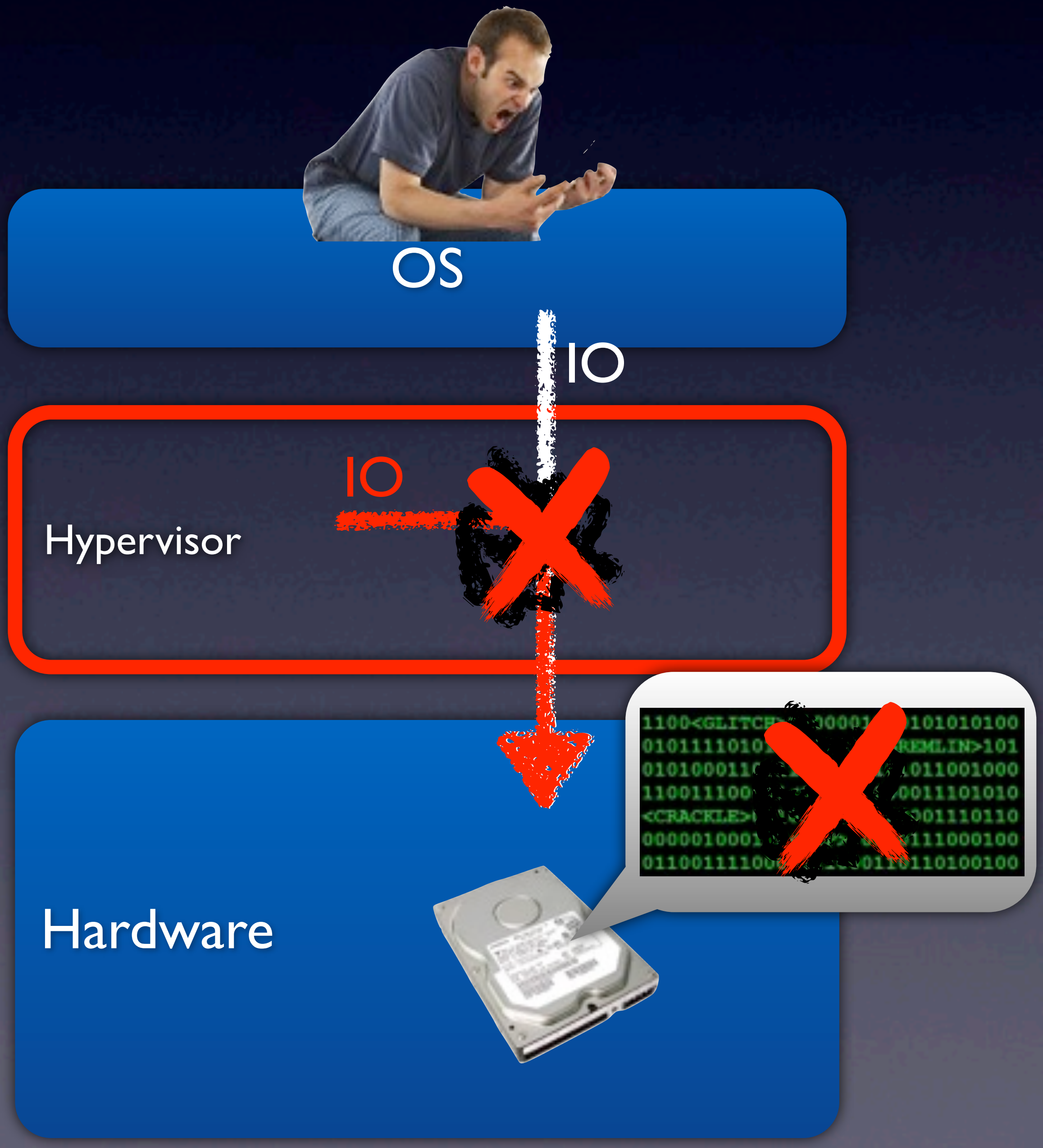
- Guest performance
- IO intermixture
- Read/write timing



Background Encryption in Hypervisor

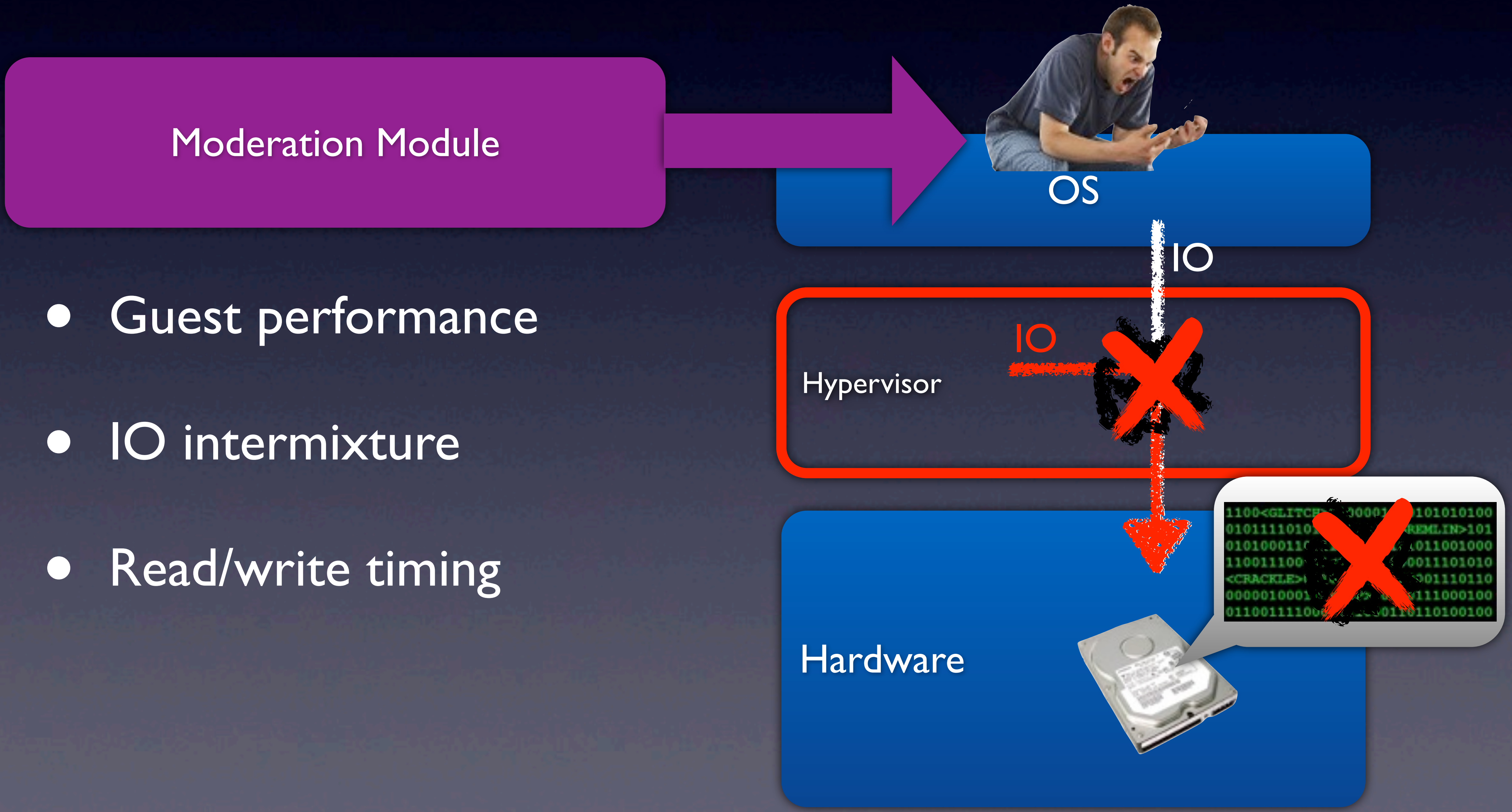
Hypervisor reads/encrypts/writes disk in parallel with guest OS

- Guest performance
- IO intermixture
- Read/write timing



Background Encryption in Hypervisor

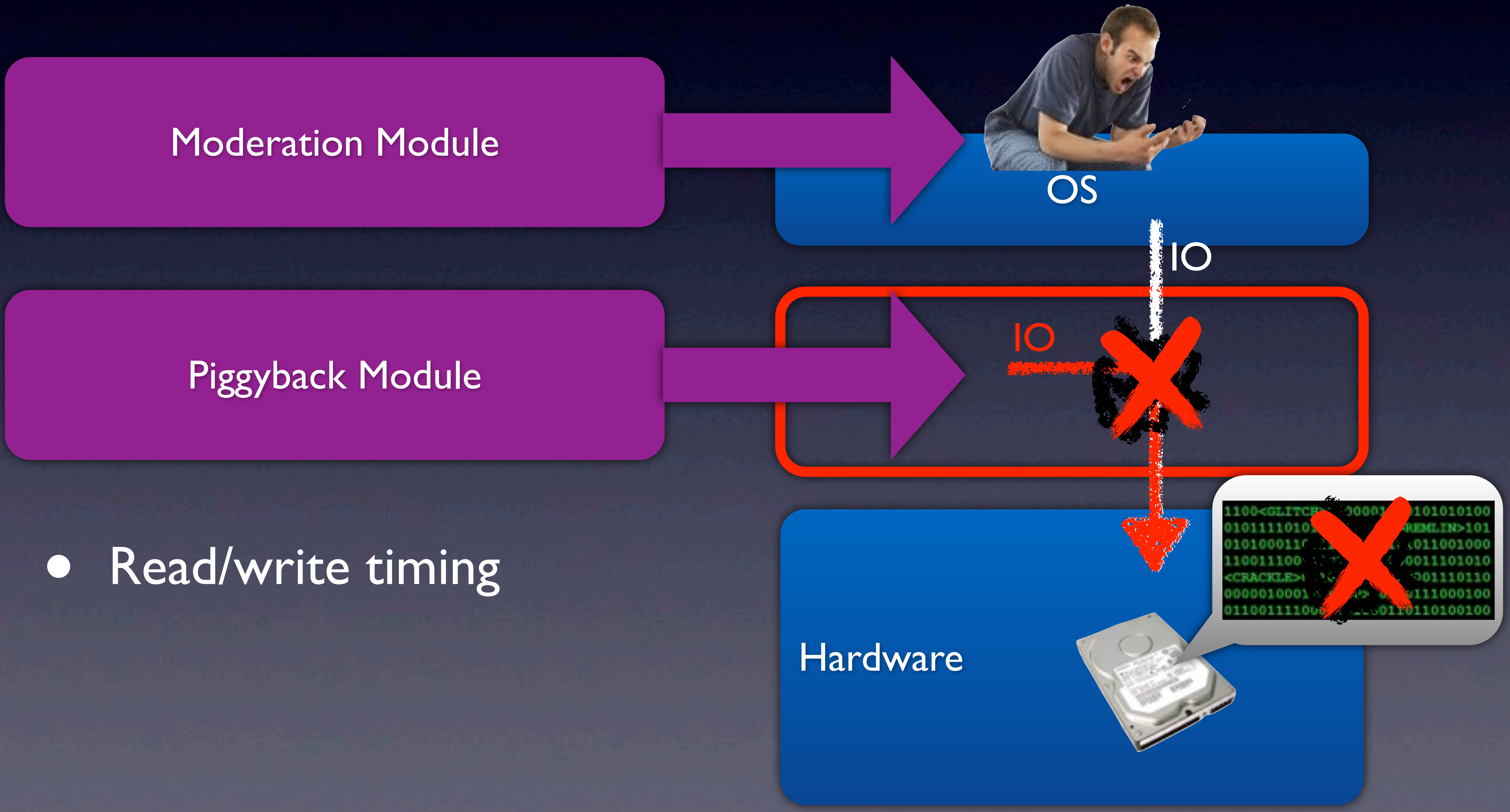
Hypervisor reads/encrypts/writes disk in parallel with guest OS



- Guest performance
- IO intermixture
- Read/write timing

Background Encryption in Hypervisor

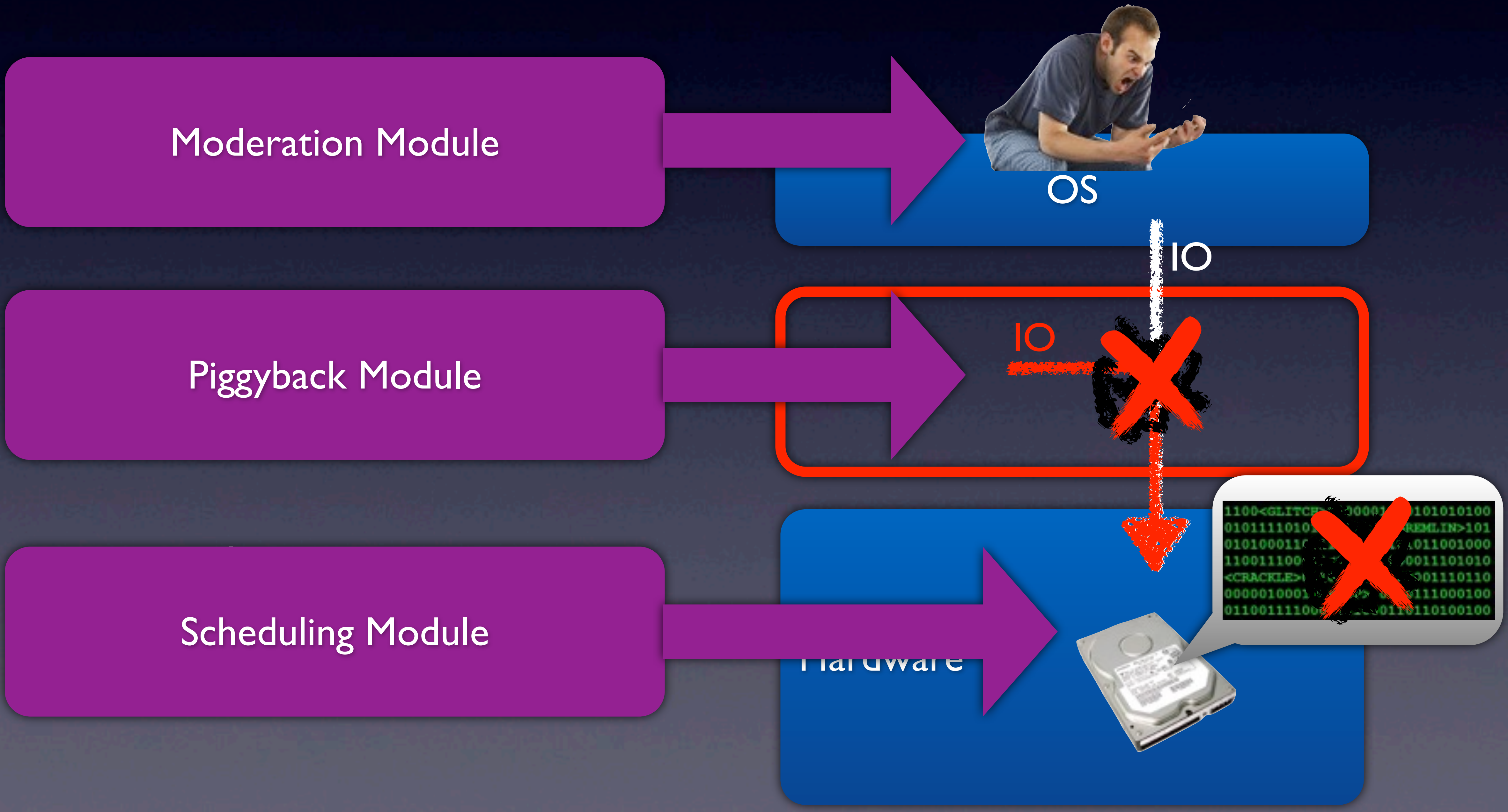
Hypervisor reads/encrypts/writes disk in parallel with guest OS



- Read/write timing

Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS


Moderation Module

Piggyback Module

Scheduling Module

OS

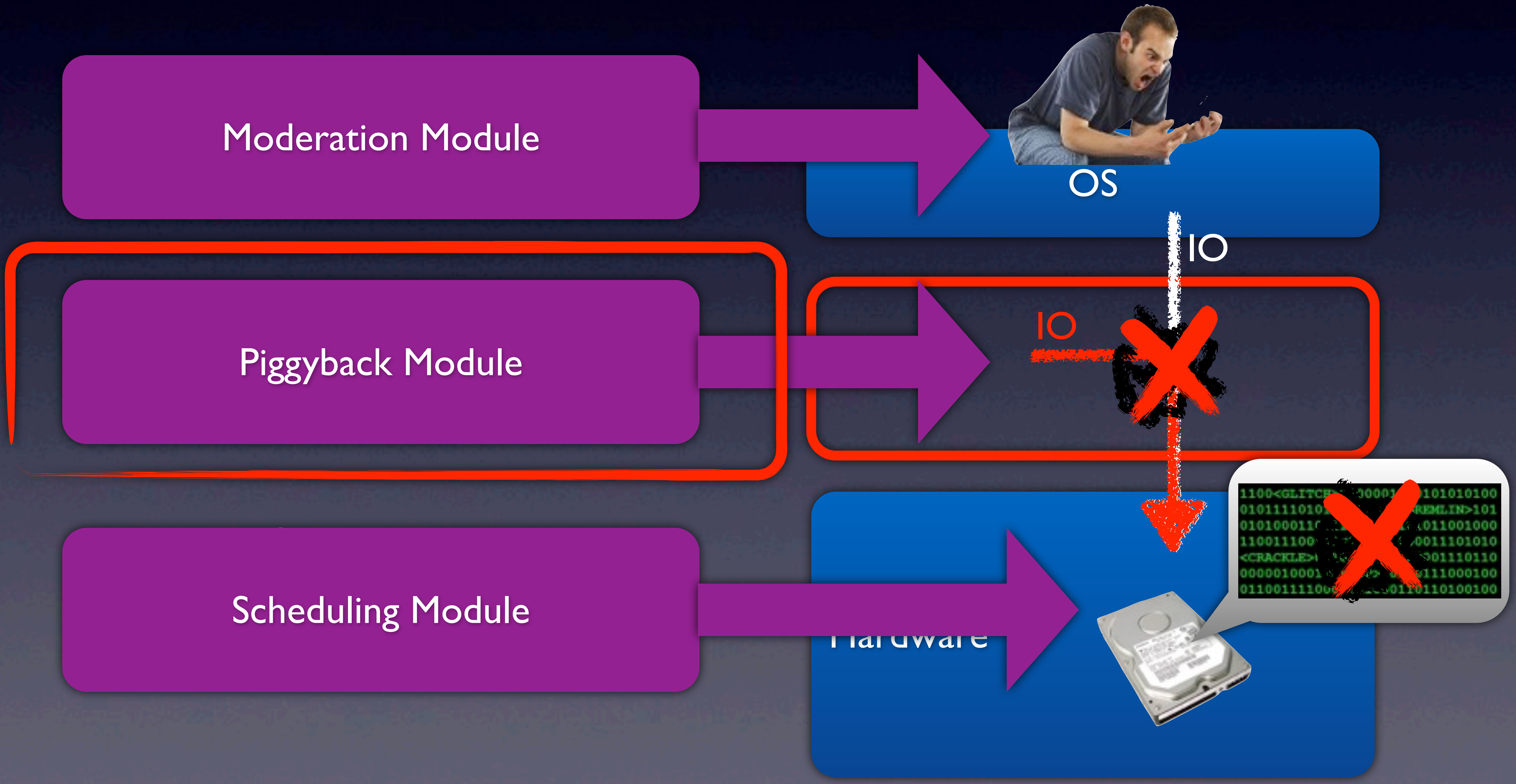
IO

IO

Hardware

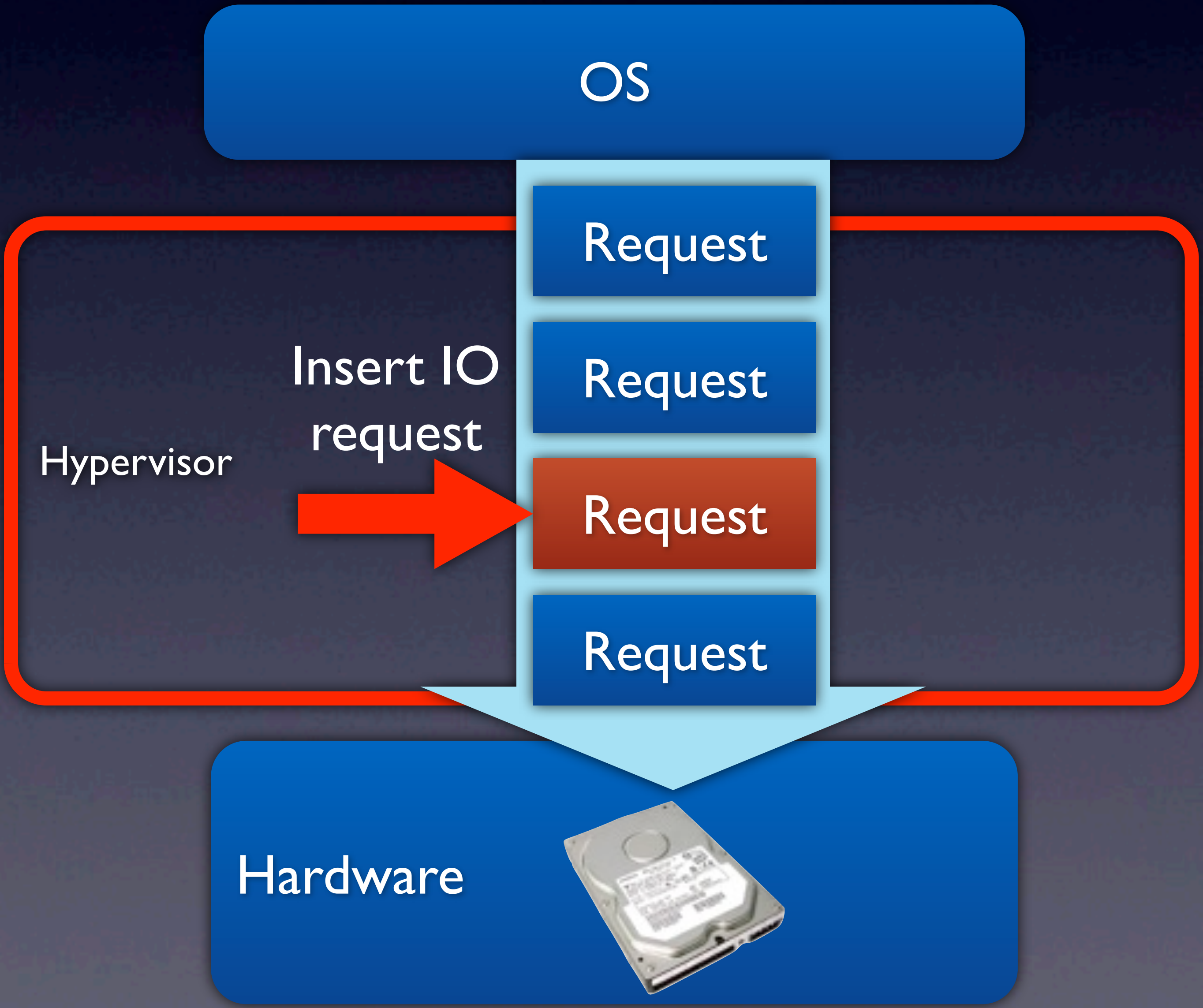
Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS



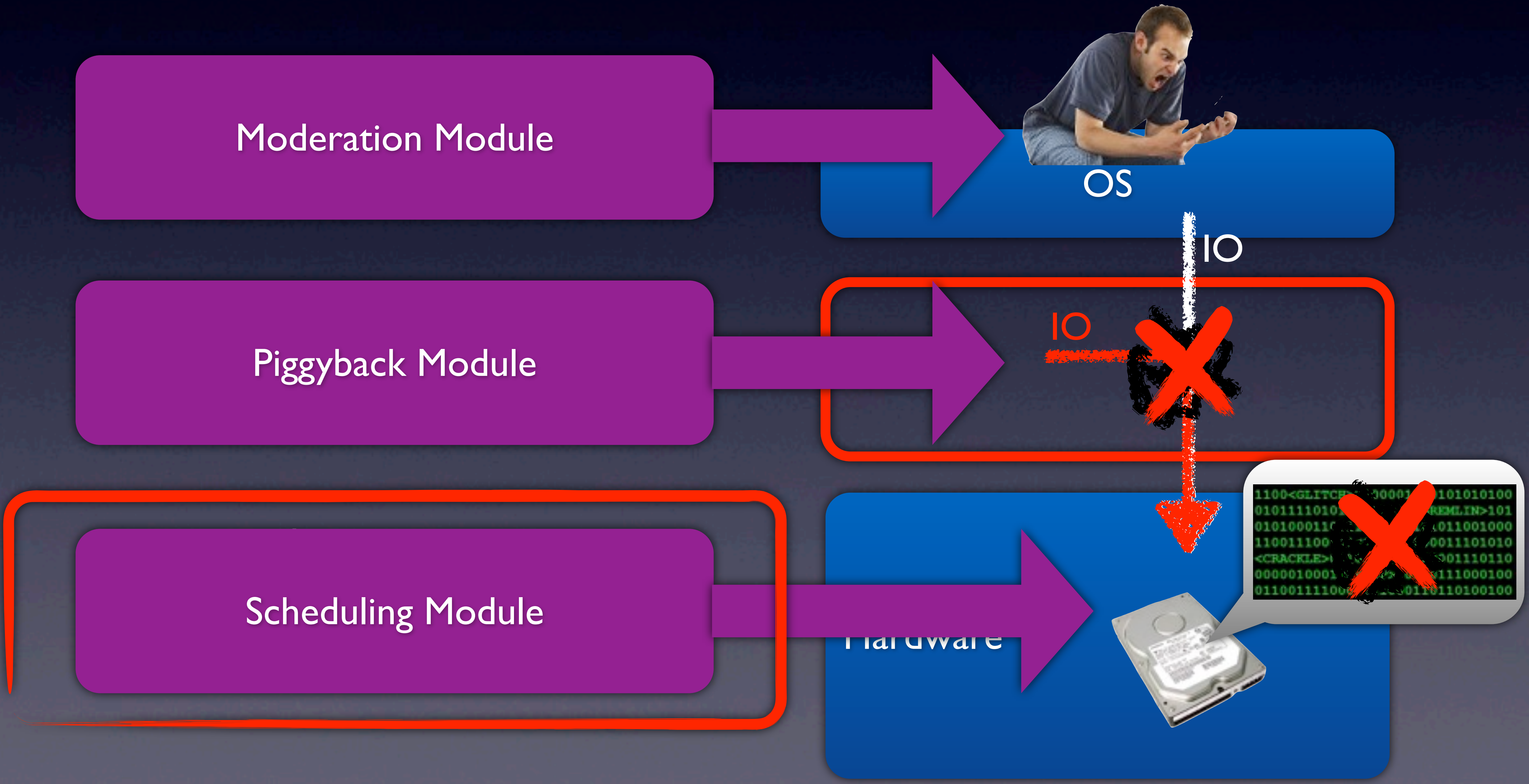
Piggyback Module

- Transparently insert hypervisor IO requests between guest requests
- Not virtualize disk interface to avoid P2V



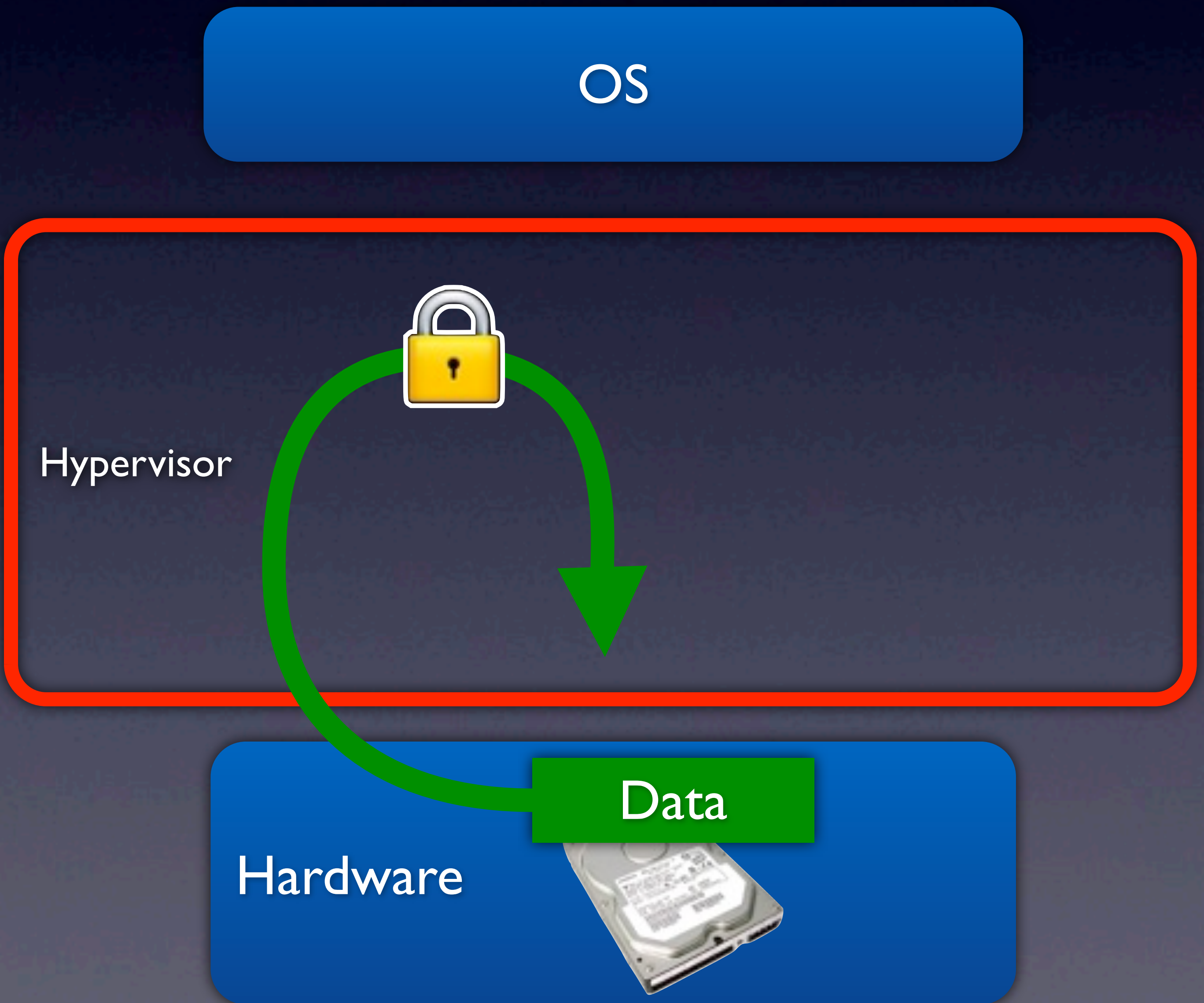
Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS



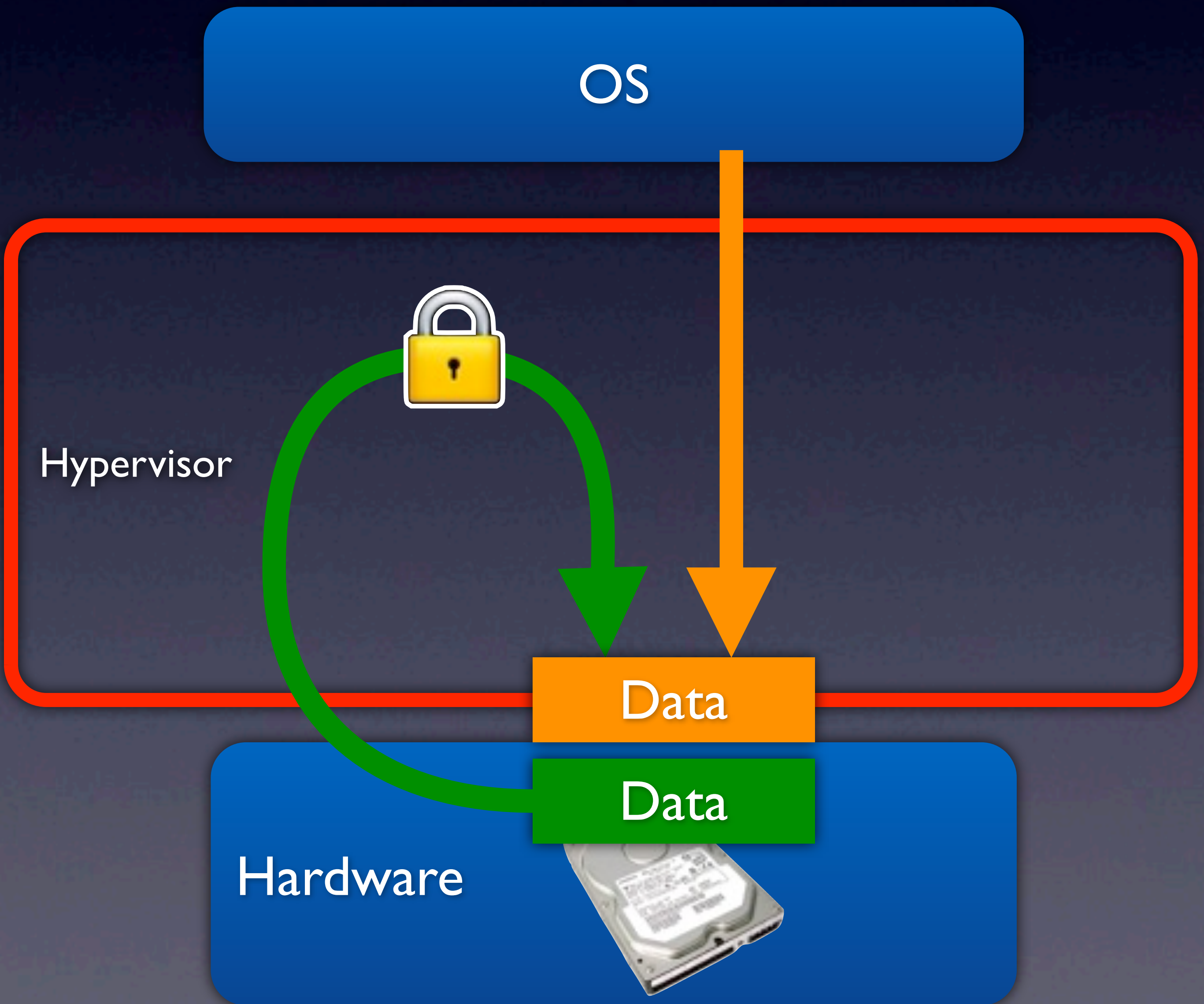
Scheduling Module

- Just before write, check if data to be written is the latest
  - Read/encrypt/CHECK&write
- If not the latest, read/encrypt again



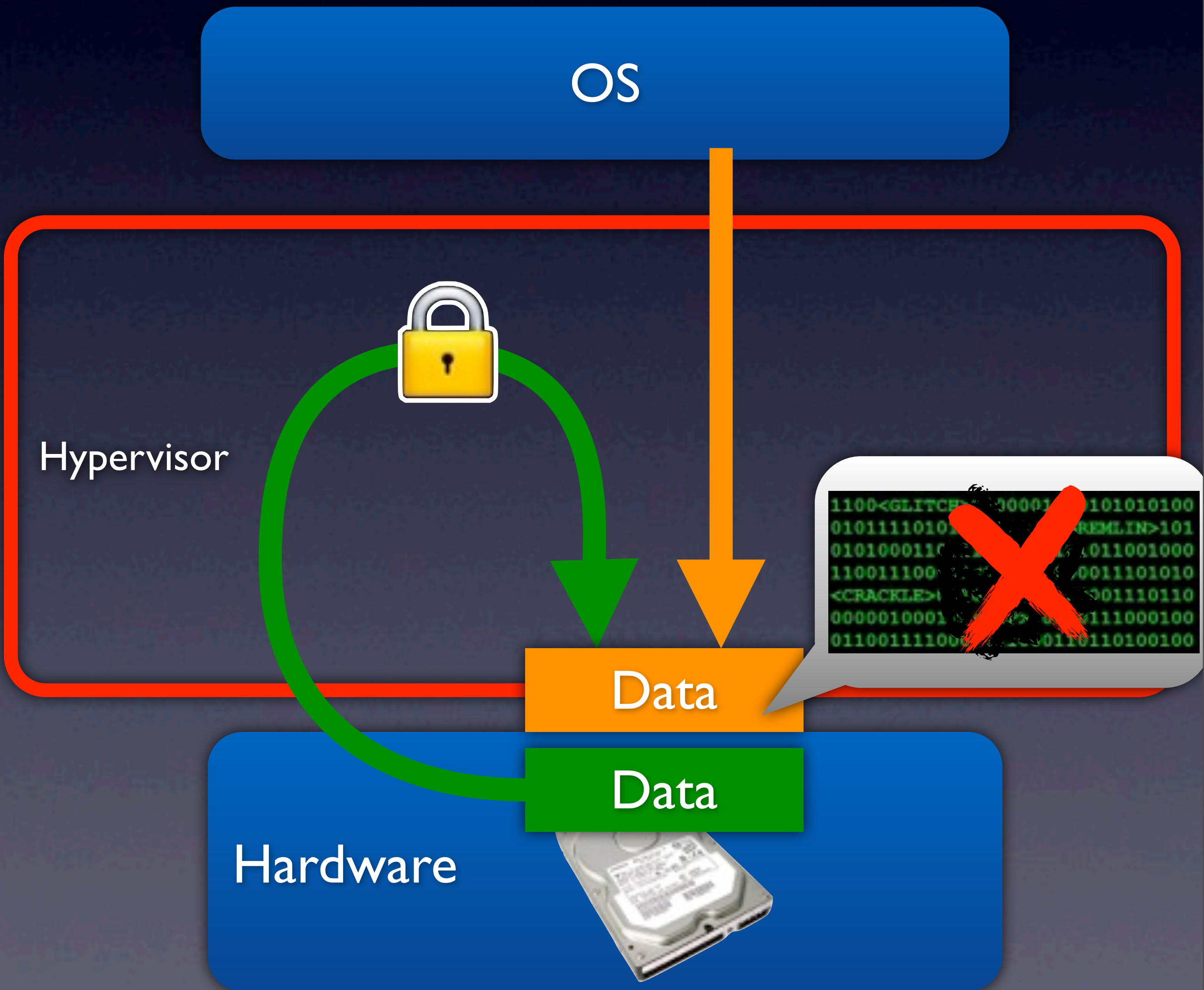
Scheduling Module

- Just before write, check if data to be written is the latest
  - Read/encrypt/CHECK&write
- If not the latest, read/encrypt again



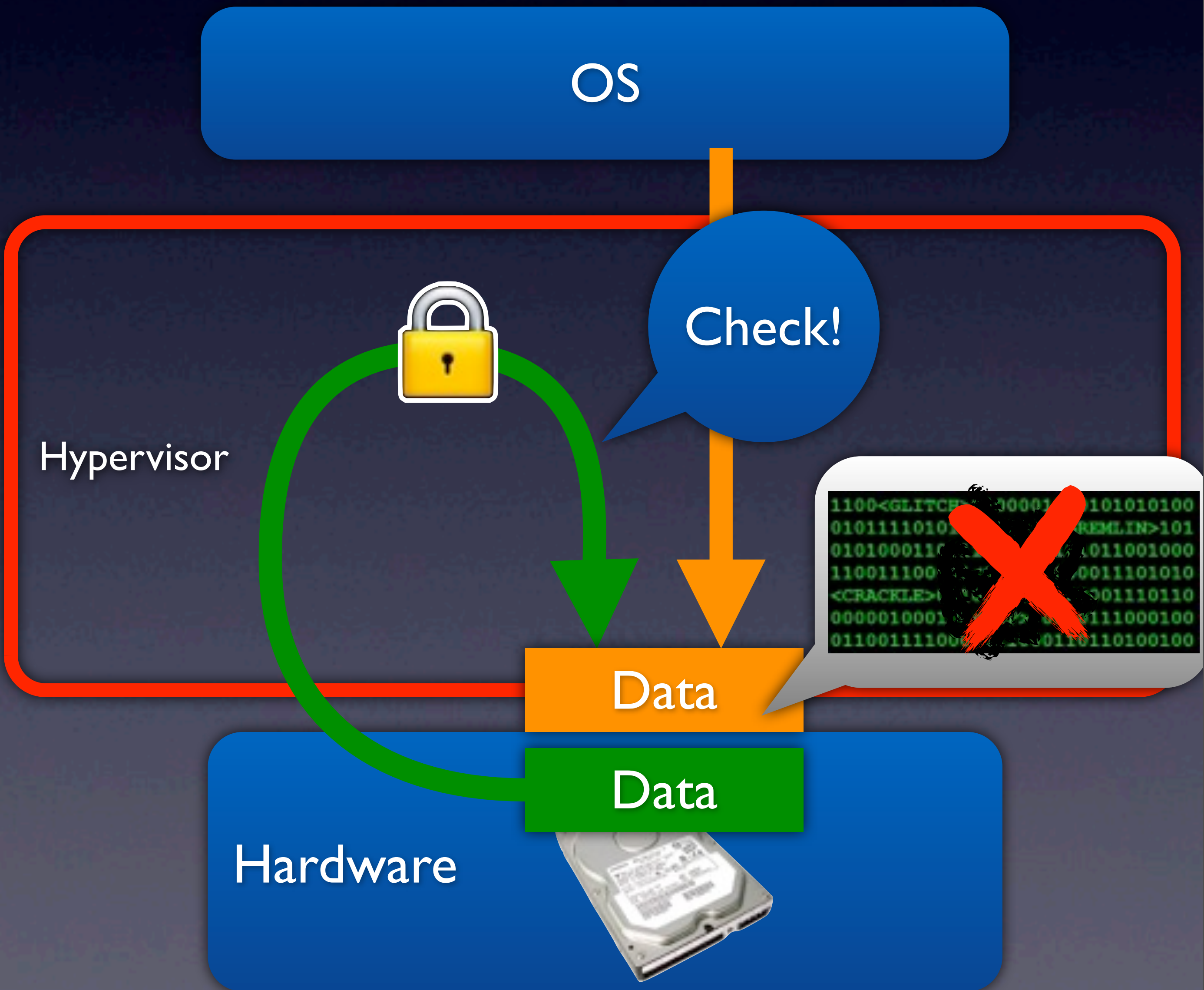
Scheduling Module

- Just before write, check if data to be written is the latest
  - Read/encrypt/ CHECK&write
- If not the latest, read/ encrypt again



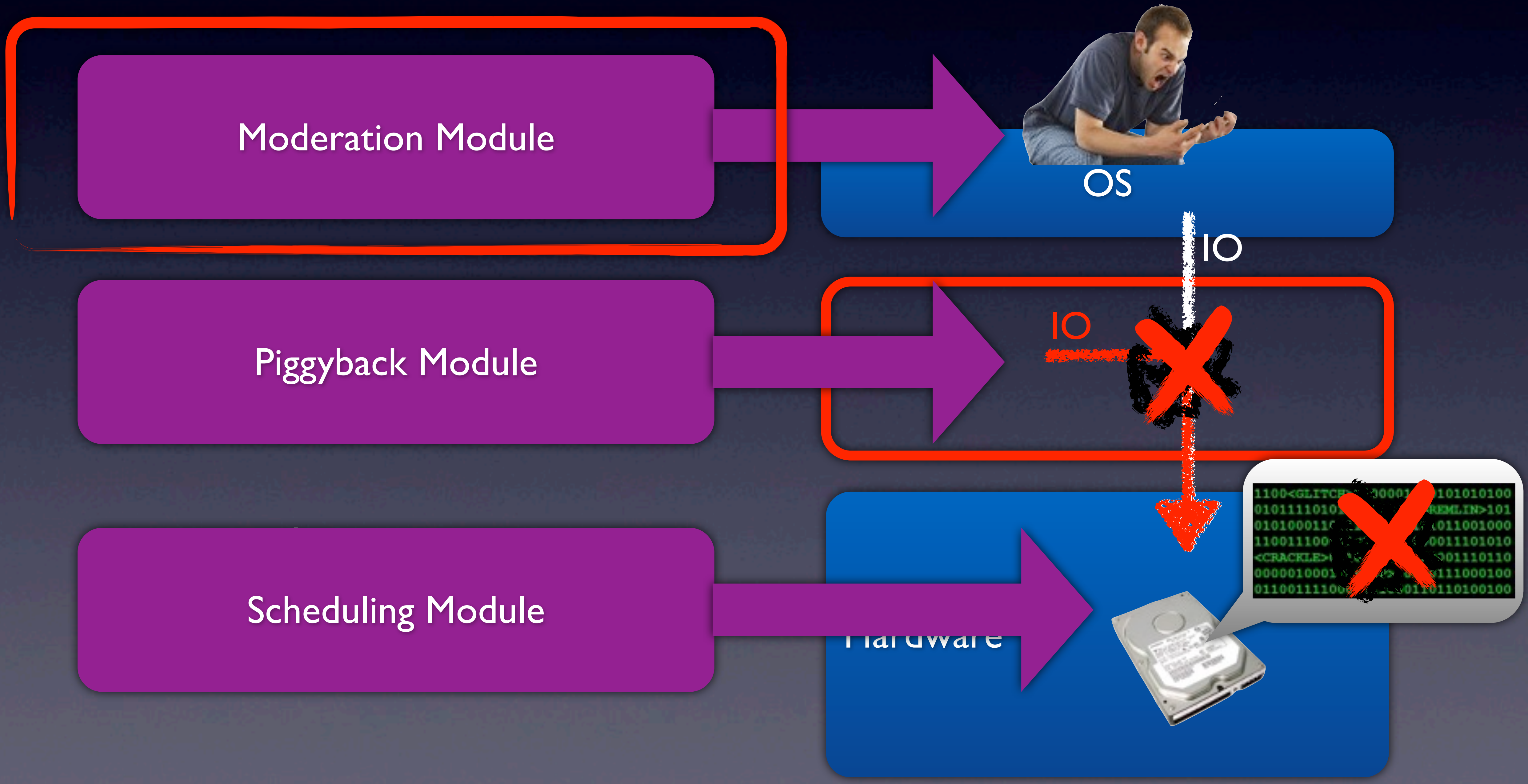
Scheduling Module

- Just before write, check if data to be written is the latest
  - Read/encrypt/CHECK&write
- If not the latest, read/encrypt again



Background Encryption in Hypervisor

Hypervisor reads/encrypts/writes disk in parallel with guest OS



Moderation Module

Piggyback Module

Scheduling Module

OS

IO

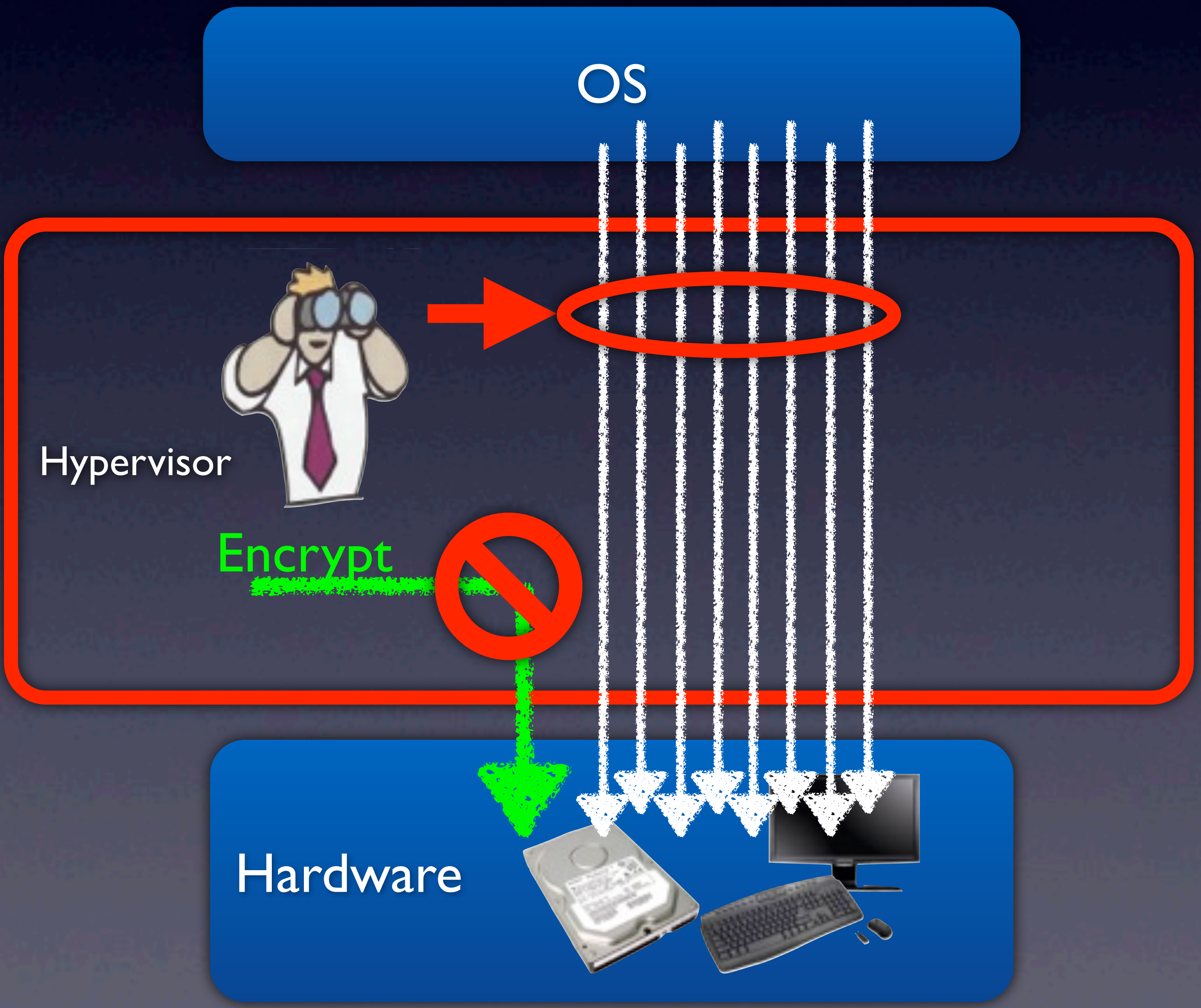
IO

Hardware

Moderation Module

- Observe guest OS activity for moderation

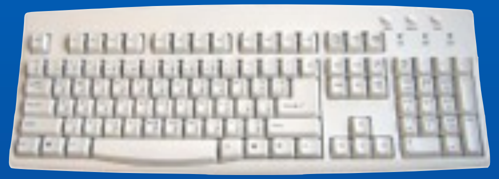
- Sleep encryption operation if guest OS is busy



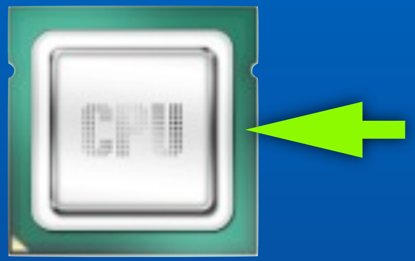
Implementation of Encryption Moderation

Disk IO freq.
> 5 (IOs/sec)

Mouse IO freq.
> 100 (IOs/sec)

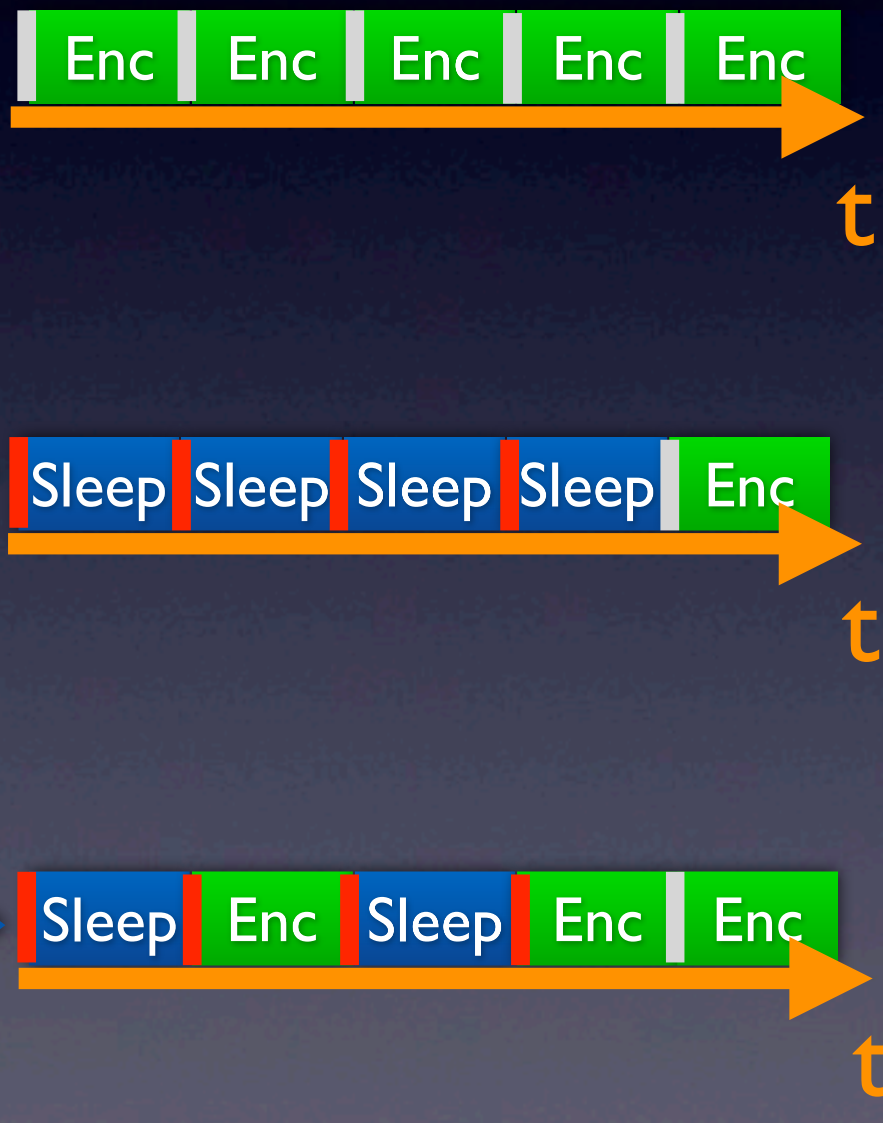


KBD IO freq.
> 5 (IOs/sec)



External Interrupt freq.
> 1000 (ints/sec)

Full Speed Encryption



🟥 Busy ▮ Idle

Evaluation

- Guest disk access throughput
- Application benchmark
- Deployment cost of our system

Experimental Environment

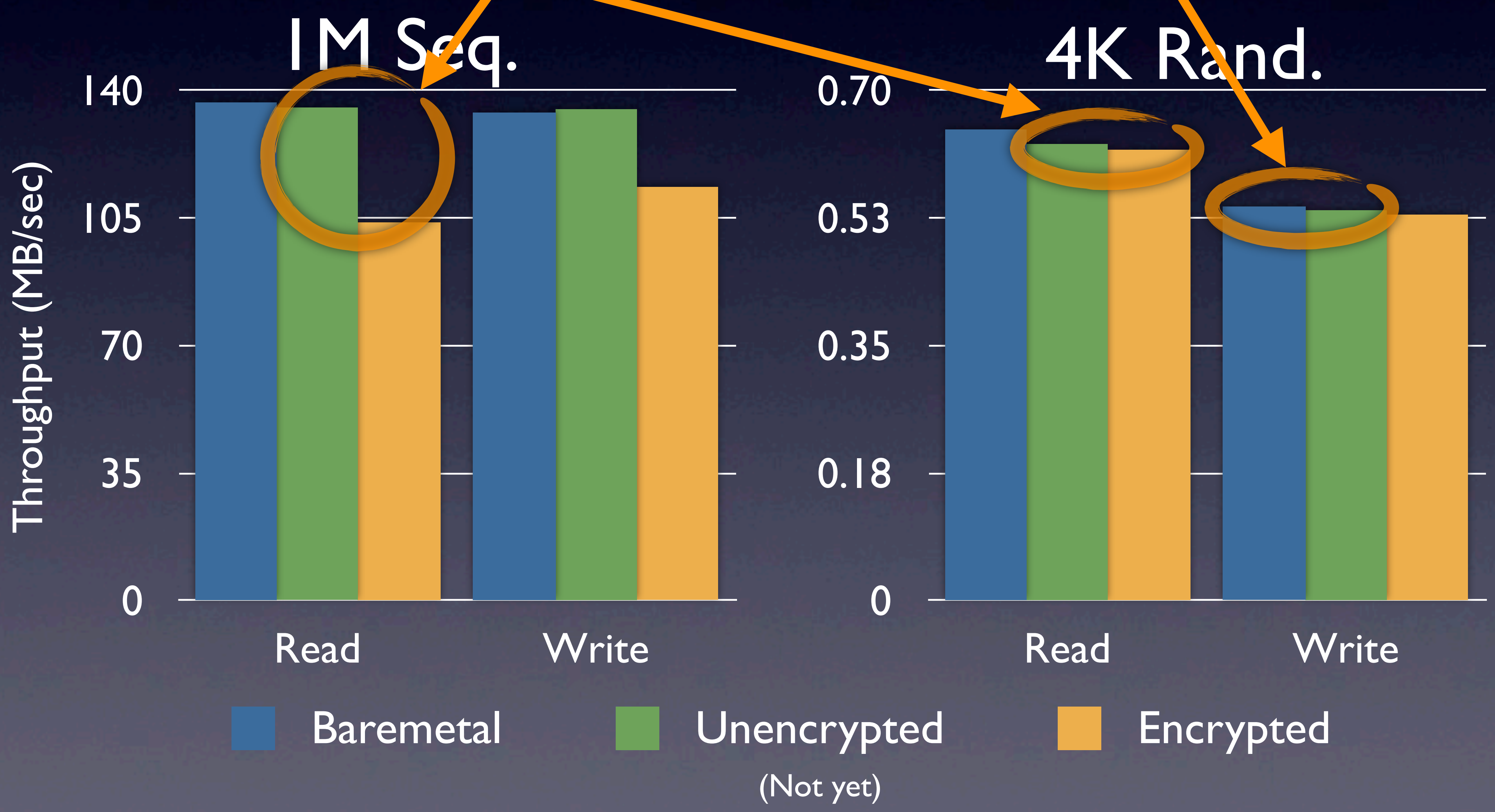
CPU	Intel Core 2 Quad Q9550 2.83GHz
RAM	PC2-6400 4GB
HDD	Seagate Barracuda 7200.12 1TB
OS	Windows 7 Professional 32-bit

Guest Disk Access Throughput

(Crystal Disk Mark)

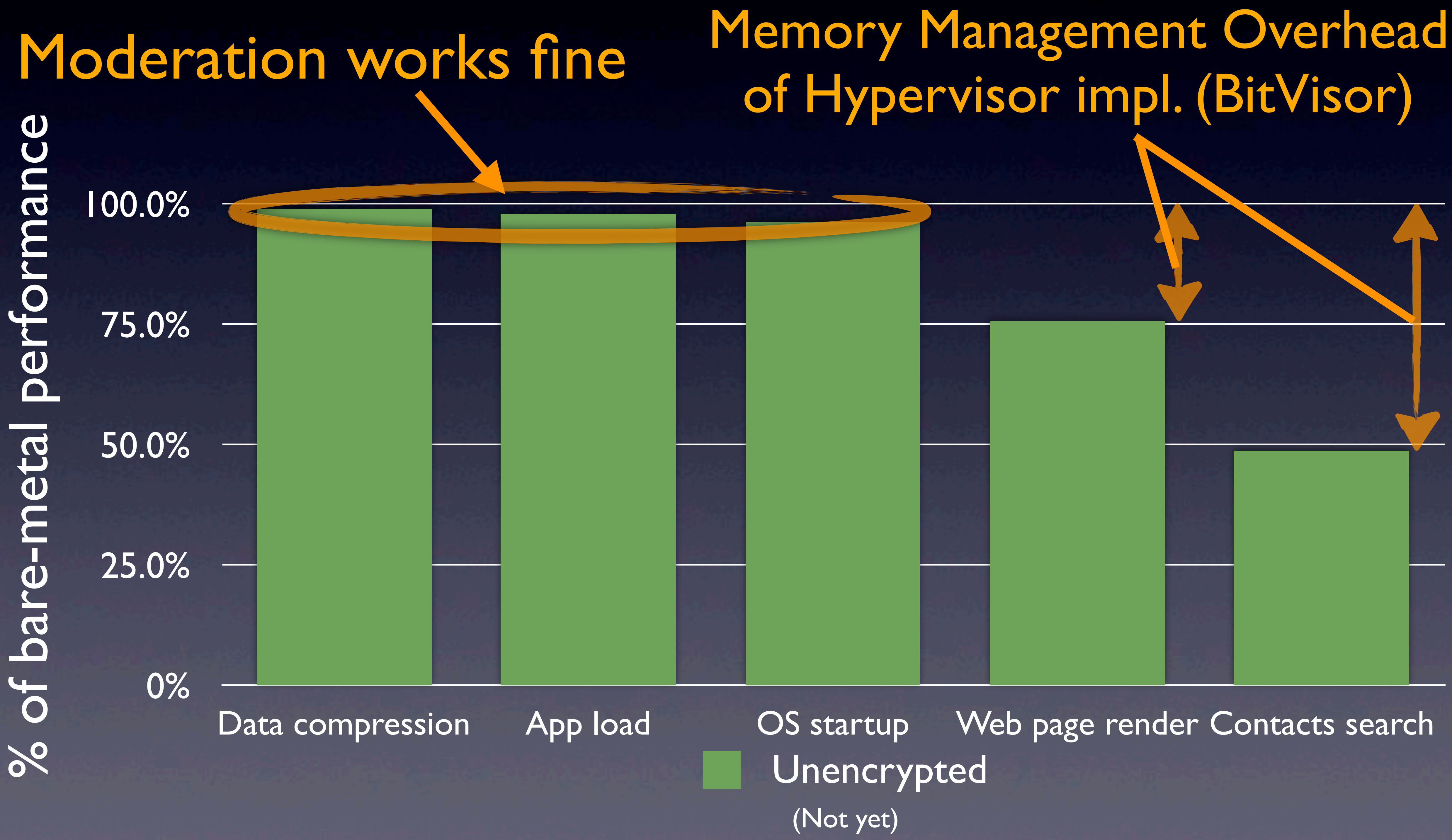
Enc/Dec overhead is 2%-24%
(not so big)

Moderation works fine



Application Benchmark

(PCMark 7)



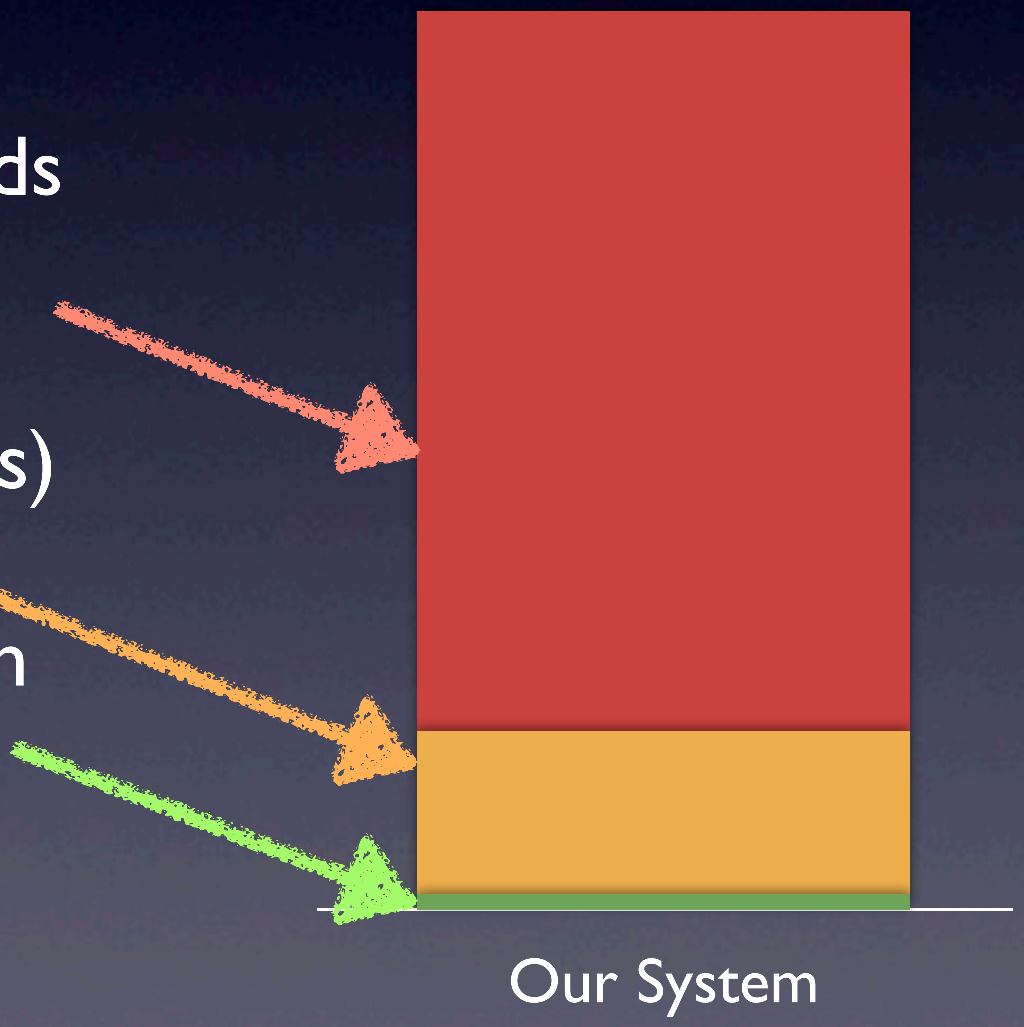
Moderation works fine

Memory Management Overhead of Hypervisor impl. (BitVisor)

Thursday, November 6, 14

Deployment cost of our system

- 5-10 minutes deployment
  - Configuration (depends on people, 5-10 mins)
  - One Reboot (1-2 mins)
  - Hypervisor installation (within a min)



Summary and Future Work

- Summary
  - Design and implementation of hypervisor-based background encryption system
    - Instant deployment on pre-install OS (5-10 mins)
- Future Work
  - Auto optimization of moderation criteria

Thank you!