# Retrofitting XoM for Stripped Binaries without Embedded Data Relocation

**Chenke Luo**[*+], Jiang Ming[+], Mengfei Xie[*], Guojun Peng[*], Jianming Fu[*]

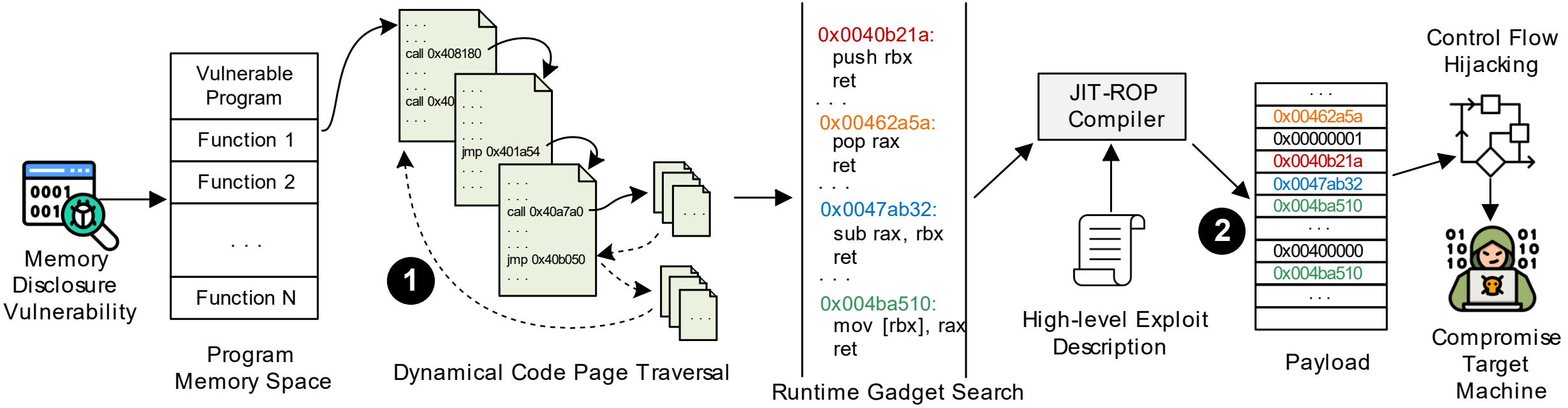
* Wuhan University

+ Tulane University

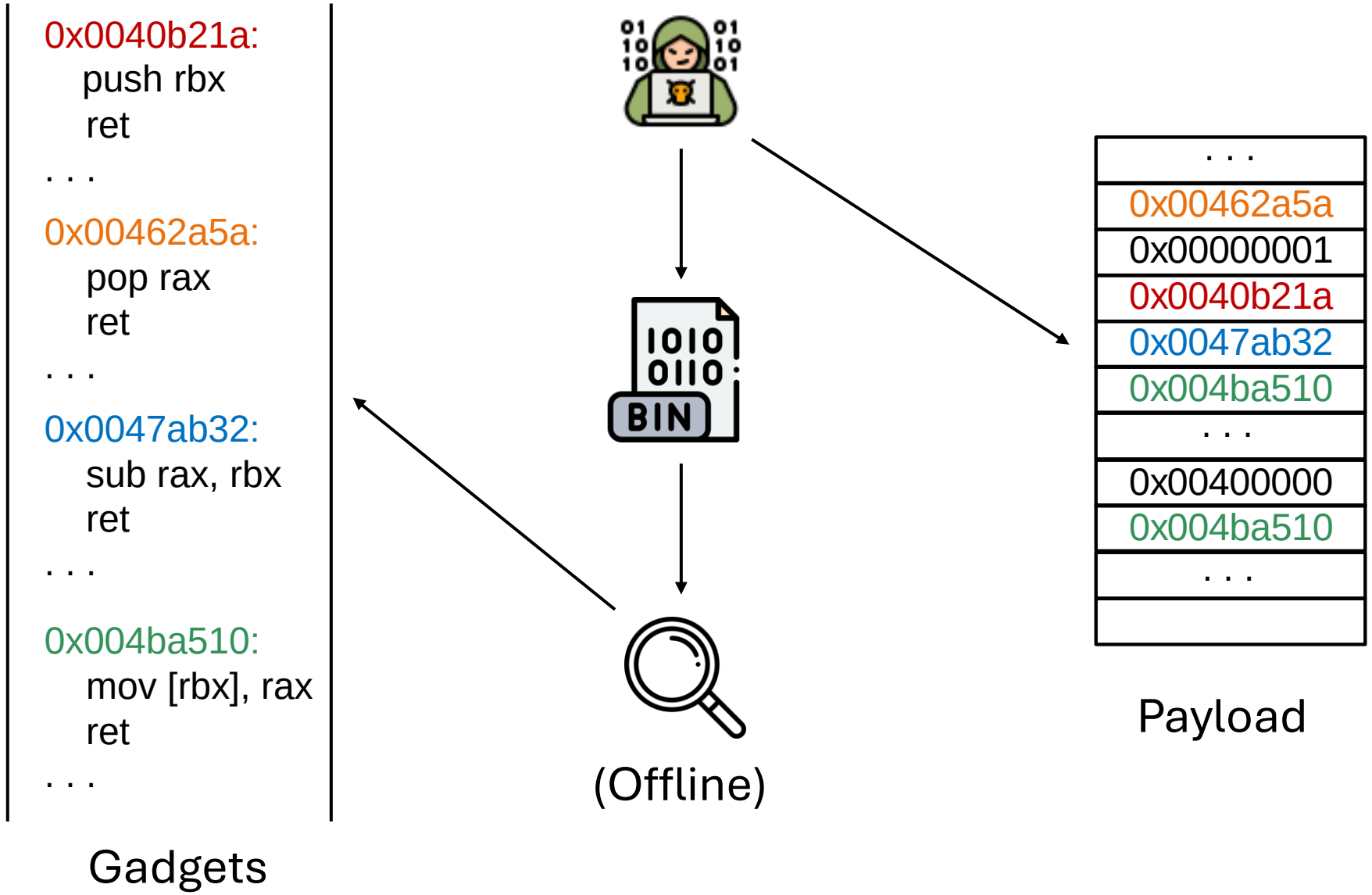


WUHAN
UNIVERSITY

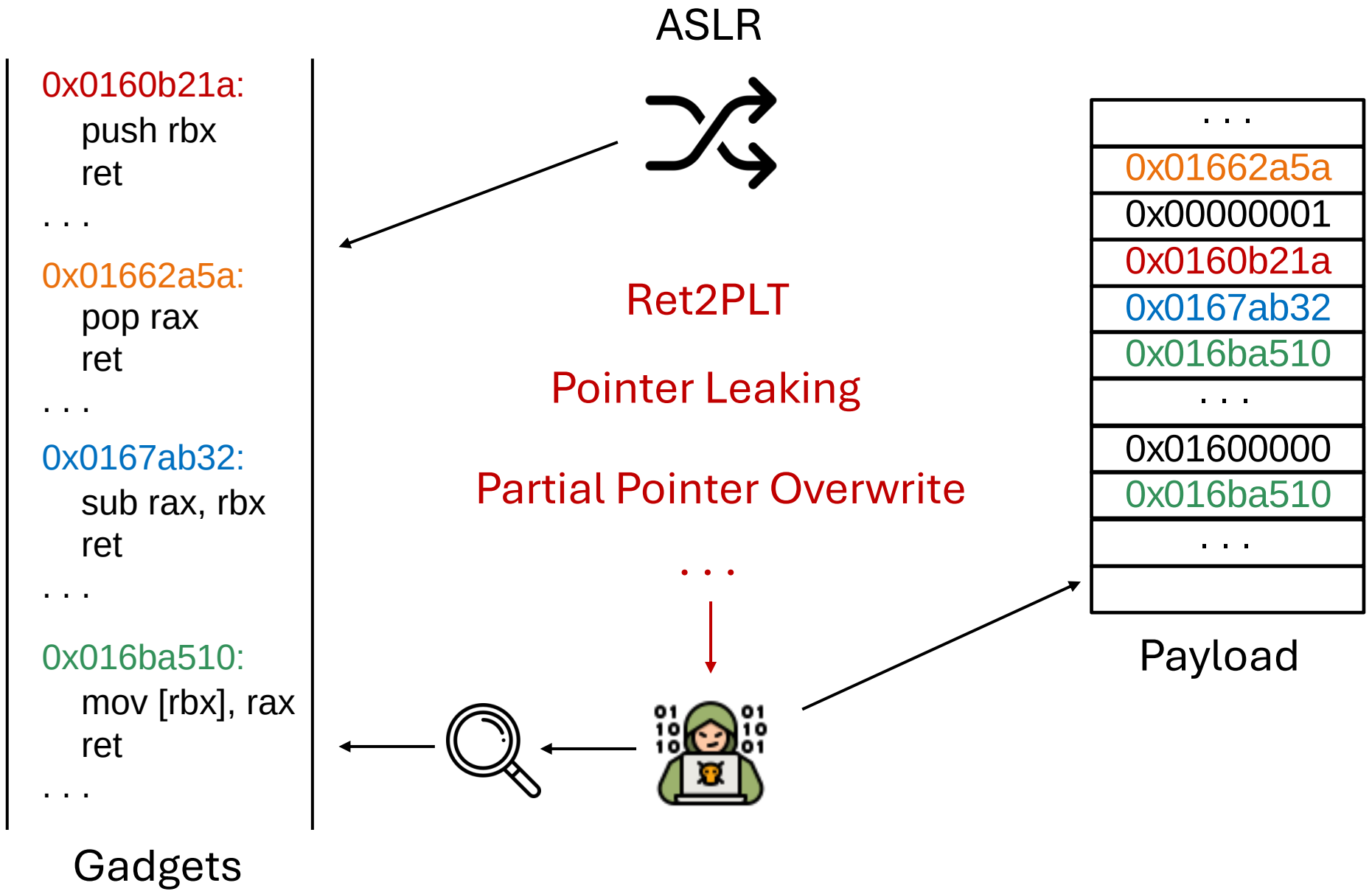
# Just-In-Time Return-Oriented Programming (JIT-ROP)



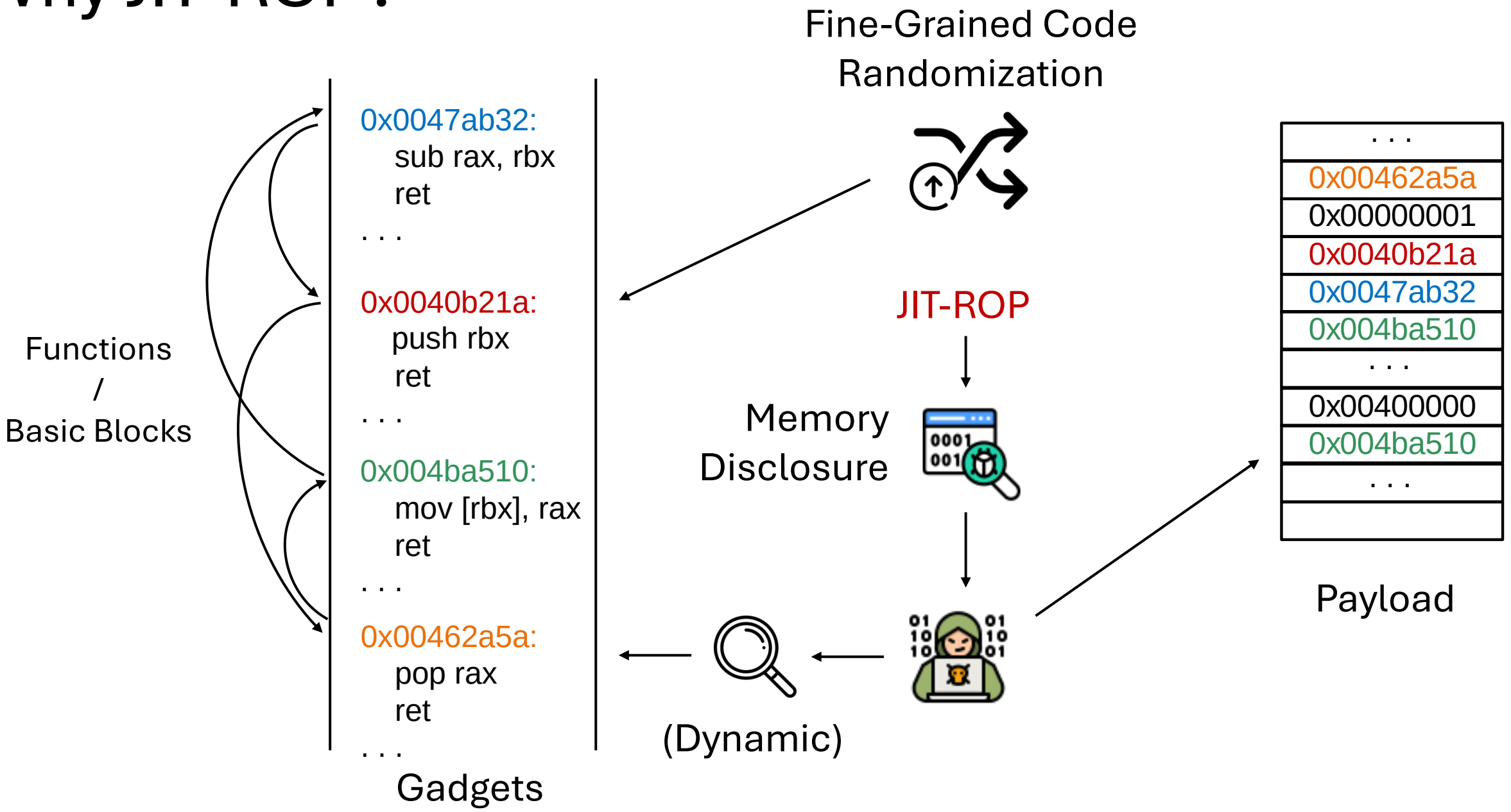
# Why JIT-ROP?


0x0040b21a:
push rbx
ret
. . .
0x00462a5a:
pop rax
ret
. . .
0x0047ab32:
sub rax, rbx
ret
. . .
0x004ba510:
mov [rbx], rax
ret
. . .
Gadgets
BIN
(Offline)
. . .
0x00462a5a
0x00000001
0x0040b21a
0x0047ab32
0x004ba510
. . .
0x00400000
0x004ba510
. . .
Payload

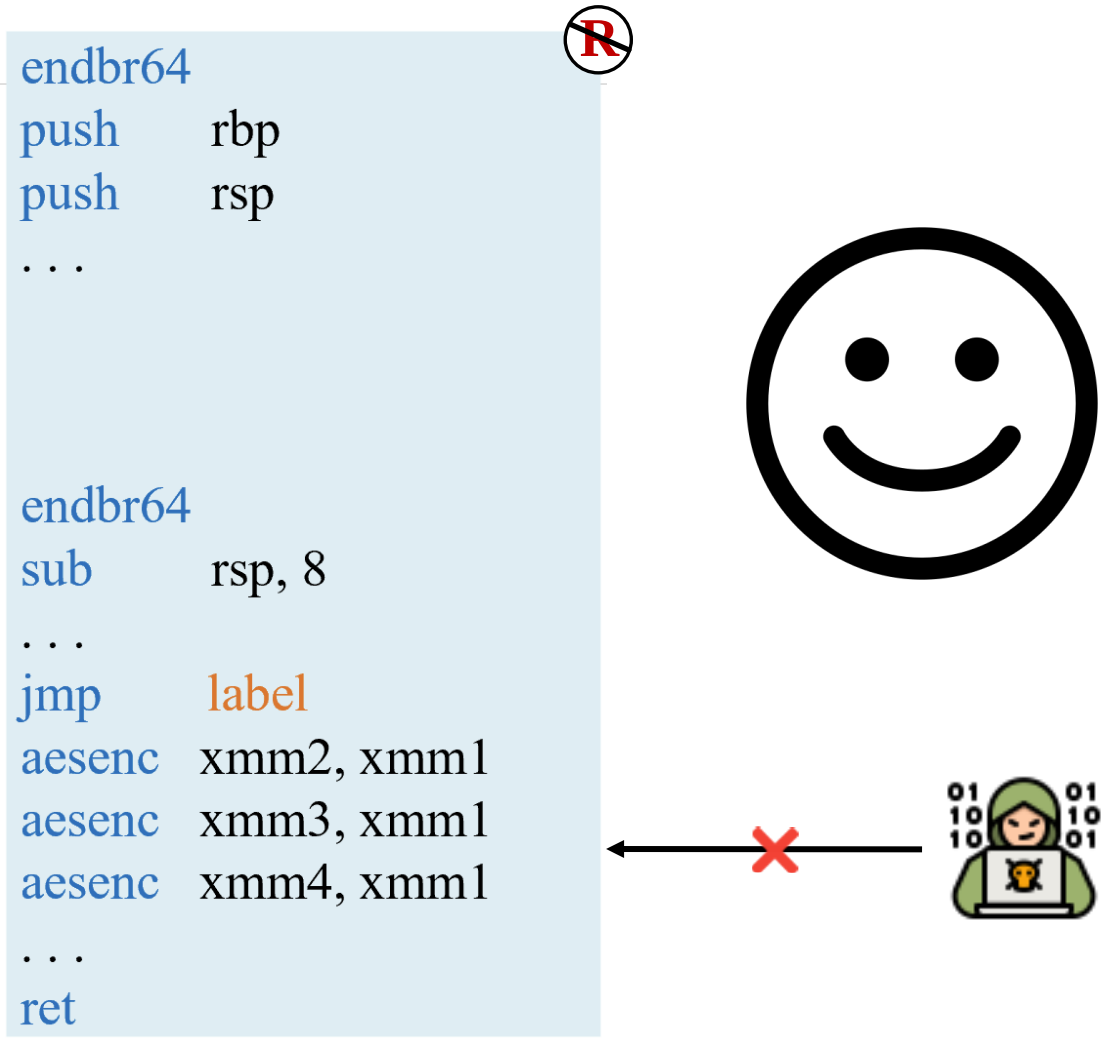
# Why JIT-ROP?


ASLR
0x0160b21a:
push rbx
ret
. . .
0x01662a5a:
pop rax
ret
. . .
0x0167ab32:
sub rax, rbx
ret
. . .
0x016ba510:
mov [rbx], rax
ret
. . .
Gadgets
Ret2PLT
Pointer Leaking
Partial Pointer Overwrite
. . .
. . .
0x01662a5a
0x00000001
0x0160b21a
0x0167ab32
0x016ba510
. . .
0x01600000
0x016ba510
. . .
Payload

# Why JIT-ROP?

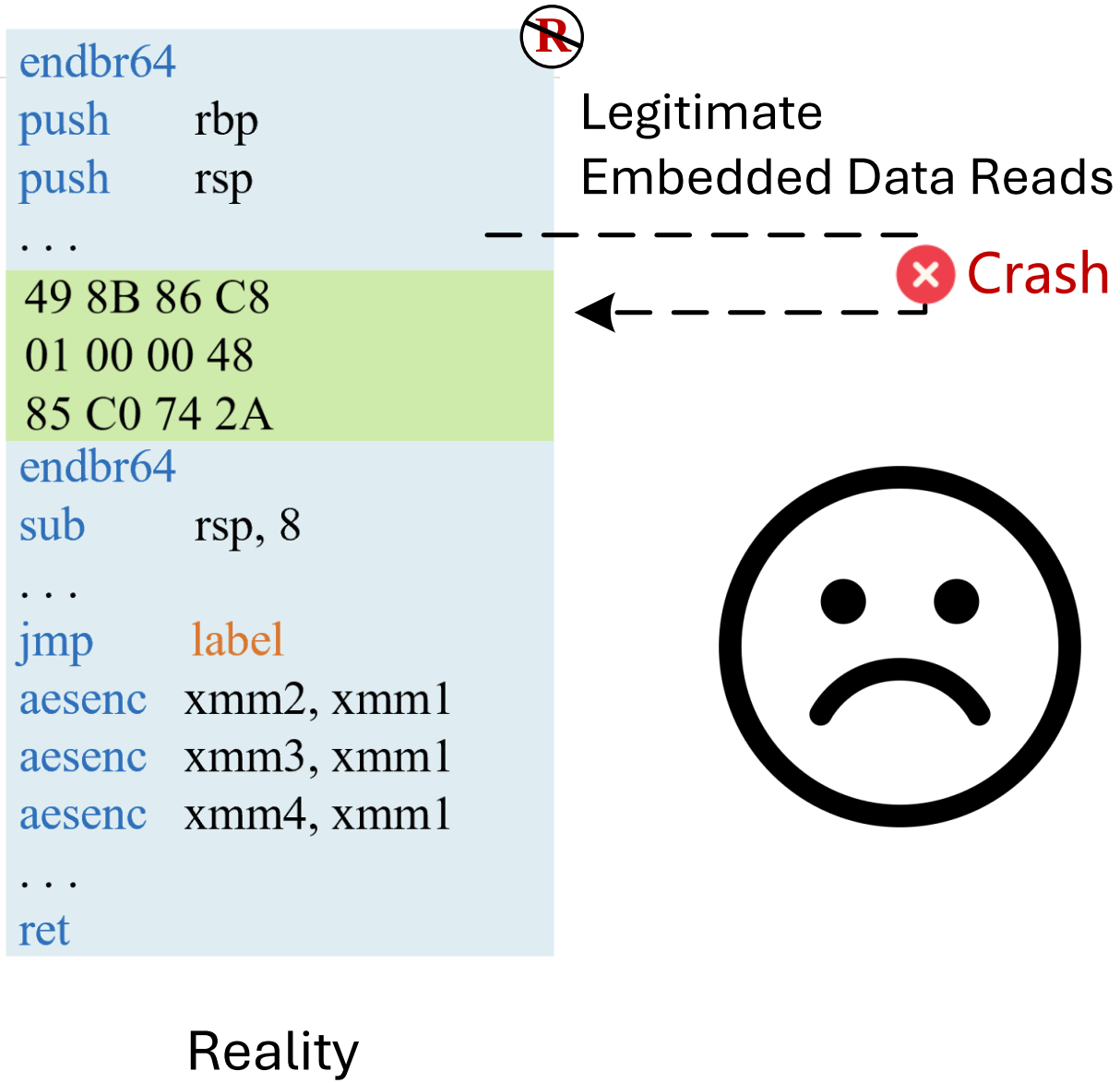

Fine-Grained Code Randomization
Functions / Basic Blocks
0x0047ab32:
sub rax, rbx
ret
. . .
0x0040b21a:
push rbx
ret
. . .
0x004ba510:
mov [rbx], rax
ret
. . .
0x00462a5a:
pop rax
ret
. . .
Gadgets
JIT-ROP
Memory Disclosure
(Dynamic)
. . .
0x00462a5a
0x00000001
0x0040b21a
0x0047ab32
0x004ba510
. . .
0x00400000
0x004ba510
. . .
Payload

# Execute-only Memory (XoM)

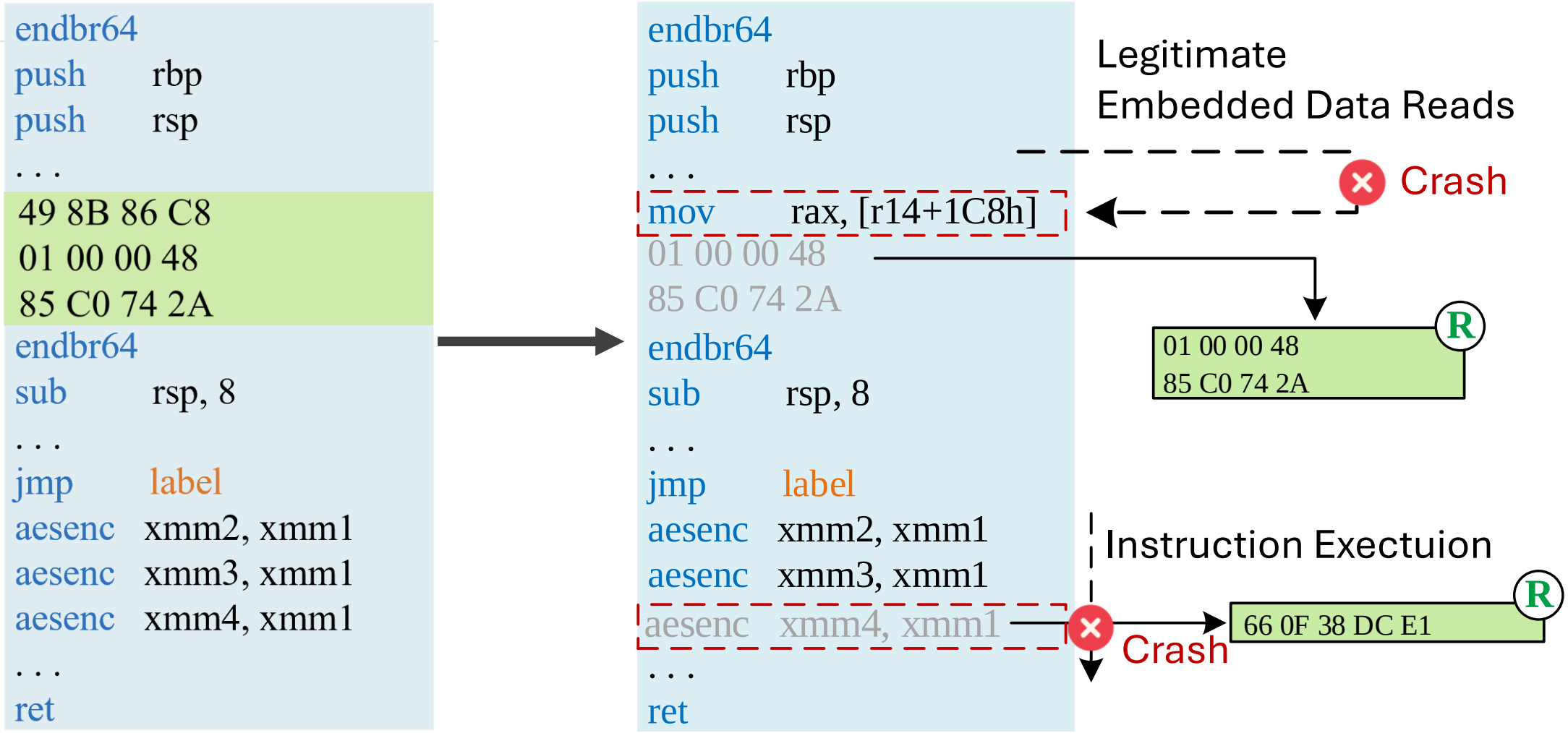



Ideal

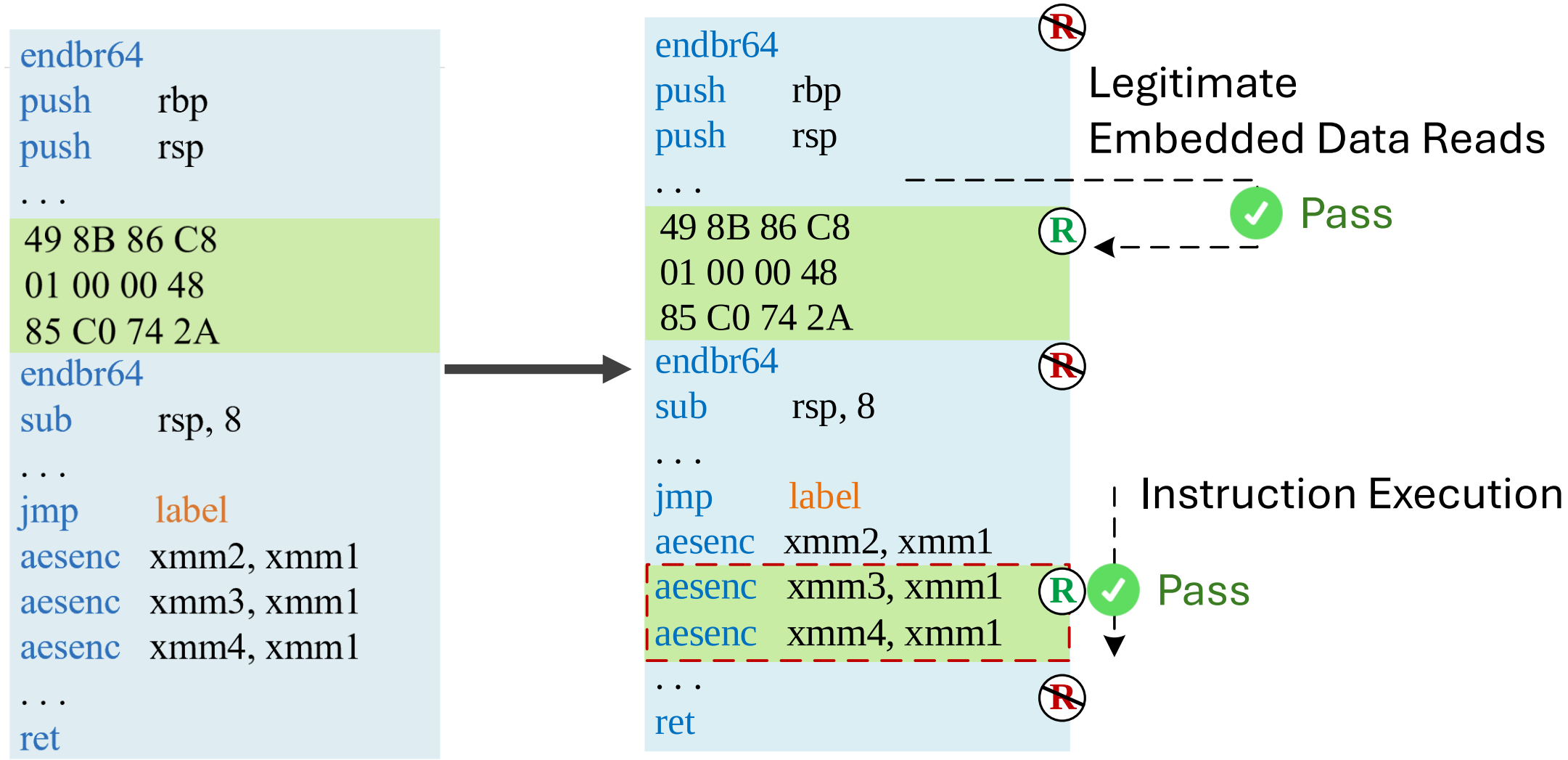
# Execute-only Memory (XoM)



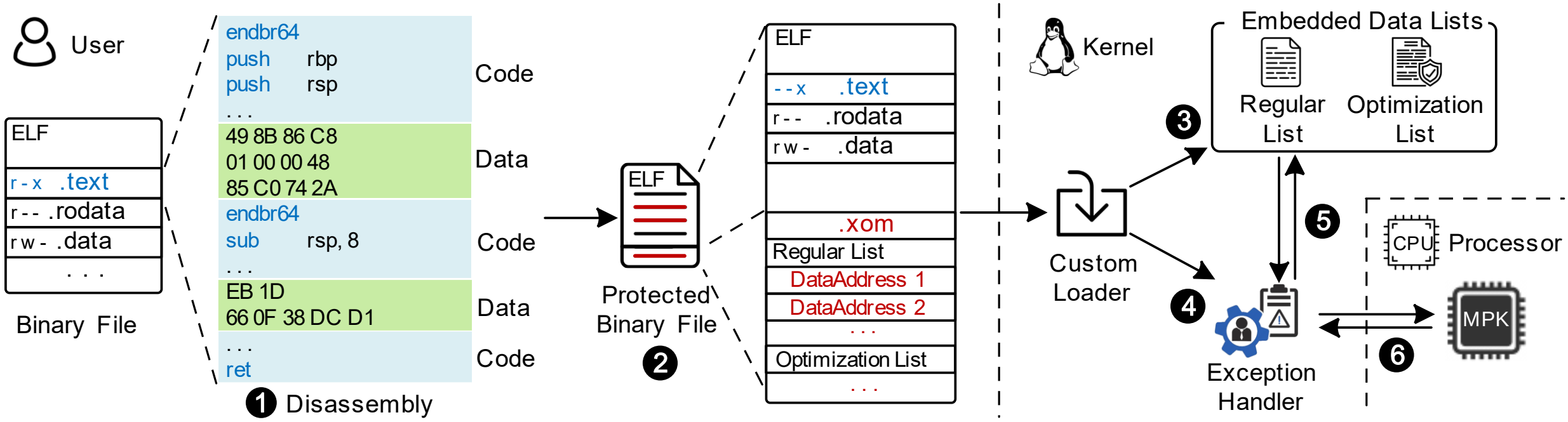
# Current Binary-Based XoM



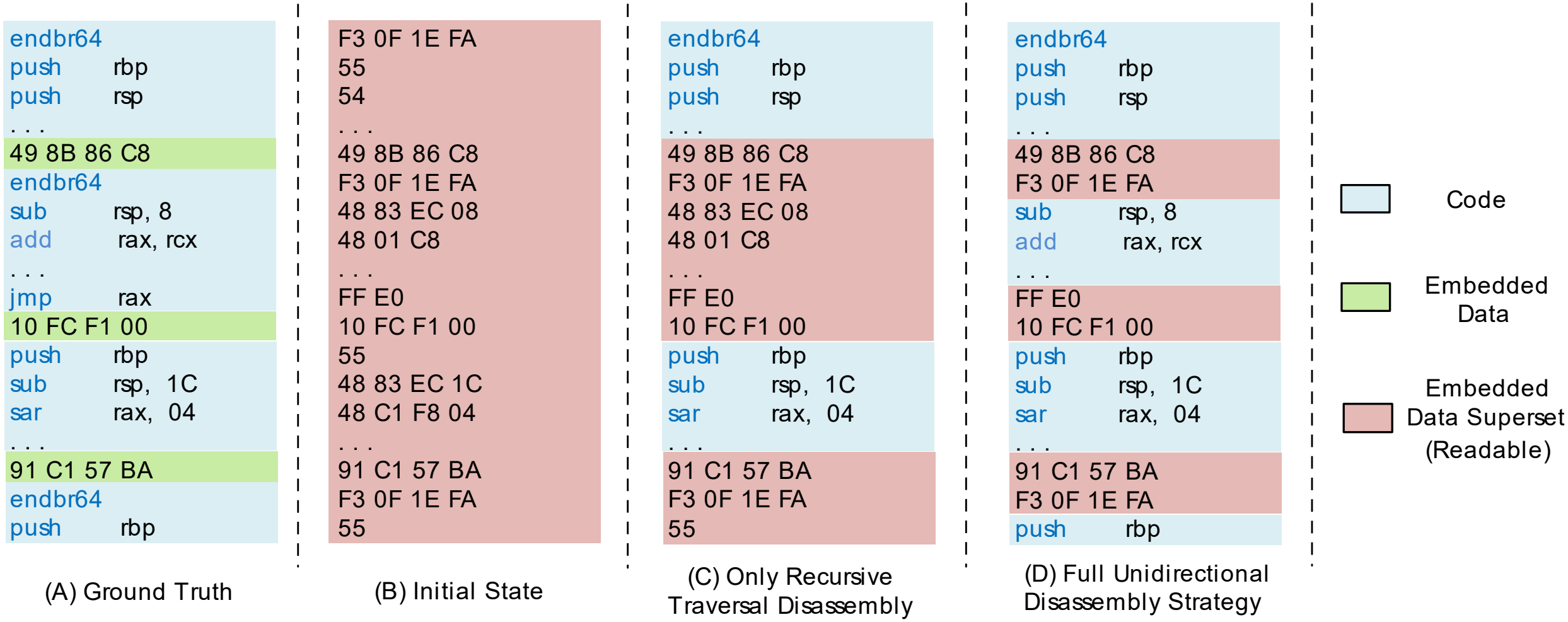
# PXoM (This Work)



# Overview


User
ELF
r-x .text
r-- .rodata
rw- .data
. . .
Binary File
endbr64
push rbp
push rsp
. . .
49 8B 86 C8
01 00 00 48
85 C0 74 2A
endbr64
sub rsp, 8
. . .
EB 1D
66 0F 38 DC D1
. . .
ret
Code
Data
Code
Data
Code
1 Disassembly
ELF
Protected
Binary File
2
ELF
--x .text
r-- .rodata
rw- .data
.xom
Regular List
DataAddress 1
DataAddress 2
. . .
Optimization List
. . .
Kernel
Custom
Loader
3
Embedded Data Lists
Regular
List
Optimization
List
4
5
6
Exception
Handler
CPU
Processor
MPK

# Unidirectional Disassembly



# Security Evaluation

Code Coverage: $$CC = \frac{Disassembled\ Code\ Bytes}{Real\ Code\ Bytes}$$

Overall Coverage: $$OC = \frac{Disassembled\ Code\ Bytes}{Real\ Code + Embedded\ Data}$$

# Security Evaluation

| Benchmark | Code Coverage | Overall Coverage | #. of EDB | Avg. EDB Size (B) |
|---|---|---|---|---|
| SPEC 2017 | 97.58% | 96.34% | 3020 | 30 |
| Webservers | 99.39% | 98.96% | 593 | 9 |
| Databases | 97.67% | 98.29% | 9408 | 17 |
| OpenSSL | 95.61% | 86.43% | 8142 | 31 |
| Pang et al. [38] | 96.01% | 95.79% | 1096 | 52 |
| Overall | 97.07% | 95.29% | 4290 | 31 |

# Security Evaluation

| COTS Application | Overall Coverage | #. of EDB | Avg. EDB Size (B) |
|---|---|---|---|
| Skype (8.129.0.202) | 99.98% | 718 | 58 |
| DaVinci Resolve (19.0.1) | 98.39% | 425 | 41 |
| IBM DB2 (15.5.9) | 98.95% | 401 | 15 |
| LiteSpeed (6.3.1) | 99.91% | 43 | 68 |
| Matlab (R2024b) | 98.94% | 690 | 125 |
| AutoDesk Maya (2025_2) | 98.67% | 1254 | 17 |
| OracleDB (193000) | 86.44% | 577 | 31 |
| Spotify (1.2.45.454) | 99.75% | 1637 | 39 |
| Intel DPC++ (2.1.79) | 92.59% | 2233 | 68 |
| Intel Fortran (2.1.80) | 92.19% | 2559 | 75 |
| Steam (1726604483) | 99.27% | 1190 | 16 |
| TeamViewer (15.58.4) | 94.49% | 2461 | 25 |
| Unity (6000.0.20f1) | 98.90% | 434 | 51 |
| VMWare (17.6.0) | 98.65% | 780 | 109 |
| Zoom (6.2.0) | 97.00% | 2740 | 90 |
| Overall | 96.94% | 1217 | 55 |

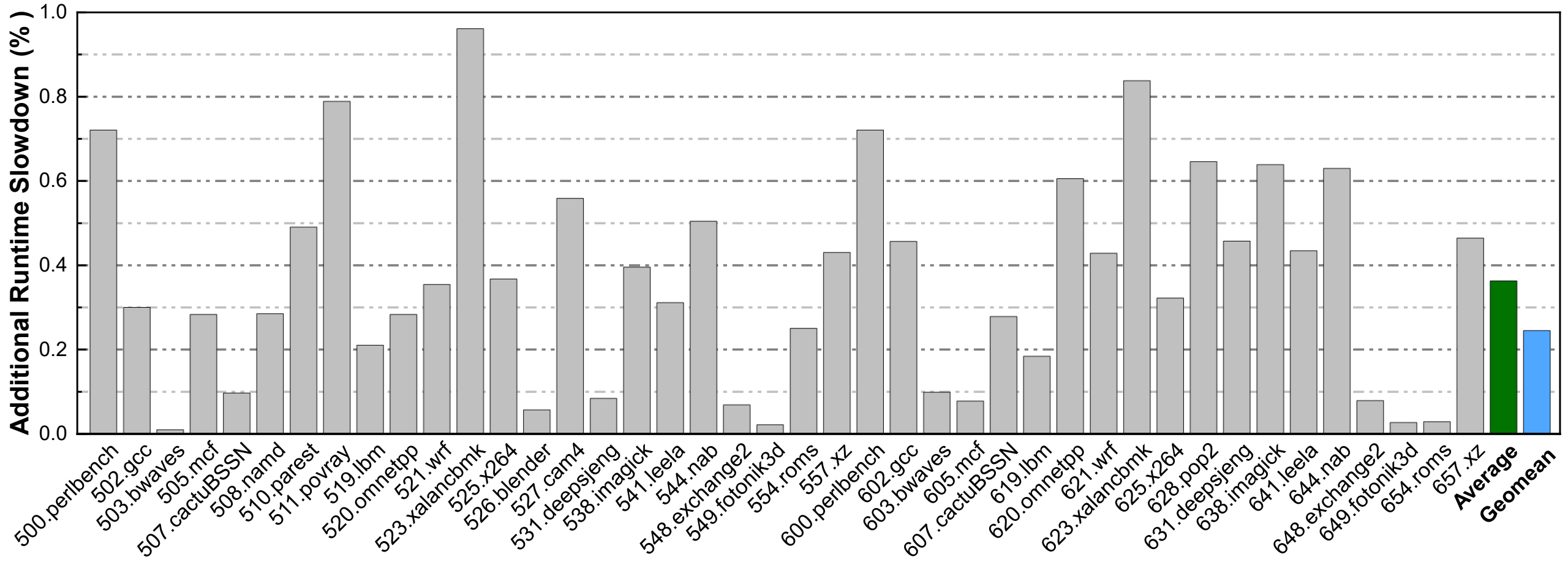
# Performance Evaluation

LMBench:

| Kernel | Fork Proc | Exec Proc | Page Fault | Prot Fault | Prot Fault* |
|---|---|---|---|---|---|
| Standard | 109 | 339 | 0.776 | 0.484 | 0.484 |
| PXoM | 110 | 341 | 0.780 | 0.487 | 1.548 |
| Overhead | 0.92% | 0.60% | 0.52% | 0.62% | 3.20X |

# Performance Evaluation

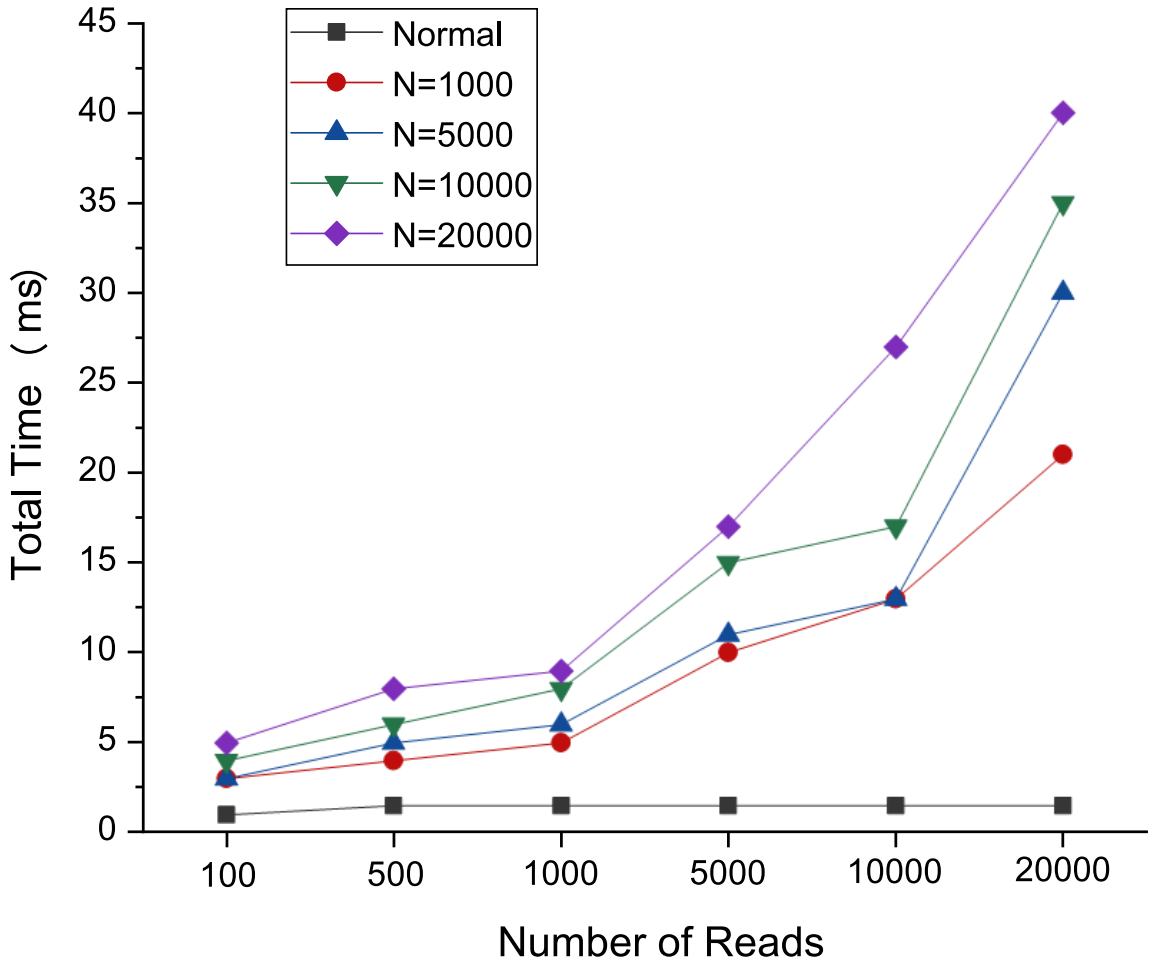
## SPEC CPU 2017:

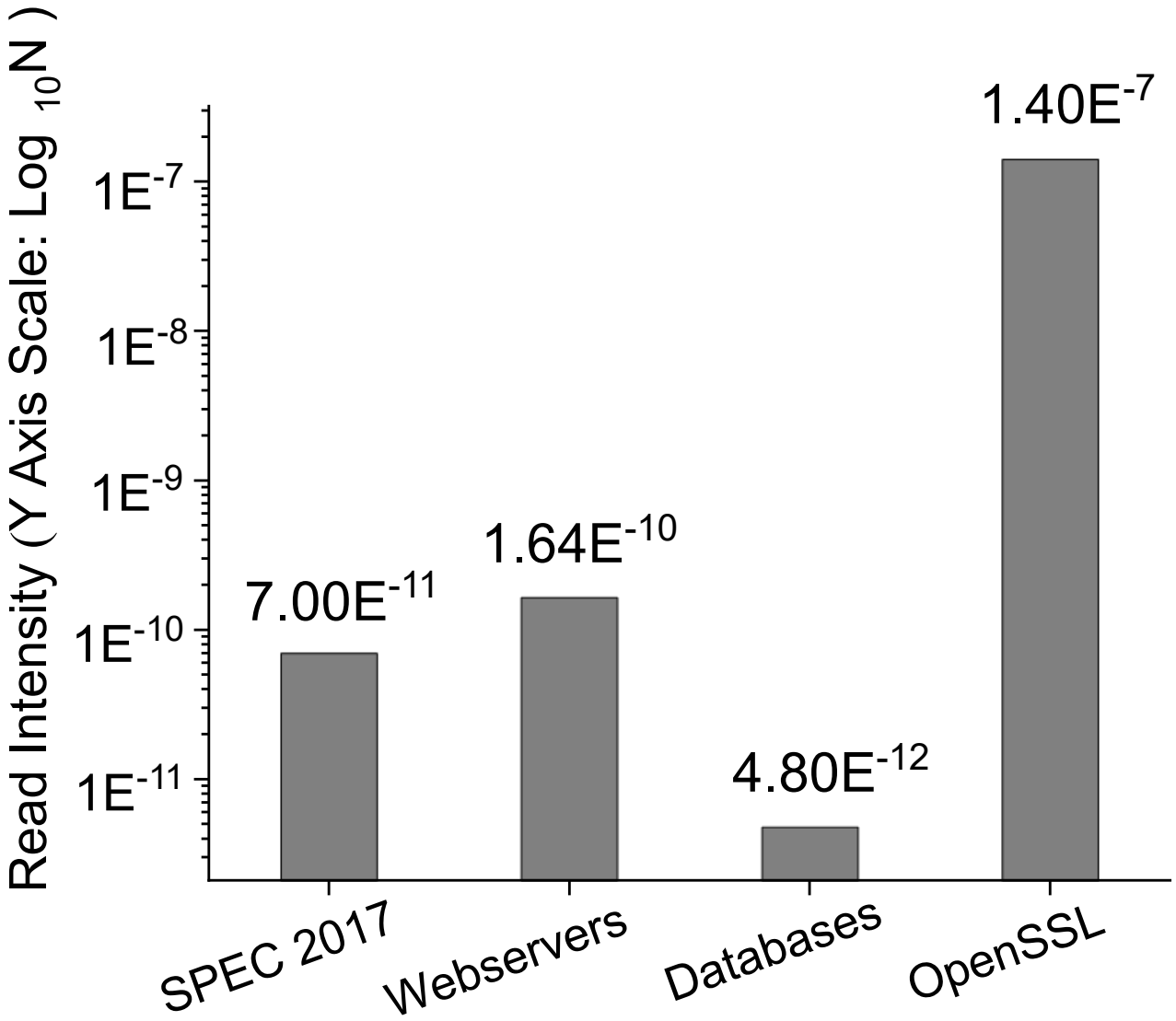



Average: 0.36%  Geomean: 0.25%

# Performance Evaluation

$$Read\ Intensity = \frac{\#\ of\ Read\ Requests}{\#\ of\ Executed\ Instructions}$$



# Conclusion

- Current Binary-Based XoM requires relocation of code and data
- However, precise separation of code and data is an inherent problem
- PXoM retrofits XoM for stripped binaries without embedded data relocation
- The performance loss is negligible

Out-Of-Box VM: https://zenodo.org/records/13892220

Source Code: https://zenodo.org/records/14251050

Document: https://zenodo.org/records/14251155

# Q & A