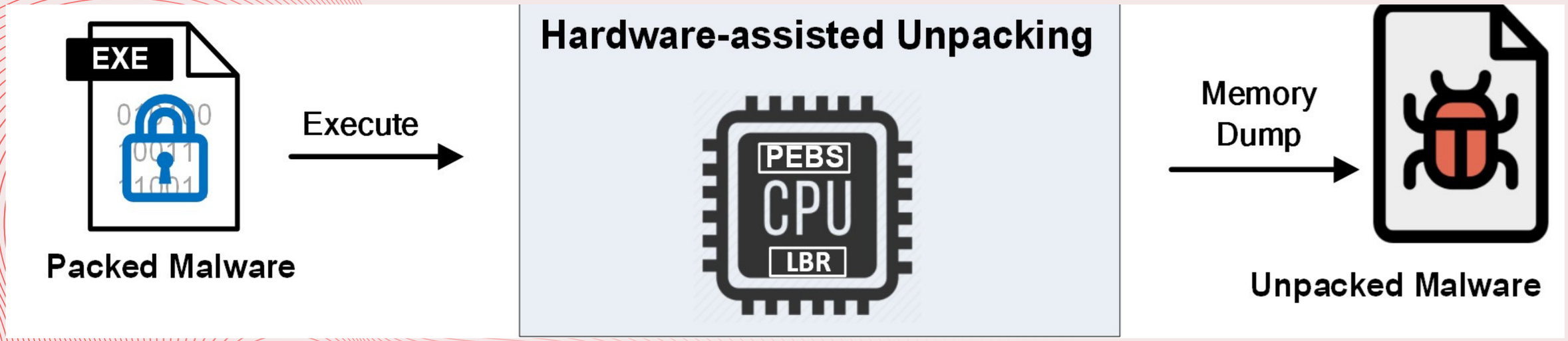
USENIX SECURITY '23

ON THE FEASIBILITY OF MALWARE UNPACKING VIA HARDWARE-ASSISTED LOOP PROFILING

Binlin Cheng, Erika A Leal, Haotian Zhang and Jiang Ming

About This Presentation

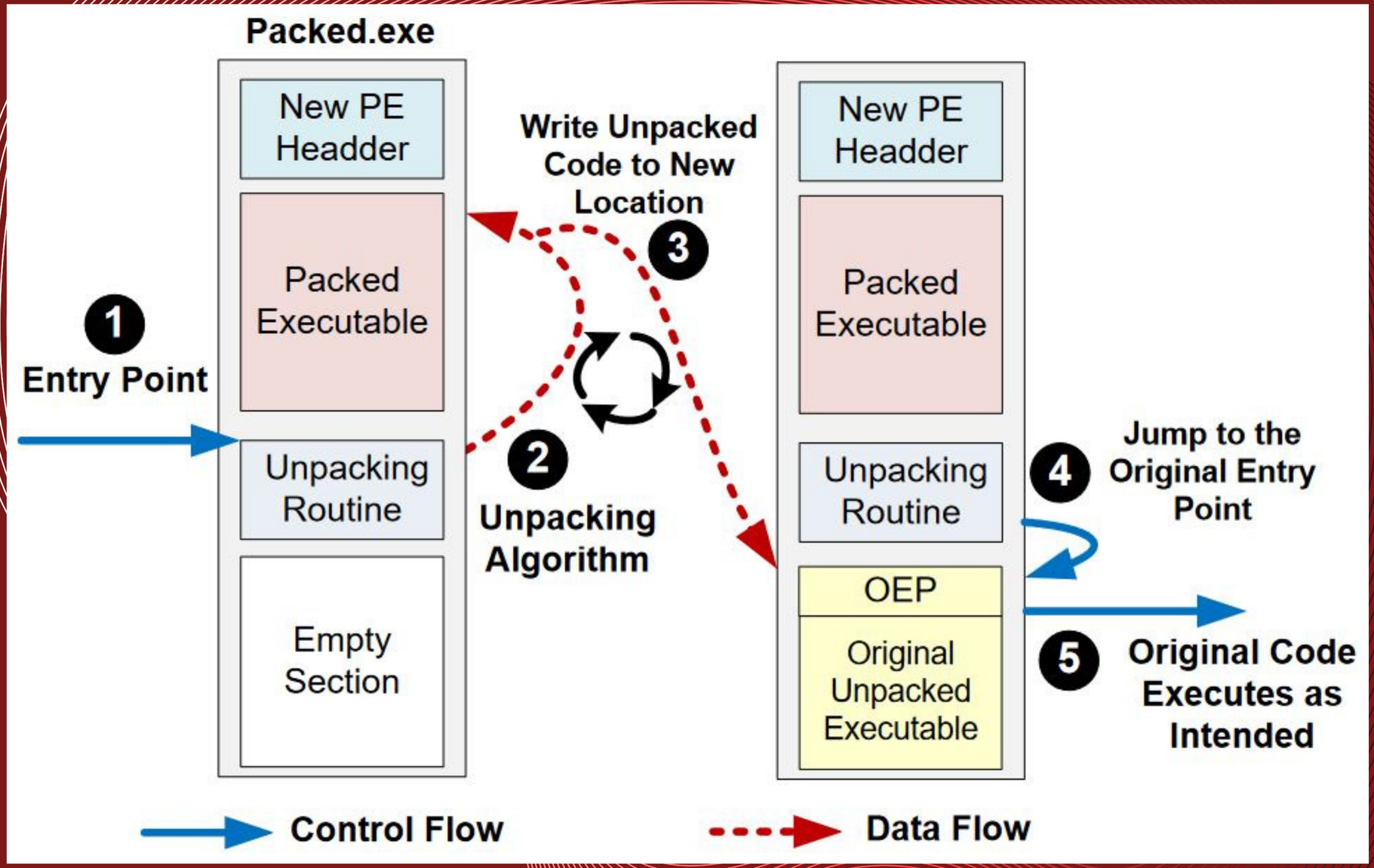
- Loop HPC
- Loop–Centric Profiling
- Hardware Performance Counters
- Unpacking Malware
- Resilience, Consistent, and Effective



A Bit of Background Knowledge....

Unpacking/Packing can use	**93–99% OF THE CPU**
Most malware is packed	~80% AND RISING
HPCs are non-deterministic in nature	ADDRESSED IN ONLY 10% OF HPC RESEARCH

The Unpacking Process



Hardware Performance Counters

Special registers found in the CPU

100s exist within a processor

37 Candidate events for our study

Non-Deterministic

The Semantic Gap critiscism

Non-Determinism Can Happen In HPCs By...

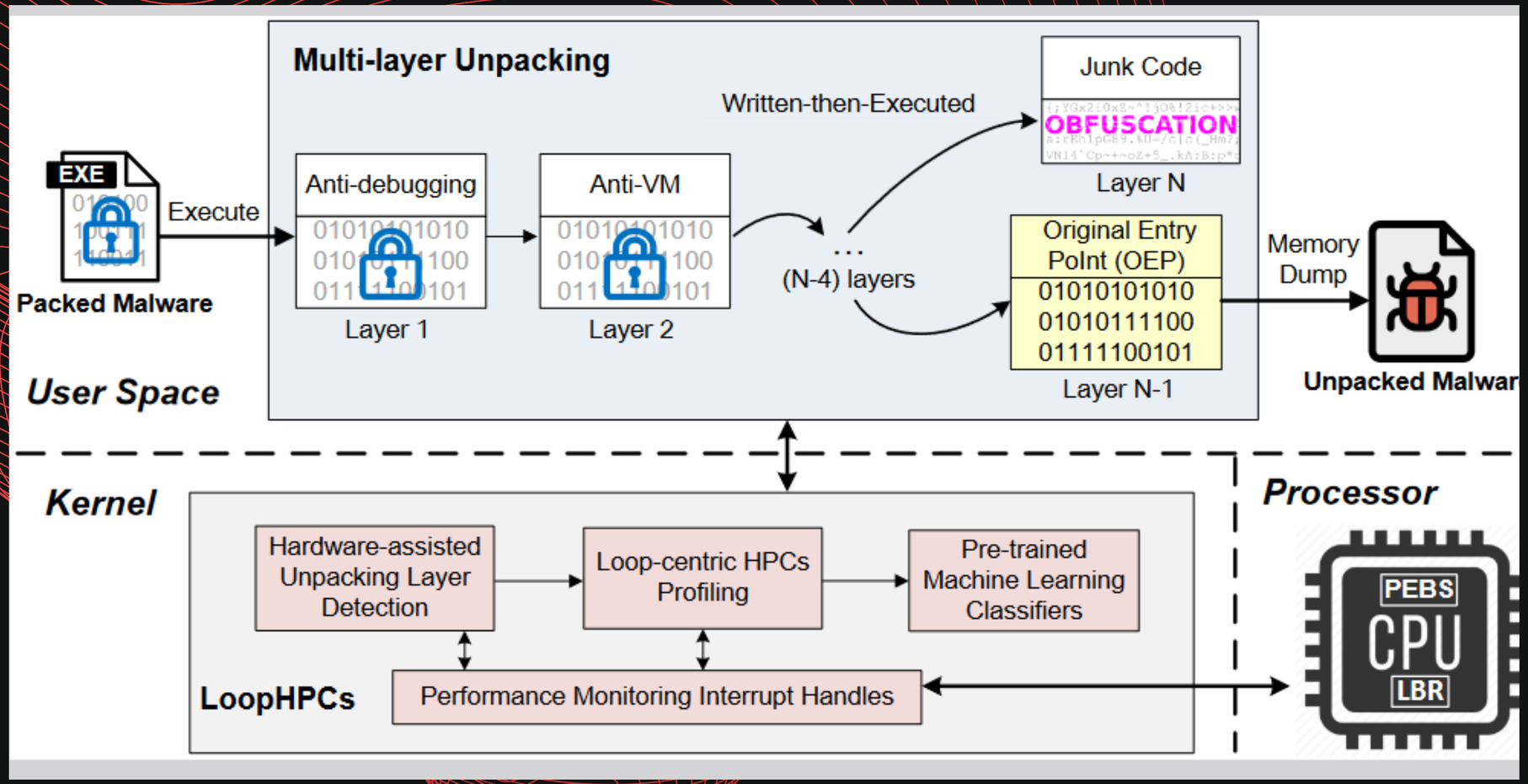
- Multiplexing
- Multi-Cores
- Interrupt Skid
- Multi Processes
- Page Faults

Interrupt Skid vs. Effect of LoopHPC

```
void multiply_matrices()
{
 1:  for (int i = 0; i < 10; i++) {
 2:     for (int j = 0; j < 10; j++) {
 3:        float sum = 0.0;
 4:        for (int k = 0; k < 10; k++) {
 5:           temp =matrix_a[i][k] * matrix_b[k][j];
 6:            sum = sum + temp;      }
 7:        matrix_r[i][j] = sum;  } } }
```

	Interrupt Skid Impact		Loop-centric HPCs Profiling	
	Expected Value	Observed Value	Expected Value	Observed Value
Line 4		764	2000	1999
Line 5	2000	152		
Line 6		1083		
Line 7		1		1

LoopHPC


Multi-layer Unpacking
Written-then-Executed
Junk Code
OBFUSCATION
Layer N
EXE
Execute
Anti-debugging
Anti-VM
Packed Malware
Layer 1
Layer 2
(N-4) layers
Original Entry PoInt (OEP)
01010101010
01010111100
01111100101
Layer N-1
Memory Dump
Unpacked Malwar
User Space
Kernel
Processor
Hardware-assisted Unpacking Layer Detection
Loop-centric HPCs Profiling
Pre-trained Machine Learning Classifiers
LoopHPCs
Performance Monitoring Interrupt Handles
PEBS
CPU
LBR

"Hot Loops"

UPX

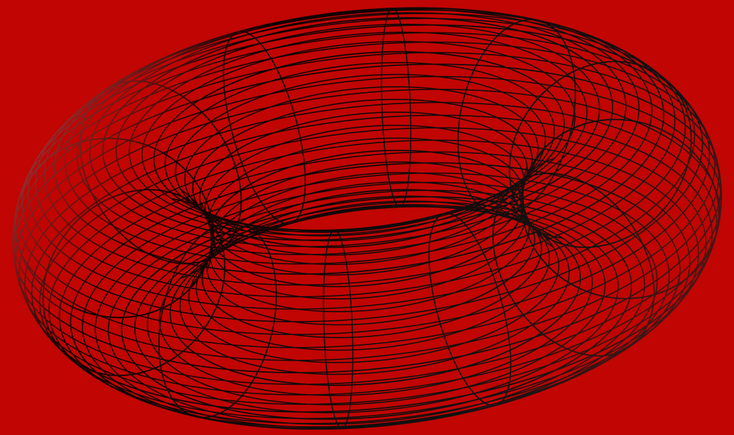
```
loop:
  dec   esi
  mov   eax, ebx
  mov   ecx, esi
  shr   eax, cl
  and   eax, 0x1
  ...
  test  esi, esi
  jne   loop
```

(a) Compression Packer

tElock

```
loop:
  ...
  rol   byte  ptr  [ebx+ecx], 0x5
  add   byte  ptr  [ebx+ecx], cl
  xor   byte  ptr  [ebx+ecx], 0x67
  inc   byte  ptr  [ebx+ecx]
  dec   ecx
  jnle  loop
```

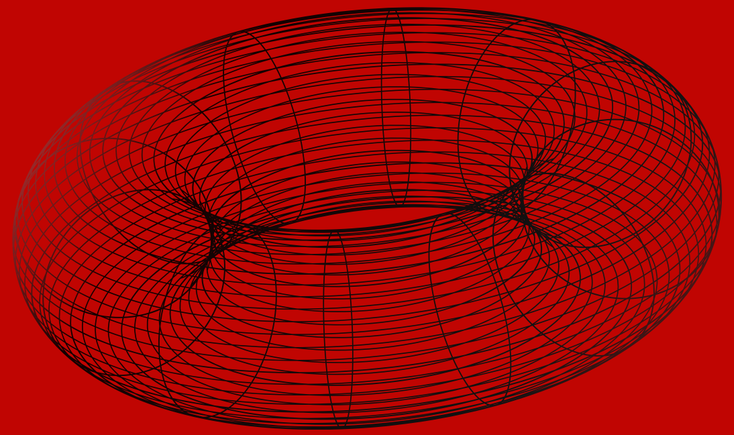
(b) Encryption Packer



hot loop examples in an unpacking routine

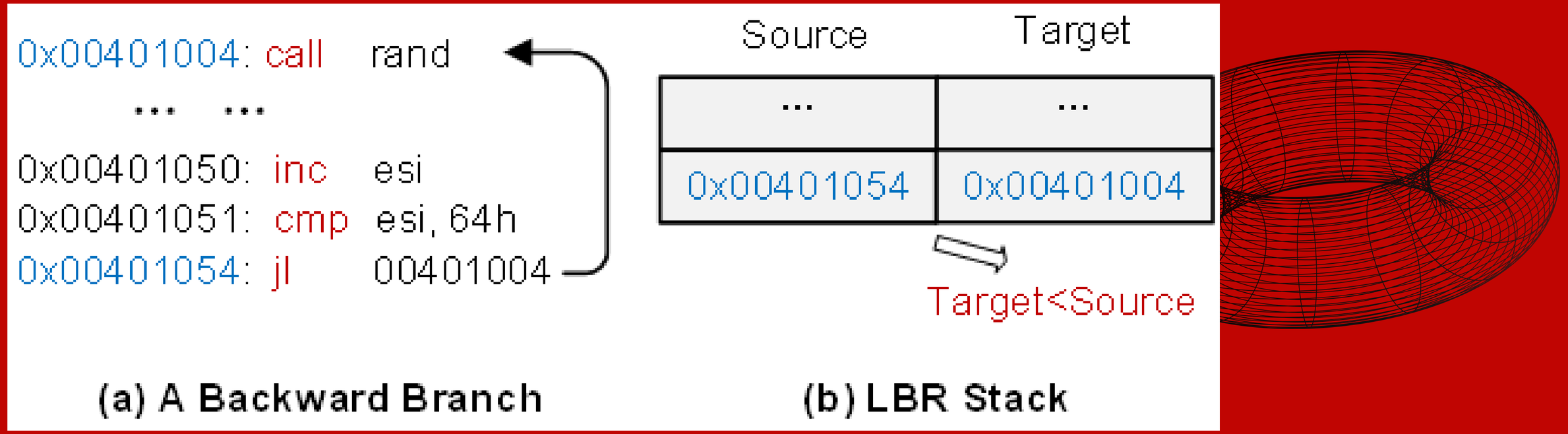
"Hot Loops"

Sample	# of Max Iterations	Inst (%)	Cycle (%)
UPX	3,359,627	99%	99%
Enigma	432,110	95%	98%
Yoda's Protector	920,837	97%	98%
Obsidium	698,330	90%	94%
SoftwarePassport	3,145,470	91%	93%
Pelock	3,451,282	97%	98%
Telock	945,821	99%	98%
Pespin	418,183	92%	97%
Armadillo	3,361,391	93%	97%
ACProtect	918,139	92%	99%



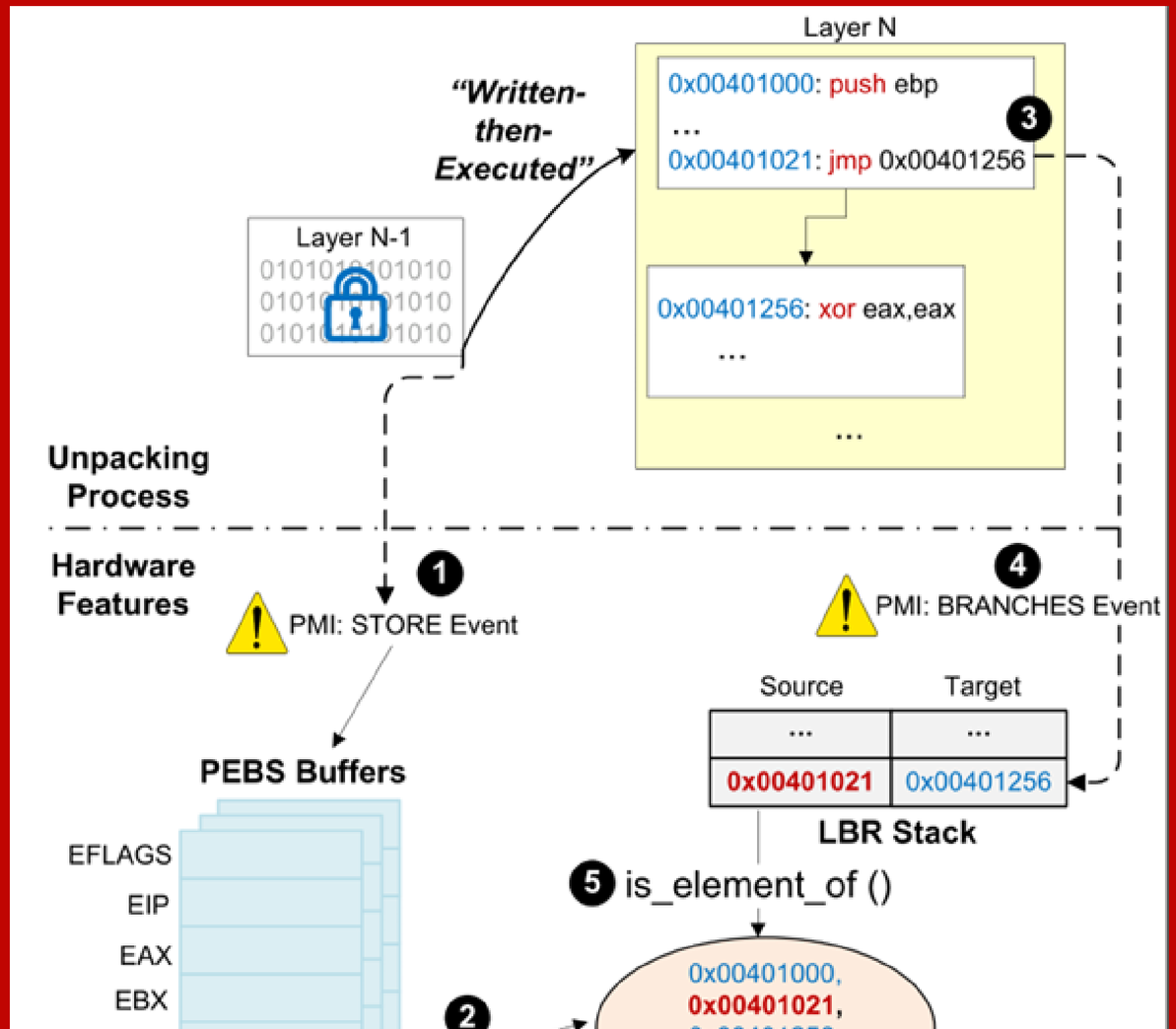
# of iterations per packer

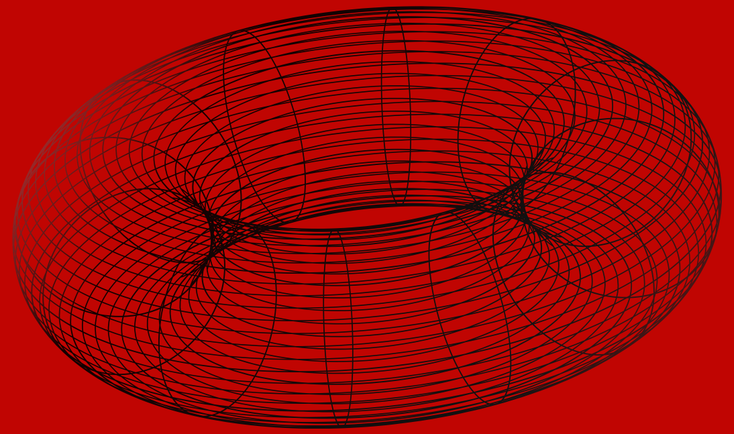
How To Detect A Loop



an example of loop detection using LBR

How To Detect Unpacking Layers



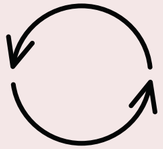


capture unpacking layers via PEBS and LBR

Determining Original Code

STEP # 1

Define the sum of loop centric HPCs values



STEP # 2

Use the loop layers classified as original code or not

STEP # 3

Train & Test 5 ML Classifiers

Evaluation

29 off the shelf packers

CAPE, Olly, Arancino

100% success rate in study

Large scale evalution on 74,938 wild malware

96.5% success rate on wild malware

Smaller samples do not reveal hotloops

Possible Attacks

DETECTION ATTACK

TIME BASED ATTACK

HIDING HOTLOOP

MIMICRY ATTACK

FAKE HOT LOOP

Have Questions? Connect with us..

BINLIN CHENG binlincheng@163.com

JIANG MING jming@tulane.edu

Thank you!