CERIAS

the center for education and research in information assurance and security

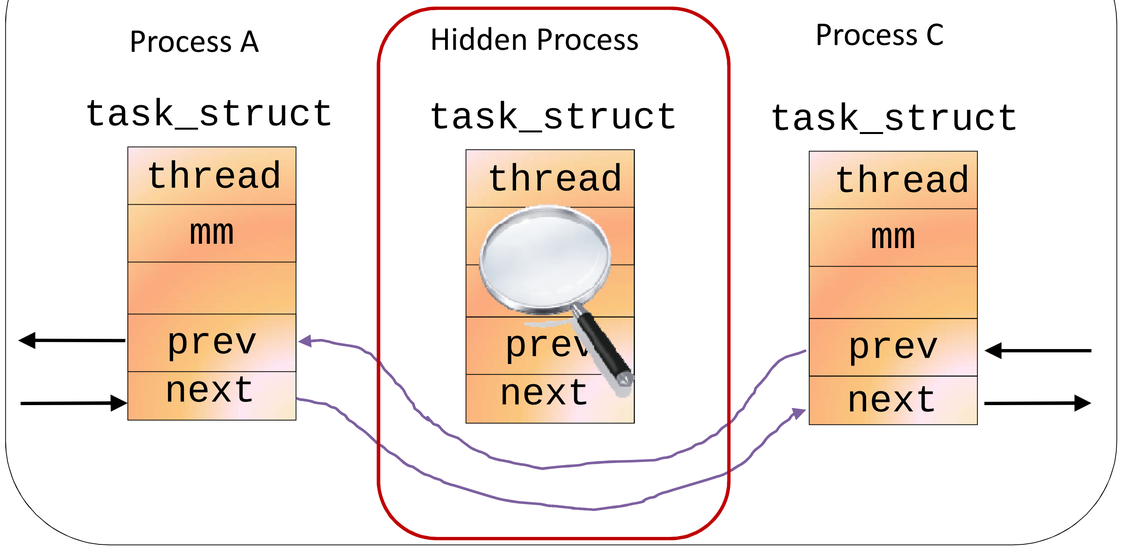
Graph-based Signatures for Kernel Data Structures

Zhiqiang Lin[1] Jungwhan Rhee[1] Xiangyu Zhang[1] Dongyan Xu[1] Xuxian Jiang[2]

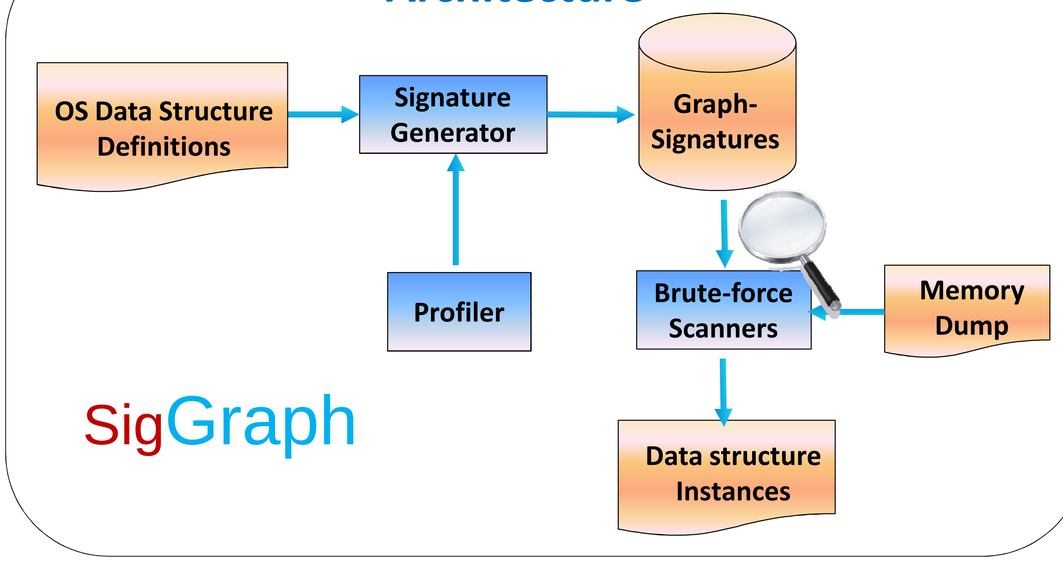
[1]Department of Computer Science and CERIAS, Purdue University

[2]Department of Computer Science, North Carolina State University

Motivation



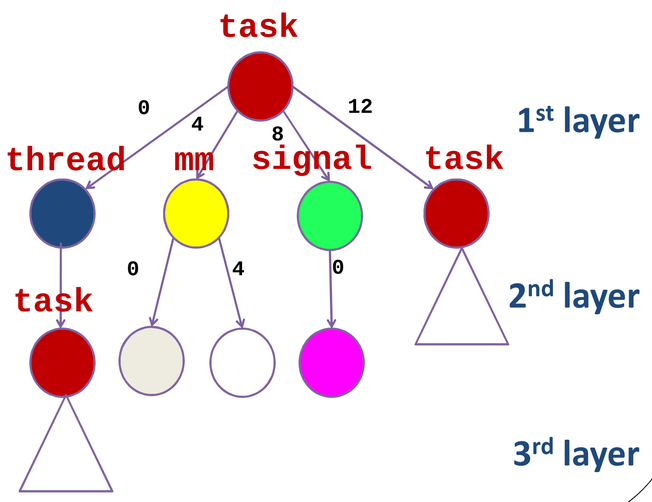
Architecture



Key Ideas

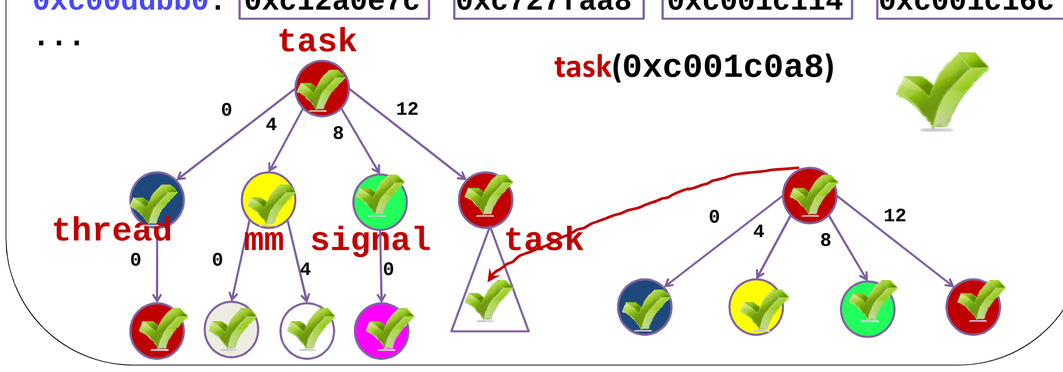
```
struct task {
  [0] struct thread *thread;
  [4] struct memory *mm;
  [8] struct signal *signal;
 [12] struct task *parent;
}

struct thread {
  [0] struct task *task;
}

struct memory {
  [0] struct vma *mmap;
  [4] void (*map_area)
      (struct memory* mmap);
}

struct signal {
  [0] struct task_status *status;
}
```

task(x) ← thread(*(x+0)) ∧ mm(*(x+4)) ∧ signal(*(x+8)) ∧ task(*(x+12))



How to Use SigGraph

```
0xc001c0a8: 0xc002c0a8  0xc002bee0  0xc002caa0  0xc00ddbb0
...
0xc002c0a8: 0xc12a0e7c  0xc727faa8  0xbfbb9195  0x00000009
...
0xc002bee0: 0xc001c114  0xc001c16c  0xffb29122  0x00201001
...
0xc002caa0: 0xb002ca20  0xb021d00a  0xc05b9f5c  0x00000000
...
0xc00ddbb0: 0xc12a0e7c  0xc727faa8  0xc001c114  0xc001c16c
...
```



Experimental Evaluation I: Memory Forensics

Data Struct of Interest	"True" Instance	SigGraph		Value-invariant	
		FP%	FN%	FP%	FN%
task_struct	88	0.00	0.00	0.00	0.00
thread_info	88	0.00	0.00	6.45	1.08
mm_struct	52	0.00	0.00	0.00	0.00
vm_area_struct	2174	0.40	0.00	7.52	0.00
files_struct	53	0.00	0.00	0.00	0.00
fs_struct	52	0.00	0.00	0.00	0.00
dentry	31816	0.01	0.00	0.01	0.00
sysfs_dirent	2106	0.52	0.00	97.63	0.00
socket	55	0.00	0.00	0.00	12.24
sock	55	0.00	0.00	0.00	27.90
user_struct	10	0.00	0.00	99.91	0.00

Experimental Evaluation II: Rootkit Detection

Rootkit Name	Target Object	Inside View	SigGraph	
		#obj.s	#obj.s	detected
adore-ng-2.6	module	23	24	✓
adore-ng-2.6'	task_struct	62	63	✓
cleaner-2.6	module	22	23	✓
enyelkm 1.0	module	23	24	✓
hp-2.6	task_struct	56	57	✓
linuxfu-2.6	task_struct	59	60	✓
modhide-2.6	module	22	23	✓
override	task_struct	58	59	✓

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center