CERIAS

the center for education and research in information assurance and security

REWARDS: Automatic Reverse Engineering of Program Data Structures from Binary Execution

Zhiqiang Lin Xiangyu Zhang Dongyan Xu

Department of Computer Science, Purdue University

Data Structure Knowledge Is Valuable to Many Security Applications

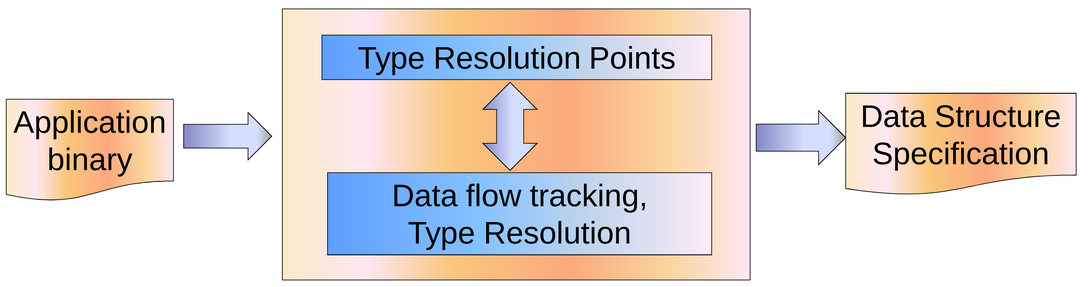
Memory Forensics

Vulnerability Discovery

Penetration Test

Virtual Machine Introspection

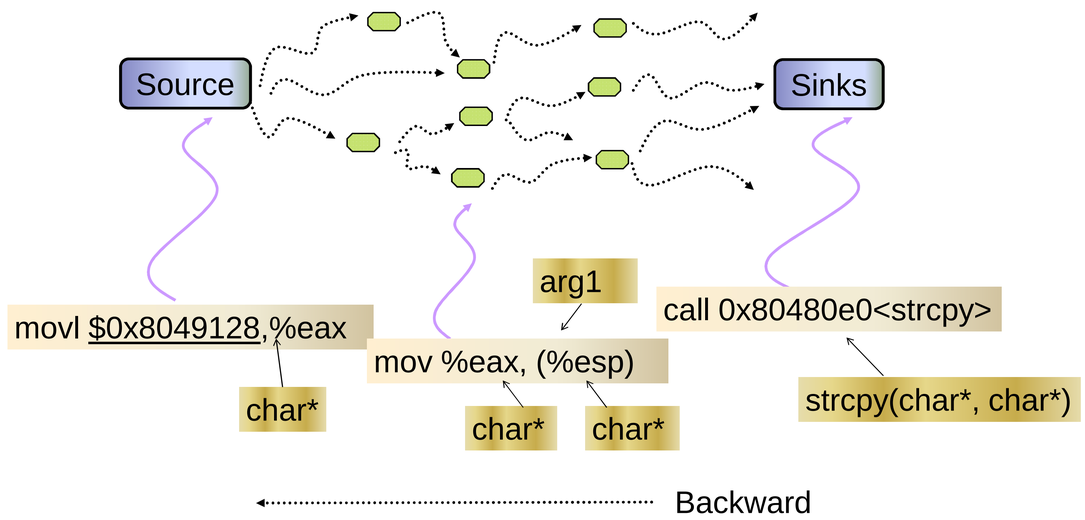
REWARDS

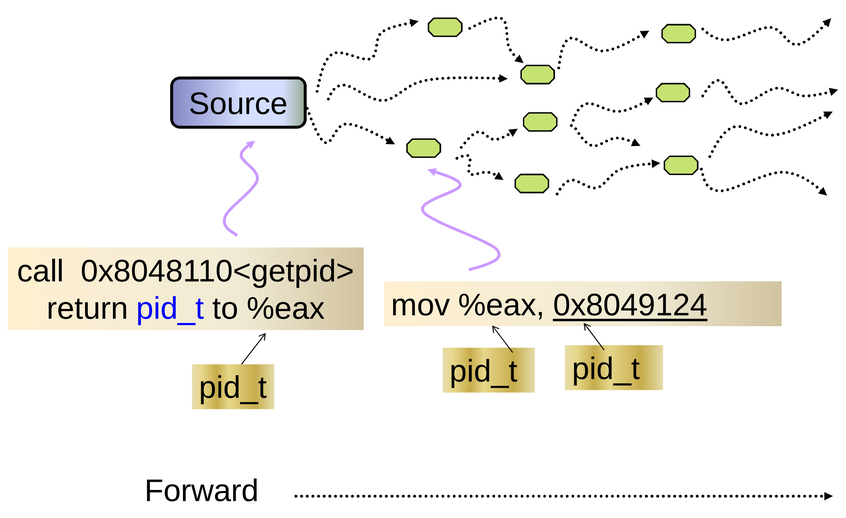


*R*everse *E*ngineering *W*ork for *A*utomatic *R*evelation of *D*ata *S*tructures

PIN QEMU open source processor emulator Valgrind

Key Technique: Two-way Data Flow Tracking and Type Resolution Using Dynamic Binary Instrumentation





Experimental Evaluation I: Memory Forensics

```
08052170  b0 5b fe b7 b0 5b fe b7  05 00 00 00 02 00 92 7e
08052180  0a 00 00 0b 00 00 00 00  00 00 00 00 c7 b0 af 4a
08052190  c7 b0 af 4a 00 00 00 00  58 2a 05 08 00 00 00 00
080521a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
...
```

```
struct 0x804dd4f {
00:     pthread_t;              b0 5b fe b7
04:     int;                    b0 5b fe b7
08:     socket;                 05 00 00 00
12:     struct sockaddr_in;     02 00 92 7e 0a 00 00 0b .. 00
28:     time_t;                 c7 b0 af 4a
32:     time_t;                 c7 b0 af 4a
36:     unused[4];              00 00 00 00
40:     struct 0x804ddfb*;      58 2a 05 08
};
```

Experimental Evaluation II: Vulnerability Discovery

Program	buffer overflow		integer overflow		format string	
	#total	#real	#total	#real	#total	#real
ncompress-4.2.4	1	1	0	0	0	0
bftpd-1.0.11	3	1	0	0	0	0
gzip-1.2.4	3	1	0	0	0	0
nullhttpd-0.5.0	5	1	2	1	0	0
xzgv-5.8	3	0	8	1	0	0
gnuPG-1.4.3	0	1	3	1	0	0
ipgrab-0.9.9	0	1	5	1	0	0
cfingerd-1.4.3	4	0	0	0	1	1
ngircd-0.8.2	12	0	0	0	1	1

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center