Review “Hardware Feature For Debug”

Name: Wenhui Zhang

Paper Name :

Zhang, F., Leach, K., Stavrou, A., Wang, H., & Sun, K. (2015, May). Using hardware features for increased debugging transparency. In *Security and Privacy (SP), 2015 IEEE Symposium on* (pp. 55-69). IEEE.

Contribution:

In this paper proposes a method of using System Management Mode (SMM) of x86 for debugging and analysis of malware behaviors.

Motivation:

There are lots of malwares attacking systems. In the current ecosystem, we have lots of applications vulnerable and exposed to these malwares. Thus there is a calling for an environment for analyzing malware behaviors. Traditionally, people execute malwares in isolated VMs, running malware inside of a VM, and running analysis tools outside of the VM. However, the traditional approach depends on the fact that hypervisor has a small TCB. And it is incapable of analyzing rootkits with this setup. Furthermore, we are unable to analyze malwares with packing, such as malwares packed with anti-debugging, anti-virtualization and anti-emulation techniques.

Related works:

COMPARISON WITH OTHER DEBUGGERS

	MALT	BareBox [17]	V2E [7]	Anubis [8]	Virt-ICE [9]	Ether [4]	VAMPiRE [26]	SPIDER [5]	IDAPro [19]
No VM/emulator	✓	✓					✓		✓
Debug ring0 malware	✓		✓	✓	✓	✓		✓	
Trusted code base	***BIOS***	OS	KVM+QEMU	QEMU	QEMU	Xen	OS	KVM	OS
SLOC of TCB (K)	**1.5**	16,281	13,397	786	786	509	16,281	12,593	16,281

Methodology:

This bare metal debugging system, MALT, provides 4 techniques for debugging armored malwares and rootkits: (1) instruction level; (2) branch level; (3) far control level and (4) near return transfer level. The MALT system includes two parts: (1) debugging client for malware analyst; and (2) debugging server, of which includes SMI handler and the target debugging application.

Results:

MALT is transparent in terms of anti-debugging, anti-virtualization and anti-emulation packing techniques. Performance of switching SMI modes is good, as is shown below:

Testbed Specification
- Motherboard: ASUS M2V-MX SE
- CPU: 2.2 GHz AMD LE-1250
- Chipsets: AMD K8 Northbridge + VIA VT8237r Southbridge
- BIOS: Coreboot + SeaBIOS

Table: SMM Switching and Resume (Time: μs)

Operations	Mean	STD	95% CI
SMM switching	3.29	0.08	[3.27,3.32]
SMM resume	4.58	0.10	[4.55,4.61]
Total	7.87		

Take away:

MALT is not fully transparent, as it is not transparent to external timing attacks.

On the other hand, we could make remote debugging client side fatter, by adding IDA pro etc. etc.