Rench: A Benchmark for Return-Oriented Programming

· Feifei Wang

NC STATE UNIVERSITY

Motivation and problem

Defense systems against Returned Oriented Programming (ROP) all use different security evaluation methods. It is hard to measure the effectiveness and make comparision.

We propose the first benchmark for ROP defense systems called Rench.

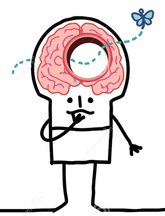
Threat model

Vul App	Rench
Defense System	
Operating System	

ability: vulnerable app · local access
inability: OS and Rench
goal: bypass DEP by various ROP

Research questions

Existing design and countermeasures?
Commonly used evaluation methods?
Features should be included in Rench?



Design

ASLR	>3 rets, <=5 intrs
DynIMA	<3 rets, <=5 intrs
DROP	>3 rets, >5 intrs
TRUSS	Jmps
ROPdefender	
ROPGUARD	Call-preceded&Executable
KBouncer	

Implementation

```
# POP EBX # RETN [audconv.dll]
# 0x00000001-> ebx
# POP ECX # RETN [audconv.dll]
# 0x00000040-> ecx
```

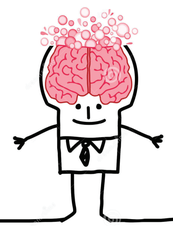
```
# POP ESI # POP EBP # XOR EAX,EAX # POP EBX # POP ECX # RETN
# VirtualAlloc
# & call esp [audconv.exe]
# 0x00000001-> ebx
# 0x00000040-> ecx
```

```
# POP EAX # RETN [audconv.dll]
# 0x1002186e-> eax
# pop edx; pop ecx; jmp eax
```

```
# pop eax; retn
# VirtualAlloc
# call eax; add esp,8; retn
# add esp,8; retn
# shellcode
```

Evaluation

ROPGuard	
<3 rets, <=5 intrs	YES
>3 rets, >5 intrs	YES
Jmps	YES
Call-preceded &Executable	NO



Take-aways

Make hands dirty.
Trust tools but not totally trust tools

References

- ASLR: The pax team. In http://pax.grsecurity.net/.
- DynIMA: L. Davi et al. Dynamic integrity measurement and attestation: towards defense against return-oriented programming attacks (2009)
- DROP:P. Chen et al. Drop: Detecting return-oriented programming malicious code (2009)
- TRUSS: S. Sinnadurai et al. Transparent runtime shadow stack: Protection against malicious return address modifications (2008)
- ROPdefender: L. Davi et al. Ropdefender: A detection tool to defend against return-oriented programming attacks (2011)
- ROPGuard: I. Fratric. Runtime prevention of return-oriented programming attacks (2012)
- KBouncer: V. Pappas et al. Transparent rop exploit mitigation using indirect branch tracing (2013)