Review “Hacking in darkness”

Name: Wenhui Zhang

Paper Name：

Lee, J., Jang, J., Jang, Y., Kwak, N., Choi, Y., Choi, C., ... & Kang, B. B. (2017, August). Hacking in darkness: Return-oriented programming against secure enclaves. In *USENIX Security* (pp. 523-539).

Contribution:

This paper proposes a method on how to conduct ROP on encrypted binaries. In this paper, authors: (a) detect the number of register pops before a ret instruction, (b) reveal enclave register values, and (c) leak the secret enclave memory contents.

Motivation:

Addresses and data are encrypted and protected through SGX enclaves.

Related works:

ROP; SGX.

Methodology:

Step 1: looking for pop gadgets, CR2 is the register, the value of which suggests how many pops are there; Step 2: looking for ENCLU, which is a opcode representing multiple functionalities, the rax value represents different switch values; Step 3: looking for pop rax; ret; Step 4: deciphering pop gadgets, in search of r?? Registers; Step 5: looking for memcpy(dst*,some valid address, 0x10).

Results:

Case study 0: Dumping confidential data;

Case study 1: Compromising sealed data;

Case study 2: hijacking remote attestation, MiTM (Emulated Enclave) between enclave and attestation server, masquerading the enclave to deceive remote attestation server.

Take away:

This paper proposes a method on leaking sensitive information, and permanently parasite to the enclave program by performing a MiTM attack. We need a filter for memcpy.

- The first practical ROP attack on real SGX hardware
- Exploits a memory-corruption vulnerability
- Demonstrates how the security of SGX can be disarmed.
- Exfiltrate all memory contents from the enclave
- Bypass the SGX attestation
- Break the data-sealing properties
- Encourage the community
- Explore the SGX characteristic-aware defense mechanisms
- Develop an efficient way to reduce the TCB in the enclave.