Software Side-Channel Attacks Against Intel SGX Enclaves

CS 658 Research Paper

Colin Howes
University of Waterloo
200 University Ave. W
Waterloo, ON N2L 3G1
chowes@uwaterloo.ca

ABSTRACT

Intel Software Guard Extensions (SGX) is a set of hardware instructions extending the Intel architecture that allows user-level software to run securely when all other software on the system is untrusted. SGX uses secure enclaves running in processor reserved memory combined with software attestation to provide confidentiality, integrity, and freshness guarantees to users wishing to execute software on an untrusted remote system. However, SGX is vulnerable to a number of software side-channel attacks, which leverage performance measurements to determine memory access patterns in order to derive secrets from software executing in secure SGX enclaves. SGX vulnerabilities to software side-channel attacks and directions for future research are discussed.

1 INTEL SGX

Intel Software Guard Extensions (SGX) is a set of hardware extensions designed to allow legacy programs to run securely in an environment where all software on a remote host machine is potentially untrusted. SGX was designed to address the problem of *secure remote computation*, that is, secure execution of software on a remote system controlled by an untrusted party. Under this threat model, *all* software on a remote system is potentially malicious, including the operating system and hypervisor. SGX was therefore designed to provide a method for secure computation while protecting user-level software executing on behalf of a remote user from malicious software running at higher privilege levels. This is acheived through a set of CPU instructions that sequester a user-level process into a secure *enclave* running in processor reserved memory.

2 SOFTWARE SIDE-CHANNEL ATTACKS

Side-channel attacks are a class of attacks that leverage information about the physical properties of a system in order to infer secrets protect by the system. Some side-channel attacks require physical access to a machine, and are both difficult and expensive to employ. However, software side-channel attacks leverage physical information gained about a system acquired exclusively through software.

Cache timing attacks are used to infer memory access information by exploiting timing differences.

Page fault attacks can be employed by a malicious operating system to determine when a program is accessing specific pages.

3 ATTACKS AGAINST SGX ENCLAVES

Both cache timing attacks and page fault attacks have been demonstrated against SGX enclaves in proof-of-concept attacks.

4 COUNTERMEASURES

A number of countermeasures have been proposed, both for future development of secure hardware, and additional security measures that can be employed by security conscious developers working with the current implementation of SGX.

5 FUTURE DIRECTIONS

6 CONCLUSIONS

REFERENCES

[1] Victor Costan and Srinivas Devadas. 2016. Intel SGX Explained. *IACR Cryptology ePrint Archive* 2016 (2016), 86. https://pdfs.semanticscholar.org/2d7f/3f4ca3fbb15ae04533456e5031e0d0dc845a.pdf