TCP Congestion Control

CS 656 Research Paper

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

ABSTRACT

1 INTEL SGX

Intel Software Guard Extensions (SGX) is a set of hardware extensions designed to allow programs to run securely in an environment where all software on the 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 [1]. Under this threat model, *all* software on a remote system is potentially malicious, including the operating system and hypervisor. Thus SGX must provide protection from malicious software running at higher privilege levels to user-level programs [**?**].

SGX provides confidentiality and integrity freshness guarantees through the use of trusted hardware that sequesters a user-level program into a secure container called an *enclave*, and proves to a user that he or she is running unmodified software protected in an enclave by secure hardware [1]. This proof is based on *software attestation*, which provides a cryptographic signature encompassing a measurement of the enclaves contents [**?**].

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 carry out an attack. While physical side-channel attacks against modern hardware are difficult and costly, requiring advanced tools and physical access to the victim machine, software side-channel attacks are inexpensive to deploy and can be executed by anyone with remote access to a system [**?**]. The software side-channel attacks discussed here exploit hardware and software implementation details to acquire information about memory access patterns, which can be used to infer secrets from an otherwise secure system [**? ? ? ?**].

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] Intel Corporation. 2016. Intel Software Guard Extensions. (2016). https://software.intel.com/en-us/sgx