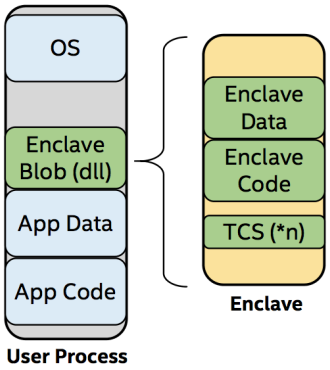
Security Behind Intel SGX

Kristopher Willis

Introduction

Computer security is an ongoing threat to users around the world and to national security here in the United States. Intel has created a new way of securing personal and identifiable data using extra processor instructions they call Software Guard Extensions(SGX). Intel SGX enables applications to execute code and protect secrets from within the protected enclave giving developers direct control over application security.

Intel SGX reduces the trusted footprint which allows for shorter logs and faster forensics. SGX prevents software attacks at the OS, hardware, and even virtual environment level. SGX also prevents memory cache exploits by encrypting memory images.



Their are many usage cases for Intel SGX. Intel SGX utilizes a secure enclave which could replace TPM and TXT with SGX. This means you could have the piece of mind of storing username and password information without having the information compromised even if the machine is totally infected. Digital rights management could also be improved using SGX specifically to eliminate HDCP limitations and allow 4k content streaming. You could also securely communicate using messaging and even VOIP which has been difficult to encrypt end to end because of data bandwidth. The most important usage case I believe is that you could use this to end-to-end encrypt virtual machines in Cloud datacenter without datacenter admins eavesdropping. This could allow for more hosted cloud adoption which could decrease consumer hardware costs but push users to tier based models which is being pushed heavily by Microsoft, Google, and Apple.

Intel SGX requires at least a 6th generation Skylake processor and the software developer has to compile application code using the Intel SGX SDK. It should be noted that there is an SDK that has been developed independently to work on Linux however,

currently you must use Microsoft Windows to take full advantage of SGX. Speaking with a Intel SGX developer at Defcon, memory image encrypting also requires special memory modules to take full advantage.

Related Work

Intel SGX is brand new. Intel announced SGX would be available to consumers when Skylake shipped in late 2015. There is also not many applications that take advantage of Intel SGX because of the alienation of the market. Essentially, at the moment SGX is too new to be used for consumer applications.

This does not mean that Intel SGX has not been extensively looked at in the last year. MIT student, Srinivas Devadas did an extensive look into SGX and criticized it for not being as secure as its competitors in the market. Florida Institute of Technology has also looked into SGX however, at a very basic level on how it works and what are the potential usage cases.

AMD is also looking at competing with SGX with both SEV and SME. Currently, both of these products will not be released in till AMD releases ZEN processors in 2017.

Outline For Final Report

A. Why I want to work on this?

The main reason I seek to learn more about Intel SGX is because of another Intel security IP that relies on SGX called CET(control flow enforcement technology). Intel CET protects against return oriented programming and jump oriented programming exploitation. CET is bleeding edge software security which will take years to see in applications. My goal is to learn more about how SGX works and then use techniques to try and exploit any security flaws that could reside in Intel's platform. Im also very curious about shadow stacks which SGX utilizes. More and more applications are starting to use shadow stacks which if not implemented correctly can easily be a good attack vector.

B. Prior Experience

I have experince in bypassing NOP, ROP, ASLR, and Canary software protections. I have also recently bypassed shadow stacks to get full stack access. I know many different instruction sets and exploitation techniques for x86, x64, ARM, ARM64, MIPs, and PPC. I have the tools to do this including IDA-Pro+Hexrays, BinaryNinja, and Qura. I have been competing in CTFs for over 5yrs now and have competed at DEFCON-CTF the most elite hacking competition in the world which focuses mostly on software reverse engineering. I also have several CVEs and hold zero-days in heavily used applications.

C. Expectations

1. Experiment with SGX and get a low level look at how the instructions work using disassemblers, debuggers, and hexdump.
2. Create some simple applications compiled with SGX to find holes.
3. Compare the results with the Intel SGX reference guide
4. Find common weaknesses in SGX
5. Try and exploit
6. If exploit found submit for CVE and Zero-Day Initiative
7. Publish paper with either results of exploit or which exploits were tried and failed.

D. Final Report Outline

1. Introduction
2. Related Work
3. How Intel SGX works
4. Experimentation
5. Vulnerability Assessment
6. Conclusion

Conclusion

Regardless if I can produce an exploit or not there is very little low level publications of Intel SGX. My goal is to produce interesting research that gives insight into the low level workings of SGX and to see if common weaknesses or vulnerabilities exist.

Future Work

1. Create some small applications to test SGX instructions
2. Disassemble applications in IDA and BinaryNinja
3. Look for common weaknesses
4. find potential exploit and experiment
5. conclusion

Bibliography

Baiju Patel on June 9, 2016, “Intel release new technology specifications to protect against ROP attacks,” Intel Software and Services. [Online]. Available: http://blogs.intel.com/evangelists/2016/06/09/intel-release-new-technology-specifications-protect-rop-attacks/. [Accessed: 26-Sep-2016].

“Intel SGX Homepage,” Intel® Software. [Online]. Available: https://software.intel.com/en-us/sgx. [Accessed: 26-Sep-2016].

“Intel® Software Guard Extensions Programming Reference,” Intel® Software Guard Extensions Programming Reference, Oct. 2014.
Intel, Software Guard Extensions Programming Reference. http://software.intel.com/sites/default/files/329298-001.pdf

L. Merino, “SGX Secure Enclaves in Practice,” BlackHat. [Online]. Available: https://www.blackhat.com/docs/us-16/materials/us-16-aumasson-sgx-secure-enclaves-in-practice-security-and-crypto-review.pdf.

S. Davenport and R. Ford, “SGX: the good, the bad and the downright ugly,” Virus Bulletin :: Jul-2014. [Online]. Available: https://www.virusbulletin.com/virusbulletin/2014/01/sgx-good-bad-and-downright-ugly. [Accessed: 26-Sep-2016].

V. Costan and S. Devadas, “Intel SGX Explained,” Intel SGX Explained, 2016.