Cairo University **Cryptography and Network Security**

Faculty of Engineering **Spring 2020**

Security Research Assignment-1

Name	**Yahia Ali Mohammed Anwar Abusaif**
الأسم	**يحيى علي محمد أنور أبوسيف**

Report on program obfuscation

Paper topic	**program obfuscation**
Paper Title	**A Commodity Obfuscation Engine on Intel SGX**
Authors	**Adil Ahmad** **Byunggill Joe** **Yuan Xiao** **Yinqian Zhang** **Insik Shin** **Byoungyoung Lee**
Publication Location Name of Journal	**Network and Distributed Systems Security (NDSS)**
Year of publication	**February 2019**

Review Paper Report
On
A Commodity Obfuscation Engine on Intel SGX, Adil Ahmad ,Byunggill Joe ,Yuan Xiao ,Yinqian Zhang ,Insik Shin , Byoungyoung Lee, Network and Distributed Systems Security (NDSS),February 2019.

1- Paper Overview

In this paper the authors do several things:

- Study if obfuscation is feasible based on Intel SGX.
- Talk about the types of attacks that need to be handled and design issues.
- Present OBFUSCURO, the first program obfuscation system built on top of Intel SGX.
- Evaluate security analysis of OBFUSCURO and empirical attack evaluations.
- Showing OBFUSCURO will secure execution of the SGX program
- Provide performance benchmark results of OBFUSCURO.

2-Problem Statement:

Despite of side channel constraints, the pervious obfuscation schemes are vulnerable if extended directly to Intel SGX. Hence the authors present OBFUSCURO, the first system that uses Intel SGX to provide software obfuscation. Pervious research relies on special purpose hardware, but OBFUSCURO is designed to run on Intel SGX, which is very common on the market.

It is found that these instruction codes made by Intel (i. e. SGX) can be accessed critically with some type of attacks that depends on patterns and side channels.

3- Basic Research directions of the related work so far in literature.

There is a lot of work to achieve the obfuscation of the system but with overhead efficiency. A systemic breakthrough has recently occurred; HOP (Hardware makes Obfuscation Practical) which achieves program obfuscation through relaxed assumptions of trust on the underlying hardware.

HOP relies on special-purpose hardware so HOP system relies in particular on custom RISC-V processors to conveniently transplant the root of confidence to execute the core security logic and contain the program code securely. Deploying these custom-built hardware on a majority of end user machines or cloud computing devices will be difficult and impractical.

By designing an efficient register-based stash the OBFUSCURO improves on the previously proposed secure ORAM implementations.

4-Summary of the paper solution of the research problem.

OBFUSCURO is a software framework that enables obfuscated execution of enclave programs for SGX. The idea behind OBFUSCURO is to allow execution of cache-line-granular code and access to data, protected by the use of ORAM operations, thereby displaying traces of memory that are oblivious to the program.

This system:

- Transforms the regular program layout into a side channel compatible layout.
- Ensures that its ORAM controller performs data oblivious accesses to protect itself from all memory-based side-channels.
- Ensures that the program is safe from timing attacks by ensuring that the program always runs at a fixed time interval.
- Introduces a systematic optimization such as register-based ORAM stash.

There are 2 ways for the attacker to steal information from SGX enclaves using side-channels.

1. He can abuse observed access-patterns to infer some information about the program or its input.
2. He can perform timing-based attacks to leak some information.

OBFUSCURO can stand against all of them.

5- Paper scientific contribution.

The paper proposes a system (called OBFUSCURO) which makes program obfuscation possible using Intel SGX.

OBFUSCURO actively protects the SGX enclave from leakage of information across all side channels, thereby neutralizing all memory and timing footprints to create a virtual black box to execute an obfuscated program.

The evaluation shows that the system can provide good guarantees of obfuscation within Intel SGX, thus performing better than existing cryptographic schemes and being more accessible to implementation than existing solutions.

The performance overhead of the system is high but it is still faster than the state-of-the-art cryptographic obfuscation schemes.

6- My evaluation: to the paper.

I think the paper is a bit small compare to the content that had been discussed. But overall, the paper is good except for the formatting and styling. They could've organized it more clearly, added more formatting like bullet lists, numbered lists, bold text and underlines. More than once, I felt it would've been appropriate to include a figure or graph to explain the discussed ideas.

The paper explains the main ideas and concepts quite well. However, the authors assume that the reader is already familiar with many terms and concepts. Those aren't the main focus of the paper, but it would have been helpful to include short explanations of those concepts.