Can I trust my machine? Modern and future challenges for Trusted Execution Environments

Submitted by

Flavio TOFFALINI

Thesis Advisor

Prof. Zhou JIANYING

ISTD

A thesis submitted to the Singapore University of Technology and Design in fulfillment of the requirement for the degree of Doctor of Philosophy

2021

PhD Thesis Examination Committee

TEC Chair:	Prof. Lu Wei
Main Advisor:	Prof. Zhou Jianying
Co-advisor(s):	Prof. Mauro Conti (University of Padua)
Co-advisor(s):	Prof. Lorenzo Cavallaro (King's College London)
Internal TEC member 1:	Prof. Sudipta Chattopadhyay
Internal TEC member 2:	Prof. Dinh Tien Tuan Anh

Abstract

ISTD

Doctor of Philosophy

Can I trust my machine?
Modern and future challenges for
Trusted Execution Environments

by Flavio TOFFALINI

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Publications

Journal Papers, Conference Presentations, etc...

Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

Contents

List of Figures

List of Tables

For/Dedicated to/To my...

Chapter 1

Introduction

TODO thesis in a glance. ◁ My thesis argues that Trusted Execution Environments (TEE), such as SGX, are powerful tools that isolate portion of code against strong adversaries (*i.e.*, the OS itself). However, TEEs are not the silver-bullet of cyber security and they suffer of limitations in terms of scalability and security.

I argue that we can further extend the TEE properties by carefully choosing smarter software design without the need of changing the TEE modules (and thus changing the hardware). Throughout the dissertation, I first investigate the TEE limitations, then, I will propose relative solutions. TODO I have to discuss every point carefully, this is just a memory for me. ◁

Overall, my study covers five TEE aspect:

- TODO Scalability untrusted code protection ◁ First, I will face a scalability issues that affect many modern TEE technologies (Chapter 3).
- TODO New defenses for the untrusted code ◁ Then. I will use TEE to implement runtime protection for untrusted memory (Chapter 4).
- TODO New threats ◁ At this point, I covered static and runtime protection for the untrusted code, now I will investigate new type of threats for the *enclaves* themselves (Chapter 5).
- TODO New defenses for the trusted code ◁ From this point, I will design new defenses for TEE *encalves* (Chapter 6)
- TODO Forensic analysis ◁ Finally, I will investigate the new challenges introduced by TEE technologies in terms of memory-forensic analysis (Chapter 7).

Chapter 2

Background

This chapter provides a background knowledge of Truest Execution Environments (Section 2.1), Control-Flow Attacks (Section 2.2), and Anti-Tampering Techniques (Section 2.3). In the final part, we focus on Software Guard eXtension (Section 2.4). These concepts will stem at the base of the following chapters.

2.1 Trusted Execution Environments

A Trusted Execution Environment (TEE) is a secure area that is contained in the main memory (RAM) and handled by the main CPU (Sabt, Achemlal, and Bouabdallah, 2015). A TEE ensures isolation of the code and data contained against external threats, such as the operating system (OS).

The first TEE standard has been defined by OMTP, a forum of mobile manufactures, and the specifications were mainly designed for mobile platforms (*Advanced Trusted Environment: OMTP TR 1*). Nowadays, TEEs have evolved and they are deployed in varied scenarios that range from mobile platforms to cloud servers (Schuster et al., 2015b; *SGX-Tor* 2018). In the following, we first discuss the two main concepts useful for this thesis: memory isolation (Section 2.1.1) and remote attestation (Section 2.1.2). In the end, we discuss the attacker model (Section 2.1.3).

2.1.1 Memory Isolation

One of the main property of a TEE is the capability of isolating a portion of memory, that is considered secure, from the rest of the system, that is considered insecure. This property allows a TEE to define a parallel environment that can run independently by the operation system. In jargon, the protected portion of memory is called *trusted region*, while all the outside one is called *untrusted region*.

The implementation of the memory isolation differs by the actual TEE vendor. However, modern TEE technologies achieve isolation by extending the Memory Management Unit (MMU) and the CPU cache (Winter, 2008; Gilmont, Legat, and Quisquater, 1999; Rozas, 2013). In Section 2.4, we discuss the memory isolation of Intel Software Guard eXtension, which is the main technology used in this thesis.

2.1.2 Remote Attestation

Remote Attestation (RA) is a challenge response protocol that involves a *Prover* and a *Verifier* (Bajikar, 2002), with the latter responsible for verifying the current status of the

former. The *Verifier* sends a challenge to the *Prover* asking to measure specific properties. The *Prover*, then, calculates the required measurement (*e.g.,* a hash of the application loaded) and sends back a report R, which contains the measurement M along with a digital fingerprint F, for instance, $R = (M, F)$. Finally, the *Verifier* evaluates the report, considering its freshness (*i.e.,* the report has not been generated through a replay attack) and correctness (*i.e.,* the *Prover* measurement is valid). It is a standard assumption that the *Verifier* is trusted, while the *Prover* might be compromised. However, the *Prover* is able to generate a correct and fresh report due to its trusted anchor (*e.g.,* a dedicated hardware module or a TEE).

In the following sections, we describe the two main RA schemes topology: *static* RA and *runtime* RA.

Static RA. Historically, static Remote Attestation (*static RA*) is the first type of RA proposed (Bajikar, 2002). As the name suggest, RA measures static properties of a system. Usually, it measure the correct loading of a piece of code in memory by employing standard hash functions. Other technologies, instead, extend their protection and report hardware information, for instance, they provide a CPU identification (Anati et al., 2013), measure particular hardware configuration (Sailer et al., 2004).

Runtime RA. Runtime Remote Attestation (*runtime RA*) schemes are new protocols that measure dynamic properties of a system. For instance, they ensure a piece of code have been executed correctly (*i.e.,* execution-flow measurement), or they report which modules have been traversed by a variable (*i.e.,* data-flow measurement). In the literature, there are many approaches to implement a runtime RA. For what concerns runtime RA for execution-flow properties, most of them encode the complete execution path of a *Prover* in a single hash (Abera et al., 2016; Zeitouni et al., 2017; Dessouky et al., 2017); some (Abera et al., 2019) compress it in a simpler representation and rely on a policy-based verification schema; other ones (Dessouky et al., 2018) adopt symbolic execution to verify the control-flow information continuously sent by the *Prover*. Runtime RA for data-flow, instead, simply traces the module traversed by tainted variables (Nunes et al., 2020; Abera et al., 2019).

All the aforementioned works rely on a trusted anchor (*i.e.,* a TEE) to store partial results of their protocol (*e.g.,* execution-flow information) and for protecting crypto materials (*i.e.,* algorithms and keys). Furthermore, they assume the adversary cannot tamper with the trusted anchor. Finally, *runtime RA* also assume a *static RA* in place to avoid software tampering.

2.1.3 Attacker Model

In TEE scenarios, the goal of an adversary is to bypass the TEE protections (*i.e.,* memory isolation and remote attestation) and tamper with the *secure* software or alter its behavior. To achieve this goal, TEE assumes two types of adversaries: *software* and *physical*.

Software Attacks. In this case, the adversary works either from a remote location or in the *untrusted* memory of the machine (*e.g.,* the OS). In addition, the adversary may

control the network medium as in the Dolev-Yao model (Dolev and Yao, 1981). The purpose of the adversary is multifold: she may load a infected software in the TEE, alter a *trusted component* already loaded, or use classing software exploitation techniques.

The TEE memory isolation prevents an adversary to load compromised software or directly modify existing protected memory regions (Section 2.1.1). On the other hand, an adversary may exploit known exploitation techniques to alter the execution of the TEE module trough execution-flow attacks. If the *secure software* suffer of bugs (*e.g.*, a memory corruption error), the TEE itself cannot prevent an adversary to alters *secure software* execution, and finally, the TEE cannot observe the attack. We discuss execution-flow attacks in Section 2.2.

Physical Attacks. In this case, the adversary has the same goal of the *software one* and share the same properties. In addition, the physical adversary have access to the machine hardware and can control the hardware components. Modern TEE technologies alone struggle at defending such attacks, however, it is a common to assume the adversary requires a non-negligible amount of time to carry a physical attck (*e.g.*, 10 min Conti et al., 2010; Conti et al., 2008; Ibrahim et al., 2016; Ibrahim, Sadeghi, and Zeitouni, 2017; Kohnhäuser, Büscher, and Katzenbeisser, 2019; Ibrahim, Sadeghi, and Tsudik, 2018). Recently, researchers proposed advanced RA schemes to mitigate these attacks (Ibrahim et al., 2016; Visintin et al., 2019; Kohnhäuser, Büscher, and Katzenbeisser, 2019).

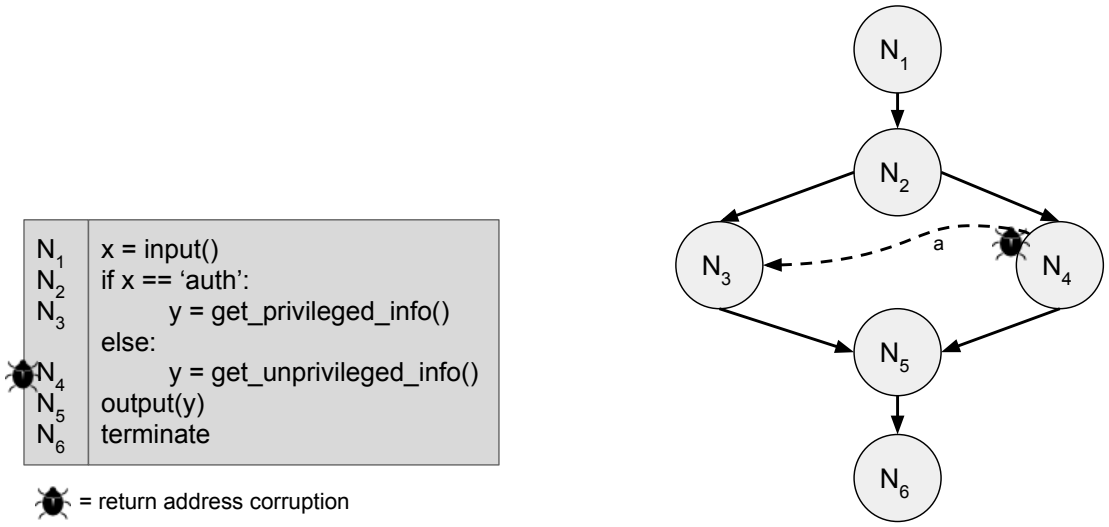
Commonly, denial of service DoS attacks are not considered in TEE scenario, and the untrusted software can avoid invoking the secure module.

2.2 Control-Flow Attacks

Solely TEE memory isolation and static RA cannot avoid classic exploitation techniques. For instance, if the *secure software* suffers of a memory corruption error, an adversary may corrupt a control structure (*i.e.*, a return address in the stack) and hijack the execution path.

To introduce control-flow attacks, we first discuss the concepts of control-flow graph (CFG), execution path, and basic-block (BBL) by using the simple program shown in Figure 2.1a as a reference example. The program starts with the acquisition of an input from the user (line 1). This is evaluated (line 2) in order to redirect the execution towards the retrieval of a privileged information (line 3) or an unprivileged one (line 4). Then, the retrieved information is stored in a variable (y), which is returned as an output (line 5), before the program properly concludes its execution (line 6).

A CFG represents all the paths that a program may traverse during its execution and it is statically computed. On the contrary, an execution path is a single path of the CFG traversed by the program at runtime. The CFG associated to the program in Figure 2.1a is depicted in Figure 2.1b and it encompasses two components: nodes and edges. The former are the BBLs of the program, while the latter represent the standard flow traversed by the program to move from a BBL towards the next one. A BBL is a linear sequence of instructions with a single entry point (*i.e.*, no incoming branches to the set of instructions other than the first), and a single exit point (*i.e.*, no outgoing branches from the set of instructions other than the last). Therefore, a BBL



(A) Pseudo-code of a program under a control-flow attack.

(B) Control-flow graph of a program under a control-flow attack.

FIGURE 2.1: Illustrative example of a control-flow attack.

can be considered an atomic unit with respect to the control-flow, as it will either be fully executed, or not executed at all on a given execution path. A BBL might end with a control-flow event, which could be one of the following in a `X86_64` architecture: procedure calls (*e.g.*, `call`), jumps (*e.g.*, `jmp`), procedure returns (*e.g.*, `ret`), and system calls (*e.g.*, `syscall`). During its execution, a process traverses several BBLs, which completely define the process execution path.

Runtime attacks, and more specifically the control-flow ones, aim at modifying the CFG of a program by tampering with its execution path. Considering Figure 2.1, we assume that an attacker is able to run the program (from the node N_1), but that he is not authorized to retrieve the privileged information. However, the attacker can, anyway, violate those controls through a memory corruption error performed on the node N_4. As soon as the attacker provides an input to the program and starts its execution, he will be redirected to the node N_4. At this point, the attacker can exploit a memory corruption error (*e.g.*, a stack overflow) to introduce a new edge from N_4 to N_3 (edge labeled as a) and retrieve the privileged information. As a result, the program traverses an unexpected execution path not belonging to its original CFG. Even though several solutions have been proposed to mitigate such attacks (*e.g.*, ASLR - Kil et al., 2006), attackers still manage to perform them (Veen, Cavallaro, and Bos, 2012).

This illustrative example about how to manipulate the execution path of a program is usually the basic step to perform more sophisticated attacks like exploiting a vulnerability to take control of a process (Yuan, Zeng, and Ding, 2015) or installing a persistent data-only malware without injecting new code, once the control over a process is taken by the attacker (Vogl et al., 2014).

2.3 Anti-Tampering Techniques

We say that a program P is tamper-resistant if P is designed such that an attacker would have difficulties to modify P's code. There are several strategies for achieving this goal (Nagra and Collberg, 2009). In this thesis, we mainly focus on *self-checking*. These techniques work at bytecode level, and they are structured such that the software can read its own bytecode in order to find anomalies and then reacts accordingly. We call *checkers* those sections of the software which check the software status, and *responses* those which react to the checkers' requests.

A checker's duties include reading a portion of the software's bytecode and verifying whether that code matches specific expectations. That is, the checker computes a hash code of the bytecode using a hashing function and compares the hash value with a pre-computed value. Once a mismatch is found, the software might adopt different reactions, *e.g.*, it can emit an alarm or restore the un-tampered code.

To prevent the checkers from being disabled by an attacker, they typically spread over the code and/or triggered randomly during the execution. Checkers, hash functions, and hash values can be prone to attack; therefore, an anti-tampering protection must be designed for protecting itself. This is achievable by using different techniques, *e.g.*, through obfuscation techniques (Banescu and Pretschner, 2017), or a network of checkers (which communicate with each other so that if one checker is disabled/tampered, other checkers become aware of the attack).

2.4 Software Guard eXtension

TODO This comes from the memory forensic paper. ◁

2.4.1 SGX Remote Attestation

In the SGX Remote Attestation (SGX RA) (**vill2017sgx**), the *Prover* is an *enclave*, while the *Verifier* can be either another *enclave* or a generic software. The SGX RA relies on the isolation offered by the CPU to protect the cryptographic keys. In particular, the SGX RA guarantees two properties: (i) the host machine has correctly loaded the *Prover* in memory, (ii) the *Verifier* can check the identity of the *Prover* and the machine (*i.e.*, CPU) that is loading it. However, the SGX RA does not guarantee *runtime* integrity, for instance, an adversary can exploit a memory corruption error while the *Verifer* cannot detect the attack.

TODO I could integrate this part with the memory forensic background for the CPU structures ◁

2.4.2 SGX Control-Flow Attacks

In the following, we described the two main works that describe code-reuse attacks against SGX: Guard's Dilemma (Biondo et al., 2018) and Dark-ROP (Lee et al., 2017).

Dark-ROP. Lee et. al present Dark-ROP (Lee et al., 2017), a technique to locate gadgets in an enclave. In their scenario, the attacker probes a victim enclave until triggering

an `AEX`. From the exception risen, the host can gain information about the location and the nature of the gadgets. Once enough gadgets are collected, the adversary can finally craft a payload and bypass the enclave protections. The success of this technique exploits the fact that neither the enclave nor an external observer (*e.g.,* the microcode) can backtrack the cause of a crash. In practice, the SGX isolation does not allow inspection either for *good* analysis or by adversaries.

Guard's Dilemma. Biondo et. al propose a new approach, called *Guard's Dilemma*, that does not require probing the enclave (Biondo et al., 2018). The authors abuse two critical Intel SGX SDK procedures to control the CPU registers. The first one is `asm_oret`, that restores the CPU registers after an OCALL. The second one is `continue_execution`, that is used in the exception handling. The authors use the latter to perform a stack pivoting (*i.e.,* control the `rsp` register). *Dilemma* works because the enclave has no mechanism to validate the integrity of the input of these two functions.

Chapter 3

A Practical and Scalable Software Protection enforced by TEE

In this chapter, we propsoe a technique that overcomes the limitations of both pure anti-tampering and trusted computing by combining both approaches. We extend hardware security features of trusted computing over untrusted memory regions by using a minimal (possibly fixed) amount of code. To achieve this, we harden anti-tampering functionality (*e.g.,* checkers) by moving them in trusted components, while critical code segments (which invoke the checkers stored within a trusted module) are protected by cryptographic packing. As a result, we keep the majority of the software outside of the secure container, this leads to three advantages: (i) we avoid further sophistication in communicating with the OS, (ii) we maximize the number of trusted containers issued contemporaneously, and (iii) we also maximise the number of processes protected.

Realizing our idea in practice is non-trivial. Besides the self-checking functionalities, we need to carefully design other phases of our approach such as installation, boot, and response. The installation phase must guarantee that the program is installed properly, while the boot phase should validate that the program starts untampered. Both phases require us to solve the attestation problem. The third phase, the response, is the mechanism which allows a program to react against an attack once it has been detected. Moreover, trusted computing technologies, such as SGX, do not offer standalone threads that can run independently of insecure code. Instead, protected functionality needs to be called from (potentially) insecure code regions. As a result, such technologies do not provide *availability* guarantees. Therefore, one design aspect of our solution is to cope with and mitigate *denial of service* threats.

As a proof-of-concept, we implemented a monitoring application which integrates our approach. For this example, we opted for SGX as a trusted module. The application is an agent which traces user's events (*i.e.,* mouse movements and keystrokes) and stores the data in a central server. We developed the monitoring agent in C++ and we deployed it in a Windows environment. In our implementation, we designed the checkers to monitor those functions dedicated to collect data from the OS, while the response was implemented as a digital fingerprint which represents the status of the client (*i.e.,* client secure, client tampered).

To evaluate our approach, we systematically analyze which attacks can be performed against our approach and we show that, with the user monitoring application, our solution provides better protection than previous approaches. We measure the overhead of our approach in terms of Lines of Code (LoC), execution time, and trusted memory allocated. We show that fewer than 10 LoC are required to integrate

our approach, while the trusted container requires around 300 LoC. Furthermore, the overhead in terms of execution time is negligible, i.e., on average 5.7% *w.r.t.* the original program. During our experiment, we managed to run and protect up to 90 instances at the same time.

Problem Statement: The research question we are addressing in this chapter is thus: Is it possible to extend trusted computing security guarantees to untrusted memory regions without moving the code entirely within a trusted module?

Contributions: In summary, the contributions of this paper are:

(**a**) We propose a new technique to extend trusted computing over untrusted zones minimizing the amount of code to store within a trusted module. (**b**) We propose a technique to mitigate *denial-of-service* problems in trusted computing technologies. (**c**) We propose an algorithm for achieving a secure installation and boot phase.

3.1 Threat Model

In a tampering attack, the goal of an attacker is to edit the code of a victim program Collberg and Thomborson, 2002. This goal can be achieved in different ways. One way is to change the bytecode of a program before its execution, this is called *off-line* tampering. That is, the attacker first analyzes the binary of the program and then disables/removes the anti-tampering mechanisms. The challenge for an attacker is thus to remove the anti-tampering mechanism without compromising the program logic. Using tools such as debuggers or analyzers, the attacker can deduce how the anti-tampering protection works and disable it accordingly. To cope with *off-line* attacks, it is possible to adopt anti-tampering mechanisms based on digital fingerprint mechanisms. They employ a cryptographic fingerprint of software (*e.g.,* signature, hash, checksum) to validate software status before the execution Microsoft, 2017; Abera et al., 2016. Besides *off-line* attacks, there are the so-called *on-line* attacks. In this category, the attacker aims to edit the code during the execution of the victim program. Such attacks can be performed either from the kernel-space or from the user-space. The key to such attacks is to synchronize the attacker and the victim process such that the victim code is edited in a way unnoticed by the anti-tampering mechanism.

In our scenario, an attacker can compromise the victim logic (*i.e.,* the bytecode) by using both *off-line* and *on-line* approaches. We also consider acceptable to steal the victim software, or a piece of, as long as this keeps the environment unaltered. A suitable example for our scenario is represented by distributed anti-viruses. This software is composed by a client-server infrastructure and they are commonly used in companies. In particular, the clients report the status of their host machine to a central server, and the server stores the reports and eventually notifies an intrusion. In our example, it is possible to mount a set of attacks that will be easily detected. For instance, if a client is disabled, the central server will detect the anomaly, similarly if an unauthorized client is installed. If an attacker manages to steal a copy of the client software, it may be possible to run a tampered client in a controlled environment made ah-hoc, however, as long as the attacker cannot run such client in the original infrastructure, there is not effective damage for the companies. A tampered client becomes really dangerous when the attacker manages to run such client in the corporate environment in order to allow

illicit activities. In this case, the attack has to happen such that the central server does not recognize the anomaly.

The attacker model we consider works at user-space level; therefore, we assume the kernel is healthy. Having a healthy kernel is acceptable in corporate scenarios where the machines are constantly checked. Moreover, a user-space threat (*e.g.*, user-space malware, spyware) is generally simpler to mount than one at kernel-space. Even though we assume having a trusted kernel, and we could have instantiated our approach on the kernel itself, we opted to implement our PoC by using SGX in order to raise the bar for attackers that have compromised the kernel, as we will discuss in the following sections. We also assume the machines are not virtualized, this avoids the attacker to use VMX features Uhlig et al., 2005. Moreover, we assume the task scheduler is trusted, this is crucial to avoid a perfect synchronization of two processes (see Section 3.4.5).

To sum up, the adversary we face has the following properties: (i) he can analyze and change the binary *off-line*; (ii) he can change the *on-line* memory of a victim process at runtime; (iii) he cannot tamper with the task scheduler; (iv) he cannot virtualize the victim machine.

3.2 Design

Our *anti-tampering technique* is an extension of the classic *self-checking* mechanism. In the following, we describe how we improve upon existing techniques with trusted computing technologies. We start with a description of the problem addressed and then analyze limitations of existing approaches before explaining how our idea can help to limit the attacking surface of existing approaches.

3.2.1 Challenges

In our model, a program's execution can be described as a triplet (M, b, i) where M represents the state of the program (*i.e.*, memory), b is the sequence of instruction to execute (*i.e.*, code section) and i denotes the next instruction to execute (*i.e.*, instruction pointer). For simplicity, we focus on sequential and deterministic programs, whose instructions are executed step-by-step; however, in Section 3.2 we will discuss also multi-threading scenarios. Each step of the program can be represented as follows:

$$(M, b, i) \rightarrow (M', b', j),$$

where M' is the updated memory status, b' is the updated instruction sequence, and $\rightarrow$ is the small-step semantics of the program. From a software security point of view, a program should satisfy the following properties: **(i)** the next instruction j must be decided uniquely by the program logic (*i.e.*, M and the current instruction at i); **(ii)** the program state M' must be determined according to the previous program state M, and the instruction executed i; **(iii)** instructions b must not change during the program execution (*i.e.*, $b = b'$). Note that we assume that the application code is not dynamically generated, and that input and output operations happen through writing/reading operation in the memory.

Property (**i**) is related to the control flow integrity problem Li et al., 2018, which is guaranteed neither by anti-tampering techniques Nagra and Collberg, 2009 nor by trusted computing Lee et al., 2017. But it is tackled by tools such as Microsoft, 2015; Tice et al., 2014 and discussed in previous works Onarlioglu et al., 2010; Wang and Jiang, 2010; Abadi et al., 2005; Zhang and Sekar, 2013; Davi et al., 2014.

Property (**ii**) can be guaranteed by moving only sensitive data inside a trusted module and using *get()\set()* functions for interacting with them. This was already implemented by Joshua et al. Lind et al., 2017 in their Glamdring tool. Such a solution is prone to space constraint because it keeps data within the trusted module (*i.e.,* an enclave).

Property (**iii**) can be implemented by moving all code inside trusted modules, which was the first approach employed Baumann, Peinado, and Hunt, 2015; Arnautov et al., 2016a; Tsai, Porter, and Vij, 2017b.

However, simply moving all code into the trusted module has two problems. First, a trusted module has a limited amount of memory available, and therefore only certain critical sections can be executed securely. Second, the application needs access to other OS layers to interact with the environment (network, peripherals). Our approach aims to address these limitations.

A naive *anti-tampering* mechanism is to run a *checker* function over the entire code b right before executing any instruction. This is described as follows:

$$(M, b, i) \rightarrow check(b) \rightarrow (M', b', j),$$

where the $check()$ function verifies the integrity of the code b. This approach verifies the integrity of the entire application code at each step. However, this is inefficient since a program must read its entire code at each step. Furthermore, we must protect the *checker* function throughout the program.

In order to address space and efficiency constraints, as suggested in Brumley and Song, 2004; Singaravelu et al., 2006; Smith and Thober, 2006, we may consider only certain parts of the program to be sensitive, which are referred to as *critical sections* (CS) hereafter. CSs include delicate parts of the software such as license checking in commercial products. We could thus focus on protecting only the critical part of the program and checking a block of instructions instead of the entire program (*i.e.,* CSs). That is, instead of checking every instruction in every step, we check only the CSs. Therefore, the function `check()` is executed when we encounter an instruction starting a CS. This is illustrated as follows:

$$(M, b, i) \xrightarrow{\text{if } i \in \text{CS}} check(CS) \rightarrow (M', b', j)$$
$$(M, b, i) \xrightarrow{\text{else}} (M', b', j),$$

where $i \in$ CS means the instruction i is the beginning of a critical section *CS* and *check(CS)* checks the critical section CS.

Intuitively, even though the above idea improves the efficiency of the anti-tampering mechanism, it is still subject to attacks. Firstly, it is subject to just-in-time patch & repair. That is, an attacker could synchronize its actions to change the victim code right after the checking and restore the original code before the checker is executed again. To conduct such an attack (without having to compromise the task scheduler), the attacker

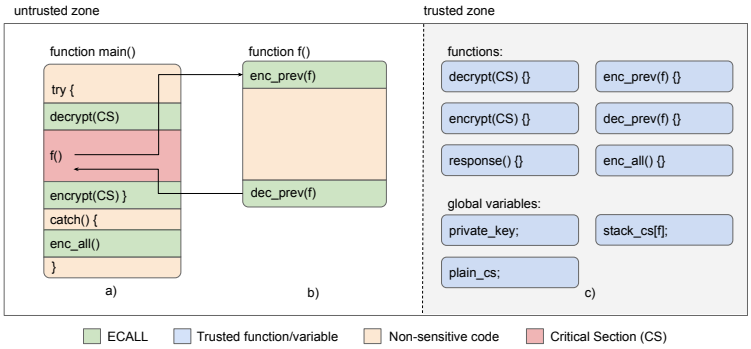


FIGURE 3.1: An overview of our schema for single-thread applications, the memory is split in trusted and untrusted zones. The trusted zone contains all methods required for our technique, while in the untrusted zone we show the interaction of those methods with the CSs.

and the software to be protected must run as concurrent processes, and the attack must time its actions according to the task scheduler. We argue that this attack is practically very challenging to carry out. In Section 3.4.5, we discuss the feasibility of such attacks in more depth. Secondly, an attacker may compromise the anti-tampering mechanisms (*i.e.,* modify the checkers and responses). Defenses against these attacks already exist. For instance, one may employ code obfuscation on *checkers* and *responses* so that the attacker would not identify them; or design the *checkers* and *responses* such that they are strongly interconnected with the application code Biondi and Desclaux, 2006 so it is challenging to compromise the anti-tampering mechanisms without compromising the application logic; or move part of the code (*e.g.,* checkers and responses) to the server Viticchié et al., 2016. These approaches are however prone to a similar threat, *i.e.,* all of them allocate their detection system in untrusted zones, and therefore, with enough time any attacker can understand and disarm these systems.

3.2.2 Anti-Tampering based on Trusted Computing

In this section, we will present the technical solutions to realize our approach in a real system. To achieve this, we require a trusted module to harden anti-tampering techniques. For the sake of coherence with our proof-of-concept implementation (see Section 3.3), we use the Intel Software Guard eXtension (SGX) Rozas, 2013 terminology. However, it is possible to use other trusted modules (see Section 3.5).

Unlike previous solutions that simple "hide" checking functions by adopting obfuscation or anti-reversing techniques Banescu and Pretschner, 2017; Chang and Atallah, 2001; Chen et al., 2016; Viticchié et al., 2016, we store code relevant to the anti-tampering mechanism in a trusted module (*i.e.,* an enclave), through which we monitor and react to attacks conducted on the untrusted memory region. Saving anti-tampering mechanisms within trusted containers is significantly different from previous purely software-based solutions since an attacker cannot directly tamper with them. This is illustrated in Figure 3.1, which presents an overview of our technique. In detail, a given application is divided into two zones: an untrusted zone (on the left side) and

a trusted zone (on the right side). The untrusted zone contains the entire application code, whereas the trusted zone contains all functions and global variables employed by our anti-tampering technique, such as *checkers* and *responses* (shown in blue). The untrusted zone is further divided into different regions: the CSs which we aim to protect (shown in red), the non-sensitive blocks (shown in pale yellow) and the code for calling the trusted functions in the trusted zone (shown in green). We also included three labels (*i.e.*, a, b, and c) to identify specific regions that will be used ahead in the discussion. By using this structure, we can check the status of the untrusted zone by being inside the trusted zone.

Critical Section Definition A CS is any continuous region of code which is surrounded by two instructions, respectively labeled as *CS_Begin* and *CS_End*, and that satisfies the following rules:

1. *CS_Begin* and *CS_End* must be in the same function.
2. For each program execution, *CS_Begin* is always executed before *CS_End*.
3. Every execution path from a *CS_Begin* must reach only the corresponding *CS_End*.
4. Every execution path which connects *CS_Begin* and a *CS_End* must not encounter other *CS_Begin* instructions.
5. A CS cannot contain try/catch blocks
6. We consider function calls from within a CS as atomic, *i.e.*, we do not consider the called function as a part of the CS.
7. The loops contained by a CS must be bounded to a known constant.

Points (2) and (3) can be implemented by using a forward analysis Møller and Schwartzbach, 2012 of all possible branches from *CS_Begin* to *CS_End*, and considering all function calls as atomic operations. We also desire that a CS contains only unwinding loops to minimize the time in which a CS is plain. The other points are simply static patterns. The above rules are implemented by static analysis at compilation time. If a CS does not satisfy one of those requirements, the compilation process is interrupted. Therefore, we assume having only valid CSs at runtime.

In order to maintain the application stable, and to reduce the attacker surface, we desire that at most one CS remains decrypted (plain) during each thread execution. This is achieved by introducing a global variable, called *plain_cs*, within the trusted zone (as illustrated in Figure 3.1-c). The variable *plain_cs* indicates which CS is currently decrypted. Also, as we will illustrate later, the value of *plain_cs* is updated by `encrypt()` and `decrypt()` functions. For sake of simplicity, we describe the following techniques by considering only single-thread programs. While we extend our approaches to multi-threading programs at the end of this section.

Overcoming Denial of Service Issues Even if a trusted function is protected from being tampered with, usually trusted computing components do not provide availability guarantees, in the sense that the code in the trusted zone must be invoked externally. We overcome this limitation by employing *packing* Ugarte-Pedrero et al., 2016, a technique which is often used by malware to hide its functionality, combined with a heartbeat Ghosh, Hiser, and Davidson, 2010. Our intuition is to force the untrusted zone to call trusted functions in order to execute application logic. This configuration is depicted in Figure 3.1-a. In the beginning, CSs are encrypted (red shape). Therefore an attacker cannot directly change CSs' content, and the code cannot be executed unless unpacked. Each CS is surrounded by calls to two functions, which are called `decrypt()` and `encrypt()`. In our design, `decrypt()` and `encrypt()` functions has the role of *checkers*. Those functions take a CS identification (*e.g.*, CS address) as an input, then they apply cryptographic operations to the CS by using a `private key`. The `private key` is stored inside the trusted module (see Figure 3.1-c). The first call (green shape) points to the `decrypt()` function which performs three operations: (i) it decrypts the CS, (ii) it sets *plain_cs* to CS, and (iii) it performs a hash of the code to check the CS integrity. Once this checker is executed, the CS contains plain assembly code that can be processed. As a result, the untrusted zone *must* call the checker in order to execute the CS's code. After the CS, a second call (green shape) points to the `encrypt()` function which performs three operations: (i) it encrypts the CS, (ii) it sets *plain_cs* to *NULL*, and (iii) it performs a hash of the code to check the CS integrity. Note that `decrypt()` and `encrypt()` are considered as atomic. These functions are used as primitive to build more sophisticated mechanisms later. We illustrate the runtime packing algorithm in Figure 3.2. In the beginning, the CS is encrypted (*i.e.*, $E[CS]$) while the `decrypt()` function is executed (Figure 3.2-1). After the decryption phase, the CS is plain (white color) and it is normally executed (Figure 3.2-2). Finally, the `encrypt()` function is executed and the CS gets encrypted again (Figure 3.2-3).

Together with the packing mechanism already explained, we employ a parallel heartbeat as a response, which is depicted in Figure 3.1-c. The heartbeat is implemented by calling a `response()` function which resides within the trusted zone. The response's duty is to select a random CS and validate its hash value along with its respective decrypt and encrypt function calls, the outcome of this check is an encrypted packet shipped to a server that validates the application status. The heartbeat does not prevent software tampering, it is a *responsive* strategy to alert a central system about an attack. To implement a heartbeat, it is possible to adopt different strategies, *e.g.*, we can set a dedicated thread which is risen according to a time series, or else we can merge the heartbeat with a communication channel between the client and the server (as we opted in our proof-of-concept application).

Function Calls and Recursions Since we allow a CS to host function calls, a CS might remain plain after a call. This potentially increases the attacker surface. To mitigate this issue, we desire that a CS is encrypted once the control leaves the CS itself, and decrypted again right after. This is achieved by introducing two new functions, namely `enc_prev(f)` and `dec_prev(f)`, which are handled by the trusted module, as described in Figure 3.1-b. At compilation time, we instrument all functions that are directly called from within a CS by adding a function call toward `enc_prev(f)` in their

preamble, and toward `dec_prev(f)` for each of its exit point (*i.e.*, return operation). Both `enc_prev(f)` and `dec_prev(f)` functions require a parameter `f`, this parameter identifies which is the function that calls `enc_prev(f)` and `dec_prev(f)`. Since several CSs can call the same function `f`, we introduce a stack for each function `f` to handle these cases, as depicted in Figure 3.1-c. These stacks are global variable inside the trusted module, we identify the stack for the function `f` as follows:

$$stack\_cs[f] = \text{stack<CS>}().$$

The `enc_prev(f)`, `dec_prev(f)` functions and the `stack_cs[f]` interact through each other in the following way. Once `enc_prev(f)` is called, it identifies whether the control comes from a CS by checking the global variable *plain_cs*. If it is the case, the function performs two operations: (i) it pushes *plain_cs* in `stack[f]`, and (ii) it calls `encrypt(plain_cs)`. Therefore, after calling `enc_prev(f)` the system reaches this status: (i) the outer CS is encrypted (and thus protected), (ii) *plain_cs* is set to *NULL*, and (iii) the thread is ready to handle a new CS. Similarly, once the control leaves the function `f`, the epilogue calls `dec_prev(f)`. This function performs two operations: (i) it pops the last CS from `stack[f]` into *plain_cs*, and (ii) it restores the previous CS status by calling `decrypt(plain_cs)`. As a result, the control can safe pass to the outer CS. In the opposite scenario, once the control enters in the function `f` and the *plain_cs* is set to *NULL*, it means that the function `f` was not called by a CS; and therefore, `enc_prev(f)` and `dec_prev(f)` do nothing. Stacks allow us to handle recursions, if the function `f` is repetitively called, we trace all previous CSs.

Exceptions within Critical Section We can handle exceptions from within a CS by introducing a new function, namely `enc_all()`, which is handled by the trusted module, as described in Figure 3.1-c. This function is an alias for `encrypt(plain_cs)`. That is, we wrap any CS with a try/catch block at compilation time, as described in Figure 3.1-a. The exception block is made such that (i) to catch all exceptions, (ii) to run `enc_all()`, (iii) to throw the exception again. In this way, we restore the anti-tampering mechanism as soon as an exception appears. Thus, after an exception, we encrypt all the plain CSs and the application can continue normally. Note that the *response* function has to be extended in order to protect the *catch* block, or else, an attacker might raise an exception in order force a CS to be plain[1].

[1]We do not deal with runtime attacks to exception handlers, such as SEH, since they do not belong to anti-tampering problems.

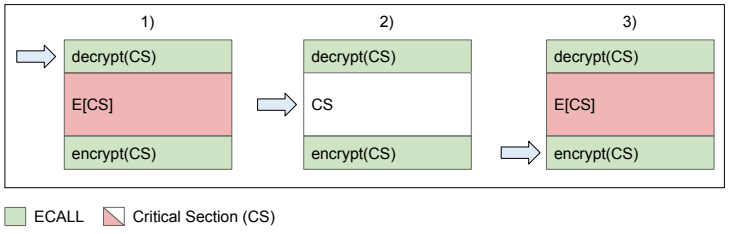


FIGURE 3.2: Packing mechanism of our schema.

Multi-threading programs We can extend the previous techniques in order to handle parallel computation, this is possible because some trusted computing technologies allow multi-threading programming, like SGX (see Section **??** TODO reference ◁). To achieve multi-threading, we maintain a *plain_cs* and a `stack_cs[f]` for each thread. Moreover, we introduce a counter for each CS. These global variables represent the number of threads which are executing a CS in a specific moment. In the beginning, the CSs' counters are set to *zero*. Then, they are increased and decreased by `decrypt()` and `encrypt()` functions respectively.

Ensuring a Secure Booting Phase Our approach requires that the program has a secure booting phase, which means having the following assumptions for the *encrypt*, *decrypt* and *response*: the key for crypto algorithms must be loaded in a secure way together with a table which describes where the CSs are located (*i.e.,* their address and length) with their hash values. We refer to this table as *block table*. We assume a trusted loading of this information by adopting SGX sealing and attestation mechanisms. Those mechanisms ensure to store information on a disk or to establish a secure channel with other enclaves within the same machine (*i.e.,* local) or with a remote one (*i.e.,* remote) in a trusted way. Details on sealing and attestation are discussed in Section **??** TODO add background ◁.

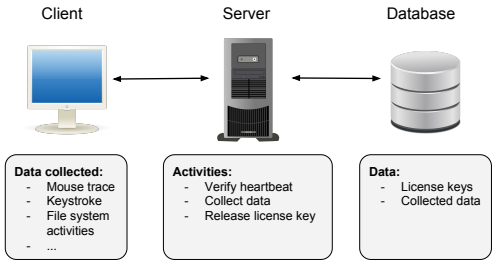
3.3 Implementation

In this section, we describe a proof-of-concept implementation of our anti-tampering technique, whose architecture is depicted in Figure 3.3a. The application is composed by a central server that handles a set of clients which are spread over a network. Each client is a monitoring application that traces user's activities (*i.e.,* keystrokes and mouse traces) and sends the data to the central server. As a trusted module, we opted for the Intel Software Guard eXtension (SGX) Rozas, 2013, however, it is possible to use other solutions that involves the kernel (*e.g.,* TPM ISO, 2015). We deployed the architecture in a Windows environment. Through this application we describe the specific technical solutions we adopted for the client, and how we implemented installation phase, boot phase, and response.

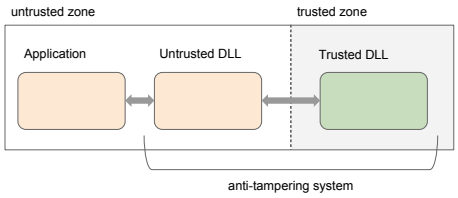
3.3.1 Client

We describe the internal structure of the client in order to clarify some practical implementation strategies. We developed this application in C++ and we deployed it on Windows machines. For sake of simplicity, we did not implement Address Space Layout Randomization (ASLR) Snow et al., 2013, however, it is possible to deduct the right address offset by employing a Drawbridge system Porter et al., 2011.

Software Architecture The client is formed by three modules: the main program, and two dynamic linked libraries (DLL) namely untrusted DLL and trusted DLL. This architecture is depicted in Figure 3.3b, the application communicates with the untrusted DLL to call the functions described in Section 3.2. The untrusted DLL works together with the trusted DLL (*i.e.,* the enclave) to handle the whole anti-tampering technique.



(A) The architecture of proof-of-concept program. The client is a monitoring agent which collects user's activities, the server handles clients, and the database stores collect data and license keys.



(B) The software organization of the client.

FIGURE 3.3: Careful-Packing architecture.

We choose this architecture to simplify the integration of our anti-tampering system. In this way, the developer can focus on the main program and integrate the anti-tampering system later. Each component of the architecture is described as follows:

- **Application:** this is the client that we aim to enforce. Natively, it contains all the functionalities for collecting information from the underline OS and ship them to the server.
- **Untrusted DLL:** this contains the untrusted functions for interacting with the enclave. Also, it keeps track of the status of the enclave (*i.e.,* enclave pointer) and exposes routines procedures.
- **Trusted DLL (enclave):** this is the enclave. It contains the trusted functions described in Section 3.2 (*e.g.,* checkers, response) along with some extra routine functions (*i.e.,* installation and boot).

Critical Section Definition Since this client is a monitoring agent, we identify as CSs those functions used to collect the information issued by the OS: `PAKeyStroked`, which collects keystroked, and its twin `PAMouseMovement`, which collects mouse events. These functions are callback risen by the OS along with the relative event information. For sake of simplicity, we trust in argument passed by the OS. The main duties of these functions are: (i) collecting the data, (ii) crafting a packet with the data collected, (iii) signing the packet, and finally (iv) shipping it to the server. Since in our implementation we required only integrity, we implemented a digital fingerprint.

Packaging Algorithm The packaging algorithm adopted is an AES-GCM encryption schema Zhou, Michalik, and Hinsenkamp, 2007 between the assembly code and the license key. SGX natively provides an implementation of this algorithm Intel, 2018.

Heartbeat The heartbeat is implemented as a digital fingerprint which is used on all packets exchanged between client and server, our strategy allows the server to validate

client status by testing the digital fingerprint itself and also for mitigating *denial-of-service*.

The digital fingerprint is created by feeding a *sha256* function with the concatenation of the message to sign, the license key, and a special byte called *check byte*, which can have two values (*safe*, or *corrupted*) according to the status of the program. The digital fingerprint algorithm randomly selects a CS and sets the *check byte* accordingly. Then, the server verifies the digital fingerprint by guessing the *check byte* value used at the client side. That is, the server crafts the two digital fingerprints by using the two possible values of the *check byte*. If one of the generated digital fingerprints matches the original one, the server can infer the status of the client (*i.e.,* it is healthy or tampered). Otherwise, that means the message was corrupted, or it was originated by the wrong machine. This simple heartbeat implementation allows the sever to identify *denial-of-service* at client side. If an attacker switches off the monitor agent, the communication will be immediately affected.

In our implementation, we adopted semaphores in order to avoid conflicts with checking functions, and we added timestamps to exchanged packets for avoiding replay attacks.

Block Table Packaging and heartbeat functions require the coordinates of all CSs (start address, size, and hash-value) along with the license key for running. This information can be handled mainly in two ways: a) the client loads the entire table in the enclave memory; b) the client loads the entire table in the untrusted zone and adds a digital fingerprint to guarantee entries integrity.

Both approaches have pro and cons. The first approach guarantees also confidentiality at the table. Moreover, since the table is stored in the enclave, all trusted functions can retrieve the entries faster. On the other hand, if the table is too large the enclave might be overloaded. The second approach is lighter in term of memory consumption because it keeps all rows within the untrusted zone. However, in this case, the algorithm results slowly because it has to inspect the untrusted zone to retrieve the entries and to verify their integrity. In our implementation, we opted for the second option where each entry is protected by using the license key and stored within the untrusted memory region.

3.3.2 Installation Phase

We achieve a secure installation by using an authentication protocol based on SGX remote attestation, the entire protocol is depicted in Figure 3.4. In this scenario, the server has a database which contains all license keys, all the CSs, and the block table of each client. On the other side, each client is only formed by the program to protect, with the encrypted CSs already replaced, and its enclave, which contains *checkers*, *responses*, and *installation* routines.

Licensing System The goal of the installation phase is to deliver the correct *license key* to the respective client in a secure fashion. To achieve this, each client instance uses a different *private key* to decrypt its CSs. The *private key* is directly derived from the *license key*. That is, each client instance requires its own *license key* to work properly. In the following paragraph, we exploit this fact to authenticate a client to the server.

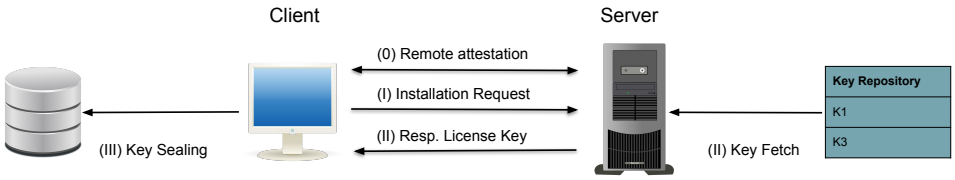


FIGURE 3.4: Secure installation protocol between client and server.

Installation Procedure In this phase, the aim of the client is to perform a remote attestation with the server, this latter then verifies client's identity and releases the relative license key and the block table, which allows the client to run properly. In order to establish a remote attestation, the enclave is signed by a certification authority and the server is awarded for the certificates shared with clients.

In the beginning, the client and the server follow the remote attestation mechanism described by Intel in Intel, 2016b (Figure 3.4-0). After this, both entities can rely on a secure end-to-end channel. Also, this allows the server to obtain the client measurement, which is a cryptographic hash that probes the client enclave version and the client hardware. This information is used by the server to bind client identity and license key. Once the channel is created, the client sends an installation request to the server (Figure 3.4-I), the request is an encrypted CS which is randomly taken from the client itself. The server receives the installation requests, and it verifies which license key belongs to the CSs. Then, the server binds the client measurements with the license key, and it releases this latter to the client along with the block table (Figure 3.4-II). When the enclave receives the license key and the block table, it will seal all in the client machine. At this point, only the client can read these information through SGX sealing process (Figure 3.4-III). Even if a malicious client forces a signed enclave to send an installation request with a CS to the server, the retrieved license key will be sealed on the machine, and only the signed enclave can read it.

At this point, the installation phase is concluded: the server has the information about the location of the client and the key license and block table are securely stored on the client machine.

3.4 Evaluation

We evaluated our technique from different perspectives. At first, we quantify the overhead in terms of Lines of Code (LoC), execution time (microbenchmark), and memory required by our enclave. Then, we discuss the impact of several security threats to the infrastructure proposed. Finally, we perform an empirical evaluation of the likelihood to accomplish a just-in-time attack.

3.4.1 Lines-of-Code Overhead

A useful metric to measure the impact of our technique is the amount of code added to the original program, this is illustrated in Table 3.1. Looking at the table, it is possible to notice that the majority part of the code is contained in the main program ($96,5\%$). The Untrusted and Trusted DLL, which implement our anti-tampering technique, require

respectively $2,0\%$ and $1,5\%$ of the code. Within the main program, each CS contains only two lines of code, one for calling `decrypt()` function and another for calling `encrypt()` function. We remark that through our technique it is possible to protect an indefinite number of CSs by using always the same amount of code in the enclave.

TABLE 3.1: Number of LoC for each module

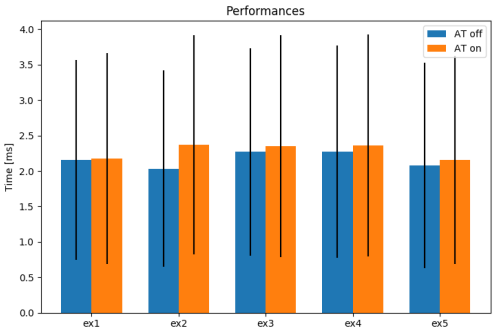
Module	LoC	Perc.
Main program	12175	96,5%
Untrusted DLL	248	2,0%
Trusted DLL	186	1,5%

3.4.2 Microbenchmark Measurements

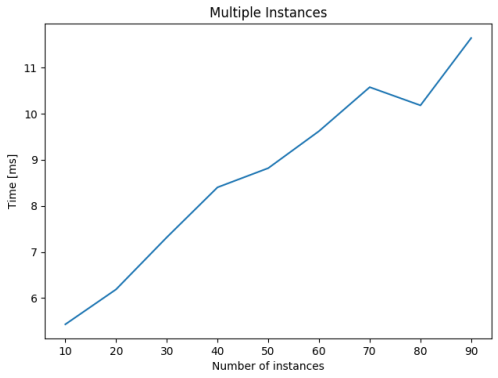
In these experiments, we perform a set of microbenchmark to measure the overhead in time introduced by our technique. As a use case, we measure the execution time of the CSs in our proof-of-concept monitoring agent (see Section 3.3). At first, we briefly introduce the experiment setup. Then, we measure the execution time of the CSs with and without our anti-tampering technique. Finally, we measure the execution time of the CSs in case of multiple instances. All execution times are measured in milliseconds.

User-Simulator Bot For performing the following tests, we developed a user-simulator bot which mimics the standard user activity by stroking keys and moving the cursor. The bot is a Python script which is based on the *PyWin32* library. Since we aim at measuring the monitoring agent's performances, we designed a very basic user-simulator's behavior. The user-simulator generates keystrokes on a text program (*i.e.*, notepad) and randomly moves the mouse around the screen. Keystroke frequency is around 100 words per minute, while mouse speed is around 500 pixel per second. This bot allows us to easily repeat the experiments.

Single Instance Microbenchmark We measure the impact of our anti-tampering technique to the performances of the CSs in our proof-of-concept monitoring agent. In this experiment, we performed 5 exercises, each of one is composed by two runs, namely with and without the anti-tampering technique. For each run, we traced the CS's execution time. The outcome of the experiment is plotted in Figure 3.5a. In the plot, each bar represents the average elapsed time for a run and each pair of bars represents a single exercise. More precisely, orange bars mean runs with the anti-tampering technique active, while blue bars mean runs without. Looking at the graph, we can see that functions require on average between 2ms and 2.4ms for being executed. It is also evident that with the anti-tampering technique the performances are slightly degraded. On average, the delta time is 0.12ms, with a peak of 0.34ms for the second instance. Also, time overhead is less than 6% on average, with a peak of 16.61% in the second instance. This peak depends on the system status at execution time. According to our experiments, we conclude that the performances degradation is negligible after the introduction of our anti-tampering system.



(A) Average response time with and without anti-tampering technique



(B) Average response time with multiple instances

FIGURE 3.5: Careful-Packing evaluation.

Multiple Instances We empirically investigate whether our approach can be deployed over multiple processes at the same time. We performed this test by running a different number of instances of our proof-of-concept monitoring agent and then measuring the average execution time of their CSs.

The outcome of the experiment is depicted in Figure 3.5b. The plot shows the average execution time of the CS on the y-axis (expressed in milliseconds), while the number of instances is indicated on the x-axis (from 10 to 90). Looking at the plot, it is possible to notice that the average execution time grows linearly *w.r.t.* the number of instances. The average execution time is around 5ms in case of 10 parallel instances, while it degrades to 11ms in case of 90. This means that the performances get only halved after decupling the number of instances; therefore, our technique results scalable.

3.4.3 Enclave Size Considerations

In our proof-of-concept monitoring agent, we used an enclave that occupies at around $300KB$. As we stated, in our approach the enclave size does not depend by the size of the software to protect. This allows us to estimate the number of processes we can protect at the same time. In a common machine SGX featured (*e.g.*, Dell XPS 13 9370), we can dedicate at most $128MB$ for enclaves. If we consider the enclave used in our proof-of-concept, we can roughly estimate at around 400 enclaves contemporaneously loaded that will protect the same number of processes.

3.4.4 Threat Mitigation

We explain how our approach mitigates threats according to the attacker model described in Section 3.1.

Protection of checkers and responses. In our approach, the functions for anti-tampering mechanisms (*e.g.*, *checker* and *response*) reside in a trusted module. Since we assume

trusted computing guarantees hardware isolation, those functions are protected by design.

Protection against disarm. An attacker can always disarm a function by removing its invocation. Moreover, SGX is prone to *denial-of-service attacks* due to its nature (see Section **??** TODO reference ◁). We protect trusted invocations by adopting the packaging tactic discussed in Section 3.2. The software contains parts of code which are encrypted and they need checkers action for being executed properly.

Just-in-time Patch & Repair Mitigation After a *decryption* function is run, the CS is plain and ready to be executed. At this moment, there is a chance for the attacker to replace the code within a CS and restore it before the next *encryption*. This is called just-in-time patch & repair attack.

Assuming the attacker cannot directly tamper with the task scheduler (as described in Section 3.1), it is still possible to perform attacks from the user-space Gullasch, Bangerter, and Krenn, 2011. However, those attacks are not strong enough to bypass our defense for mainly three reasons: (i) they are tailored for specific contexts (*e.g.*, single core, OS version), (ii) they aim at slowing down a process and not to achieve a perfect synchronization between adversary and victim, (iii) modern OSs mount task schedulers which are designed to resist (or at least mitigate) such attacks Kernel.org, 2018. To achieve an *on-line* tampering, as introduced in Section 3.1, an attacker must replace a CS code such that `encrypt()` and `decrypt()` functions do not notice the replacement. This means that a single error will be detected by the server. None of the attacks from user-space can achieve such precision. An alternative approach is to adopt virtualization to debug a process step-by-step at runtime, but this contradicts the assumptions of our threat model (*i.e.*, the original infrastructure is not altered). We, however, try to estimate the likelihood that this attack might happen by performing an empirical experiment which will be described in Section 3.4.5.

Reverse Engineering An attacker may attempt to reverse the application code in order to extract the plain code hidden in the encrypted blocks, and then build a new executable which does not contain any checker. The new executable is therefore prone to any manipulation. This goal can be achieved by using debuggers and/or analyzers. Even though the literature contains several anti-debugging techniques and most of them can be enforced by using our anti-tampering technique, we assume that an attacker can bypass all of them. However, an attacker cannot debug the software inside the trusted zone, which is true for SGX enclaves compiled in release mode Intel, 2016a. The best an attacker can do is debugging the code within the untrusted memory region and considering the enclave as a black box. After applying these considerations, we can state an attacker can manage to dump the plain code after that *decryption* functions are called, and even make a new custom application. However, this attack is still coherent with our threat model (see Section 3.1) because the new application cannot work into the original infrastructure (*i.e.*, the heartbeat cannot work properly) and therefore it is useless. For instance, in the implementation presented in Section 3.3, the monitoring agent can work properly only if the software contains all the functions employed by our technique along with the original CSs. If this is not respected (*i.e.*, by removing

checkers) the application cannot emit a correct heartbeat, and therefore the attack is not considered accomplished.

3.4.5 Study of Just-in-Time Patch & Repair Attack

In this experiment, we investigate the likelihood of a just-in-time patch & repair attack in a real context. Here, the attacker's goal is to temporarily replace the bytecode within a CS such that the injected code is executed but the system cannot realize the attack. The setup is formed by a victim process (*i.e.*, our agent) and an attacker process. Also, we consider a trusted task scheduler, and that each process is executed on a dedicated core. Both attacker and victim are written in C++ and developed for Windows, the experiments were run on a Windows 10 machine with 16GB RAM and Intel® Core™ i7-7500 $2,70$GHz processor.

The victim process is formed by an infinite loop which continuously updates an internal variable through a CS. This latter is enforced by self-checking mechanisms. Moreover, the victim process contains a checker to validate the status of the program. If the internal status is set wrongly, that will be logged. The attacker process, instead, is a concurrent process which can edit the victim process at runtime. Attacker's goal is to replace the victim CS such that the internal variable of the victim process will contain an incongruent value. We attempted the attack for 10.000 times, but the self-checking mechanism managed to detect all attacks. Therefore, we consider that this kind of attack is not practical in case of a trusted task scheduler.

3.5 Discussion

We have shown how to implement our technique by means of a case study involving a monitor agent, however there are few aspects to note about the validity of our evaluation effort. First, although the application code is protected, an attacker can still analyze and change variable values at runtime, thus potentially harming its normal execution. Note that our approach could be extended in order to mitigate this issue by using cryptographic hashes to validate the integrity of certain critical variables. Moreover, our design and implementation requires a healthy kernel, otherwise it would be possible to mount attacks such as the just-in-time patch and repair attack we discussed previously (by manipulating the scheduler). We believe that even with a compromised kernel mounting those attacks would require significant effort, but we leave a more thorough investigation for future work. Other aspects, such as an evaluation of applying our technique a different granularities (such as basic-block level), or extending protection to *PLT*, *GOT*, and *exception table* are also left for future work.

Chapter 4

Scalable Runtime Remote Attestation for Complex Systems

In this chapter, we propose ScaRR, the first runtime RA schema for complex systems. In particular, we focus on environments such as Amazon Web Services (*Amazon Web Services (AWS)* 2006) or Microsoft Azure (*Microsoft Azure* 2010). Since we target such systems, we require support for features such as multi-threading. Thus, ScaRR provides the following achievements with respect to the current solutions supporting runtime RA: (i) it makes the runtime RA feasible for any software, (ii) it enables the *Verifier* to verify intermediate states of the *Prover* without interrupting its execution, (iii) it supports a more fine-grained analysis of the execution path where the attack has been performed. We achieve these goals thanks to a novel model for representing the execution paths of a program, which is based on the fragmentation of the whole path into meaningful sub-paths. As a consequence, the *Prover* can send a series of intermediate partial reports, which are immediately validated by the *Verifier* thanks to the lightweight verification procedures performed.

ScaRR is designed to defend a *Prover*, equipped with a trusted anchor and with a set of the standard solutions (*e.g.*, W$\oplus$X/DEP Pinzari, 2003, Address Space Layout Randomization - ASLR Kil et al., 2006, and Stack Canaries Baratloo, Singh, and Tsai, 2000), from attacks performed in the user-space and aimed at modifying the *Prover* runtime behaviour. The current implementation of ScaRR requires the program source code to be properly instrumented through a compiler based on LLVM Lattner and Adve, 2004. However, it is possible to use lifting techniques *McSema* 2014, as well. Once deployed, ScaRR allows to verify on average $2M$ control-flow events per second, which is significantly more than the few hundred per second Dessouky et al., 2018 or the thousands per second Abera et al., 2019 verifiable through the existing solutions.

Contribution. The contributions of this work are the following ones:

- We designed a new model for representing the execution path for applications of any complexity.
- We designed and developed ScaRR, the first schema that supports runtime RA for complex systems.
- We evaluated the ScaRR performances in terms of: (i) attestation speed (*i.e.,* the time required by the *Prover* to generate a partial report), (ii) verification speed (*i.e.,* the time required by the *Verifier* to evaluate a partial report), (iii) overall generated network traffic (*i.e.,* the network traffic generated during the communication between *Prover* and *Verifier*).

4.1 Threat Model and Requirements

In this section, we describe the features of the *Attacker* and the *Prover* involved in our threat model. Our assumptions are in line with other RA schemes Costan and Devadas, 2016; Winter, 2008; Abera et al., 2016; Abera et al., 2019; Dessouky et al., 2018.

Attacker. We assume to have an attacker that aims to control a remote service, such as a Web Server or a Database Management System (DBMS), and that has already bypassed the default protections, such as Control Flow Integrity (CFI). To achieve his aim, the attacker can adopt different techniques, among which: Return-Oriented Programming (ROP)/ Jump-Oriented Programming (JOP) attacks Carlini and Wagner, 2014; Bletsch et al., 2011, function hooks Rudd et al., 2017, injection of a malware into the victim process, installation of a data-only malware in user-space Vogl et al., 2014, or manipulation of other user-space processes, such as security monitors. In our threat model, we do not consider physical attacks (our complex systems are supposed to be virtual machines), pure data-oriented attacks (*e.g.,* attacks that do not alter the original program CFG), self-modifying code, and dynamic loading of code at runtime (*e.g.,* just-in-time compilers Suganuma et al., 2000). We refer to Section 4.5.4 for a comprehensive attacker analysis.

Prover. The *Prover* is assumed to be equipped with: (i) a trusted anchor that guarantees a static RA, (ii) standard defence mitigation techniques, such as W⊕X/DEP, ASLR. In our implementation, we use the kernel as a trusted anchor, which is a reasonable assumption if the machines have trusted modules such as a TPM Tomlinson, 2017. However, we can also use a dedicated hardware, as discussed in Section 4.6. The *Prover* maintains sensitive information (*i.e.,* shared keys and cryptographic functions) in the trusted anchor and uses it to generate fresh reports, that cannot be tampered by the attacker.

4.2 ScaRR Control-Flow Model

ScaRR is the first schema that allows to apply runtime RA on complex systems. To achieve this goal, it relies on a new model for representing the CFG/execution path of a program. In this section, we illustrate first the main components of our control-flow model (Section 4.2.1) and, then, the challenges we faced during its design (Section 4.2.2).

4.2.1 Basic Concepts

The ScaRR control-flow model handles BBLs at assembly level and involves two components: *checkpoints* and *List of Actions (LoA)*.

A *checkpoint* is a special BBL used as a delimiter for identifying the start or the end of a sub-path within the CGF/execution path of a program. A *checkpoint* can be: *thread beginning/end*, if it identifies the beginning/end of a thread; *exit-point*, if it represents

an exit-point from an application module (*e.g.,* a system call or a library function invocation); *virtual-checkpoint*, if it is used for managing special cases such as *loops* and *recursions*.

A *LoA* is the series of significant edges that a process traverses to move from a *checkpoint* to the next one. Each edge is represented through its source and destination BBL and, comprehensively, a *LoA* is defined through the following notation:

$$[(\text{BBL}_{s1}, \text{BBL}_{d1}), \ldots, (\text{BBL}_{sn}, \text{BBL}_{dn})].$$

Among all the edges involved in the complete representation of a CFG, we consider only a subset of them. In particular, we look only at those edges that identify a unique execution path: procedure call, procedure return and branch (*i.e.,* conditional and indirect jumps).

To better illustrate the ScaRR control-flow model, we now recall the example introduced in Section **??**. Among the six nodes belonging to the CFG of the example, only the following four ones are *checkpoints*: N_1, since it is a *thread beginning*; N_3 and N_4, because they are *exit-points*, and N_6, since it is a *thread end*. In addition, the *LoAs* associated to the example are the following ones:

$$\begin{aligned} N_1 - N_3 &\Rightarrow [(N_2, N_3)] \\ N_1 - N_4 &\Rightarrow [(N_2, N_4)] \\ N_3 - N_6 &\Rightarrow [] \\ N_4 - N_6 &\Rightarrow []. \end{aligned}$$

On the left we indicate a pair of *checkpoints* (*e.g.,* $N_1 - N_3$), while on the right the associated *LoA* (empty *LoAs* are considered valid).

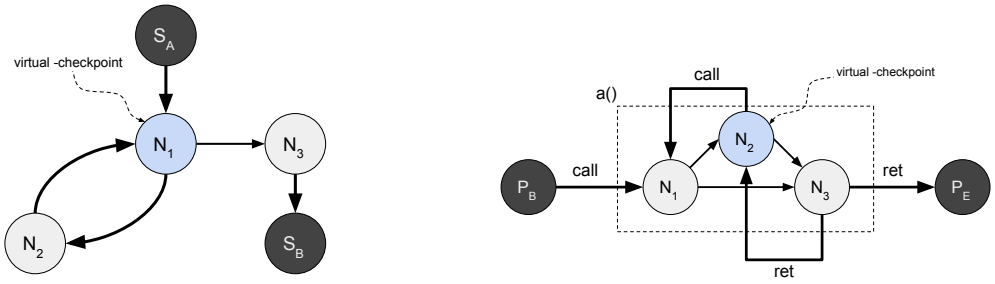
4.2.2 Challenges

Loops, *recursions*, *signals*, and *exceptions* involved in the execution of a program introduce new challenges in the representation of a CFG since they can generate uncountable executions paths. For example, *loops* and *recursions* can generate an indefinite number of possible combinations of *LoA*, while *signals*, as well as *exceptions*, can introduce an unpredictable execution path at any time.

Loops. In Figure 4.1a, we illustrate the approach used to handle *loops*. Since it is not always possible to count the number of iterations of a loop, we consider the conditional node of the *loop* (N_1) as a *virtual-checkpoint*. Thus, the *LoAs* associated to the example shown in Figure 4.1a are as follows:

$$\begin{aligned} S_A - N_1 &\Rightarrow [] \\ N_1 - N_1 &\Rightarrow [(N_1, N_2)] \\ N_1 - S_B &\Rightarrow [(N_1, N_3)]. \end{aligned}$$

Recursions. In Figure 4.1b, we illustrate our approach to handle *recursions*, *i.e.,* a function that invokes itself. Intuitively, the *LoAs* connecting P_B and P_E should contain



(A) Loop example in the ScaRR control-flow model.

(B) Recursion example in the ScaRR control-flow model.

FIGURE 4.1: ScaRR model challenges.

all the possible invocations made by `a()` towards itself, but the number of invocations is indefinite. Thus, we consider the node performing the recursion as a *virtual-checkpoint* and model only the path that could be chosen, without referring to the number of times it is really undertaken. The resulting *LoAs* for the example in Figuree 4.1b are the following ones:

$$
\begin{aligned}
P_B - N_2 &\Rightarrow [(P_B, N_1), (N_1, N_2)] \\
N_2 - N_2 &\Rightarrow [(N_2, N_1), (N_1, N_2)] \\
N_2 - N_2 &\Rightarrow [(N_2, N_1), (N_1, N_3), (N_3, N_2)] \\
N_2 - P_E &\Rightarrow [(N_2, N_1), (N_1, N_3), (N_3, P_E)] \\
P_B - P_E &\Rightarrow [(P_B, N_1), (N_1, N_3), (N_3, P_E)].
\end{aligned}
$$

Finally, the *virtual-checkpoint* can be used as a general approach to solve every situation in which an indirect jump targets a node already present in the *LoA*.

Signals. When a thread receives a *signal*, its execution is stopped and, after a context-switch, it is diverted to a dedicated handler (*e.g.,* a function). This scenario makes the control-flow unpredictable, since an interruption can occur at any point during the execution. To manage this case, ScaRR models the signal handler as a separate thread (adding *beginning/end thread checkpoints*) and computes the relative *LoAs*. If no handler is available for the *signal* that interrupted the program, the entire process ends immediately, producing a wrong *LoA*.

Exception Handler. Similar to *signals*, when a thread rises an *exception*, the execution path is stopped and control is transferred to a catch block. Since ScaRR has been implemented for Linux, we model the catch blocks as a separate thread (adding *beginning/end thread checkpoints*), but it is also possible to adapt ScaRR to fulfill different exception handling mechanisms (*e.g.,* in Windows). In case no catch block is suitable for the *exception* that was thrown, the process gets interrupted and the generated *LoA* is wrong.

4.3 System Design

To apply runtime RA on a complex system, there are two fundamental requirements: (i) handling the representation of a complex CFG or execution path, (ii) having a fast verification process. Previous works have tried to achieve the first requirement through different approaches. A first solution Abera et al., 2016; Zeitouni et al., 2017; Dessouky et al., 2017 is based on the association of all the valid execution paths of the *Prover* with a single hash value. Intuitively, this is not a scalable approach because it does not allow to handle complex CFG/execution paths. On the contrary, a second approach Dessouky et al., 2018 relies on the transmission of all the control-flow events to the *Verifier*, which then applies a symbolic execution to validate their correctness. While addressing the first requirement, this solution suffers from a slow verification phase, which leads toward a failure in satisfying the second requirement.

Thanks to its novel control-flow model, ScaRR enables runtime RA for complex systems, since its design specifically considers the above-mentioned requirements with the purpose of addressing both of them. In this section, we provide an overview of the ScaRR schema (Section 4.3.1) together with the details of its workflow (Section 4.3.2), explicitly motivating how we address both the requirements needed to apply runtime RA on complex systems.

4.3.1 Overview

Even if the ScaRR control-flow model is composed of *checkpoints* and *LoAs*, the ScaRR schema relies on a different type of elements, which are the *measurements*. Those are a combination of *checkpoints* and *LoAs* and contain the necessary information to perform runtime RA. Figure 4.2 shows an overview of ScaRR, which encompasses the following four components: a *Measurements Generator*, for identifying all the program valid *measurements*; a *Measurements DB*, for saving all the program valid *measurements*; a *Prover*, which is the machine running the monitored program; a *Verifier*, which is the machine performing the program runtime verification.

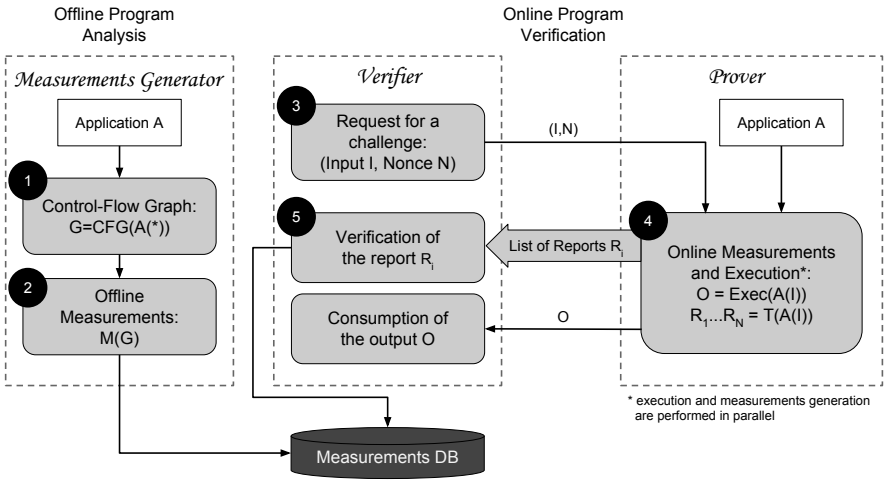


FIGURE 4.2: ScaRR system overview.

As a whole, the workflow of ScaRR involves two separate phases: an *Offline Program Analysis* and an *Online Program Verification*. During the first phase, the *Measurements Generator* calculates the CFG of the monitored *Application A* (Step 1 in Figure 4.2) and, after generating all the *Application A* valid *measurements*, it saves them in the *Measurements DB* (Step 2 in Figure 4.2). During the second phase, the *Verifier* sends a challenge to the *Prover* (Step 3 in Figure 4.2). Thus, the *Prover* starts executing the *Application A* and sending partial reports to the *Verifier* (Step 4 in Figure 4.2). The *Verifier* validates the freshness and correctness of the partial reports by comparing the received new *measurements* with the previous ones stored in the *Measurements DB*. Finally, as soon as the *Prover* finishes the processing of the input received from the *Verifier*, it sends back the associated output.

4.3.2 Details

As shown in Figure 4.2, the workflow of ScaRR goes through five different steps. Here, we provide details for each of those.

(1) Application CFG. The *Measurements Generator* executes the *Application A()*, or a subset of it (*e.g.,* a function), and extracts the associated CFG G.

(2) Offline Measurements. After generating the CFG, the *Measurements Generator* computes all the program *offline measurements* during the *Offline Program Analysis*. Each *offline measurement* is represented as a key-value pair as follows:

$$(\text{cp}_A, \text{cp}_B, H(\text{LoA})) \Rightarrow [(\text{BBL}_{s1}, \text{BBL}_{d1}), \ldots, (\text{BBL}_{sn}, \text{BBL}_{dn})]$$

The key refers to a triplet, which contains two *checkpoints* (*i.e.,* cp_A and cp_B) and the hash of the *LoA* (*i.e., H(LoA)*) associated to the significant BBLs that are traversed when moving from the source *checkpoint* to the destination one. The value refers only to a subset of the BBLs pairs used to generate the hash of the *LoAs* and, in particular, only to procedure calls and procedure returns. Those are the control-flow events required to mount the shadow stack during the verification phase.

(3) Request for a Challenge. The *Verifier* starts a challenge with the *Prover* by sending it an input and a nonce, which prevents replay attacks.

(4) Online Measurements. While the *Application A* processes the input received from the *Verifier*, the *Prover* starts generating the *online measurements* which keep trace of the *Application A* executed paths. Each *online measurement* is represented through the same notation used for the keys in the *offline measurements*, *i.e.,* the triplet $(\text{cp}_A, \text{cp}_B, H(\text{LoA}))$.

When the number of *online measurements* reaches a preconfigured limit, the *Prover* encloses all of them in a partial report and sends it to the *Verifier*. The partial report is defined as follows:

$$P_i = (R, F_K(R||N||i))$$
$$R = (T, M).$$

In the current notation, P_i is the i-th partial report, R the payload and $F_K(R||N||i)$ the digital fingerprint (*e.g.,* a message authentication code Bellare, Kilian, and Rogaway, 2000). This is generated by using: (i) the secret key K, shared between *Prover* and *Verifier*, (ii) the nonce N, sent at the beginning of the protocol, and (iii) the index i,

which is a counter of the number of partial reports. Finally, the payload R contains the *online measurements* M along with the associated thread T.

The novel communication paradigm between *Prover* and *Verifier*, based on the transmission and consequent verification of several partial reports, satisfies the first requirement for applying runtime RA on complex systems (*i.e.,* handling the representation of a complex CFG/execution path). This is achieved thanks to the ScaRR control-flow model, which allows to fragment the whole CFG/execution path into sub-paths. Consequently, the *Prover* can send intermediate reports even before the *Application A* finishes to process the received input. In addition, the fragmentation of the whole execution path into sub-paths allows to have a more fine-grained analysis of the program runtime behaviour since it is possible to identify the specific edge on which the attack has been performed.

(5) Report Verification. In runtime RA, the *Verifier* has two different purposes: verifying whether the running application is still the original one and whether the execution paths traversed by it are the expected ones. The first purpose, which we assume to be already implemented in the system Costan and Devadas, 2016; Winter, 2008, can be achieved through a static RA applied on the *Prover* software stack. On the contrary, the second purpose is the main focus in our design of the ScaRR schema.

As soon as the *Verifier* receives a partial report P_i, it first performs a formal integrity check by considering its fingerprint $F_K(R||N||i)$. Then, it considers the *online measurements* sent within the report and performs the following checks: (C1) whether the *online measurements* are the expected ones (*i.e.,* it compares the received *online measurements* with the offline ones stored in the *Measurements DB*), (C2) whether the destination *checkpoint* of each *measurement* is equal to the source *checkpoint* of the following one, and (C3) whether the *LoAs* are coherent with the stack status by mounting a shadow stack. If one of the previous checks fails, the *Verifier* notifies an anomaly and it will reject the output generated by the *Prover*.

All the above-mentioned checks performed by the *Verifier* are lightweight procedures (*i.e.,* a lookup in a hash map data structure and a shadow stack update). The speed of the second verification mechanism depends on the number of procedure calls and procedure returns found for each *measurement*. Thus, also the second requirement for applying runtime RA on complex systems is satisfied (*i.e.,* keeping a fast verification phase). Once again, this is a consequence of the ScaRR control-flow model since the fragmentation of the execution paths allows both *Prover* and *Verifier* to work on a small amount of data. Moreover, since the *Verifier* immediately validates a report as soon as it receives a new one, it can also detect an attack even before the *Application A* has completed the processing of the input.

4.3.3 Shadow Stack

To improve the defences provided by ScaRR, we introduce a shadow stack mechanism on the *Verifier* side. To illustrate it, we refer to the program shown in Figure 4.3, which contains only two functions: `main()` and `a()`. Each line of the program is a BBL and, in particular: the first BBL (*i.e., S*) and the last BBL (*i.e., E*) of the `main()` function are a *beginning thread* and *end thread checkpoints*, respectively; the function `a()` contains a function call to `printf()`, which is an *exit-point*. According to the ScaRR control-flow

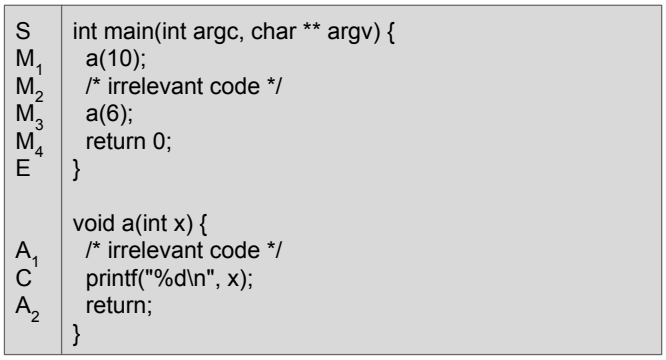


FIGURE 4.3: Illustrative example to explain the shadow stack on the ScaRR *Verifier*.

model, the *offline measurements* are the following ones:

$$(S, C, H_1) \Rightarrow [(M_1, A_1)],$$
$$(C, C, H_2) \Rightarrow [(A_2, M_2), (M_3, A_1)],$$
$$(C, E, H_3) \Rightarrow [(A_2, M_4)].$$

The significant BBLs we consider for generating the *LoAs* are: (i) the ones connecting the BBL S to the *checkpoint* C, (ii) the ones connecting two *checkpoints* C, and (iii) the ones to move from the *checkpoint* C to the last BBL E.

In this scenario, an attacker may hijack the return address of the function `a()` in order to jump to the BBL M_3. If this happens, the *Prover* produces the following *online measurements*:

$$(S, C, H_1) \rightarrow (C, C, H_2) \rightarrow (C, C, H_2) \rightarrow \dots.$$

Although generated after an attack, those measurements are still compliant with the checks $(C1)$ and $(C2)$ of the *Verifier*. Thus, to detect this attack, we introduce a new relation (*i.e.,* `ret_to`) to illustrate the link between two edges. The *Measurements Generator* computes all the `ret_to` relations during the *Offline Program Analysis* and saves them in the *Measurements DB* using the following notation:

$$(A_2, M_2) \texttt{ ret\_to } (M_1, A_1),$$
$$(A_2, M_4) \texttt{ ret\_to } (M_3, A_1).$$

Figure 4.4 shows how the *Verifier* combines all these information to build a remote shadow stack. At the beginning, the shadow stack is empty (*i.e.,* no function has been invoked yet). Then, according to the *online measurement* (S, C, H_1), the *Prover* has invoked the `main()` function passing through the edge (M_1, A_1), which is pushed on the top of the stack by the *Verifier*. Then, the *online measurement* (C, C, H_2) indicates that the execution path exited from the function *a()* through the edge (A_2, M_2), which is in relation with the edge on the top of the stack and therefore is valid. Moving forward, the *Verifier* pops from the stack and pushes the edge (M_3, A_1), which corresponds to the second invocation of the function `a()`. At this point, the third measurement (C, C, H_2) indicates that the *Prover* exited from the function `a()` through the edge (A_2, M_2), which

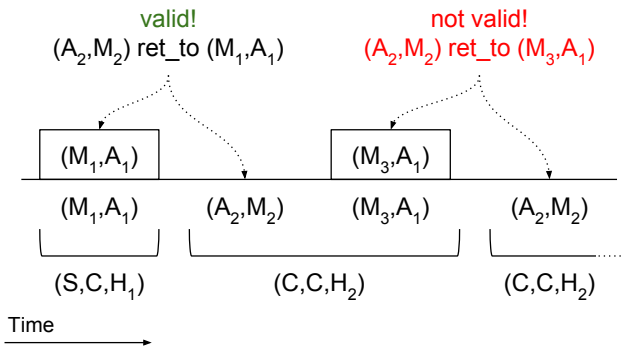


FIGURE 4.4: Implementation of the shadow stack on the ScaRR *Verifier*.

is not in relation with (M_3, A_1). Thus, the *Verifier* detects the attack and triggers an alarm.

4.4 Implementation

Here, we provide the technical details of the ScaRR schema and, in particular, of the *Measurements Generator* (Section 4.4.1) and of the *Prover* (Section 4.4.2).

4.4.1 Measurements Generator

The *Measurements Generator* is implemented as a compiler, based on LLVM Lattner and Adve, 2004 and on the CRAB framework Gange et al., 2016. Despite this approach, it is also possible to use frameworks to lift the binary code to LLVM intermediate-representation (IR) *McSema* 2014.

The *Measurements Generator* requires the program source code to perform the following operations: (i) generating the *offline measurements*, and (ii) detecting and instrumenting the control-flow events. During the compilation, the *Measurements Generator* analyzes the LLVM IR to identify the control-flow events and generate the *offline measurements*, while it uses the CRAB LLVM framework to generate the CFG, since it provides a heap abstract domain that resolves indirect forward jumps. Again during the compilation, the *Measurements Generator* instruments each control-flow event to invoke a tracing function which is contained in the trusted anchor. To map LLVM IR BBLs to assembly BBLs, we remove the optimization flags and we include dummy code, which is removed after the compilation through a binary-rewriting tool. To provide the above-mentioned functionalities, we add around 3.5K lines of code on top of CRAB and LLVM 5.0.

4.4.2 Prover

The *Prover* is responsible for running the monitored application, generating the application *online measurements* and sending the partial reports to the *Verifier*. To achieve the second aim, the *Prover* relies on the architecture depicted in Figure 4.5, which encompasses several components belonging either to the user-space (*i.e., Application Process*

and *ScaRR Libraries*) or to the kernel-space (*i.e., ScaRR sys_addaction*, *ScaRR Module*, and *ScaRR sys_measure*).

Each component works as follows:

- *Application Process* - the process running the monitored application, which is equipped with the required instrumentation for detecting control-flow events at runtime.
- *ScaRR Libraries* - the libraries added to the original application to trace control-flow events and *checkpoints*.
- *ScaRR sys_addaction* - a custom kernel syscall used to trace control-flow events.
- *ScaRR Module* - a module that keeps trace of the *online measurements* and of the partial reports. It also extracts the BBL labels from their runtime addresses, since the ASLR protection changes the BBLs location at each run.
- *ScaRR sys_measure* - a custom kernel syscall used to generate the *online measurements*.

When the *Prover* receives a challenge, it starts the execution of the application and creates a new *online measurement*. During the execution, the application can encounter *checkpoints* or control-flow events, both hooked by the instrumentation. Every time the application crosses a control-flow event, the *ScaRR Libraries* invoke the *ScaRR sys_addaction* syscall to save the new edge in a buffer inside the kernel-space. While, every time the application crosses a *checkpoint*, the *ScaRR Libraries* invoke the *ScaRR sys_measure* syscall to save the *checkpoint* in the current *online measurement*, calculate the hash of the edges saved so far, and, finally, store the *online measurement* in a buffer located in the kernel-space. When the predefined number of *online measurements* is reached, the *Prover* sends a partial report to the *Verifier* and starts collecting new *online measurements*. The *Prover* sends the partial report by using a dedicated kernel thread. The whole procedure is repeated until the application finishes processing the input of the *Verifier*.

The whole architecture of the *Prover* relies on the kernel as a trusted anchor, since we find it more efficient in comparison to other commercial trusted platforms, such as SGX and TrustZone, but other approaches can be also considered (Section 4.6). To develop the kernel side of the architecture, we add around 200 lines of code to a Kernel version v4.17-rc3. We also include the Blake2 source Aumasson et al., 2014; *BLAKE2* 2013, which is faster and provides high cryptographic security guarantees for calculating the hash of the *LoAs*.

4.5 Evaluation

We evaluate ScaRR from two perspectives. First, we measure its performance focusing on: attestation speed (Section 4.5.1), verification speed (Section 4.5.2) and network impact (Section 4.5.3). Then, we discuss ScaRR security guarantees (Section 4.5.4).

We obtained the results described in this section by running the bench-marking suite SPEC CPU 2017 over a Linux machine equipped with an Intel i7 processor and 16GB of memory [1]. We instrumented each tool to detect all the necessary control-flow

[1] We did not manage to map assembly BBL addresses to LLVM IR for 519.lbm_r and 520.omnetpp_r.

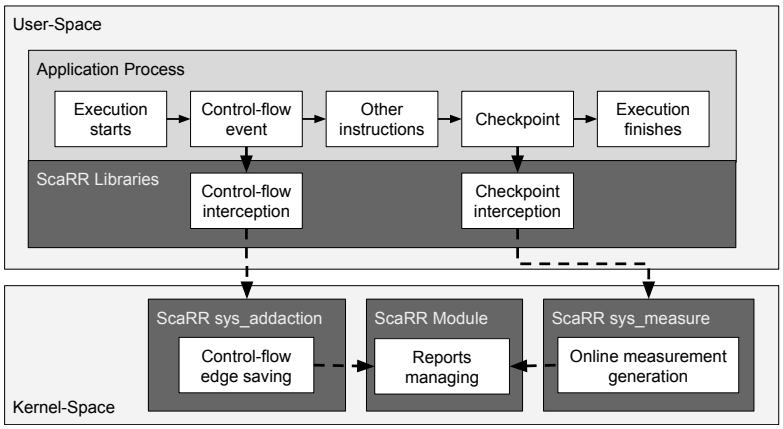


FIGURE 4.5: Internal architecture of the *Prover*.

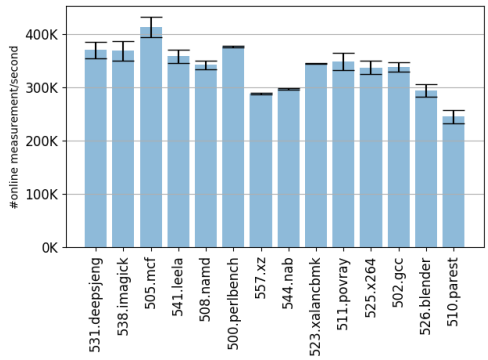
events, we then extracted the *offline measurements* and we ran each experiment to analyze a specific performance metrics.

4.5.1 Attestation Speed

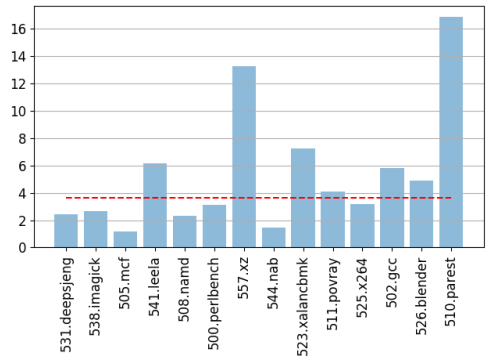
We measure the attestation speed as the number of *online measurements* per second generated by the *Prover*. Figure 4.6a shows the average attestation speed and the standard deviation for each experiment of the SPEC CPU 2017. More specifically, we run each experiment 10 times, calculate the number of *online measurements* generated per second in each run, and we compute the final average and standard deviation. Our results show that ScaRR has a range of attestation speed which goes from 250K (510.parest) to over 400K (505.mcf) of *online measurements* per second. This variability in performance depends on the complexity of the single experiment and on other issues, such as the file loading. Previous works prove to have an attestation speed around $20K$ / $30K$ of control-flow events per second Abera et al., 2019; Abera et al., 2016. Since each *online measurement* contains at least a control-flow event, we can claim that ScaRR has an attestation speed at least 10 times faster than the one offered by the existing solutions.

4.5.2 Verification Speed

During the validation of the partial reports, the *Verifier* performs a lookup against the *Measurements DB* and an update of the shadow stack. To evaluate the overall performance of the *Verifier*, we consider the verification speed as the maximum number of *online measurements* verified per second. To measure this metrics, we perform the following experiment for each SPEC tool: first, we use the *Prover* to generate and save the *online measurements* of a SPEC tool; then, the *Verifier* verifies all of them without involving any element that might introduce delay (*e.g.*, network). In addition, we also introduce a digital fingerprint based on AES Stallings, 2002 to simulate an ideal scenario in which the *Prover* is fast. We perform the verification by loading the *offline measurements* in an in-memory hash map and performing the shadow stack. Finally, we compute the average verification speed of all tools.



(A) Average attestation speed measured as number of online measurements per second.



(B) Average number of procedure calls and procedure returns found during the *Online Program Analysis* of the SPEC CPU 2017 tools.

FIGURE 4.6: ScaRR evaluation of attestation speed, and number the procedures invoked.

According to our experiments, the average verification speed is 2M of *online measurements* per second, with a range that goes from 1.4M to 2.7M of *online measurements* per second. This result outperforms previous works in which the authors reported a verification speed that goes from 110 Dessouky et al., 2018 to 30K Abera et al., 2019 of control-flow events per second. As for the attestation speed, we recall that each *online measurement* contains at least one control-flow event.

The performance of the shadow stack depends on the number of procedure calls and procedure returns found during the generation of *online measurements* in the *Online Program Analysis* phase. To estimate the impact on the shadow stack, we run each experiment of the SPEC CPU 2017 tool and count the number of procedure calls and procedure returns. Figure 4.6b shows the average number of the above-mentioned variables found for each experiment. For some experiments (*i.e.*, 505.mcf and 544.nab), the average number is almost one since they include some recursive algorithms that correspond to small *LoAs*. If the average length of the *LoA*s tends to one, ScaRR behaves similarly to other remote RA solutions that are based on cumulative hashes Abera et al., 2016; Abera et al., 2019. Overall, Figure 4.6b shows that a median of push/pop operations is less than 4, which implies a fast update. Combining an in-memory hash map and a shadow stack allows ScaRR to perform a fast verification phase.

4.5.3 Network Impact and Mitigation

A high sending rate of partial reports from the *Prover* might generate a network congestion and therefore affect the verification phase. To reduce network congestion and improve verification speed, we perform an empirical measurement of the amount of data (*i.e.*, MB) sent on a local network with respect to the verification speed by applying different settings. The experiment setup is similar to Section 4.5.2, but the *Prover* and the *Verifier* are connected through an Ethernet network with a bandwidth of 10Mbit/s. At first, we record 1M of *online measurements* for each SPEC CPU 2017 tool. Then, we

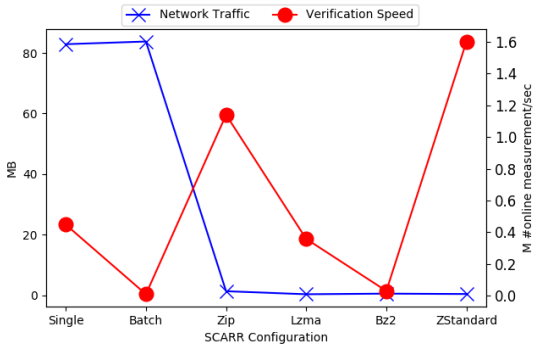


FIGURE 4.7: Comparison of different approaches for generating partial repors in terms of network traffic and verification speed.

send the partial reports to the *Verifier* over a TCP connection, each time adopting a different approach among the following ones: *Single*, *Batch*, *Zip* *ZLib* 2017, *Lzma* Leavline and Singh, 2013, *Bz2* *Bzip2* 2002 and *ZStandard* *Zstandard* 2016. The results of this experiment are shown in Figure 4.7. In the first two modes (*i.e.*, *Single* and *Batch*), we send a single *online measurement* and 50K *online measurements* in each partial report, respectively. As shown in the graph, both approaches generate a high amount of network traffic (around 80MB), introducing a network delay which slows down the verification speed. For the other four approaches, each partial report still contains 50K *online measurements*, but it is generated through different compression algorithms. All the four algorithms provide a high compression rate (on average over 95%) with a consequent reduction in the network overload. However, the algorithms have also different compression and decompression delays, which affect the verification speed. The *Zip* and *ZStandard* show the best performances with 1.2M of *online measurements*/s and 1.6M of *online measurements*/s, respectively, while *Bz2* (30K of online measurements/s) and *Lzma* (0.4M of online measurements/s) are the worst ones. The number of *online measurements* per partial report might introduce a delay in detecting attacks and its value depends on the monitored application. We opted for 50K because the SPEC CPU tools generate a high number of *online measurements* overall. However, this parameter strictly depends on the monitored application. This experiment shows that we can use compression algorithms to mitigate the network congestion and keep a high verification speed.

4.5.4 Attack Detection

Here, we describe the security guarantees introduced by ScaRR.

Code Injection. In this scenario, an attacker loads malicious code, *e.g.*, *Shellcode*, into memory and executes it by exploiting a memory corruption error Smith, 1997. A typical approach is to inject code into a buffer which is under the attacker control. The adversary can, then, exploit vulnerabilities (*e.g.*, buffer overflows) to hijack the program control-flow towards the shellcode (*e.g.*, by corrupting a function return address).

When a W⊕X protection is in place, this attempt will generate a memory protection error, since the injected code is placed in a writable memory area and it is not

executable. In case there is no W⊕X enabled, the attack will generate a wrong *LoA* detected by the *Verifier*.

Another strategy might be to overwrite a node (*i.e.*, a BBL) already present in memory. Even though this attempt is mitigated by W⊕X, as executable memory regions are not writable, it is still possible to perform the attack by changing the memory protection attributes through the operating system interface (*e.g.*, the `mprotect` system call in Linux), which makes the memory area writable. The final result would be an override of the application code. Thus, the static RA of ScaRR can spot the attack.

Return-oriented Programming. Compared to previous attacks, the code-reuse ones are more challenging since they do not inject new nodes, but they simply reorder legitimate BBLs. Among those, the most popular attack Shacham, 2007a is ROP Carlini and Wagner, 2014, which exploits small sequences of code (gadgets) that end with a `ret` instruction. Those gadgets already exist in the programs or libraries code, therefore, no code is injected. The ROP attacks are Turing-complete in nontrivial programs Carlini and Wagner, 2014, and common defence mechanisms are still not strong enough to definitely stop this threat.

To perform a ROP attack, an adversary has to link together a set of gadgets through the so-called ROP chain, which is a list of gadget addresses. A ROP chain is typically injected through a stack overflow vulnerability, by writing the chain so that the first gadget address overlaps a function return address. Once the function returns, the ROP chain will be triggered and will execute the gadget in sequence. Through more advanced techniques such as stack pivoting Dai Zovi, 2010, ROP can also be applied to other classes of vulnerabilities, *e.g.*, heap corruption. Intuitively, a ROP attack produces a lot of new edges to concatenate all the gadgets, which means invalid *online measurements* that will be detected by ScaRR at the first *checkpoint*.

Jump-oriented Programming. An alternative to ROP attacks are the JOP ones Yao, Chen, and Venkataramani, 2013; Bletsch et al., 2011, which exploit special gadgets based on indirect `jump` and `call` instructions. ScaRR can detect those attacks since they deviate from the original control-flow.

Function Reuse Attacks. Those attacks rely on a sequence of subroutines, that are called in an unexpected order, *e.g.*, through virtual functions calls in C++ objects. ScaRR can detect these attacks, since the ScaRR control-flow model considers both the calling and the target addresses for each procedure call. Thus, an unexpected invocation will result in a wrong *LoA*. For instance, in Counterfeit Object-Oriented Programming (COOP) attacks Schuster et al., 2015a, an attacker uses a loop to invoke a set of functions by overwriting a *vtable* and invoking functions from different calling addresses generates unexpected *LoAs*.

4.6 Discussion

In this section we discuss limitations and possible solutions for ScaRR.

Control-flow graph. Extracting a complete and correct CFG through static analysis is challenging. While using CRAB as abstract domain framework, we experienced some problems to infer the correct forward destinations in case of virtual functions. Thus, we will investigate new techniques to mitigate this limitation.

Reducing context-switch overhead. ScaRR relies on a continuous context-switch between user-space and kernel-space. As a first attempt, we evaluated SGX as a trusted platform, but we found out that the overhead was even higher due to SGX clearing the Translation-Lookaside Buffer (TLB) Stravers and Waerdt, 2013 at each enclave exit. This caused frequent page walks after each enclave call. A similar problem was related to the Page-Table Isolation (PTI) Watson et al., 2018 mechanism in the Linux kernel, which protects against the Meltdown vulnerability. With PTI enabled, TLB is partially flushed at every context switch, significantly increasing the overhead of syscalls. New trusted platforms have been designed to overcome this problem, but, since they mainly address embedded software, they are not suitable for our purpose. We also investigated technologies such as Intel PT Ge, Cui, and Jaeger, 2017 to trace control-flow events at hardware level, but this would have bound ScaRR to a specific proprietary technology and we also found that previous works Ge, Cui, and Jaeger, 2017; Hu et al., 2018 experienced information loss.

Physical attacks. Physical attacks are aimed at diverting normal control-flow such that the program is compromised, but the computed measurements are still valid. Trusted computing and RA usually provide protection against physical attacks. In our work, we mainly focus on runtime exploitation, considering that ScaRR is designed for a deployment on virtual machines. Therefore, we assume to have an adversary performing an attack from a remote location or from the user-space and the hosts not being able to be physically compromised. As a future work, we will investigate new solutions to prevent physical attacks.

Data-flow attestation. ScaRR is designed to perform runtime RA over a program CFG. Pure data-oriented attacks might force the program to execute valid, but undesired paths without injecting new edges. To improve our solution, we will investigate possible strategies to mitigate this type of attacks, considering the availability of recent tools able to automatically run this kind of exploit Hu et al., 2016.

Toward a full semantic RA. We will investigate new approaches to validate series of *online measurements* by using runtime abstract interpretation Ge, Cui, and Jaeger, 2017; Hu et al., 2018; Liu, Zhang, and Wang, 2018.

Chapter 5

Advanced attacks against SGX Enclaves

In this chapter, we explore a new attack scenario a in which an adversary attempts at taking control of a TEE *enclave* while hiding its presence from the operating system. More precisely, we pose the following new research question:

Can we carry out an attack against SGX enclaves without being noticed by an healthy Operating System?

We answer this question with a new approach that pushes further the stealthiness of code-reuse attacks in non-compromised OSs. Our intuition is to implant a permanent payload inside the target enclave as a backdoor, thus exploiting the SGX protections to avoid inspection. Our strategy definitely overcomes the limitations of the state-of-the-art; the adversary does not need to repeat the attack and we minimize the traces left. We implement our intuition in SnakeGX, a framework to implant data-only backdoors in legitimate enclaves. We build on the concept of data-only malware Vogl et al., 2014 but extend it with a novel architecture to adhere to the strict requirements of SGX environments.

Contrary to prior one-shot attacks Biondo et al., 2018; Lee et al., 2017, our backdoor acts as an additional secure function (Section 5.3), which is: (i) **persistent** in the context of the enclave, (ii) **stateful** as it maintains an internal state, (iii) **interactive** with the host by means of seamless context switches. Core to this is the identification of a design flaw that affects the Intel SGX Software Development Kit (SDK) and allows an attacker to trigger arbitrary code in enclaves (Section 5.2)[1]. SnakeGX facilitates the creation of versatile backdoors concealed in enclaves that evade memory forensic analysis by inheriting all the benefits SGX provides. Our aim is to raise awareness of TEEs—and SGX in particular—and how attackers may abuse that, which requires the community to reason more on the need of monitoring systems and advanced forensic techniques for SGX.

We evaluate the properties of SnakeGX against StealthDB Vinayagamurthy, Gribov, and Gorbunov, 2019, an open-source project that implements an encrypted database on top of SGX enclaves. In particular, StealthDB uses dynamically generated AES keys to protect the database's fields, thus urging the need of multiple one-shot attacks. SnakeGX exfiltrates the keys upon the verification of specific conditions with a minimum footprint. Our evaluation focuses on three aspects of SnakeGX (Section 5.4). First, we illustrate our use-case: we show how SnakeGX achieves its goals while preserving the original functionality of the enclave. Second, we measure and compare

[1] We reported the flawed behavior to Intel, which acknowledged it.

the stealthiness of SnakeGX against the state-of-the-art. Finally, we discuss possible countermeasures.

In summary, we make the following contributions:

- We propose SnakeGX, a framework built around an Intel SGX SDK design flaw (Section 5.2), and a novel architecture designed to create persistent, stateful, and interactive data-only malware for SGX (Section 5.3).
- We demonstrate the feasibility of SnakeGX on a real-world open source project[2].
- We measure and compare the attack footprint with current SGX state-of-the-art techniques (Section 5.4).

5.1 Threat Model and Assumptions

In this section, we first describe our threat model. Then, we perform a preliminary analysis to measure the widespread of our assumptions over real SGX open-source projects.

Threat Model. One of the differences between SnakeGX and the previous one-shot code-reuse works is in the threat model. Advanced code-reuse techniques require an unprivileged attacker Biondo et al., 2018. However, a non-compromised host can identify the presence of an adversary in the system memory (Section **??** TODO in background ◁). Therefore, we have to consider three players in our scenarios: the attacker, the victim enclave, and the host. Below, we list their requirements, respectively.

Attacker Capabilities. In our scenario, the attacker is highly motivated and has the following assumptions:

- **The enclave contains a memory corruption vulnerability.** The adversary is aware of a memory corruption error (*e.g.,* a buffer overflow) in the target enclave. This error can be exploited to take control of the enclave itself. Having a memory-corruption is an assumption already taken by similar works Biondo et al., 2018; Lee et al., 2017. This is even more likely in projects that use SGX as a sub-system container Baumann, Peinado, and Hunt, 2015; Tsai, Porter, and Vij, 2017a; Seo et al., 2017; Arnautov et al., 2016b. Such projects host out-of-the-box software and, therefore, enclaves inherit their vulnerabilities.
- **A code-reuse technique.** SnakeGX does not require any specific code-reuse techniques (*e.g.,* ROP, JOP, BROP, SROP) as long as this enables the attacker to take control of the enclave execution. For the sake of simplicity, we use the term *chain* to indicate a generic code-reuse payload (*e.g.,* a ROP-chain).
- **Knowledge of victim enclave memory layout.** The attacker can infer the memory layout by inspecting the victim address-space. It is also possible to leak memory information from within the enclave, as also assumed in Biondo et al., 2018.

[2]SnakeGX's source code is available at https://github.com/tregua87/snakegx.

- **Adversary Location.** In our scenario, the adversary resides in user-space. SnakeGX will reduce the adversary footprint, thus evading standard memory forensic techniques Stancill et al., 2013; Polychronakis and Keromytis, 2011; Kittel et al., 2015; Graziano, Balzarotti, and Zidouemba, 2016, whose effectiveness relies on the amount of traces left in memory (see Section **??** TODO background ◁).

Enclaves Capabilities. These are the assumptions for the enclave:

- **Legitimate enclaves.** The system contains one or more running enclaves. It is possible to exploit enclaves based on both SGX 1.0 or 2.0.
- **Intel SGX SDK usage.** The victim enclave should be implemented by using the standard Intel SGX Software Development Kit (SDK), we tested our approach with all the SDK versions currently available.[3] This is a reasonable assumption since the Intel SGX SDK provides a framework for developing applications on different OSs: Linux and Windows.
- **Multi-threading.** This is not strictly required, but the victim enclave should have at least two threads for a more general approach. The rationale behind this requirement is that the proposed implementation may disable a trusted thread *Intel® Software Guard Extensions (Intel®SGX) - Developer Guide* 2013 and in case of a single-thread application this is a problem. An enclave without free threads cannot process secure functions, thus attracting the analysts attention. We might partially ease this requirement with the introduction of SGX 2.0. However, multi-thread enclaves are a reasonable assumption since different open-source projects use already this feature *SGX_SQLite*; *SGX-Tor* 2018; *Technology preview: Private contact discovery for Signal* 2017; Tsai, Porter, and Vij, 2017a; Vinayagamurthy, Gribov, and Gorbunov, 2019 and SGX-based applications are growing in complexity.

Host Capabilities. This is the assumption for the host:

- **Memory Inspection.** The host can inspect the processes memory and use standard approaches to detect traces of previous or ongoing attacks Stancill et al., 2013; Polychronakis and Keromytis, 2011; Kittel et al., 2015; Graziano, Balzarotti, and Zidouemba, 2016.

We extend the threat model of previous works Biondo et al., 2018 by assuming the host can perform memory forensic analysis. Therefore, an adversary has the need of hiding her presence in the machine and minimizing the interactions with the victim enclave.

Preliminary Analysis of Assumptions. We collected a set of 27 stand-alone SGX open-source projects from an online hub *Awesome SGX Open Source Projects* 2019 to investigate the correctness of our assumptions (see full list in Appendix A). The results show that among the 27 projects, 24 of them were based on the Intel SGX SDK, while others were developed with Graphene Tsai, Porter, and Vij, 2017a, Open Enclave

[3] At the time of writing, the last SDK version is 2.9.

SDK Microsoft, 2019, or contained mocked enclaves. From the Intel SGX SDK based projects, we counted 31 enclaves in total, among which 24 were multi-threading (77%). This preliminary analysis indicates that our threat model fulfills real scenarios. Furthermore, we discuss the porting of SnakeGX over SDKs other than the Intel one in Section 5.5.

5.2 Intel SGX SDK Design Limitation

SnakeGX can trigger a payload inside the enclave without the need of repeating a new attack. This feature is challenging because the enclave has a fixed entry point, thus an adversary cannot activate arbitrary code inside the enclave from the untrusted memory. SnakeGX achieves this goal through a design error that affects all the SGX Software Development Kit (SDK) versions released by Intel. In this section, we make a deep analysis of the Intel SGX SDK in order to highlight these issues and propose possible mitigations.

5.2.1 SDK Overview

SGX specifications define only basic primitives for creating and interacting with an enclave. Thus, Intel also provides an SDK that helps building SGX-based applications. The Intel SGX SDK contains a run-time library that is composed by two parts: an untrusted run-time library (`uRts`) that is contained in the host process, and a trusted run-time library (`tRts`) that is contained in the enclave. Specifically, `uRts` handles operations like multi-threading, while `tRts` manages secure functions dispatching and context-switch.

The Intel SGX SDK exposes a set of APIs that are built on top of the leaf functions described in Section **??** TODO background ◁. `ECALL`, `ERET`, `OCALL`, and `ORET` are the most important APIs for SnakeGX. Figure 5.1 shows the interaction between the host process and the enclave. At the beginning, the host process invokes a secure function by using an `ECALL`, which is implemented by means of an `EENTER` (Figure 5.1, step 1). When a secure function is under execution, it may need to interact with the OS (*e.g.*, for writing a file). Since a secure function cannot directly invoke syscalls, Intel SGX SDK uses additional functions that reside in the untrusted memory (*i.e.*, called outside functions). A secure function can invoke an outside function by using an `OCALL` (Figure 5.1, point 2), that performs two steps: (i) save the enclave state, and (ii) pass the control to the outside function. More precisely, `OCALL` first saves the secure function state by using a dedicate structure called `ocall_context`, which we deeply analyze in Section 5.2.2. Then, `OCALL` uses the `EEXIT` leaf function to switch the context back to the `uRts`, that finally dispatches the actual outside function. Once an outside function ends, the control passes back to the secure function by using an `ORET` (Figure 5.1, point 3). Since SGX does not allow to trigger arbitrary code from the untrusted memory (*i.e.*, the enclave entry point is fixed), the Intel SGX SDK implements `ORET` as a special secure function (whose index is -2) that follows the standard `ECALL` specifications. As we discuss in the next sessions, `ORET` has the ability of activating arbitrary portion of code in an enclave. Normally, the `ORET` restores the state previously stored

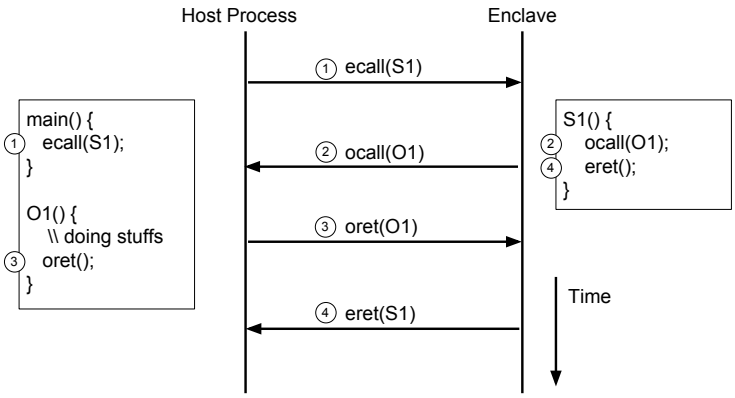


FIGURE 5.1: Example of interaction between host process and enclave by using the Intel SGX SDK. The host process invokes the secure function S1 from the main function (ECALL). S1 function invokes O1 (OCALL), and this latter returns to S1 (ORET). Finally, S1 returns back to the main function (ERET).

by the OCALL. Once the ORET is done, the secure function can continue its execution, and finally, invoke an ERET to terminate (Figure 5.1, point 4).

5.2.2 OCALL Context Setting

The ocall_context is the structure that holds the enclave state once an OCALL is invoked. The way in which the structure is set slightly differs between Intel SGX SDK before and after version 2.0. In this discussion, we consider the case of the Intel SGX SDK greater than 2.0. However, a similar approach can be also applied to previous versions.

New ocall_contextes are located on top of the stack, as shown in Figure 5.2, moreover, the new structures should follow a specific setting. In particular, three ocall_context fields should be tuned:

- pre_last_sp must point to a previous ocall_context or to the stack base address. This needs to handle a chain of nested ECALLs, which are basically ECALLs performed by an outside function.
- ocall_ret is used from SDK 2.0 to save extended process state *Intel Architecture Instruction Set Extensions Programming Reference* 2018. More precisely, the system allocates a xsave_buff pointed by ocall_ret. This buffer must be located after the new ocall_context.
- rbp must point to a memory location that contains the new frame pointer and the return address, consecutively. This is because the asm_oret() function will use this structure as epilogue Biondo et al., 2018.

It is important to underline that SGX does not validate ocall_context integrity. Therefore, an attacker that takes control of an enclave may craft a fake ocall_context.

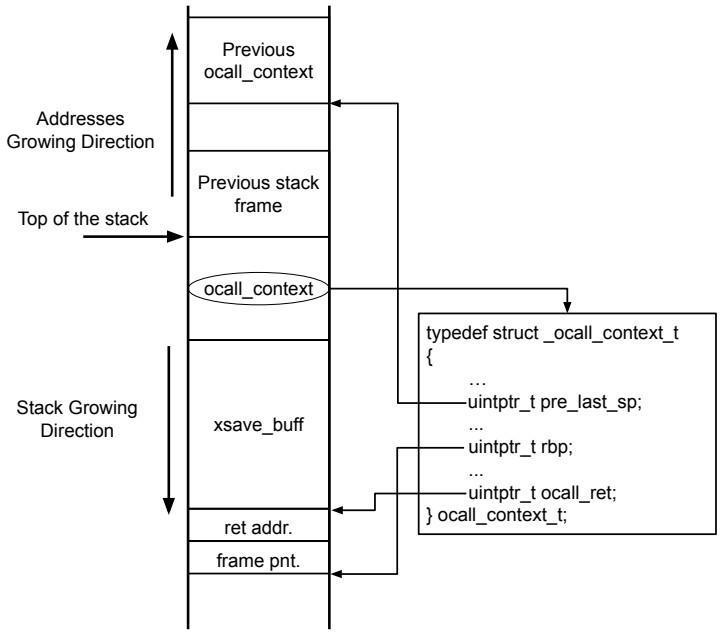


FIGURE 5.2: Example of `ocall_context` disposition in an enclave stack, the fields point to structures within the stack itself in a precise order.

This problem has been existing in all SDK version available so far. In the next section, we discuss why this is an underestimated problem and what threats can lead to.

5.2.3 Exploiting an ORET as a Trigger

`ORET` is the only secure function that can trigger arbitrary code in an enclave. Therefore, an adversary enabled to abusing this function has also privileged access to the enclave itself. To understand why it is possible, we analyze the pseudo-code in Figure 5.3, which shows the `do_oret()` secure function implementation. Essentially, `do_oret()` extracts the thread-local storage (TLS) from the current thread (Line 6). The TLS contains information of the last `ocall_context` saved. After some formal controls (Line 8), the `ocall_context` structure is used to restore the secure function execution through the `asm_oret()` function (Line 15). The formal checks performed by `do_oret()` over the previous `ocall_context` are quite naive. There are three basic requirements: (i) the `ocall_context` must be within the current stack space, (ii) the `ocall_context` must contain a constant (hard-coded) magic number, and (iii) the `pre_last_sp` must point before the actual `ocall_context`.

After the previous analysis, we realized that the Intel SGX SDK has no strict mechanisms to verify the integrity of an `ocall_context`. In other words, any `ocall_context` that fulfills the previous conditions can be used to restore any context in an enclave. First steps in this direction were explored by previous works Biondo et al., 2018, which exploited `asm_oret()` simply to control the processor registers in a one-shot code-reuse attack. However, we want to push further the limitation of the Intel SGX SDK

```
1  sgx_status_t do_oret()
2  {
3  // TLS structure
4  tls = get_thread_data();
5  // last ocall_context structure
6  ocall_context = tls->last_sp;
7
8  if (!formal_requirements(ocall_context))
9  return SGX_ERROR_UNEXPECTED;
10
11 // set TLS to point to previous ocall_context
12 tls->last_sp = ocall_context->pre_last_sp;
13
14 // restore last ocall_context
15 asm_oret(ocall_context);
16
17 // in the normal execution
18 // the control should not reach this point
19 return SGX_ERROR_UNEXPECTED;
20 }
21
```

FIGURE 5.3: Simplified `do_oret()` pseudo-code.

and show which consequences these issues can lead to. In fact, SnakeGX uses a combination of `ORET` and tampered `ocall_context`es to restore arbitrary *chains* inside the enclave without performing further exploits. In particular, SnakeGX abuses of this flaw for two reasons: (i) as a trigger to activate a custom payload hidden inside the enclave; (ii) for the payload to perform a reliable context-switch between host and enclave. Therefore, crafting malicious `ocall_context`es leads to the possibility of implanting backdoor in a trusted enclave without tampering the enclave code itself. As such, the backdoor is shielded by the SGX features by design. Moreover, the fact of using a single `ORET` to trigger the backdoor reduces the interactions required by a weak adversary for new attacks. We discuss technical details in Section 5.3 and show our proof-of-concept (PoC) in Section 5.4.

5.2.4 Mitigations

There are many strategies to improve the `ocall_context` integrity. A pure software solution could be computing an encrypted hash of `ocall_context` when it is generated. The hash might be appended as an extra field to the structure. Another approach, instead, could be encrypting the entire structure itself. However, pure software mitigation can be potentially bypassed by any code-reuse attack. Once the attacker gains control of the enclave, she can basically revert or fake any encrypted processes. A stronger solution could be introducing dedicated leaf functions that manage the generation and consumption of `ocall_context`es. For instance, during an `OCALL`, the enclave might use a dedicated leaf function that creates an `ocall_context` and saves a copy (*i.e.*, an hash) in a memory location out of the attacker control (similar to TCS

or SECS pages Costan and Devadas, 2016). An `ORET`, then, should use another leaf function that performs extra checks and validate the integrity of the `ocall_context`. This solution might raise the bar for attacks, but it has two important drawbacks: (i) it forces Intel to re-thinking the SGX structures at low level, (ii) it leaves less freedom to developers that want to adapt the Intel SGX SDK to their own needs (*e.g.,* to customize or introduce new structures). After this consideration, we believe this issue would last for long before being fixed. We reported this limitation to Intel that is reviewing its memory corruption protections.

5.3 SnakeGX

SnakeGX is the first framework that facilitates the implanting of persistent, stateful, and interactive backdoors inside SGX enclaves. The framework design is challenging because we want to preserve the original enclave functionality and configuration. Even though SGX 2.0 encompasses run-time page permissions setting *Intel® Software Guard Extensions Programming Reference* 2013, an unexpected configuration may attract analysts attention (*i.e.,* the host can read the enclave page permissions). On the contrary, our solutions purely rely on code-reuse techniques that do not affect the enclave functionality and configuration. To the best of our knowledge, no previous works on SGX code-reuse attacks never addressed these challenges. We also recall we assume two conditions: (i) the target enclave has to be built with the Intel SGX SDK, and (ii) it contains at least one exploitable memory-corruption vulnerability (*e.g.,* a stack-based buffer overflow).

5.3.1 Overview

The backdoor implanting is composed by three main phases: (i) enclave memory analysis, (ii) installation phase, and (iii) payload triggering.

Enclave Memory Analysis. In this phase, the attacker has to achieve two goals: (i) inspect the process memory layout to identify enclave elements, and (ii) find a suitable location to install SnakeGX. Since SGX does not implement any memory layout randomization, an adversary can easily inspect the victim process memory by only using user-space privileges (*e.g.,* the enclave pages are assigned to a virtual device called *isgx* in Linux environments). Moreover, we target enclaves made with the Intel SGX SDK that follow the Enclave Linear Address Range (ELRANGE) Costan and Devadas, 2016. As a result, an adversary with solely user-space privileges can obtain: (i) the enclave base address, (ii) the size, and (iii) the enclave trusted thread locations. In Section 5.3.2, we discuss how to obtain a reliable memory location.

Payload Installation. The installation phase is a one-shot attack that exploits an enclave vulnerability and uses a code-reuse technique for installing the payload. This attack has to achieve three goals: (i) copy the payload inside an enclave (*e.g.,* the *chain* and the fake `ocall_context`), (ii) set a hook to trigger the payload, (iii) resume the normal application behavior. These three goals make this phase quite critical for three reasons. First, either enclave and host process have to remain available after the payload installation, or else we have to re-start the enclave. Second, the enclave behavior does have not to change, or else the host should realize the attack. Finally, we have to

remove the payload in the untrusted memory, or else it could be detected. This phase can be implemented by using any current code-reuse attacks for SGX enclaves Lee et al., 2017; Biondo et al., 2018.

Payload Triggering. After the installation phase, the adversary only needs to trigger an `ORET` to activate the payload (Section 5.3.3). This allows an external adversary to activate the payload without attacking the enclave from scratch. The payload contains the logic for interacting with the OS and the enclave. To achieve persistence, we design a generic architecture that fits the SGX realm (Section 5.3.4). Moreover, since the payload can potentially leave the enclave, we designed a generic context-switch mechanism that enables the payload to keep control over the enclave (Section 5.3.5).

5.3.2 Getting a Secure Memory Location

We employ a trusted thread as backdoor location because it allows us to abuse the design error described in Section 5.2. If an enclave does not have any available trusted thread, SnakeGX can still work by stealing one of the available threads. In this case, the target application may notice some degradation of the performances. However, the system does not raise any exception because it is not possible to determinate the real cause. In this way, we can take control of an enclave trusted thread without affecting enclave functionality. These properties are SGX specific and were not considered in previous code-reuse works.

Un-releasing a Trusted Thread. This technique is based on a misbehaviour of the thread binding mechanisms in the `uRts` library. Once a secure function is invoked through the Intel SGX SDK, the `uRts` searches a free trusted thread and marks it as *busy*. Then, the trusted thread is released when the secure function ends. However, an attacker can exploit a secure function and leaves the enclave skipping the *releasing* phase in the `uRts`. As a result, the trusted thread remains *busy* and it will never be assigned to future executions, in this way it is stolen. The strategy of this technique is composed by two phases: (i) invoking and exploiting a secure function, then (ii) exiting from the enclave (*e.g.,* by using EEXIT) and skipping the *releasing* of the trusted thread. This approach requires the enclave has at least two trusted threads, otherwise the application might realize that the enclave is unavailable. We use this approach for our PoC.

Making a New Thread. SGX 2.0 and recent versions of the Intel SGX SDK allow creating trusted threads at run-time. Therefore, an attacker may force the enclave to create a new trusted thread without tampering with the pool. However, this approach should be used wisely, otherwise unexpected trusted threads may attract the analyst attention, thus affecting the stealthiness of SnakeGX.

5.3.3 Set a Payload Trigger

We design our trigger on top of the Intel SGX SDK flaw highlighted in Section 5.2. We assume that an attacker has already gained control of an enclave by means of a code-reuse attack. Moreover, either the payload and the trigger must be tuned for the trusted thread under attack.

To install the trigger, the adversary has to mimic an `OCALL` such that the next `ORET` will activate the backdoor (*i.e.,* a *chain*) instead of resuming the execution of a secure function. To achieve this goal, the adversary has to perform three main operations: (i) set a fake `ocall_context` on the stack that satisfies the formal requirements as described in Section 5.2.2; (ii) call the function `save_xregs()` (which is contained in `tRts`) to save extended process features, the function should take as an argument the `xsave_buff` location of the fake `ocall_context` previously copied; (iii) call the function `update_ocall_lastsp()` (which is contained in `tRts`) by passing the pointer to the fake `ocall_context`. This function will set TLS `last_sp` to the fake `ocall_context`, thus simulating an `OCALL`.

This setting allows us to resume the payload execution by performing an `ORET` on the attacked trusted thread. More precisely, `asm_oret()` will restore the context previously installed and it will activate the first gadget. By default, `ocall_context` does not perform a pivot (*i.e.,* it does not set the `rsp` register). To bypass this issue, we used a pivot gadget that is contained in `asm_oret()` function itself: `mov rsp, rbp; pop rbp; ret`. This gadget is present in any SDK version released so far, so it is a generic technique for SGX backdoors. We observed the same gadget also in Windows `tRts`. Therefore, the first instruction triggered by the fake `ocall_context` is a pivot gadget. Then, we set the `rbp` to point to a fake stack inside the stolen thread. In this way, the `ORET` always pivots to the fake stack that contains the actual payload. Notice that this mechanism just pivots to the fake address indicated by the fake `ocall_context` (*i.e.,* `rbp`). As such, an attacker only needs one fake `ocall_context` that pivots to a fixed location. Then, she can just copy different fake stacks to the same location to activate different payloads.

5.3.4 Backdoor Architecture

Figure 5.4 shows the payload architecture that we adopted for SnakeGX. This solution allows us to achieve payload persistence in an SGX enclave by only using the stack address space. By default, the Intel SGX SDK sets the stack size at 40KB, therefore, we design SnakeGX to fit this size. For the sake of simplicity, we describe the switching mechanism in Section 5.3.5.

As underlined in Vogl et al., 2014, classic code-reuse attacks (*e.g.,* ROP) are designed to be one-shot. After executing a *chain*, it may be destroyed due to gadgets side effects. Therefore, we need a location to keep a backup of the structures used. According to this consideration, we split the stack address memory in four sections:

Fake Frame. SnakeGX requires a dedicated location for installing an `ocall_context`. This structure is used to either perform the payload trigger and the context-switch (see Section 5.2). These features are crucial to implement a persistent backdoor in the SGX realm since classic techniques cannot be used.

Buffer. This area contains temporary variables that are used by payloads. For instance, our PoC stores the previous data exfiltrated (see Section 5.4).

Workspace. The fake frame previously installed is tuned to pivot the execution to this location. Generally speaking, any payload is coped here before being executed.

Backup. This location contains a copy of all the structures needed by SnakeGX to work properly. After the SnakeGX installation, this location should not be overwritten.

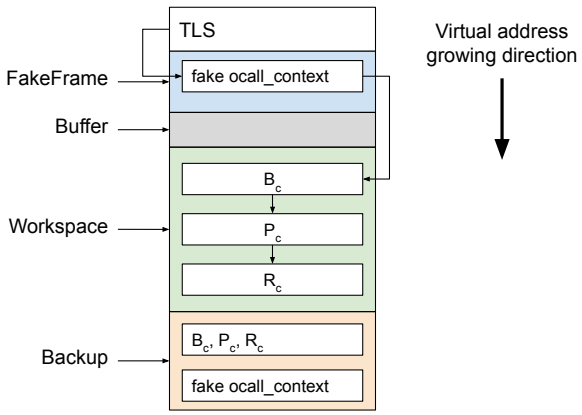


FIGURE 5.4: Trusted thread stack after SnakeGX installation. The memory is split in four areas: FakeFrame, buffer, workspace, and backup. Moreover, the stack contains copies of B_c, P_c, and R_c.

Since the *chains* used may be destroyed after payload execution, we need a mechanism that brings SnakeGX to the initial state after the payload has been executed. More precisely, it has to make the payload available for future invocations. To achieve this goal, we use three *chains*: Boot Chain (B_c), Payload Chain (P_c), and Reset Chain (R_c). Each of them is formed by a fake stack that is maintained in the backup zone and moved in the workspace on demand:

Boot Chain (B_c). This is the first chain that is triggered by the hook, its duties are: (i) copy P_c and R_c into the workspace, and (ii) pivot to P_c. This chain is usually quite short.

Payload Chain (P_c). This contains the actual payload and is strictly enclave dependent. When the payload ends, it just pivots to R_c.

Reset Chain (R_c). This *chain* resets the payload inside the enclave and makes it ready for the next calls without the need of the installation phase. This is achieved with the following operations: (i) copy B_c into workspace, (ii) copy the `ocall_context` in the fake frame, (iii) set TLS to point to `ocall_context`.

After the execution of R_c, SnakeGX can be triggered again by a new `ORET`. The loop boot-payload-reset *chain*, along the architecture shown in Figure 5.4, is a simple framework that can be used by the adversaries to design their customized payload for SnakeGX.

5.3.5 Context-Switch

To allow SnakeGX to interact with the host OS, while maintaining the enclave control, we need to perform three operations: (S1) temporarily copy part of the payload outside, (S2) leave the enclave, and (S3) resume the execution inside the enclave. The first two operations are relatively simple: the Intel SGX SDK already provides standard routines (*e.g.*, `memcpy`) to move data outside the enclave. Moreover, it is possible to pivoting outside the enclave by abusing the `EEXIT` opcode (Section **??**). On the contrary, resuming the enclave execution requires SnakeGX to invoke an `EENTER` opcode. However,

it is not possible to arbitrarily jump inside an enclave (*i.e.,* the entry point is fixed). Therefore, we abuse again of the Intel SGX SDK deign error described in Section 5.2.

To perform the context-switch, we split the payload in three chains, called outside-chain (O_c), payload-one (P_1), and payload-two (P_2). O_c is the part of the payload copied in the untrusted memory, while P_1 and P_2 remain inside the enclave. During the context-switch, we execute P_1, O_c, and P_2, consequently. More precisely, once P_1 requires to interact with the host, it performs (S1) to prepare the O_c activation, installs a fake frame (Section 5.3.4), and prepares P_2 in the workspace. At this point, P_1 can perform (S2): leave the enclave and pivot to O_c. When the operations in untrusted memory are terminated, O_c only needs to run an `ORET` that will activate P_2 (S3). Finally, P_2 can clean the traces left by O_c and continue the backdoor execution. It is possible to perform many context-switch by tuning the payload accordingly.

5.4 Evaluation

We evaluate the real impact of our framework against StealthDB Vinayagamurthy, Gribov, and Gorbunov, 2019, an open-source project that leverages on the SGX technology. We opted for StealthDB because it is a generic representation of our scenario, as we describe in Section 5.4.1. We split our evaluation in three parts: (i) a technical discussion of our use-case (Section 5.4.2), (ii) a measurement of the traces left (Section 5.4.3), and (iii) a discussion about the countermeasures (Section 5.4.4).

5.4.1 StealthDB

StealthDB Vinayagamurthy, Gribov, and Gorbunov, 2019 is a plugin for PostgreSQL Drake and Worsley, 2002 that uses Intel SGX enclaves to implement an encrypted database. This project is the ideal use-case for SnakeGX: StealthDB lifetime is bounded to PostgreSQL, thus we can rely on its enclaves as a secure save point for storing the payload and launching the attacks.

StealthDB uses a single SGX enclave to handle encrypted fields and operations that are performed inside the enclave itself. In this way, the database can securely save encrypted fields on disk, while the plain values are handled only inside the enclave. The encryption algorithm is AES-CTR with keys 128 bits long. These keys are sealed on the disk through the standard SGX features. A user can define multiple keys that are loaded on-demand inside the enclave, however, the StealthDB enclave maintains in memory only a single key at a time. In this scenario, one-shot state-of-the-art techniques require multiple interactions to obtain all the keys. This approach leaves more copies of the payload in the memory, thus increasing the risk of being detected. Even if an adversary manages to obtain all the sealed keys, she still has to perform new attacks whenever a new key is generated. SnakeGX is able to understand when a new key is loaded and performs the exfiltration steps accordingly. In this way, the attacker transparently hides and activates complex logic that resides inside a trusted enclave.

5.4.2 Use-Case Discussion

In this section, we discuss the properties of our PoC payload and some implementation details. For more technical details about our payload see Appendix B. Our setup is

composed by an application that loads StealthDB enclave and performs the attacks. We extracted the gadgets for the *chains* by running ROPGadget *ROPgadget - Gadgets finder and auto-roper* 2011 on the compiled enclave. As our threat model details in Section 5.1, we introduced a memory corruption vulnerability in StealthDB to simplify the payload delivery. We developed our data-only malware for SGX in a host OS running Linux with kernel 4.15.0 and Intel SGX SDK version 2.9.

We composed our PoC of three steps. First, the application starts and loads the enclave. Second, we exploit the enclave vulnerability and implant the payload. Third, we alternatively invoke normal secure functions and the backdoor. This shows that SnakeGX does not alter the normal enclave functionality. Once the backdoor is triggered, SnakeGX exfiltrates the keys only when the condition is satisfied. Without using SnakeGX, the adversary has to perform many attacks to achieve the same goal, which potentially leaves traces for an analyst. Moreover, SnakeGX avoids the burden of crafting new payloads at each exfiltration.

The Payload. Our payload shows three important features: (i) persistence, (ii) internal state, and (iii) context-switch. More precisely, the payload exfiltrates a key if and only if it changes. This is crucial in our threat model (Section 5.1), which assumes a non-compromised host, thus the attacker has to reduce un-useful actions. In fact, all the payload structures are kept inside the enclave, and an adversary only needs to trigger an `ORET` against the compromised thread. Once activated, the payload is able to self-check its status, and in case, leak the key. The payload is composed by three *chains*:

- **P_1** is the first payload to be activated. It checks if the key changed, and in case activates the exfiltration.
- **O** is the outside-chain that actually exfiltrates the key. It is temporary copied in the untrusted memory by P_1.
- **P_2** is the second payload that is triggered by O after the exfiltration. The purpose of P_2 is to wipe out all the temporary structures previously copied in the untrusted memory, *i.e.,* O and the key.

From an external analyzer, all the structures (*i.e.,* P_1, P_2, and O) are always contained in the enclave when the payload is not activated. The only *chain* temporary copied outside is O, but P_2 cleans its traces. Moreover, to activate the payload, the attacker only needs to trigger an `ORET` instead of preparing complex code-reuse attacks. In Section 5.4.3, we measure and compare the traces of SnakeGX *w.r.t.* the state-of-the-art attacks.

Chains Composition. Our payload maintains an internal state and interacts with the host. To handle the state, the payload is able to perform a conditional pivoting by comparing the current key and a copy of the last key exfiltrated Shacham, 2007b. The conditional chain is implemented in P_1. Once the key changes, P_1 will pivot to a *chain* that performs the exfiltration. Otherwise, the payload will pivot to another *chain* that simply resumes the normal enclave behavior. We describe the gadgets used to perform conditional pivoting in Appendix C. The interaction with the OS, instead, requires two types of *chains*: some that run inside the enclave (*i.e.,* P_1 and P_2), and others that run outside (*i.e.,* O). Table 5.1 shows some statistics about *chains* composition. The *chains* inside the enclave are entirely composed by gadgets from the `tRts`. More precisely, P_1 and P_2 invokes 27 and 13 functions such as `memcpy()`,

Chain	# fnc/sys	# gadgets	size [B]
P_1	27	23	2816
P_2	13	7	1232
O	4	20	312
sum	44	50	4360

TABLE 5.1: Statistics of the gadgets used for the payload.

and `update_ocall_lastsp()`, respectively. In terms of memory, P_1 and P_2 occupy 2816 and 1232 byes, respectively. The chain O, instead, is composed by classic gadgets from `libc`. More precisely, O is composed by 20 small standard gadgets. The internal ecosystem of `tRts`, and the `libc` in Linux systems, provide enough gadgets and functions to create useful payloads. We describe the gadgets used for these *chains* in Appendix C.1.

5.4.3 Trace Measurements

We analyze our PoC and measure the advantages SnakeGX introduces. We recall that our threat model assumes a weak adversary which has no control of the host, and therefore, she has to improve her stealthiness. To perform the same goal of our PoC by using state-of-the-art one-shot attacks Biondo et al., 2018, an attacker has to leave in the untrusted memory around 4KB of structures (*i.e.*, P_1, P_2 and O). These traces can be found by using previous results already shown in the literature Stancill et al., 2013; Polychronakis and Keromytis, 2011; Kittel et al., 2015; Graziano, Balzarotti, and Zidouemba, 2016. Moreover, their identification results even simpler since they use peculiar structures such as `sgx_exception_info_t` (see Appendix B). On the contrary, SnakeGX requires only one `ORET` to trigger the payload. In particular, our PoC implements an `ORET` by using only 4 gadgets and leaving a negligible footprint of 56 byes in memory. As a result, the trigger used by SnakeGX is able to activate payloads arbitrary complex by leaving a minimal footprint.

5.4.4 Countermeasures

SnakeGX poses new challenges for forensic investigators and backdoor analysts as well as for experienced reverse engineers. The current state-of-the-art tools cannot detect and dissect this new threat. It is necessary to develop new tools and techniques for the detection and possibly the prevention of threats affecting SGX and similar technologies. Here, we discuss some possible directions for the detection that can be used to observe the presence of SnakeGX in a system. Moreover, we analyze how the current state-of-the-art defenses can mitigate our attack and which future research lines can be taken. This is not a comprehensive study and we leave this part for future work. We hope this research paves the way for new works in the malware analysis field.

Memory Forensic Analysis. SnakeGX is an infector of legitimate enclaves and is by definition stealthier. This means that any form of memory forensics is no more possible. The memory of the enclave cannot be inspected. As explained in Section **??**, SGX makes impossible to read memory pages that belong to an enclave. Any attempts at reading

such pages will result in a fake value 0xFF. Another possible approach is to use new attacks based on microcode flaws Bulck et al., 2018 or fault injections Murdock et al., 2020 to dump an enclave content. Alternatively, it is possible to use side-channel attacks to infer specific enclave manipulations, as discussed in Oleksenko et al., 2018. It should also be pointed out that it is still possible to retrieve `uRts` information. For instance, we could compare the number of trusted threads in `uRts` and the number of trusted threads in the `ELRANGE` structure. An inconsistency will bring to clues regarding the state of that enclave.

Sandboxes. Recently, researchers proposed sandboxes to reduce the interaction of a malware-enclave and the system Weiser et al., 2019. These solutions are designed for systems that cannot assess the origin of an enclave beforehand, thus they do not trust it. These defenses can, in principle, reduce the attack surface of SnakeGX. However, since we target only systems that host known and trusted enclaves, we do not expect sandboxes in place. In the worst case, we can still detect the presence of a sandbox by probing the process (*i.e.*, through a syscall) and interrupt the attack.

Syscalls Trace. Even though the payload is hidden from reading, it is still possible to analyze the syscall interaction of the outside-chains. This approach has been extensively studied and it is quite common in the field of malware analysis. Researchers may design a tracer and superficially focus on the interaction with the enclave. For instance, this tool may spot that SnakeGX generated a file operation that did not appear in previous interactions. In this way, analysts can infer the behaviour of the code inside the enclave.

Control Flow Integrity Checks. Control Flow Integrity checks (CFI) are strong weapons already used in standard programs to mitigate code-reuse attacks. Such mechanisms rely on different strategies to force a program to execute only valid paths at run-time. In the current enclave implementation, the system relies on classic stack canary to avoid buffer overflow. However, Lee et al. Lee et al., 2017 discussed a technique to bypass such protection. Other non-standard systems, such as SGX Shield Seo et al., 2017, implement a custom CFI to mitigate these issues. However, Biondo et al. Biondo et al., 2018 managed to bypass their protection too. So far, there are not effective defenses against code-reuse attacks in the context of enclaves. This approach might raise the bar for attackers who would attempt to deploy SnakeGX or to perform code-reuse attacks in general.

Detecting Fake Structures. SnakeGX exploits the possibility to craft fake structures that are used in critical `tRts` functions, *i.e.*, `ocall_context`. We deeply analyzed this issues and proposed mitigation strategies in Section 5.2.4.

5.5 Discussion

Here, we discuss various aspects of SnakeGX generalization.

5.5.1 SnakeGX Portability

The current implementation of SnakeGX is based on a specific version of the Intel SGX SDK, for a specific application and operating system. In this section, we study the portability of our PoC and show the approach is generic and can be easily adapted

to other SDKs and OSs. Recently, new SGX frameworks were released on the market, or research prototypes, to provide an abstraction layer that simplifies the enclave development. In particular, projects such as Open Enclave Microsoft, 2019, Google Asylo Google, 2018, and SGX Shield Baumann, Peinado, and Hunt, 2015 use the standard Intel SGX SDK to perform host interaction (*i.e.*, `OCALL/ORET`), thus inheriting the same limitations described in Section 5.2. From our point of view, we can implant SnakeGX in any enclave developed with these frameworks if they follow our threat model assumptions (Section 5.1). We also analyzed the Intel SGX SDK for Windows, in which we found and tested the same flaw described in our work. Finally, the standard `tRts` libraries contain all the gadgets used in our PoC. In general, SnakeGX can potentially affect enclaves developed on different SDKs as long as: (i) they are abstraction layers of the Intel SGX SDK, or (ii) they use a host interaction that relies on unprotected structures like `ocall_context`. In this paper, we proposed an instance of SnakeGX targeting StealthDB on Linux. However, the idea is generic and the persistence, stateful, and context-switch properties can be found and achieved also in other OSs and popular SDKs based on the Intel one.

5.5.2 Persistence Offline

SnakeGX maintains persistence in memory as long as the host enclave is loaded. This is similar to what Vogl et al. Vogl et al., 2014 have shown with "Chuck". In their proof of concept they achieved persistence on the running system. Their ROP rootkit did not survive after reboot. In our scenario, SnakeGX may achieve a more complete persistence by exploiting the sealing mechanism. In this case, the malicious payload would not be affected if the enclave is restarted. This sealing mechanism is a common SGX practice. It saves the enclave state (*i.e.*, its data) before the enclave shuts down. If the victim enclave has a loophole in the restoring phase, this could be exploited to inject SnakeGX again after a reboot. However, this is strictly enclave-dependent and therefore we did not include in our discussion and it is left for the future.

5.5.3 SnakeGX 32bit

In this paper, we designed our PoC for 64bit architectures. However, Intel SGX supports also 32bit code to run in enclaves. From our point of view, the main difference between 32bit and 64bit is the calling convention. Therefore, the techniques we discussed and used for SnakeGX are still valid and can be easily ported to 32bit applications.

Chapter 6

A Novel Runtime Remote Attestation Schema for SGX Enclaves

The attack described in 5 requires a study of new defenses and analyses of *enclaves*. The answer to this question is addressed in the papers:

- SgxMonitor: A Novel Runtime Remote Attestation Schema for SGX Enclaves (under review).

Chapter 7

Memory forensics in SGX environment

After discussing the attacks in 5, and see the defences in 6. I want to answer a last question, **what evidence can we extract from the memory and which conclusion do they lead to?**

- Following the evidence beyond the wall: memory forensics in SGX environment (under review).

Chapter 8

Conclusion

These are the conclusions.

Appendix A

Preliminary Analysis of Assumptions

Table A.1 contains a list of 27 stand-alone SGX projects extracted from *Awesome SGX Open Source Projects* 2019. For each project, we indicate their category, if it used the Intel SGX SDK, the number of trusted threads for each enclave of the project, and a note. We also list details for each enclave, if the project contains many. We counted 24 out of 27 projects developed on top of Intel SGX SDK, two projects use alternative SDKs (*i.e.*, Open Enclave SDK Microsoft, 2019 and Graphene Tsai, Porter, and Vij, 2017a), while one contains a simulated enclave. Among the projects based on the Intel SGX SDK, we counted a total of 31 enclaves, and 24 out of 31 are multi-threading (77%).

Category/Project	Intel SGX SDK	# of threads
Blockchain		
teechain	✓	10
private-data-objects	✓	10
	✓	1
	✓	2
fabric-secure-chaincode	✓	10
	✓	8
eevm	Open Enclave SDK Microsoft, 2019	
lucky	Based on a mock SGX implementation	
node-secureworker	✓	1
town-crier	✓	10
	✓	10
	✓	1
	✓	6
bolos-enclave	✓	1
Machine Learning Framework		
gbdt-rs	✓	1
bi-sgx	✓	1
slalom	✓	4
Applications		
sgxwallet	✓	16
sgx-tor	✓	10
	✓	10
obscuro	✓	50
channel-id-enclave	✓	10
sfaas	✓	3
phoenix	Graphene Tsai, Porter, and Vij, 2017a	
posup	✓	4
tresorsgx	✓	10
Private Key/Passphrase Management		
sgx-kms	✓	8
keystore	✓	1
safekeeper-server	✓	10
Database		
talos	✓	50
opaque	✓	10
stealthdb	✓	10
sgx_sqlite	✓	10
shieldstore	✓	8

TABLE A.1: SGX open-source projects extracted from *Awesome SGX Open Source Projects* 2019.

Appendix B

Code-Reuse Technique

To show the feasibility of SnakeGX, we choose for our proof-of-concept the technique described by Biondo et al. Biondo et al., 2018. This means that SnakeGX uses ROP. However, as stated in Section 4.1, SnakeGX does not rely on a specific technique, but it does require one to control its behavior. Moreover, we adapted their approach to work on the Intel SGX SDK newer versions.

In the original approach, the authors exploited `asm_oret()` and `continue_execution()` functions. More precisely, they crafted a set of fake frame in order to create a loop between these functions. In the x64 architecture, the first four function parameters are passed by registers. Therefore, the authors used `asm_oret()` for setting `continue_execution()` registers pointing to a controlled structure. However, as also Biondo underlined, it is more complicated to use `asm_oret()` for SDK 2.0. This is why in our approach we substituted `asm_oret()` with a *glue gadget*. This might be any gadget that sets the input register for the `continue_execution()` function. Since we developed our proof-of-concept for Linux 64bit, `continue_execution()` expects the first argument (*i.e.*, a `sgx_exception_info_t` address) in the `rdi` register. This is achievable by using a classic `pop rdi` gadget. Windows, instead, follows a different calling convention and `continue_execution()` expects an `ocall_context` address shifted by 8 byes in the `rcx` register. Therefore we used a `pop rcx` as a *glue gadget*. In our evaluation, we found `pop rdi` and `pop rcx` gadgets in the Intel SGX SDK version for Linux and Windows, respectively.

Figure B.1 describes our code-reuse technique. The attacker crafts a fake stack that can reside inside or outside the enclave, we used both approaches. The fake stack is composed by frames, one of which contains in order: (i) a *glue gadget* address, (ii) a fake `sgx_exception_info_t` address, (iii) the `continue_execution()` address. Once the first *glue gadget* is triggered, it will set `rdi` (or `rcx` in Windows) register pointing to the fake `sgx_exception_info_t` structure. Then, the `continue_execution()` will set registers according to `sgx_exception_info_t` and it will also pivot to the actual gadget. Since `continue_execution()` allows us to control all general registers, we can easily invoke another function instead of a simple gadget (*e.g.*, `memcpy` in Frame 1). Finally, the gadget will return at the beginning of the next frame. At this point, the CPU will trigger a new *glue gadget* and the attack continues.

Our technique is more flexible compared to the one described by Biondo. By using a *glue gadget*, we can easily drive `continue_execution()` without relying on other SDK functions that might change in future versions.

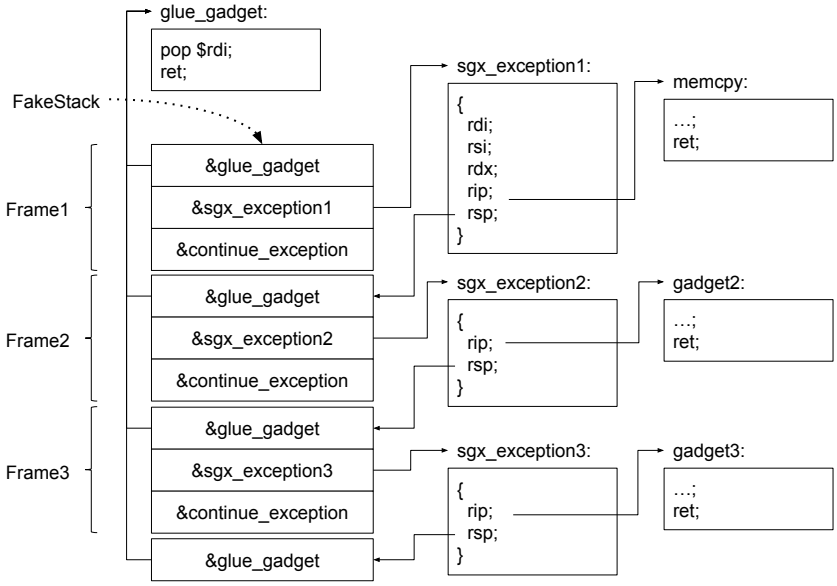


FIGURE B.1: Chain used in the proof-of-concept of SnakeGX.

Appendix C

Conditional Chain

Conditional ROP-chain, the chain is triggered by using `sgx_exception_info_t` structure that configures the initial registers (see Appendix B). The `SP` register is perturbed if the value of `&lastKey` differs from the value of `&key` in order to pivot a true or a false ROP-chain, respectively.

```
/// we set the following registers through
/// a sgx_exception_info_t structure:
/// rdi = &lastKey; last key exfiltrated
/// rax = &key; current key loaded
/// rdx = #offset; to pivot to the false ROP-chain
/// rcx = &true-chain; address of the true ROP-chain
mov eax, dword ptr [rax] ; ret
mov rdi, qword ptr [rdi + 0x68] ; ret
cmp eax, edi ; sete al ; movzx eax, al ; ret
neg eax ; ret
and eax, edx ; ret
add rax, rcx ; ret
xchg rax, rsp ; ret
// 0x80 nops for padding
// beginning of true ROP-chain
pop rdi ; ret
// context to pivot to the ROP-chain that implements the true
  branch
&context_true
// address of continue_execution function
&continue_execution
// beginning of false ROP-chain
pop rdi ; ret
// context to pivot to the ROP-chain that implements the false
  branch
&context_false
// address of continue_execution function
&continue_execution
```

C.1 Context-Switch Chain

Details of the `sgx_exception_info_t` structures used to leak the key and to switch outside the enclave. The structures are used according to the techniques described in Appendix B.

```
/* ...previous sgx_exception_info_t structures... */
// leaks the key outside the enclave
// memcpy(key, buff)
ctxPc[2].cpu_context.rsi = &key; // address of the key
ctxPc[2].cpu_context.rdi = &buff; // memory regions where leaking
    the key
ctxPc[2].cpu_context.rdx = KEY_LENGTH; // length of the key
ctxPc[2].cpu_context.rip = &memcpy;
// prepares the next boot chain in the workspace
// memcpy(boot_chain, workspace)
ctxPc[3].cpu_context.rdi = &workspace; // workspace address
ctxPc[3].cpu_context.rdx = sizeof(boot_chain);
ctxPc[3].cpu_context.rsi = &boot_chain_backup;
ctxPc[3].cpu_context.rip = &memcpy;
// set the fake OCALL frame in the enclave
// memcpy(fake_frame, enclave)
ctxPc[4].cpu_context.rdi = &fake_frame;
ctxPc[4].cpu_context.rdx = sizeof(fake_frame);
ctxPc[4].cpu_context.rsi = &fake_frame_backup;
ctxPc[4].cpu_context.rip = &memcpy;
// saves CPU extended states for asm_oret
// save_xregs(xsave_buffer)
ctxPc[5].cpu_context.rdi = &xsave_buffer;
ctxPc[5].cpu_context.rip = &save_xregs;
// sets the trusted thread as it is performing an OCALL
// update_ocall_lastsp(fake_frame)
ctxPc[6].cpu_context.rdi = fake_frame;
ctxPc[6].cpu_context.rip = &update_ocall_lastsp;
// pivots to the outside-chain
// eenclu[exit] -> outside_chain
ctxPc[7].cpu_context.rax = 0x4; // EEXIT
ctxPc[7].cpu_context.rsp = &outside_chain_stack;
ctxPc[7].cpu_context.rbx = &outside_chain_first_gadget;
ctxPc[7].cpu_context.rip = &enclu;
```

Details of the outside ROP-chains used to resume payload inside the enclave.

```
/* ...previous gadgets for shipping the password remotely... */
// gadgets to resume payload within the enclave
pop rax ; ret
0x2 // EENTER
pop rbx ; ret
&tcs_address
pop rdi ; ret // rdi = -2 -> ORET
0xfffffffffffffffe // -2
pop rcx ; ret // for async exit handler
&Lasync_exit_pointer
&enclu_urts
```

Bibliography

Abadi, Martín et al. (2005). "Control-flow integrity". In: *Proceedings of the 12th ACM conference on Computer and communications security*. ACM, pp. 340–353.

Abera, Tigist et al. (2016). "C-FLAT: control-flow attestation for embedded systems software". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, pp. 743–754.

Abera, Tigist et al. (2019). "DIAT: Data Integrity Attestation for Resilient Collaboration of Autonomous Systems". In: URL: https://www.ndss-symposium.org/ndss-paper/diat-data-integrity-attestation-for-resilient-collaboration-of-autonomous-systems/.

Amazon Web Services (AWS) (2006). Last access March 2019. URL: https://aws.amazon.com/.

Anati, Ittai et al. (2013). "Innovative technology for CPU based attestation and sealing". In: *Proceedings of the 2nd international workshop on hardware and architectural support for security and privacy*. Vol. 13.

Arnautov, Sergei et al. (2016a). "SCONE: Secure Linux Containers with Intel SGX." In: *OSDI*, pp. 689–703.

Arnautov, Sergei et al. (2016b). "SCONE: Secure Linux Containers with Intel SGX". In: *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*. Savannah, GA: USENIX Association, pp. 689–703. ISBN: 978-1-931971-33-1. URL: https://www.usenix.org/conference/osdi16/technical-sessions/presentation/arnautov.

Aumasson, Jean-Philippe et al. (2014). "BLAKE2". In: *The Hash Function BLAKE*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 165–183. ISBN: 978-3-662-44757-4. DOI: 10.1007/978-3-662-44757-4_9. URL: https://doi.org/10.1007/978-3-662-44757-4_9.

Awesome SGX Open Source Projects (2019). https://github.com/Maxul/Awesome-SGX-Open-Source. Last access June 2020.

Bajikar, Sundeep (2002). "Trusted platform module (tpm) based security on notebook pcs-white paper". In: *Mobile Platforms Group Intel Corporation* 1, p. 20.

Banescu, Sebastian and Alexander Pretschner (2017). "A tutorial on software obfuscation". In: *Advances in Computers*.

Baratloo, Arash, Navjot Singh, Timothy K Tsai, et al. (2000). "Transparent run-time defense against stack-smashing attacks." In: *USENIX Annual Technical Conference, General Track*, pp. 251–262.

Baumann, Andrew, Marcus Peinado, and Galen Hunt (2015). "Shielding applications from an untrusted cloud with haven". In: *ACM Transactions on Computer Systems (TOCS)* 33.3, p. 8.

Bellare, Mihir, Joe Kilian, and Phillip Rogaway (2000). "The security of the cipher block chaining message authentication code". In: *Journal of Computer and System Sciences* 61.3, pp. 362–399.

Biondi, Philippe and Fabrice Desclaux (2006). "Silver needle in the Skype". In: *Black Hat Europe* 6, pp. 25–47.

Biondo, Andrea et al. (2018). "The guard's dilemma: Efficient code-reuse attacks against intel sgx". In: *Proceedings of 27th USENIX Security Symposium*.

BLAKE2 (2013). Last access March 2019. URL: https://github.com/BLAKE2/BLAKE2.

Bletsch, Tyler et al. (2011). "Jump-oriented programming: a new class of code-reuse attack". In: *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM, pp. 30–40.

Brumley, David and Dawn Song (2004). "Privtrans: Automatically partitioning programs for privilege separation". In: *USENIX Security Symposium*, pp. 57–72.

Bulck, Jo Van et al. (Aug. 2018). "Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution". In: *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, 991–1008. ISBN: 978-1-939133-04-5. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/bulck.

Bzip2 (2002). Last access March 2019. URL: http://www.sourceware.org/bzip2/.

Carlini, Nicholas and David Wagner (2014). "ROP is Still Dangerous: Breaking Modern Defenses." In: *USENIX Security Symposium*, pp. 385–399.

Chang, Hoi and Mikhail J Atallah (2001). "Protecting software code by guards". In: *Digital Rights Management Workshop*. Vol. 2320. Springer, pp. 160–175.

Chen, Ping et al. (2016). "Advanced or not? A comparative study of the use of anti-debugging and anti-VM techniques in generic and targeted malware". In: *IFIP International Information Security and Privacy Conference*. Springer, pp. 323–336.

Collberg, Christian S. and Clark Thomborson (2002). "Watermarking, tamper-proofing, and obfuscation-tools for software protection". In: *IEEE Transactions on software engineering* 28.8, pp. 735–746.

Conti, Mauro et al. (2008). "Emergent properties: detection of the node-capture attack in mobile wireless sensor networks". In: *Proceedings of the first ACM conference on Wireless network security*, pp. 214–219.

Conti, Mauro et al. (2010). "The smallville effect: social ties make mobile networks more secure against node capture attack". In: *Proceedings of the 8th ACM international workshop on Mobility management and wireless access*, pp. 99–106.

Costan, Victor and Srinivas Devadas (2016). "Intel SGX Explained." In: *IACR Cryptology ePrint Archive* 2016, p. 86.

Dai Zovi, Dino (2010). "Practical return-oriented programming". In: *SOURCE Boston*.

Davi, Lucas et al. (2014). "Stitching the Gadgets: On the Ineffectiveness of Coarse-Grained Control-Flow Integrity Protection." In: *USENIX Security Symposium*. Vol. 2014.

Dessouky, Ghada et al. (2017). "LO-FAT: Low-Overhead Control Flow ATtestation in Hardware". In: *Design Automation Conference (DAC), 2017 54th ACM/EDAC/IEEE*. IEEE, pp. 1–6.

Dessouky, Ghada et al. (2018). "LiteHAX: Lightweight Hardware-assisted Attestation of Program Execution". In: *Proceedings of the International Conference on Computer-Aided Design*. ICCAD '18. San Diego, California: ACM, 106:1–106:8. ISBN: 978-1-4503-5950-4. DOI: 10.1145/3240765.3240821. URL: http://doi.acm.org/10.1145/3240765.3240821.

Dolev, D. and A. C. Yao (1981). "On the Security of Public Key Protocols". In: *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*. SFCS '81. Washington, DC, USA: IEEE Computer Society, pp. 350–357. DOI: 10.1109/SFCS.1981.32. URL: https://doi.org/10.1109/SFCS.1981.32.

Drake, Joshua D and John C Worsley (2002). *Practical PostgreSQL*. " O'Reilly Media, Inc."

Gange, Graeme et al. (2016). "An abstract domain of uninterpreted functions". In: *International Conference on Verification, Model Checking, and Abstract Interpretation*. Springer, pp. 85–103.

Ge, Xinyang, Weidong Cui, and Trent Jaeger (2017). "GRIFFIN: Guarding Control Flows Using Intel Processor Trace". In: *Proceedings of the Twenty-Second International Conference on Architectural Support for Programming Languages and Operating Systems*. ASPLOS '17. Xi'an, China: ACM, pp. 585–598. ISBN: 978-1-4503-4465-4. DOI: 10.1145/3037697.3037716. URL: http://doi.acm.org/10.1145/3037697.3037716.

Ghosh, Sudeep, Jason D Hiser, and Jack W Davidson (2010). "A secure and robust approach to software tamper resistance". In: *International Workshop on Information Hiding*. Springer, pp. 33–47.

Gilmont, Tanguy, J-D Legat, and J-J Quisquater (1999). "Enhancing security in the memory management unit". In: *Proceedings 25th EUROMICRO Conference. Informatics: Theory and Practice for the New Millennium*. Vol. 1. IEEE, pp. 449–456.

Google (2018). *Asylo*. https://github.com/google/asylo. Last access March 2020.

Graziano, Mariano, Davide Balzarotti, and Alain Zidouemba (2016). "ROPMEMU: A Framework for the Analysis of Complex Code-Reuse Attacks". In: *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. ASIA CCS '16. Xi'an, China: ACM, pp. 47–58. ISBN: 978-1-4503-4233-9. DOI: 10.1145/2897845.2897894. URL: http://doi.acm.org/10.1145/2897845.2897894.

Gullasch, D., E. Bangerter, and S. Krenn (2011). "Cache Games – Bringing Access-Based Cache Attacks on AES to Practice". In: *2011 IEEE Symposium on Security and Privacy*, pp. 490–505. DOI: 10.1109/SP.2011.22.

Hu, Hong et al. (2016). "Data-oriented programming: On the expressiveness of non-control data attacks". In: *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, pp. 969–986.

Hu, Hong et al. (2018). "Enforcing Unique Code Target Property for Control-Flow Integrity". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. Toronto, Canada: ACM, pp. 1470–1486. ISBN: 978-1-4503-5693-0. DOI: 10.1145/3243734.3243797. URL: http://doi.acm.org/10.1145/3243734.3243797.

Ibrahim, Ahmad, Ahmad-Reza Sadeghi, and Gene Tsudik (2018). "US-AID: Unattended Scalable Attestation of IoT Devices". In: *37th IEEE International Symposium on Reliable Distributed Systems*. DOI: 10.1109/SRDS.2018.00013. URL: https://ieeexplore.ieee.org/document/8613950.

Ibrahim, Ahmad, Ahmad-Reza Sadeghi, and Shaza Zeitouni (2017). "SeED: secure non-interactive attestation for embedded devices". In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 64–74.

Ibrahim, Ahmad et al. (2016). "DARPA: Device Attestation Resilient to Physical Attacks". In: *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. WiSec '16. Darmstadt, Germany: ACM, pp. 171–182. ISBN: 978-1-4503-4270-4. DOI: 10.1145/2939918.2939938. URL: http://doi.acm.org/10.1145/2939918.2939938.

Intel (2016a). *Intel SGX: Debug, Production, Pre-release what's the difference?* Last visit on 30 Nov 2017. URL: https://software.intel.com/en-us/blogs/2016/01/07/intel-sgx-debug-production-prelease-whats-the-difference.

— (2016b). *Remote (Inter-Platform) Attestation*. Last visit on 6 Dec 2017. URL: https://software.intel.com/en-us/node/702984.

— (2018). *Rijndael AES-GCM encryption API*. Last visit on 10 Mar 2017. URL: https://software.intel.com/en-us/node/709139.

Intel Architecture Instruction Set Extensions Programming Reference (2018). https://software.intel.com/sites/default/files/managed/b4/3a/319433-024.pdf?_ga=1.118002441.1853754838.1418826886. Last access November 2018.

Intel® Software Guard Extensions (Intel®SGX) - Developer Guide (2013). https://download.01.org/intel-sgx/linux-2.1.3/docs/Intel_SGX_Developer_Guide.pdf. Last access June 2020.

Intel® Software Guard Extensions Programming Reference (2013). https://software.intel.com/sites/default/files/managed/48/88/329298-002.pdf. Last access June 2020.

ISO (2015). *ISO/IEC 11889-1:2015*. Last visit 13 Nov 2017. URL: https://www.iso.org/standard/66510.html.

Kernel.org (2018). *CFS Scheduler*. Last visit on 20 Aug 2018. URL: https://www.kernel.org/doc/Documentation/scheduler/sched-design-CFS.txt.

Kil, Chongkyung et al. (2006). "Address space layout permutation (ASLP): Towards fine-grained randomization of commodity software". In: *Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual*. IEEE, pp. 339–348.

Kittel, Thomas et al. (2015). "Counteracting data-only malware with code pointer examination". In: *International Symposium on Recent Advances in Intrusion Detection*. Springer, pp. 177–197.

Kohnhäuser, Florian, Niklas Büscher, and Stefan Katzenbeisser (2019). "A Practical Attestation Protocol for Autonomous Embedded Systems". In: *4th IEEE European Symposium on Security and Privacy (EuroS&P'19)*. DOI: 10.1109/EuroSP.2019.00028. URL: http://tubiblio.ulb.tu-darmstadt.de/114633/.

Lattner, Chris and Vikram Adve (2004). "LLVM: A compilation framework for lifelong program analysis & transformation". In: *Proceedings of the international symposium*

on Code generation and optimization: feedback-directed and runtime optimization. IEEE Computer Society, p. 75.

Leavline, E Jebamalar and DAAG Singh (2013). "Hardware implementation of LZMA data compression algorithm". In: *International Journal of Applied Information Systems (IJAIS)* 5.4, pp. 51–56.

Lee, Jaehyuk et al. (2017). "Hacking in darkness: Return-oriented programming against secure enclaves". In: *USENIX Security*, pp. 523–539.

Li, J. et al. (2018). "Fine-CFI: Fine-Grained Control-Flow Integrity for Operating System Kernels". In: *IEEE Transactions on Information Forensics and Security* 13.6, pp. 1535–1550. ISSN: 1556-6013. DOI: 10.1109/TIFS.2018.2797932.

Lind, Joshua et al. (2017). "Glamdring: Automatic application partitioning for Intel SGX". In: *Proceedings of the USENIX Annual Technical Conference (ATC)*, p. 24.

Liu, Daiping, Mingwei Zhang, and Haining Wang (2018). "A Robust and Efficient Defense Against Use-after-Free Exploits via Concurrent Pointer Sweeping". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS '18. Toronto, Canada: ACM, pp. 1635–1648. ISBN: 978-1-4503-5693-0. DOI: 10.1145/3243734.3243826. URL: http://doi.acm.org/10.1145/3243734.3243826.

McSema (2014). Last access Feb 2019. URL: https://github.com/trailofbits/mcsema.

Microsoft (2015). *Control Flow Guard (CFG)*. Last visit on 28 Nov 2017. URL: https://msdn.microsoft.com/en-us/library/windows/desktop/mt637065(v=vs.85).aspx.

— (2017). *Driver Signing*. Last visit on 02 Mar 2018. URL: https://docs.microsoft.com/en-us/windows-hardware/drivers/install/driver-signing.

— (2019). *Open Enclave SDK*. https://openenclave.io/sdk/. Last access March 2020.

Microsoft Azure (2010). Last access March 2019. URL: https://azure.microsoft.com/en-us/.

Møller, Anders and Michael I Schwartzbach (2012). *Static program analysis*.

Murdock, Kit et al. (2020). "Plundervolt: Software-based Fault Injection Attacks against Intel SGX". In: *Proceedings of the 41st IEEE Symposium on Security and Privacy (S&P'20)*.

Nagra, Jasvir and Christian Collberg (2009). *Surreptitious software: obfuscation, watermarking, and tamperproofing for software protection*. Pearson Education.

Nunes, Ivan De Oliveira et al. (Aug. 2020). "APEX: A Verified Architecture for Proofs of Execution on Remote Devices under Full Software Compromise". In: *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, pp. 771–788. ISBN: 978-1-939133-17-5. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/nunes.

Oleksenko, Oleksii et al. (2018). "Varys: Protecting SGX Enclaves from Practical Side-Channel Attacks". In: *2018 USENIX Annual Technical Conference (USENIX ATC 18)*. Boston, MA: USENIX Association, pp. 227–240. ISBN: 978-1-931971-44-7. URL: https://www.usenix.org/conference/atc18/presentation/oleksenko.

Onarlioglu, Kaan et al. (2010). "G-Free: defeating return-oriented programming through gadget-less binaries". In: *Proceedings of the 26th Annual Computer Security Applications Conference*. ACM, pp. 49–58.

Pinzari, Gian Filippo (2003). *Introduction to NX technology*.

Platform, Open Mobile Terminal. *Advanced Trusted Environment: OMTP TR 1*.

Polychronakis, Michalis and Angelos D Keromytis (2011). "ROP payload detection using speculative code execution". In: *2011 6th International Conference on Malicious and Unwanted Software*. IEEE, pp. 58–65.

Porter, Donald E et al. (2011). "Rethinking the library OS from the top down". In: *ACM SIGPLAN Notices*. Vol. 46. 3. ACM, pp. 291–304.

ROPgadget - Gadgets finder and auto-roper (2011). https://github.com/JonathanSalwan/ROPgadget. Last access March 2020.

Rozas, Carlos (2013). "Intel® Software Guard Extensions (Intel® SGX)". In:

Rudd, E. M. et al. (2017). "A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions". In: *IEEE Communications Surveys Tutorials* 19.2, pp. 1145–1172. DOI: 10.1109/COMST.2016.2636078.

Sabt, M., Mohammed Achemlal, and A. Bouabdallah (2015). "Trusted Execution Environment: What It is, and What It is Not". In: *2015 IEEE Trustcom/BigDataSE/ISPA* 1, pp. 57–64.

Sailer, Reiner et al. (2004). "Design and Implementation of a TCG-based Integrity Measurement Architecture." In: *USENIX Security symposium*. Vol. 13, pp. 223–238.

Schuster, Felix et al. (2015a). "Counterfeit object-oriented programming: On the difficulty of preventing code reuse attacks in C++ applications". In: *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, pp. 745–762.

Schuster, Felix et al. (2015b). "VC3: Trustworthy data analytics in the cloud using SGX". In: *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE, pp. 38–54.

Seo, Jaebaek et al. (2017). "SGX-Shield: Enabling address space layout randomization for SGX programs". In: *Proceedings of the 2017 Annual Network and Distributed System Security Symposium (NDSS), San Diego, CA*.

SGX-Tor (2018). https://github.com/kaist-ina/SGX-Tor. Last access November 2018.

Shacham, Hovav (2007a). "The geometry of innocent flesh on the bone: Return-into-libc without function calls (on the x86)". In: *Proceedings of the 14th ACM conference on Computer and communications security*. ACM, pp. 552–561.

— (2007b). "The Geometry of Innocent Flesh on the Bone: Return-into-libc Without Function Calls (on the x86)". In: *Proceedings of the 14th ACM Conference on Computer and Communications Security*. CCS '07. Alexandria, Virginia, USA: ACM, pp. 552–561. ISBN: 978-1-59593-703-2. DOI: 10.1145/1315245.1315313. URL: http://doi.acm.org/10.1145/1315245.1315313.

Singaravelu, Lenin et al. (2006). "Reducing TCB complexity for security-sensitive applications: Three case studies". In: *ACM SIGOPS Operating Systems Review*. Vol. 40. 4. ACM, pp. 161–174.

Smith, Nathan P (1997). *Stack smashing vulnerabilities in the UNIX operating system*.

Smith, Scott F and Mark Thober (2006). "Refactoring programs to secure information flows". In: *Proceedings of the 2006 workshop on Programming languages and analysis for security*. ACM, pp. 75–84.

Snow, Kevin Z et al. (2013). "Just-in-time code reuse: On the effectiveness of fine-grained address space layout randomization". In: *Security and Privacy (SP), 2013 IEEE Symposium on*. IEEE, pp. 574–588.

Stallings, William (July 2002). "The Advanced Encryption Standard". In: *Cryptologia* 26.3, pp. 165–188. ISSN: 0161-1194. DOI: 10.1080/0161-110291890876. URL: http://dx.doi.org/10.1080/0161-110291890876.

Stancill, Blaine et al. (2013). "Check my profile: Leveraging static analysis for fast and accurate detection of ROP gadgets". In: *International Workshop on Recent Advances in Intrusion Detection*. Springer, pp. 62–81.

Stravers, Paulus and Jan-Willem van de Waerdt (2013). *Translation lookaside buffer*. US Patent 8,607,026.

Suganuma, Toshio et al. (2000). "Overview of the IBM Java just-in-time compiler". In: *IBM systems Journal* 39.1, pp. 175–193.

Technology preview: Private contact discovery for Signal (2017). https://signal.org/blog/private-contact-discovery/. Last access November 2018.

Tice, Caroline et al. (2014). "Enforcing Forward-Edge Control-Flow Integrity in GCC & LLVM." In: *USENIX Security Symposium*, pp. 941–955.

Tomlinson, Allan (2017). "Introduction to the TPM". In: *Smart Cards, Tokens, Security and Applications*. Springer, pp. 173–191.

Tsai, Chia che, Donald E. Porter, and Mona Vij (2017a). "Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX". In: *2017 USENIX Annual Technical Conference (USENIX ATC 17)*. Santa Clara, CA: USENIX Association, pp. 645–658. ISBN: 978-1-931971-38-6. URL: https://www.usenix.org/conference/atc17/technical-sessions/presentation/tsai.

Tsai, Chia-Che, Donald E Porter, and Mona Vij (2017b). "Graphene-SGX: A practical library OS for unmodified applications on SGX". In: *Proceedings of the 2017 USENIX Annual Technical Conference, Santa Clara, CA*.

Ugarte-Pedrero, Xabier et al. (2016). "Rambo: Run-time packer analysis with multiple branch observation". In: *Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, pp. 186–206.

Uhlig, Rich et al. (2005). "Intel virtualization technology". In: *Computer* 38.5, pp. 48–56.

Veen, Victor Van der, Lorenzo Cavallaro, Herbert Bos, et al. (2012). "Memory errors: The past, the present, and the future". In: *International Workshop on Recent Advances in Intrusion Detection*. Springer, pp. 86–106.

Vinayagamurthy, Dhinakaran, Alexey Gribov, and Sergey Gorbunov (2019). "StealthDB: a Scalable Encrypted Database with Full SQL Query Support". In: *Proceedings on Privacy Enhancing Technologies* 2019.3.

Visintin, Alessandro et al. (2019). "SAFEˆ d: Self-Attestation For Networks of Heterogeneous Embedded Devices". In: *arXiv preprint arXiv:1909.08168*.

Viticchié, Alessio et al. (2016). "Reactive Attestation: Automatic Detection and Reaction to Software Tampering Attacks". In: *Proceedings of the 2016 ACM Workshop on Software PROtection*. ACM, pp. 73–84.

Vogl, Sebastian et al. (2014). "Persistent Data-only Malware: Function Hooks without Code." In: *NDSS*.

Wang, Zhi and Xuxian Jiang (2010). "Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity". In: *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, pp. 380–395.

Watson, Robert NM et al. (2018). *Capability Hardware Enhanced RISC Instructions (CHERI): Notes on the Meltdown and Spectre Attacks*. Tech. rep. University of Cambridge, Computer Laboratory.

Weiser, Samuel et al. (Sept. 2019). "SGXJail: Defeating Enclave Malware via Confinement". In: *22nd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2019)*. Chaoyang District, Beijing: USENIX Association, pp. 353–366. ISBN: 978-1-939133-07-6. URL: https://www.usenix.org/conference/raid2019/presentation/weiser.

Winter, Johannes (2008). "Trusted computing building blocks for embedded linux-based ARM trustzone platforms". In: *Proceedings of the 3rd ACM workshop on Scalable trusted computing*. ACM, pp. 21–30.

Yao, Fan, Jie Chen, and Guru Venkataramani (2013). "Jop-alarm: Detecting jump-oriented programming-based anomalies in applications". In: *Computer Design (ICCD), 2013 IEEE 31st International Conference on*. IEEE, pp. 467–470.

yerzhan7. *SGX_SQLite*. https://github.com/yerzhan7/SGX_SQLite. Last access January 2019.

Yuan, Pinghai, Qingkai Zeng, and Xuhua Ding (2015). "Hardware-assisted fine-grained code-reuse attack detection". In: *International Workshop on Recent Advances in Intrusion Detection*. Springer, pp. 66–85.

Zeitouni, Shaza et al. (2017). "Atrium: Runtime attestation resilient under memory attacks". In: *Proceedings of the 36th International Conference on Computer-Aided Design*. IEEE Press, pp. 384–391.

Zhang, Mingwei and R Sekar (2013). "Control Flow Integrity for COTS Binaries." In: *USENIX Security Symposium*, pp. 337–352.

Zhou, Gang, Harald Michalik, and Laszlo Hinsenkamp (2007). "Efficient and high-throughput implementations of AES-GCM on FPGAs". In: *Field-Programmable Technology, 2007. ICFPT 2007. International Conference on*. IEEE, pp. 185–192.

ZLib (2017). Last access March 2019. URL: http://www.zlib.net/.

Zstandard (2016). Last access March 2019. URL: https://facebook.github.io/zstd/.