

Trusted Reference Monitors for Linux using Intel SGX Enclaves

Alexander Harri Bell-Thomas
Jesus College



*A dissertation submitted to the University of Cambridge
in partial fulfilment of the requirements for the degree of
Master of Engineering in Computer Science*

University of Cambridge
Computer Laboratory
William Gates Building
15 JJ Thomson Avenue
Cambridge CB3 0FD
UNITED KINGDOM

Email: Alexander.Bell-Thomas@cl.cam.ac.uk

June 12, 2020

Declaration

I, Alexander Harri Bell-Thomas of Jesus College, being a candidate the Part III of the Computer Science Tripos, hereby declare that this report and the work described in it are my own work, unaided except as may be specified below, and that the report does not contain material that has already been used to any substantial extent for a comparable purpose.

Total word count: 0

Signed:

Date:

This dissertation is copyright © 2020 Alexander Harri Bell-Thomas.
All trademarks used in this dissertation are hereby acknowledged.

Abstract

Write a summary of the whole thing. Make sure it fits in one page.

Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 1 |
| 2 | Background | 3 |
| 2.1 | Information Flow Control | 3 |
| 2.1.1 | Motivation, History, and <i>Decentralised IFC</i> | 4 |
| 2.1.2 | Security Labels and the Reference Monitor | 5 |
| 2.1.3 | Modelling | 6 |
| 2.2 | Intel SGX | 8 |
| 2.2.1 | Security Characteristics | 9 |
| 2.2.2 | Architecture and Implementation | 10 |
| 2.2.3 | Enclave Lifecycle | 12 |
| 2.2.4 | Attestation | 14 |
| 2.2.5 | Sealing | 16 |
| 2.2.6 | SGX Versions | 16 |
| 2.3 | Aspects of the <i>Linux</i> Kernel | 17 |
| 2.3.1 | Virtual File System | 17 |
| 2.3.2 | Linux Security Modules | 18 |
| 3 | Related Work | 21 |
| 3.1 | <i>Flume</i> and <i>CamFlow</i> | 21 |
| 3.2 | Interoperation between Linux and SGX | 23 |
| 3.3 | Dataflow Protection using SGX | 24 |
| 4 | Design and Implementation | 25 |
| 4.1 | Motivation | 25 |
| 4.2 | Challenges | 26 |
| 4.3 | The CITADEL IFC Model | 29 |
| 4.3.1 | Reservations | 29 |
| 4.3.2 | Permissible Operations | 30 |
| 4.4 | Implementation | 32 |

| | | |
|----------|--------------------------------|-----------|
| 5 | Evaluation | 33 |
| 6 | Summary and Conclusions | 35 |

List of Figures

| | | |
|-----|--|----|
| 2.1 | Abstract overview of SGX's protection in an adversarial environment. . | 9 |
| 2.2 | A high-level overview of the SGX hardware and software architecture. | 10 |
| 2.3 | The process of creating and initialising an enclave; details given in § 2.2.3. Purple components belong to the SGX platform. | 13 |
| 4.1 | Abstract <i>syscall</i> control flow route. Grey components show the natural Linux design. Green additions highlight the externalised enclave LSM component. | 27 |
| 4.2 | | 28 |
| 4.3 | Abstract overview of an SGX enclave's protections. | 32 |

List of Tables

| | | |
|-----|---|----|
| 2.1 | Overview of the four core IFC events used in § 2.1.3. | 6 |
| 2.2 | Overview of notable SGX x86 instructions in an enclave’s lifecycle. [1] | 15 |

Chapter 1

Introduction

The task of defending computer systems against malicious programs and enforcing the isolation of protected components has always been exceedingly challenging to achieve. A system's *Trusted Computing Base*, or *TCB*, defines the minimal set of software, firmware, and hardware components critical to establish and maintain system security and integrity. This traditionally includes, amongst others; the OS kernel; device drivers; device firmware; and the hardware itself. Compromise of a trusted component inside a system's *TCB* is a direct threat to any secure application running on it. A common approach to hardening a system's security is to minimise its *TCB*, diminishing its potential *attack surface*.

A increasingly common trend is the outsourcing of a system's physical layer to a foreign party, for example a *cloud provider* — this is beneficial both in terms of cost and flexibility, but confuses many security considerations which assume that the physical layer itself can be trusted. In this context there is no guarantee of this, as the physical layer is usually provided as a *virtual machine*, inflating the system's *TCB* with an external and transparent software layer, the underlying *hypervisor*.

Trusted Execution Environments, *TEEs*, is a concept that has been explored by the security community for a very long time as potential protection against this. It generates isolated processing contexts in which an operation can be securely executed irrespective of the rest of the system — one such example is software *enclaves*. *Enclaves* are

general-purpose *TEEs* provided by the CPU, protecting the logic found inside at the architectural level. Intel’s Software Guard Extensions (SGX) is the most prolific example of a *TEE*, affording a *black-box* environment and runtime for arbitrary apps to execute under.

An alternative approach to policing components in a system is via the use of *Information Flow Control* (IFC). Enforced using a *reference monitor*, IFC models how and where data is allowed to move and be manipulated by a system at a granular level.

The aim of this work is to explore methods of hardening Linux with an SGX-driven *reference monitor* to track and protect host OS resources using IFC methods. Further, it aims to reason what the future relationship between an OS and the enclaves it hosts should be, and whether complete isolation between them is the natural answer in a number of common situations.

Contributions

- A prototype implementation of a modular *reference monitor* protected using Intel SGX, empowering *information flow control* techniques to operate with autonomy and protection from the host operating system. Enforcement is achieved using a *Linux Security Module* embedded in the Linux kernel, with an overall *TCB* of only a minimal footprint of the kernel alongside the enclave application.
- A userspace interposition library to near-transparently integrate unmodified applications to fully function under the new restrictions.
- A full port of the *libtomcrypt* cryptography library for use inside an SGX enclave.
- A rigorous investigation of the performance implications of this approach, featuring a lightly-modified version of the *Nginx* production webserver. Worst-case performance shows a 35% decrease in request throughput, with the common case reporting 7 – 11%. Additionally we report a median overhead of $39\ \mu s$ (IQR $26 - 72\ \mu s$, $n = 10^6$) per affected *system call*, matching or surpassing similar, non-enclave-based, systems.

Chapter 2

Background

This chapter will cover a number of topics essential to understanding the rationale and implementation of the design as discussed in § 4. These include; an introduction to *Information Flow Control (IFC)*, the Intel SGX platform, and an overview of key aspects of the Linux kernel relevant to the architecture of the prototype.

2.1 Information Flow Control

IFC regulates how and where data is permitted to move and be transformed in a computer system. [2] This differs from access control, which defines *what* resources may be used by an entity — IFC allows granular control over *how* they may be used once accessed, including restricting propagation between components.

Formally, IFC defines and enforces a non-interference policy between abstract *security contexts*. A simple, atomic example is the distinction between *unclassified* and *classified* data — here, information is only allowed to flow *up*, ensuring that an *unclassified* entity does not learn anything marked as *classified*. [3] In general this form of relationship can be represented as a partial ordering over *security contexts*, formulated as a lattice. [4]

However, practical systems often require dataflow adhering to a more complicated policy set — for example, supporting *declassification*. [5] Work undertaken by Pasquier et al., [6] which will be the core influence of the IFC model developed in this project, constructs a pliable and efficient *decentralised information flow control (DIFC)* model suitable for provenance enforcement and auditing in the Linux kernel.

The concepts presented are primarily derived from Pasquier [6] and Krohn et al. [7].

2.1.1 Motivation, History, and *Decentralised IFC*

IFC has, in recent years, been increasing in support as a powerful methodology for ensuring granularly privacy whilst simultaneously not unduly restricting access to sensitive information. IFC annotates data records with opaque *labels* that refer to either their confidentiality or integrity status. Rather than simply restricting access to sensitive data, as would be the action taken by an access control mechanism, IFC opts to track data as it propagates — if an entity attempts to move this into an unknown, untrusted, or conflicting *security context* the IFC system prevents this to ensure data is not improperly released.

IFC originated from research conducted in the mid-1970s [4] but has not, as of yet, seen mainstream adoption. A major reason for this is that early schemes were designed around the *multi-level security (MLS)* doctrine set out in the *Orange Book*: [8] this locked IFC to a shallow set of broad labels, mirroring existing institutional segregation (such as *restricted*, *secret*, *top secret*). Policies were managed centrally, something easily applicable in settings with rigorous hierarchies such as the military, but unwieldy in an organisation with manifold security protocols.

The majority of recent research in this area has advocated *decentralised information flow control (DIFC)*, introduced by Myers and Liskov. [9, 10, 11] DIFC is more granular than schemes adhering to the *MLS* model, for example, creating two distinct *security contexts* for two files in the same folder. Policies are *discretionary*, allowing users to specify and modify the enforced policies for assets they own.

2.1.2 Security Labels and the Reference Monitor

A DIFC system relies on *tags* and *labels* to annotate the entities it tracks. Let \mathcal{T} be a large set of opaque tokens, or *tags*. An individual tag does not carry any particular meaning by itself, but is used as an abstract identifier for the integrity or secrecy of an entity's *security context*. A *label*, $l \subseteq \mathcal{T}$, is a collection of tags that are concretely attached to assets, such as files; these form a lattice under the subset-relation partial order. For each process a there are two labels, one for secrecy, a_s , and one for integrity, a_i . For a tag t , $t \in a_s$ implies, conservatively, that process a has seen information associated with tag t . Likewise, $t \in a_i$ indicates that every input to a has been endorsed for an integrity level marked with t .

Walkthrough — Secrecy Enforcement In a typical environment, a user can only convince themselves that a text editor is safe to use if they, or someone they trust, audits the program's source code. With IFC however, it is possible to reason that if the system can provide the following four guarantees, it cannot leak sensitive data without the user's permission.

1. If a process a read a file with a secrecy tag t , then $t \in a_s$.
2. $t \in a_s$ implies that a cannot communicate with another process, b , where $t \notin b_s$.
3. a cannot remove t from a_s without permission.
4. $t \in a_s$ restricts a 's access to an uncontrolled medium, such as a network.

The heart of an IFC implementation is its *Reference Monitor*, which tracks the labelling for each process, granting or rejecting permission to execute an operation before being served to the operating system. Different solutions handle this process differently: *Flume*, [7] for example, implements a full system interposition layer, forcing all *syscalls* to pass through its userspace *reference monitor* before reaching the OS, whereas *CamFlow* [6] embeds its *reference monitor* in the kernel itself. In all schemes, however, this trusted component is responsible for the policy and its enforcement on the system. This project focusses on this implementation.

| Notation | Explanation |
|-----------------------------|--|
| $A \rightarrow B$ | Rule α ; a permissible information flow between entity A and entity B . |
| $A \Rightarrow B$ | Rule β ; a creation flow, initialising B from A as its parent. |
| $A \rightsquigarrow A'$ | Rule γ ; a context change, with A modifying its security context in accordance with its capabilities. |
| $A \xrightarrow{t_x^\pm} B$ | Rule δ ; privilege delegation, with A passing a capability t_x^\pm to B . |

Table 2.1: Overview of the four core IFC events used in § 2.1.3.

2.1.3 Modelling

In centralised IFC schemes, the reference monitor is the only entity capable of creating, changing, and assigning tags. DIFC modifies this, giving *all* processes the ability to create and modify tags for entities they hold ownership over; thus they alone have the right to declassify them.

Notation As the model we build in § 4 is closest in spirit to *CamFlow*, we, for clarity in comparison, use the same notation (as summarised in Table 2.1).

Enforcing Safe Flows (α) , below, describes the conditions in which a flow can be considered *safe*, abiding by the system’s IFC policy. Verbally, the recipient must be *at least as privileged* as the originator and cannot accept information graded below its own integrity status. Here \preceq denote any applicable preorder relation; this context uses inclusion (\subseteq). If a flow is *impermissible* it is denoted as $A \nrightarrow B$.

$$A \rightarrow B \iff A_s \preceq B_s \wedge B_i \preceq A_i \quad (\alpha)$$

Information produced within a *security context* may only flow within the same context or a related *subcontext*. Integrity functions in the same way but in the inverse; data can only flow in contexts with the same, or lower, integrity grading.

Entity Creation Correct initialisation of a new object's *security context* is shown in (β) . Logically it must be held at the same level as the environment creating it. An illustrative example is a process creating a new file; although permitted the result is subject to the same tainting as the original process.

$$A \Rightarrow B \implies A_s = B_s \wedge A_i = B_i \quad (\beta)$$

Vocational Label Management The core mantra of the *decentralised* aspect of DIFC is that processes are themselves responsible for policies governing the assets they own. To this end, a process's labelling must be dynamic. Generally, entities can be sorted into two distinct categories;

- *Active* (processes), with *mutable* security contexts.
- *Passive* (files, pipes, sockets, etc.), which merely act as data vessels for *active* entities.

Active entities have the right to modify their labelling iff they have the capability to make that modification. These capabilities come in two forms; one for addition and one for removal of tags. The set $A_s^+ \subseteq \mathcal{T}$ enumerates all the tags that entity A has the ability to add to its security labelling. Likewise, $A_s^- \subseteq \mathcal{T}$ holds all of the tags A has the ability to remove from its labelling. These sets are modified either in the process of creating an entity or in receipt of a delegated capability from a peer. The sets $A_i^\pm \subseteq \mathcal{T}$ also exist, performing the same function for integrity labels. (γ) describes this process formally.

$$\left\{ \begin{array}{ll} A'_x \leftarrow A_x \cup \{t\} & \text{if } t \in A_x^+ \\ A'_x \leftarrow A_x \setminus \{t\} & \text{if } t \in A_x^- \end{array} \right\} \implies A \rightsquigarrow A' \quad (\gamma)$$

A notable restriction is that a process has to be aware of the IFC constraints imposed on it and how to interact with the system to perform this operation. Most processes should not require this, but is an important consideration when applying DIFC to an entire system.

Capability Lifecycle and Delegation As defined by (β) , an entity automatically inherits the labelling of its creator: this process, however, does not pass on any capabilities ($A_s^\pm, A_i^\pm = \emptyset$). This raises the need for *capability delegation*.

A capability held by A , t_x^\pm , where $t \in A_x^\pm$, is permitted to be transferred to B in order for it to act on its behalf. Delegation is denoted as follows in (δ) .

$$A \xrightarrow{t_x^\pm} B \text{ only if } t \in A_x^\pm \quad (\delta)$$

As an example, delegation is vital for a web server. To transmit another entity's information over an untrusted socket the server must have permission to *declassify* it — i.e. it must hold f_s^- , where f is the secrecy label of the information to transmit.¹

Conflict of Interest The *CamFlow* model additionally specifies a formalisation to avoid violating mutually exclusive tag-pairs being held simultaneously. This will be discussed in further detail in § 5.X,² but is not essential to add to our understanding at this point.

2.2 Intel SGX

Intel's Software Guard Extensions, SGX, was first announced and detailed in a handful of whitepaper documents published from 2013. [12, 13, 14, 15] It described a novel approach to *trusted computing*, creating in-CPU containers with dedicated protected memory pools. These regions, called *enclaves*, cannot be read from or written to by an unauthorised party due to fundamental protection mechanisms provided by the x86 architecture, even if running in *Ring 0*:³ Figure 4.3 illustrates this. *Enclaves* guarantee both integrity and secrecy to the application running inside it, even in the presence of a malicious host.

¹The server process, W , must have $W_i = \emptyset$ as it holds a connection to an untrusted socket. Thus the integrity clause in (α) will not interfere.

²TODO link

³x86 offers four protection *rings*, of which Linux uses two — 0 for the kernel, and 3 for userspace.



Figure 2.1: Abstract overview of SGX’s protection in an adversarial environment.

Motivation At a high-level SGX aims to achieve security for sensitive applications by shielding them, and the resources they use, against tampering, and to provide a guarantee to end-users of an enclave’s integrity; this is achieved using attestation and measurement (described in § 2.2.4). One of many use cases [16, 17, 18] is in a cloud computing context, where users are forced to trust an outside party with both their data and business logic. By distributing encrypted, yet executable, containers targetted at a single, unique SGX core, users can be assured that their information is safe, regardless of any virtualisation that may be taking place. Only the provisioned CPU is able to decrypt and execute the enclave, strictly in accordance with the restrictions of the SGX platform.

2.2.1 Security Characteristics

At its heart SGX is designed to be *trustworthy*; this is achieved in a number of ways, including robust enclaving provisioning, sealing and attestation. Intel enumerates SGX’s protections [13, 19] as follows;

- Memory is secured against observation and modification from outside the enclave, achieved using an in-die *Memory Encryption Engine (MEE)*, [20] with a secret that rotates on every boot. This protection notably works against host hypervisors, other enclaves, and anything running in supervisor mode.
- Enclaves can *attest to*, or prove, their identity to a challenger with the help of a permanent hardware security key for asymmetric encryption.



Figure 2.2: A high-level overview of the SGX hardware and software architecture.

- Software calls are proxied to prepare and transfer control in and out of an enclave. Arguments are securely marshalled according to a static enclave definition.
- SGX does not defend against reverse engineering or side-channel attacks: [21] this is the responsibility of the developer to mitigate.
- Debugging support is only provided via a specialised tool and only when an enclave is compiled with debugging enabled.

2.2.2 Architecture and Implementation

The SGX platform comprises a number of interlocking parts, as shown in Figure 2.2. Working from the hardware up, at the heart of the platform is the extended x86 instruction set and memory protection provided by an SGX-capable CPU. Information as reported by [15, 22].

Hardware Enclaves’ data and code is stored securely in *Processor Reserved Memory, PRM*; this is a set of pages in system memory that are presided over by the *MEE*. DMA⁴

⁴Direct Memory Access

to *PRM* is always rejected. *PRM* consists of two data structures; the *Enclave Page Cache Map* (*EPCM*) and the *Enclave Page Cache* (*EPC*). An individual enclave is defined by an *SGX Enclave Control Structure*, *SECS*; this is generated when an enclave is created and stored in a dedicated entry in the *EPC*. An enclave's *SECS* contains important information such as its (system) global identifier, its measurement hash (*MRENCLAVE*, § 2.2.4) and the amount of memory it is using. Access control information is stored in the *EPCM* alongside page validity flags, the owning enclave identifier and the page's type; this is not accessible in software. An attempt to resolve a page in *PRM* is successful only if the CPU is executing in enclave mode and its *EPCM* entry states it belongs the currently executing enclave — if this is not the case the lookup returns an unused page from generic system memory.

The host OS or hypervisor manages the *EPC* just as it does with standard system memory, swapping pages in and out according to its own policy, but must do so using SGX specific instructions. The *MEE* is responsible for ensuring the integrity and confidentiality of this process, encrypting and decrypting pages as they cross the *PRM* boundary. Data is verified with the use of an integrity tree, and encryption keys are generated at boot-time. Importantly the SGX architecture relies on the host OS being SGX-aware, empowering userspace applications to function without privilege; this is provided by the SGX driver, *isgx*.

Userspace services Starting an enclave requires a *launch token* to be retrieved from Intel's *Launch Enclave*; this checks the signature and identity of the enclave to ensure it is valid. Access to the *Launch Enclave* and other architectural enclaves is provided by the AESM service; the userspace SGX libraries facilitate the communication mechanism. Other architectural enclaves include;

- The *Provisioning Enclave* — this verifies the authenticity of the platform and retrieves an enclave's *attestation key* from the *Intel Provisioning Service*'s servers.
- The *Quoting Enclave* — this provides trust in the identity of the SGX environment and enclave being attested, by converting the locally generated *attestation key* to a remotely-verifiable *quote*.

Third-party enclaves Enclaves can only be entered via userspace, as detailed in § 2.2.3, and are always accompanied by a host application which acts as its untrusted counterpart. The host application calls the SGX SDK to build an enclave on its behalf using an enclave image, packaged as a standard shared library (`enclave.so`) and returns its *global identifier*. Control is passed from the host application to the enclave by invoking an enclave function via an *ECALL*. Execution flow can temporarily leave the enclave if it calls one of the host application’s functions via an *OCALL*. Execution naturally leaves enclave-mode when an *ECALL* terminates. Both *ECALLs* and *OCALLs* are defined statically in the enclave’s interface definition (`enclave.edl`), and the necessary glue code is generated by the SGX SDK’s build toolchain at compile time; this ensures calls crossing the enclave boundary are marshalled safely and correctly.

2.2.3 Enclave Lifecycle

SGX instructions can be separated into two distinct groups; privileged and unprivileged. These, alongside a description of the function they perform, are enumerated in Table 2.2.⁵ The following description of the process of creating an enclave is illustrated in Figure 2.3.

Preparing an enclave Execution begins with the host application; it needs to initiate the creation process, but must do so via a component with *Ring 0* privilege. This facility is provided by *isgx*, the SGX driver. The application first requests *isgx* to allocate the requisite number of pages to run the enclave $\langle 1 \rangle$;⁶ this is tracked and served from the driver’s internal state $\langle 2 \rangle$.

The application continues by executing *ECREATE* with the metadata of the enclave to be loaded $\langle 3 \rangle$; the *MEE* checks that the pages being claimed are in fact vacant and populates the *SECS* page with the necessary information $\langle 4 \rangle$. Once this is complete the application prepares the remaining *EPC* pages using *EADD* $\langle 5 \rangle$ and loads the enclave’s code and data $\langle 6 \rangle$.

⁵A handful of instructions not relevant to the explanation given here are omitted.

⁶These numbers correspond to events in Figure 2.3.



Figure 2.3: The process of creating and initialising an enclave; details given in § 2.2.3. Purple components belong to the SGX platform.

At this point the enclave needs to be measured — the application calls `EEXTEND` $\langle 7 \rangle$, triggering the *MEE* to update the measurement hash in the *SECS* to aligns with the current state of the enclave’s memory $\langle 8 \rangle$. Once the *EPC* memory is prepared the application requests for it to be finalised using `EINIT` $\langle 9 \rangle$: this operation requires the application to retrieve the `EINITTOKEN` from the *Launch Enclave*, locking the execution of the measured enclave to the CPU the token is generated on. Notably, pages cannot be added after `EINIT`,⁷ and an enclave cannot be attested to or entered before it. Finally, the initialised flag is set in the *SECS* and the enclave’s hash updated for the final time $\langle 10 \rangle$.

Stepping into the enclave Once an enclave is created it can be invoked using the `EENTER` instruction; this can only jump to code explicitly defined in the enclave’s interface definition and switches the CPU core to enclave mode. SGX uses a flag in the CPU core’s *Thread Control Block* to prevent any other logical core following the current

⁷This is only strictly true in SGXv1, as explained in § 2.2.6.

one into the enclave.

Interrupts and exceptions can be served to the enclave, just as with any other application. However, control is not immediately passed over to the defined handler. Instead, the enclave's current state is saved and cleared to ensure no data is leaked. The *Asynchronous Enclave Exit* routine is then invoked and enclave mode disabled. Execution post-interruption is restarted with the ERESUME instruction. Once an enclave has finished executing the registers are erased and EEXIT called. Enclaves are terminated using the EREMOVE command; all claimed *EPC* pages are marked as invalid and the *SECS* page deleted.

A significant design decision made in the SGX architecture is that enclaves cannot be entered by a process operating in *Ring 0*; [1] the required instructions simply aren't available. This forces all host applications to run in userspace, making interoperation with the kernel challenging, as will be discussed in § 4.

2.2.4 Attestation

An essential feature of the *trusted computing* model SGX creates is attestation, the process of verifying both the authenticity and integrity of components cryptographically. SGX achieves by creating two hashed values, or *signing identifiers*, per enclave; MRENCLAVE and MRSIGNER. [14, 23]

MRENCLAVE acts as a unique identifier for the contents of an enclave. It is generated by hashing the instructions and data passed when creating the enclave with ECREATE, EADD, and EEXTEND; the value is finalised and stored in the *SECS* on EINIT. This value depends on the exact content and ordering of the enclave's *EPC* pages. As long as the enclave's source remains the same, so will its MRENCLAVE.

MRSIGNER, also known as the enclave's *Sealing Identity*, is generated during the enclave build process — all production enclaves need to be signed using an RSA key provided by the compiling user (the *Sealing Authority*). The public key from this pair is stored in *SIGSTRUCT*, the *Enclave Signature Structure*. During an enclave's launch

| Execution Mode | Instruction | Function |
|----------------|-------------|---|
| Ring 0 | ECREATE | Generate and copy the <i>SECS</i> structure to a new page in the <i>EPC</i> , initialising a new enclave. |
| | EADD | Add a new <i>EPC</i> page for the current enclave; this is used to load initial code and data. |
| | EEXTEND | Updates the enclave's measurement during attestation; modifies the <i>SECS</i> . |
| | EINIT | The terminal instruction in an enclave's initialisation, finalising its attributes and measurement. |
| | EREMOVE | Permanently remove a page from the <i>EPC</i> ; usually invoked during enclave destruction. |
| Ring 3 | EENTER | Transfer control from the host application to a pre-determined location in an enclave. |
| | ERESUME | Re-enter the enclave after an interrupt/exception and resume execution. |
| | EEXIT | Restore the original operating mode at the location EENTER was triggered and flush the TLB. |
| | EGETKEY | Access platform cryptography keys required for attestation and sealing. |
| | EREPORT | Generate a <i>report</i> for an enclave's <i>attestation key</i> for an attestation process. |

Table 2.2: Overview of notable SGX x86 instructions in an enclave's lifecycle. [1]

its signed compile-time MRENCLAVE value (held in *SIGSTRUCT*) is decrypted and cross-referenced with a freshly-computed runtime MRENCLAVE value to detect tampering. MRSIGNER is the same for all enclaves signed by the same *Sealing Authority*.

Local Attestation Two enclaves resident on the same system are able to attest their identities to each other using their MRENCLAVE and MRSIGNER values; this usually precedes the establishment of a shared secret (using a variant of *Diffie-Hellman* backed by the platform’s master SGX key)⁸ for confidential communication between them.

Remote Attestation In addition to attestation between entities on the same platform, the Intel specification also provides a workflow for an enclave to attest its identity to a remote party. The system’s *Quoting Enclave* verifies an enclave’s local *quote* and creates a digital signature of it using the CPU’s permanent hardware SGX private key. Through the use of an *Intel Enhanced Privacy Identifier (EPID)* [24] this process can be carried out anonymously; it relies on information encoded in the CPU during the manufacturing process. The *Provisioning Enclave* assists in this process, especially as production enclaves are required to attest with Intel’s provisioning service [23] before executing. Remote attestation is not explicitly required in this project’s architecture hence will not be covered in any further detail.

2.2.5 Sealing

Sealing refers to the encryption of data using a key related to the generating enclave; this key is unique to that enclave on a particular platform. SGX offers two policies for deriving the encryption key based on the platform’s *Root Sealing Key* — relative to the current enclave (MRENCLAVE) or the current enclave’s *Sealing Authority* (MRSIGNER). These serve many use cases, including, for example, allowing state to persist through enclave upgrades.

2.2.6 SGX Versions

At the time of writing there are two versions of SGX available, *v1* and *v2* — the details given here relate to *v1* as this project will be compatible with both. *v2* offers a number

⁸Note for Harri: must check these details.

of improvements on which this project does not rely, including: (a) dynamic memory management, (b) eased production enclave restrictions (‘Flexible Launch Control’), (c) increased PRM size support, and (d) support for virtualisation.

2.3 Aspects of the *Linux* Kernel

Linux needs little introduction. First created in 1991 as an open-source alternative to UNIX, it now powers over 90% of *the cloud* and 85% of smartphones. With almost 25,000 contributors to the kernel, it is immensely complex, with numerous interlocking parts. This section shall provide a brief overview of a small subset of them to support the information given in § 4.

2.3.1 Virtual File System

Linux represents almost every component as a file, for example including sockets, terminals, and driver interfaces. The role of providing this abstraction falls to the VFS, the core function of which is as a transparent layer, routing requests to the correct underlying implementation. This virtual interface relies on the following mechanisms.

Superblocks The *superblock* attached to an entity represents the characteristics and properties of the filesystem in which it sits. The metadata it holds includes: the block size, statistics on available blocks, the size and location of the filesystem inode tables, the disk block map, and block grouping data. An important marker held in the superblock is its *magic value*; this predefined code⁹ indicates the underlying implementation the filesystem belongs to. Examples include *EXT4* (EXT4_SUPER_MAGIC), *pseudo terminal devices* (Linux shells, DEVPTS_SUPER_MAGIC), or sockets via *SockFS* (SOCKFS_MAGIC).

Inodes The *inode* data structure represents information about a single file existing on a file system. All objects, not only files are *backed* by inodes. No pathname is assigned at this level; this is provided at a higher level of abstraction. An inode does

⁹Defined in `include/uapi/linux/magic.h`.

however indicate ownership information, access restrictions and content type, and is identified by its *inode number*.

Dentries Each item in the *direct entry cache* (*dcache*), shortened to *dentry*, represents a connection between an inode and the path it resides at in the VFS. This glue layer is responsible for building the tangible folder structure, and as the name suggests, metadata caching. A *file* consists of a *dentry-inode* pair.

File descriptors Whenever a process opens a file, it is presented with a *file descriptor* by the kernel (via `open()` or similar). This structure is unique to a process, providing the gateway between the process and the underlying file it describes. All active descriptors can be viewed at `/proc/<pid>/fd/`; for standard processes `0` globally refers to *stdin*, `1` to *stdout*, and `2` to *stderr*. Reads and writes to a file (or socket, pipe, etc.) are performed on the relevant file descriptor, not the object directly.

Extended Attributes

Files can have additional, external, key-value pairs attached to them. These attributes, shortened to *xattrs*, are permanent and saved to disk alongside the file's content. Values are optional and may be left empty if the attribute is just a flag, but if a value is specified it must be in the form of a null-terminated string. *xattrs* are namespace-padded to define different classes of functionality; the user namespace is open to all (e.g. `user.example_attribute`), but `trusted`, `system`, and `security` are reserved for specific uses by the kernel — the `security` namespace belongs exclusively to LSMs (§ 2.3.2).

2.3.2 Linux Security Modules

Linux supports the inclusion of third-party security models in the kernel itself using a unified framework, LSM. This provides developers with *hooks* into kernel functionality at every point a userspace *syscall* is about to access fundamental kernel primitives, such as inodes or task control structures. Each of these hooks can influence the behaviour of the kernel by allowing or denying the operation.

LSM attaches a `void*` security field to every instance of kernel primitives, such as `struct inode`, to allow security implementations to attach additional state to each, tracking them in whatever way is most appropriate. Decisions taken within an LSM affect all aspects of a Linux system; *superuser* privilege cannot override it and every component in the system can be restricted.

Integrity Measurement Architecture

Linux's IMA subsystem is responsible for calculating the hashes of files and programs as they are loaded (*measurement*), verifying them against an allowed list if required (*appraisal*). Its driving purpose is to detect if files have been maliciously altered either remotely or locally; the file's hash is stored as an *xattr* (`security.ima`). IMA supports many use cases, the majority of which are complementary to the LSM framework, but we shall focus on one here — EVM.

The Linux *Extended Verification Module*, *EVM*, hardens IMA by protecting *xattrs* in the security namespace — this covers both the IMA hash and any labels created by security modules. Two tamper-detection methods are provided:

1. The *HMAC-SHA1* hash of the security namespace is stored as `security.evm` for reference, and
2. A digital signature of this value is stored alongside using a key that is sealed either using a *TPM*¹⁰ or passphrase.

¹⁰Trusted Platform Module. [25]

Chapter 3

Related Work

There is a wealth of prior theoretical and practical research that form an essential background to the work presented here. To provide adequate grounding, a handful of the most notable shall be discussed — these are split into two distinct fields, *Information Flow Control* and Intel SGX. Little study has been conducted in this overlap, but where it exists, it will be highlighted as appropriate.

3.1 *Flume and CamFlow*

Both *Flume* [7] and *CamFlow* [6] present practical DIFC systems for generic, OS-level protection in Linux. The models they use are not too dissimilar, with *CamFlow* adopting and refining the basic *Flume* approach. A detailed overview of the *CamFlow* model has already been presented in § 2.1, but the difference in how the two works were implemented are important to understand.

Flume *Flume* takes the form of a userspace reference monitor. Processes confined by Flume are not able to perform most *syscalls* directly — an *interposition layer* replaces *syscalls* with IPC to the reference monitor, which enforcing IFC policies and ensuring operation safety on processes' behalf. The majority of complexity lies in the reference monitor, with its LSM only a small auxiliary companion. The authors report a 30 – 40% overhead.

CamFlow Contrasting with *Flume*, the *CamFlow* core IFC implementation lies entirely within its LSM, efficiently exploiting kernel functionality to minimise the overhead it creates. An 11% average overhead is reported for file operations in microbenchmark tests.

Other IFC Systems

Many different approaches to IFC have been published; the most influential to this project will be briefly summarised.

Asbestos is a prototype OS by Efstathopoulos et al. [26] that provides entity labelling and isolation as an OS primitive. Applications express individual policies via a custom kernel interface, and all dataflow is protected, including IPC and system-wide information flows. Additionally, a novel event abstraction and sub-process *security contexts* allows processes to act on behalf of multiple entities. *HiStar* (Zeldovich et al. [27]) builds on the *Asbestos* model, minimising the size of the system’s TCB — the system has no notion of *superuser*, with no code other than the kernel being fully trusted. An important consequence of this is that the risk of data leaking via *covert channels* is drastically reduced. *DStar* (Zeldovich et al. [28]) translates *HiStar* into a distributed context, translating labels between IFC-enabled hosts with the help of a globally-meaningful set of tags. In contrast, *Aeolus* (Cheng et al. [29]), derived from *Asbestos*, deploys a common TCB across all nodes in a distributed system to enforce IFC; it filters I/O and both inter- and intra- process communication.

Laminar (Roy et al. [30]) takes a similar approach to *Flume*, using an LSM for policy enforcement, but extends it with customisation to the JVM¹ to support thread-level isolation and heap-object protection. This approach has proved powerful in applying DIFC to popular processing systems such as *MapReduce* [32] and *Hadoop*. [33]

¹Java Virtual Machine. [31]

3.2 Interoperation between Linux and SGX

The relationship between SGX and Linux has at times been difficult; Intel has been attempting to upstream *isgx*, the SGX driver, into the mainline kernel for 6 years.² A source of extreme friction lies in the fact that enclaves are not operable in ring-0, forcing research seeking to use SGX to harden the kernel itself to be creative about how to integrate it.

The *TresorSGX* [34] project was one of the first to consider the practicalities of this relationship seriously, constructing an externalised interface for kernel functionality to be offloaded to an enclave via a specialised kernel module. Mainly focusing on disk encryption, the prototype achieved its security goals but struggled with performance, only being able to perform at 1% the bandwidth of its kernel-embedded counterpart. As concluded by the authors, the most prevalent performance hit came from kernel \leftrightarrow enclave communication overhead, made worse by the need to exit and re-enter kernel-mode.

Various other studies touch upon these issues, including:

- *Custos* (Paccagnella et al. [35]); tamper-detection for audit logs using SGX. The design attaches itself to the pre-existing Linux Audit Framework, deliberately avoiding execution tied to the kernel. Performance overheads are declared as 2 – 7%.
- *DelegaTEE* (Matetic et al. [36]); credential delegation between two computer systems by enforcing either centrally brokered or P2P³ *discretionary access control*. The system does not operate at the OS-layer, but presents an effective capability-sharing system for modified applications via an SGX mediator.
- *NeXUS* (Djoko et al. [37]); practical access control for remote storage systems such as *Google Drive*. The design uses a *stackable* filesystem to interface with encrypted volumes — SGX is used to protect and share these encryption keys. The authors report a 100% performance overhead.

²The *linux-sgx* patch set is currently in its 32nd revision; <https://lore.kernel.org/linux-sgx/>.

³Peer to peer.

3.3 Dataflow Protection using SGX

Research into applying the protections afforded by SGX to large-scale distributed computation has been fervent in the past few years — a handful of prominent projects are here detailed.

- *SCONE* [38] presents a secure container framework for *Docker*. [39] Using a secured version of the standard library for C it transparently encrypts/decrypts I/O crossing the container’s boundary. The authors claim $\times 0.6$ – 1.2 the performance of native throughput.
- *VC3* [40] secures *Hadoop MapReduce* computations — the *Hadoop* platform is not considered part of the TCB, thus allowing the system’s security invariants to remain unaffected if it were to be compromised. The reported performance overhead is stated to be 8% (for full read/write integrity).
- The *Maru* project [41] added support for running distributed *Apache Spark* in SGX enclaves. Data residing outside of a worker in *HDFS* is sealed, removing the need for *Hadoop* to be a part of the TCB. A notable difficulty faced was porting the *JVM*⁴ to function efficiently inside an enclave; SGXv1 restricts the EPC size to 128MB, severely penalising applications that struggle to run in relatively small memory footprints.
- *Ryoan* [42] provides a distributed sandbox environment to confine untrusted applications running on sensitive data in the cloud; a specific use case is computation outsourcing. It uses *confining labels* to create a weakened form of IFC tracking; processing nodes must be stateless and once tainted by a request cannot access resources outside the execution environment. Enforcement is managed both by SGX and *NaCl* [43] for the host application.

⁴Java Virtual Machine

Chapter 4

Design and Implementation

In this chapter we shall introduce and detail a prototype implementation of a modular, SGX-protected *reference monitor* — CITADEL. First, its necessity will be motivated, and the challenges faced discussed. Then, the three-part architecture will be explained, relating various design decisions to the DIFC model it provides. A discussion about the architecture’s performance and effectiveness is provided in § 5.

4.1 Motivation

Since its introduction in a 1972 report from Anderson [44], the reference monitor concept has time and again proved to be a reliable workhorse for a plethora of security models. It does not refer to any exact policy, nor limit itself to any particular implementation — it’s abstractness is one of its greatest strengths, reserving any judgement about what policy is *appropriate* in a particular setting. [45]

Fundamental Properties of a Reference Monitor

- *Always invoked.* Every access to the system must be mediated to guarantee that adversaries are unable to bypass the system’s security policies.
- *Evaluable.* It “must be small enough to be subject to analysis and tests, the completeness of which can be assured”; [44] to be trustworthy, it must be *auditable*,

with, ideally, a restricted TCB.

- *Tamper proof.* To ensure that an attacker cannot disable the access control and authorisation steps mandated by the security policy, the integrity of a reference monitor cannot be in question.

No computer system is every completely secure, and Linux is no exception. Having grown by a 1.7 million lines of code (LoC) in the past year alone, to stand at 27.8 million LoC in total,¹ bugs are inevitable — almost 2000 have been reported in the past year,² and 662 *severe* bugs are still outstanding.³ In this context we must question whether Linux alone can provide a reference monitor implementation the guarantees it requires, [46, 47] thus motivating the use of SGX.

Applying SGX to this problem brings two attractive benefits;

- The system’s IFC policy can be evaluable both during offline analysis and online using *attestation*, helping other enclaves’ confidence in the underlying system.
- SGX’s hardware protections are very capable at defending a reference monitor’s state, even if adversaries have ring-0 privilege or in the presence of a kernel bug.

4.2 Challenges

The natural location for a reference monitor is embedded directly in the kernel, in the path of *syscalls*’ control flows — this is provided by the LSM framework. *CamFlow* does exactly this, silently tagging processes and other entities as they are encountered by the kernel, additionally providing an external LSM-interface for any active changes. An SGX enclave is incompatible with this workflow however (§ 2.2.3), as it cannot execute alongside kernel code. Thus a major, unavoidable design decision is that the reference monitor must be distributed across rings 0 and 3 — an enclave *policy* component, and an LSM for *enforcement*.

¹https://www.theregister.com/2020/01/06/linux_2020_kernel_systemd_code/

²<https://bugzilla.kernel.org/>

³<https://www.cvedetails.com/product/47/Linux-Linux-Kernel.html>



Figure 4.1: Abstract *syscall* control flow route. Grey components show the natural Linux design. Green additions highlight the externalised enclave LSM component.

The disruption this change causes could have the potential to severely impact performance; Figure 4.1 highlights the significant change to overall control flow. Most notably, externalising part of the LSM to an enclave forces, in the worst case, an additional pair of context switches for each *syscall*.

Given a ring-3 component is unavoidable, the question becomes how to minimise the overhead caused by its integration, all while maintaining *safety* (every operation must be mediated). This problem is reminiscent of the ones that inspired the development of *exokernels* [48] — both the drawbacks and opportunities of those approaches apply here. [49] [More detail about why.](#)

Two architectures, as illustrated in Figure 4.2, were initially considered.

1. An *isolated* extension of the LSM. Only the security implementation communicates with the *policy* enclave, acting as a naïve reimplement of a fully self-contained LSM using an additional kernel module as an I/O relay.
2. An *integrated* userspace service, through which permission is *requested* ahead of time and decisions stored in the LSM before being needed. Back flow of information is facilitated asynchronously, but an additional kernel relay is not required.

Architecture 1 can be implemented without changing the base IFC model presented in § 2.1.3, easing potential concerns regarding correctness and safety. However it adds significant overhead to the critical sections [50] of core LSM functions, in most cases



Figure 4.2:

while the kernel holds locks for various objects being accessed.

Architecture 2 is more flexible, requiring all negotiation be conducted ahead of time, and importantly, without leaving userspace: any overhead only impacts the application, leaving the kernel’s critical sections to execute with minimal interference. A notable downside, however, is that the system’s security model will need to be extended to accommodate the fact that *policy decisions and enforcement are no longer one and the same*.

Preliminary experiments showed that the performance of the two architectures were similar in light workloads, but *Architecture 1* degrades significantly in the presence of any resource contention. Additionally, as will be explained in § 0.0, the dependence on a kernel module conflicts with the desired constrained TCB of the system. For these reasons *Architecture 2* was chosen for the remainder of development.

An additional challenge is one of incomplete information — the enclave will not be privy to internal kernel datastructures such as `task_struct`, which will store the taint and capabilities of processes. A potential solution would be to implement a request–response model via a custom kernel interface for any queries, though the performance impact would be severe, requiring additional context switches. The approach adopted instead (§ 0.0) uses inference based on partial information an enclave has. Any solution must be trustworthy and safe, and malicious entities must not be able to exploit any

eventually consistent components. [51]

As a final comment, it must be noted that SGX is not without its flaws; § 5.X discusses this and its impact on the project.

4.3 The CITADEL IFC Model

Before work on the final CITADEL implementation began, we constructed a formalisation describing the distributed nature of its design. A model helps reason about the safety and correctness of the final system, and provides the notation to properly discuss its features. Our model, which will now be presented, directly extends the one presented in § 2.1.3.

4.3.1 Reservations

Previously we had defined the concept of a *safe flow*, $A \rightarrow B$, which underpins the heart of our IFC restrictions. In previous works permission to perform an operation is granted while *implicitly* considering *how* the flow is to take place (4.1). An isolated *enforcement* component does not understand the concept of *flows*, forcing policy decisions to be defined *explicitly*; CITADEL uses *reservations* for this purpose (4.2). This distinction is simple but very important when introducing *laziness* and other optimisations between the two halves of the reference monitor.

$$operation \rightarrow \boxed{\text{reference monitor}} \xrightarrow{\text{decision}} \{0, 1\} \quad (4.1)$$

$$operation \rightarrow \boxed{\text{policy} \xrightarrow{\text{reservation}} \text{enforcement}} \xrightarrow{\text{decision}} \{0, 1\} \quad (4.2)$$

Let Ω be the set of all operations mediated by the reference monitor, for example `file_read` or `socket_open`. Also, let us define \mathcal{R} , the set of all *reservations*, as follows.⁴

$$\mathcal{R} = \mathcal{T} \times \wp(\Omega)$$

⁴Recalling that \mathcal{T} is the set of all tags.

Further, we define a shorthand, t^α ;

$$r \in \mathcal{R} . (r = (t, \alpha) = t^\alpha \implies t \in \mathcal{T} \wedge \alpha \subseteq \Omega)$$

We introduce, for a process A , additional state; $A_r \subseteq \mathcal{R}$, the set of all reservations it holds. Once a decision has been made, it is important for a reference monitor to be able to change it, revoking access if required. Thus we specify a notion of *validity* with an indicator function, $\mathcal{V} : \mathcal{R} \mapsto \{0, 1\}$. A reservation can only be used to obtain access to a resource if it is valid; invalid reservations are deleted.

4.3.2 Permissible Operations

Satisfiability To determine whether an operation may be permitted, the *constraint reservation* representing it is compared against reservations held by the process. As an example, $t^{\{\text{file_read}\}}$ is the constraint for reading a file tagged with t .

A constraint τ^x is said to be satisfied by a reservation τ^y ($\tau^x \lesssim \tau^y$) if the tags match and y permits *at least* the same form of access (4.3). Equations (4.4) and (4.5) define set comparison counterparts — constraint τ^x is satisfied by a set of reservations y ($\tau^x \sqsubseteq y$), and a set of constraints μ is satisfied by a set of reservations ν ($\mu \sqsubseteq \nu$).

$$\sigma^\alpha, \tau^\beta \in \mathcal{R} . (\sigma^\alpha \lesssim \tau^\beta \iff \sigma = \tau \wedge \alpha \subseteq \beta) \quad (4.3)$$

$$\sigma^\alpha \in \mathcal{R}, x \subseteq \mathcal{R} . (\sigma^\alpha \sqsubseteq x \iff \exists \tau^\beta \in x . \sigma^\alpha \lesssim \tau^\beta) \quad (4.4)$$

$$\mu, \nu \subseteq \mathcal{R} . (\mu \sqsubseteq \nu \iff \forall \alpha \in \mu . \alpha \sqsubseteq \nu) \quad (4.5)$$

From this we can define a *permissible operation*, $A \xrightarrow{\omega} t$, meaning process A may perform operations ω on an entity tagged with t . An operation is only permissible if the process holds a reservation explicitly granting permission (4.6).

$$A \xrightarrow{\omega} t \iff (\exists t^\alpha \in A_r \implies t^\omega \lesssim t^\alpha) \quad (4.6)$$

To bridge the gap between permissible flows and operations, a final definition is required; a *specific permissible flow*, $A \xrightarrow{\omega, \tau} B$, meaning that A may send information

to B using operations ω , via entities tagged with τ . Two natural statements fall out from these definitions;

$$(\exists \omega, \tau . A \xrightarrow{\omega, \tau} B) \implies A \rightarrow B \quad (4.7)$$

$$A \xrightarrow{\omega, \tau} B \implies A \xrightarrow{\omega} \tau \quad (4.8)$$

These are particularly notable as they define the relationship between an abstract policy space ($A \rightarrow B$) and concrete implementation ($A \xrightarrow{\omega} \tau$).

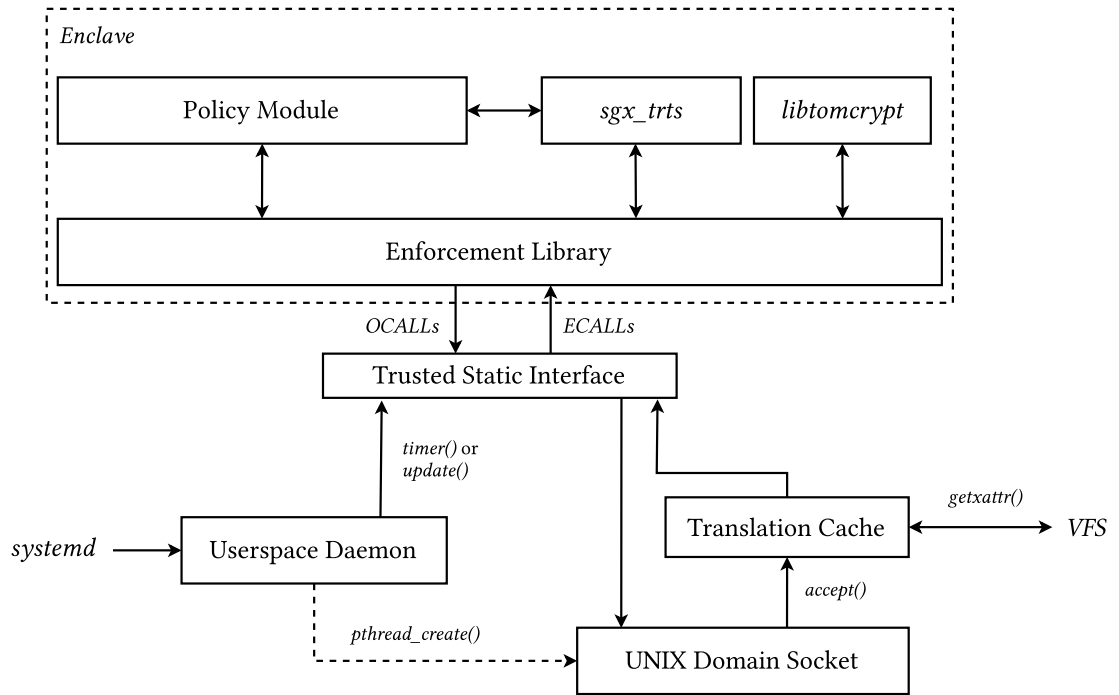


Figure 4.3: Abstract overview of an SGX enclave’s protections.

4.4 Implementation

Chapter 5

Evaluation

Chapter 6

Summary and Conclusions

Bibliography

- [1] Intel®. *Intel® Software Guard Extensions Programming Reference*, October 2014.
- [2] Heiko Mantel and David Sands. Controlled declassification based on intransitive noninterference. volume 3302, pages 129–145, 11 2004.
- [3] David Elliott Bell and Leonard J. LaPadula. *Secure computer systems: Mathematical foundations*. 1973.
- [4] Dorothy E. Denning. A lattice model of secure information flow. *Commun. ACM*, 19:236–243, 1976.
- [5] A. W. Roscoe and M. H. Goldsmith. What is intransitive noninterference? In *Proceedings of the 12th IEEE Workshop on Computer Security Foundations, CSFW '99*, page 228, USA, 1999. IEEE Computer Society.
- [6] Thomas Pasquier, Xueyuan Han, Mark Goldstein, Thomas Moyer, David Eysers, Margo Seltzer, and Jean Bacon. Practical whole-system provenance capture. In *Symposium on Cloud Computing (SoCC'17)*. ACM, 2017.
- [7] Maxwell Krohn, Alexander Yip, Micah Brodsky, Natan Cliffer, M. Frans Kaashoek, Eddie Kohler, and Robert Morris. Information flow control for standard os abstractions. *SIGOPS Oper. Syst. Rev.*, 41(6):321–334, October 2007.
- [8] Department of Defence. *Trusted Computer System Evaluation Criteria*, August 1983.
- [9] A. C. Myers and B. Liskov. Complete, safe information flow with decentralized labels. In *Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No.98CB36186)*, pages 186–197, 1998.
- [10] Andrew C. Myers and Barbara Liskov. Protecting privacy using the decentralized label model. *ACM Trans. Softw. Eng. Methodol.*, 9(4):410–442, October 2000.
- [11] Andrew C. Myers and Barbara Liskov. A decentralized model for information flow control. In *Proceedings of the Sixteenth ACM Symposium on Operating Systems*

- Principles*, SOSP '97, page 129–142, New York, NY, USA, 1997. Association for Computing Machinery.
- [12] Matthew Hoekstra, Reshma Lal, Pradeep Pappachan, Vinay Phegade, and Juan Del Cuvillo. Using innovative instructions to create trustworthy software solutions. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, HASP '13, New York, NY, USA, 2013. Association for Computing Machinery.
 - [13] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos V. Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Savagaonkar. Innovative instructions and software model for isolated execution. In *Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy*, HASP '13, New York, NY, USA, 2013. Association for Computing Machinery.
 - [14] Ittai Anati, Shay Gueron, Simon Paul Johnson, and Vincent Scarlata. Innovative technology for cpu based attestation and sealing. 2013.
 - [15] Intel®. *Intel® 64 and IA-32 Architectures. Software Developer's Manual, Volume 3D: System Programming Guide, Part 4*, September 2015.
 - [16] Seongmin Kim, Youjung Shin, Jaehyung Ha, Taesoo Kim, and Dongsu Han. A first step towards leveraging commodity trusted execution environments for network applications. In *Proceedings of the 14th ACM Workshop on Hot Topics in Networks*, HotNets-XIV, New York, NY, USA, 2015. Association for Computing Machinery.
 - [17] Andrew Baumann, Marcus Peinado, and Galen Hunt. Shielding applications from an untrusted cloud with haven. *ACM Trans. Comput. Syst.*, 33(3), August 2015.
 - [18] Olga Ohrimenko, Manuel Costa, Cédric Fournet, Christos Gkantsidis, Markulf Kohlweiss, and Divya Sharma. Observing and preventing leakage in mapreduce. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, page 1570–1581, New York, NY, USA, 2015. Association for Computing Machinery.
 - [19] Intel®. *Intel® Software Guard Extensions SDK*, March 2020.
 - [20] Shay Gueron. A memory encryption engine suitable for general purpose processors. Cryptology ePrint Archive, Report 2016/204, 2016. <https://eprint.iacr.org/2016/204>.
 - [21] Yuanzhong Xu, Weidong Cui, and Marcus Peinado. Controlled-channel attacks: Deterministic side channels for untrusted operating systems. In *Proceedings of the 2015 IEEE Symposium on Security and Privacy*, SP '15, page 640–656, USA, 2015. IEEE Computer Society.

- [22] Victor Costan and Srinivas Devadas. Intel sgx explained. *IACR Cryptol. ePrint Arch.*, 2016:86, 2016.
- [23] Intel®. *Intel® SGX: Intel® EPID Provisioning and Attestation Services*, March 2016.
- [24] Ernie Brickell and Jiangtao Li. Enhanced privacy id: A direct anonymous attestation scheme with enhanced revocation capabilities. volume 9, pages 21–30, 01 2007.
- [25] The Trusted Computing Group. *Trusted Platform Module (TPM) Summary*, January 2008.
- [26] Petros Efstathopoulos, Maxwell Krohn, Steve VanDeBogart, Cliff Frey, David Ziegler, Eddie Kohler, David Mazières, Frans Kaashoek, and Robert Morris. Labels and event processes in the asbestos operating system. In *Proceedings of the Twentieth ACM Symposium on Operating Systems Principles, SOSP '05*, page 17–30, New York, NY, USA, 2005. Association for Computing Machinery.
- [27] Nickolai Zeldovich, Silas Boyd-Wickizer, Eddie Kohler, and David Mazières. Making information flow explicit in histar. In *Proceedings of the 7th Symposium on Operating Systems Design and Implementation, OSDI '06*, page 263–278, USA, 2006. USENIX Association.
- [28] Nickolai Zeldovich, Silas Boyd-Wickizer, and David Mazières. Securing distributed systems with information flow control. In *Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, NSDI'08*, page 293–308, USA, 2008. USENIX Association.
- [29] Winnie Cheng, Dan R. K. Ports, David Schultz, Victoria Popic, Aaron Blankstein, James Cowling, Dorothy Curtis, Liuba Shrira, and Barbara Liskov. Abstractions for usable information flow control in aeolus. In *Proceedings of the 2012 USENIX Conference on Annual Technical Conference, USENIX ATC'12*, page 12, USA, 2012. USENIX Association.
- [30] Indrajit Roy, Donald E. Porter, Michael D. Bond, Kathryn S. McKinley, and Emmett Witchel. Laminar: Practical fine-grained decentralized information flow control. *SIGPLAN Not.*, 44(6):63–74, June 2009.
- [31] Oracle®. *The Java® Virtual Machine Specification*, February 2015.
- [32] Jeffrey Dean and Sanjay Ghemawat. Mapreduce: Simplified data processing on large clusters. In *OSDI'04: Sixth Symposium on Operating System Design and Implementation*, pages 137–150, San Francisco, CA, 2004.

- [33] K. Shvachko, H. Kuang, S. Radia, and R. Chansler. The hadoop distributed file system. In *2010 IEEE 26th Symposium on Mass Storage Systems and Technologies (MSST)*, pages 1–10, 2010.
- [34] Lars Richter, Johannes Götzfried, and Tilo Müller. Isolating operating system components with intel sgx. In *Proceedings of the 1st Workshop on System Software for Trusted Execution, SysTEX '16*, New York, NY, USA, 2016. Association for Computing Machinery.
- [35] Vishal Karande, Erick Bauman, Zhiqiang Lin, and Latifur Khan. Sgx-log: Securing system logs with sgx. *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017.
- [36] Sinisa Matetic, Moritz Schneider, Andrew Miller, Ari Juels, and Srdjan Capkun. Delegatee: Brokered delegation using trusted execution environments. In *Proceedings of the 27th USENIX Conference on Security Symposium, SEC'18*, page 1387–1403, USA, 2018. USENIX Association.
- [37] J. B. Djoko, J. Lange, and A. J. Lee. Nexus: Practical and secure access control on untrusted storage platforms using client-side sgx. In *2019 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 401–413, 2019.
- [38] Sergei Arnautov, Bohdan Trach, Franz Gregor, Thomas Knauth, Andre Martin, Christian Priebe, Joshua Lind, Divya Muthukumaran, Dan O’Keeffe, Mark L. Stillwell, David Goltzsche, David Eyers, Rüdiger Kapitza, Peter Pietzuch, and Christof Fetzer. Scone: Secure linux containers with intel sgx. In *Proceedings of the 12th USENIX Conference on Operating Systems Design and Implementation, OSDI'16*, page 689–703, USA, 2016. USENIX Association.
- [39] Docker. *Introduction to Container Security: Understanding the isolation properties of Docker*, August 2016.
- [40] F. Schuster, M. Costa, C. Fournet, C. Gkantsidis, M. Peinado, G. Mainar-Ruiz, and M. Russinovich. Vc3: Trustworthy data analytics in the cloud using sgx. In *2015 IEEE Symposium on Security and Privacy*, pages 38–54, 2015.
- [41] F. Kelbert, P. Pietzuch, and J. Crowcroft. *Maru: SGX-Spark Deep Dive*, November 2017.
- [42] Tyler Hunt, Zhiting Zhu, Yuanzhong Xu, Simon Peter, and Emmett Witchel. Ryoan: A distributed sandbox for untrusted computation on secret data. In *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI 16)*, pages 533–549, Savannah, GA, November 2016. USENIX Association.

- [43] Google. *NaCL: Native Client*.
- [44] J. Anderson. *Computer Security Technology Planning Study — Volume 2*, October 1972.
- [45] C. Irvine. The reference monitor concept as a unifying principle in computer security education. April 2001.
- [46] Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Anders Fogh, Jann Horn, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, and Michael Hamburg. Meltdown: Reading kernel memory from user space. In *USENIX Security Symposium*, 2018.
- [47] Adam Bates, Dave Tian, Kevin R. B. Butler, and Thomas Moyer. Trustworthy whole-system provenance for the linux kernel. In *Proceedings of the 24th USENIX Conference on Security Symposium*, SEC’15, page 319–334, USA, 2015. USENIX Association.
- [48] D. R. Engler, M. F. Kaashoek, and J. O’Toole. Exokernel: An operating system architecture for application-level resource management. In *Proceedings of the Fifteenth ACM Symposium on Operating Systems Principles*, SOSP ’95, page 251–266, New York, NY, USA, 1995. Association for Computing Machinery.
- [49] M. Frans Kaashoek, Dawson R. Engler, Gregory R. Ganger, Hector M. Briceño, Russell Hunt, David Mazières, Thomas Pinckney, Robert Grimm, John Jannotti, and Kenneth Mackenzie. Application performance and flexibility on exokernel systems. *SIGOPS Oper. Syst. Rev.*, 31(5):52–65, October 1997.
- [50] Michel Dubois, Christoph Scheurich, and Faye A. Briggs. Synchronization, coherence, and event ordering in multiprocessors. *Computer*, 21:9–21, 1988.
- [51] Werner Vogels. Eventually consistent. *Commun. ACM*, 52(1):40–44, January 2009.