Establishing Trusted I/O Paths for Client Shielded Execution Systems with Aurora

Hongliang Liang, *Member, IEEE,* Mingyu Li, Yixiu Chen, Lin Jiang, Zhuosi Xie, Tianqi Yang

***Abstract*—Nowadays, users' sensitive data in edge computing devices (desktops, laptops, and tablets, etc.) is at high risk because they run applications on potentially compromised or malicious systems. To address this problem, hardware manufacturers such as Intel released a new processor feature called Software Guard eXtension (SGX), and provisions shielded executions (i.e., enclaves) for security-sensitive computations. Regrettably, Intel SGX's design objectives omit trusted I/O paths. Without such guarantees, it is unlikely for an enclave to fulfill its security and privacy purposes because the source or sink of data may have been corrupted.**

To this end, we propose a novel architecture called AURORA to provide trusted I/O paths for enclave programs even in the presence of untrusted system software. Specifically, AURORA exploits two commercial-off-the-shelf features (System Management Mode, SMM and SGX) and establishes a secure channel between an enclave program and target device. Furthermore, we design and implement trusted paths for HID keyboard, serial port printer, hardware clocks, and USB mass storage, respectively. Leveraging these trusted paths, we protect real-world applications including OpenSSH client, OpenSSL server/client and SQLite database. Security evaluations show that AURORA mitigates several kinds of I/O related attacks. Performance evaluations demonstrate that AURORA introduces acceptable overheads.

***Index Terms*—Trusted Path, Hardware Trust, Intel SGX, System Security**

I. INTRODUCTION

Trusted computing [1] encompasses six key technologies including: 1) endorsement key, 2) protected execution, 3) sealed storage, 4) secure input and output, 5) remote attestation, and 6) trusted third party. To this end, Intel provisions Software Guard eXtensions (SGX) [2] to establish trusted execution environment that protects the integrity and confidentiality of desired computation. Intel SGX enforces strong isolation in memory for security-sensitive compartments in a user-level application, called *enclaves*, from untrusted privileged systems. Many SGX-based protection architectures [3], [4], [5], [6], [7], [8] have already been proposed to secure data and code on untrusted servers.

Unfortunately, Intel SGX enclaves have no direct access to any hardware resources because Intel SGX by design does not support any secure input/output mechanisms according to its Software Developer's Manual [9]. Concerning I/O requests, an enclave has to rely upon the untrusted compartments through system call interfaces. This unreliable dependency is susceptible to attacks such as memory-based Iago attacks [10] and I/O-based traffic analysis [11].

A trusted path between an enclave program and a target I/O device is a protected channel that assures the secrecy and authenticity of transferred data. It is extremely critical to user's privacy such as health information, financial account, personal documents, etc on personal computers. The private data can be protected inside an enclave during runtime, but it is impossible to protect it at the time of being printed since typically printer devices only understand plaintext data and the corresponding drivers are under the control of the untrusted kernel. Similarly, the textual input from users such as keystrokes can be recorded on a compromised computer, which is a very serious problem when it comes to password security [12]. Previous research like SafeKeeper [13] only protects the password on the server side, but cannot protect the user's password from keylogging threats on the client side.

Intel SGX enclaves also suffer from the loss of a high-precision trusted clock. State-of-the-art library OSes such as Haven [3], Graphene-SGX [14] and Panoply [15] relay the clock value from untrusted systems. As a result, these systems are vulnerable to time deception attacks. Blockchain systems like Town Crier [16] depend on a remote server for a trusted time; however, this clock latency is high (usually hundreds of milliseconds) and uncertain. Intel Management Engine (ME) offers a trusted clock service for SGX enclaves, but the time value is coarse-grained (second-resolution) and not absolute at all [17]. It is not satisfactory for those enclaves that request the timestamp information at a high frequency, (e.g., tens or hundreds of times per second). Hence, to achieve millisecond-resolution time, Intel SGX SSL [18] has to use *ftime*, offered by the OS, which contradicts original SGX threat model. Cryptographic libraries such as TaLos [19], mbedTLS-SGX [20], WolfSSL-SGX [21] encounter the same problem as well. Additionally, another trusted service named Intel monotonic counters are slow and the used NVRAM will wear out after a limited times of writes.

Today's SGX ecosystem has not yet come up with an off-the-shelf solution to trusted I/O paths. Enclaves themselves cannot authenticate whether they are communicating with trusted devices or not. It is significantly important to solve the problem on ***how to establish trusted I/O paths for enclaves on untrusted systems***, as almost all SGX-based projects exclude the underlying OS from the trusted computing base (TCB) while awkwardly depending on it for I/O requests.

On Intel platforms, we observe that 1) all peripheral I/O devices are connected with south-bridge to I/O Advanced Pro-

H. Liang, M. Li, Y. Chen, L. Jiang, Z. Xie, T. Yang are with Trusted Software and Intelligent System Lab, Beijing University of Posts and Telecommunications, Beijing 100876, China. e-mail: ({hliang, maxul, chenyixiu, jianglin, xiezhuosi, yangtianqi}@bupt.edu.cn)

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant No. U1713212 and 91418206.

grammable Interrupt Controller (I/O APIC), 2) I/O interrupts can be rerouted to System Management Interrupt (SMI) via configuring I/O APIC and 3) the SMI handler is initialized by Unified Extensible Firmware Interface (UEFI) which contains kinds of device drivers; thus, we hold the insight that *the SMI handler* is a perfect candidate to provide trusted I/O paths for security-critical applications.

In this paper, we present AURORA, a novel architecture that safeguards I/O paths of SGX enclaves. To directly communicate with hardware devices without depending on the untrusted software, AURORA introduces System Management RAM (SMRAM) as a special enclave. SMRAM is a tamper-proof memory region used only in System Management Mode (SMM), much like the enclave region with SGX protection in user mode. AURORA delegates I/O requests from enclaves to the SMI handler protected inside SMRAM. We call this particular SMI handler *SMVisor*. In hardware, SMVisor is safe from any corruptions by other privileged software (including OS and hypervisor). Therefore, Intel SGX enclaves can safely use I/O devices while remaining *transparent* to the underlying OS.

To summarize, this paper makes these contributions:

1) The notion of two types of trusted I/O paths (§ II-C) for security-sensitive applications (enclave programs).
2) A novel architecture named AURORA (§ III-A) leveraging two hardware features of Intel processors (SMM and SGX) to provide enclaves trusted paths transparent to untrusted OSes/HVs with a minimal trusted computing base (§ V-B).
3) Design and implementation of four types of trusted I/O paths (§ IV): keyboard, printer, clock, and storage, based on AURORA. To the best of our knowledge, we are the first to provide these *realistic* trusted I/O paths for SGX enclaves on the client side.
4) Three case studies: OpenSSH client, OpenSSL client, and SQLite database using trusted I/O paths provided by AURORA (§ VII). Experimental results show that AURORA can protect them from typical I/O related attacks (§ VI-E) with acceptable performance overhead (§ VI).

II. BACKGROUND AND PROBLEM DEFINITION

In this section, we first describe two architecture features of Intel's CPU, and then propose two types of trusted I/O paths based on the characteristics of devices. Finally, we describe the threat model and assumptions.

A. Software Guard eXtension

Intel SGX [2] provides trusted execution environments called enclaves in user level. Enclaves' code and data reside in a hardware-protected memory named enclave page cache (EPC), which is inaccessible to any software including OS/HV or SMI handler. Enclave code can access the memory outside the enclave. As enclave code is only allowed to be executed in user mode, any interaction with devices must execute outside of the enclave and through untrusted system calls. SGX enables a threat model where users only trust the Intel CPUs and the code running inside the enclaves.

Intel SGX SDK provides a function call mechanism for enclaves via ECALL and OCALL. Thus, an application can invoke an enclave's code via an ECALL and get the return values. The enclave can invoke an OCALL to execute a function in the untrusted portion of the application and receive a return value. With SGX's remote attestation ability [22], one can gain confidence that the target application is securely running within an enclave. Local attestation allows an enclave to prove to one another that it is running on the same processor.

B. System Management Mode

System Management Mode (SMM) is the most privileged mode for handling system-wide functions like power management, hardware control, etc. Upon a System Management Interrupt (SMI), the CPU saves the system states and switches to SMM, and then executes a predefined logic (SMI handler) inside system management memory (SMRAM). SMRAM is fully transparent to the OS/HV since they are essentially suspended. An *RSM* (resume) instruction is executed at the end of the SMI handler to switch back to the protected mode. SMRAM is fully isolated by the hardware, any code outside SMRAM cannot access or modify it. We deem SMRAM as a special *enclave* in SMM.

The SMI handler is initialized by UEFI, and SMRAM can be locked by configuring *D_OPEN* and *D_LCK* bits in SMRAM control register. Therefore, the SMI handler is safe from corruption after booting. Moreover, the SMI handler can access all CPU registers, I/O devices, and physical memory (except for SGX EPCs), and thus we expand the SMI Handler to design AURORA's SMVisor in § III-A.

C. Trusted I/O Paths

We define the term *trusted I/O paths* in trusted execution environments (TEEs, e.g. SGX) as follows. Given a trusted application (e.g. an SGX enclave) and a trusted peripheral device, a trusted I/O path is a secure channel of data transfers between them, even in the face of software adversaries such as host kernel, hypervisor, guest VM and kernel drivers. We classify trusted I/O paths into two categories based on their characteristics:

1) **Trusted I/O paths for data-provider/-consumer devices.** Although SGX provides user-space strong isolation for program end-points (i.e. enclaves), most of the devices provide and/or consume plaintext messages. Cases vary from human input data (e.g., keyboard scan code) to outputted data (e.g., a stream of bits to printer/display), which cannot guarantee the confidentiality and integrity in an untrusted or compromised system. Therefore, for trusted paths of this kind, AURORA encrypts/decrypts in SMRAM the data from/to devices for enclaves to protect the data from the untrusted system.
2) **Trusted I/O paths for data-storage/-transmitter devices.** Storage disks and network adapters are typical storage/transmitter devices, and they don't require the stored/transmitted data in plaintext. Instead, both kinds of devices can deal with encrypted data without learning the semantics of the data. However, both devices need a pile

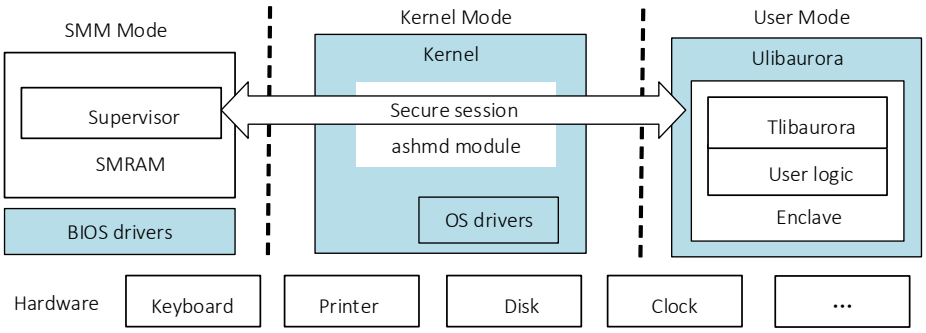

Fig. 1. AURORA's architecture. The gray areas denote untrusted parts, and the white ones represent AURORA's trusted computing base.

of software stacks (e.g., file system, network protocol) to work correctly and remain compatible. Building trusted paths for them is very challenging. One possible approach is to decompose existing software stack and port them into the trusted applications, which will greatly swell the TCB and attack vectors. As an alternative, AURORA leverages a *distrust but verify* method and reuses existing software stacks in a secure manner.

D. Threat Model

We consider an adversary that is able to compromise the target system. He can directly attack enclave interfaces visible to the OS, and actively reconfigure any devices (e.g., modify a device's MMIO region, or change the operating mode of a device) and perform arbitrary operations (e.g., trigger interrupts, issue DMA write requests) using any I/O commands.

AURORA requires a modern Intel platform with SGX and TPM support. We assume the hardware and SMRAM firmware (the microkernel we implement) of the host machine is trusted. We do not trust the UEFI drivers but verify whether they operate following their specifications, or perform unintended operations: e.g., intercept bus traffic, or write to an address that is not specified in DMA commands. Our assumptions significantly reduce the TCB on the target host as modern commodity system contains a large system software (UEFI, possibly hypervisor, kernel and other applications) when dealing with I/O devices. Even though we do not consider physical attacks on devices, side-channel attacks [23], [24], or denial-of-service attacks, we adopt side-channel free cryptographic algorithms and apply an oblivious packet transferring technique (§ III-G).

III. DESIGN

To provide trusted I/O paths, we employ the combination of SGX and SMM, both of which are processor enforced protection features. Because they are offered at the opposite ends of Intel privilege-level model, we name our framework after AURORA[1].

Establishing a trusted path in AURORA consists of the following three steps. First, AURORA builds a secure session between SMVisor and an enclave that performs an I/O request. Second, SMVisor receives the request via the secure session without leaking knowledge to the untrusted system. Third, SMVisor interacts with the target device on behalf of the enclave, and performs desired I/O operations for the request. The procedure is conceptually similar to a *syscall* or *vmcall*. We name this an *smcall* for brevity.

A. Architecture

AURORA is composed of three components: SMVisor, libaurora and a secure session established between SMVisor and libaurora, as shown in Figure 1.

1) SMVisor takes charge of the target devices from the untrusted kernel. It dispatches device interrupts to either kernel or enclaves. SMVisor securely invokes UEFI drivers outside of SMRAM (§ III-D).
2) Libaurora consists of two parts. The trusted part (Tlibaurora) complements unsupported I/O APIs in Intel SGX SDK library, helping developers secure enclave's I/O paths. The untrusted part (Ulibaurora) is responsible for forwarding *smcalls* to SMVisor.
3) The secure session exchanges encrypted messages between SMVisor and an enclave via a shared memory provided by a kernel module named ashmd. AURORA leverages a 5-tuple: *(ENCLID, DEVID, OPTYPE, PAYLOAD, MAC)* for each message. The first two arguments indicate the program endpoint and device endpoint respectively. The third stands for the type of I/O operation. The fourth carries the message data and the last is the message authentication code used for integrity protection. All the arguments are marshaled and encrypted.

Like library OSes [3], [14], [15], AURORA has few interfaces with the untrusted OS. The data plane of an enclave is protected by advanced encryption schemes accelerated by the processor (*i.e.,* AES-GCM with AES-NI support), and the data flows between the enclave and SMVisor are completely invisible to the OS. Unlike library OSes, which delegate I/O operations to the untrusted OS, AURORA ships security-sensitive parts of these operations into SMVisor, thus eliminating the reliance on untrusted OS.

B. Workflow

To help understand the workflow of a trusted path in AURORA, we break down the process of the output path and

[1] Aurora takes place in the polar regions, *i.e.,* south and north of the earth.

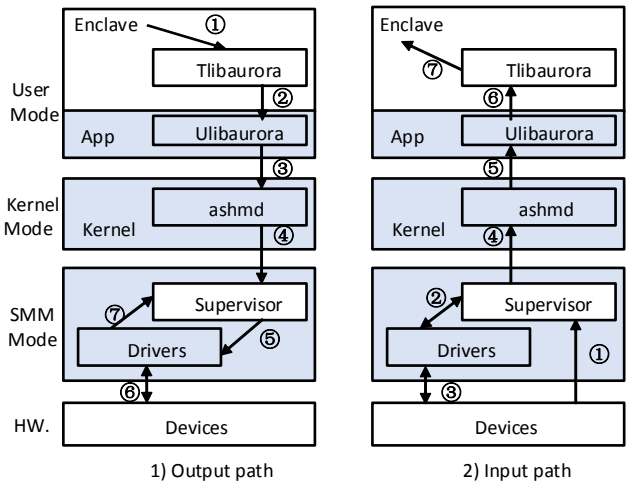

Fig. 2. The workflow of a trusted I/O path in AURORA.

input path respectively into sequential phases, as illustrated in left and right part of Figure 2.

An output request is triggered by an enclave as an exception, as depicted as follows:
① The user logic in an enclave issues an output request by invoking Tlibaurora's APIs;
② Tlibaurora marshals and encrypts the request's arguments, and invokes Ulibaurora outside the enclave to relay the request;
③ Ulibaurora *ioctls* the ashmd module to trigger an *smcall*;
④ SMVisor is notified and obtains the encrypted requests from the secure session;
⑤ SMVisor decrypts the request and invokes the driver;
⑥ The driver processes output data in PCI space or MMIO buffer;
⑦ The driver returns a result code to SMVisor. In the end, SMVisor executes *RSM* to return to protected mode.

An input request from an enclave causes a device interrupt, as depicted as follows:
① The target device triggers an interrupt, and the control flow is rerouted to SMVisor which has the interrupt handler;
② SMVisor invokes the driver to handle the input request;
③ The driver gets the raw input data and sends it to SMVisor;
④ SMVisor encrypts the data inside SMRAM, and sends it to the target enclave via the secure session;
⑤ The system switches back to protected mode and the ashmd module uses a signal to notify Ulibaurora;
⑥ Ulibaurora invokes Tlibaurora to receive the encrypted data;
⑦ The enclave decrypts the encrypted data and finally obtains the raw input data.

C. SMVisor

SMVisor is the core component in AURORA. It may take charge of multiple devices simultaneously, therefore it needs to determine which device is being requested and then invokes the corresponding driver.

Interrupt Handler. To deal with a device interrupt, SMVisor reroutes the interrupt to SMI. Specifically, SMVisor intercepts device events by configuring the *Redirection Table* defined in I/O APIC and modifying the destination of the device event to SMI. SMVisor distinguishes the interrupt source and thus notifies a certain enclave or the untrusted kernel. In order to forward the interrupt to upper software layer, it issues an inter-processor interrupt (IPI) by writing the interrupt command request (ICR) register in the local APIC.

To perform I/O operations correctly, a driver should know the exact I/O ports of the target device. At the time of system boot, SMVisor collects all device information and records their memory-mapped I/O (MMIO) base addresses into a *PCI BAR Table*, thereafter the matching drivers can manipulate the mapped PCI configuration space according to the table.

Sanitization Module. SMVisor verifies the validity of parameters passed to the drivers (e.g. a PCI structure pointer should point to one of the entries in the *PCI BAR Table* within SMRAM) and checks the return values according to the device specifications (e.g. each driver function has a specific range of error codes) as well as its functional correctness. When the parameters or return values are invalid, SMVisor notifies the enclave that a potential attack from OS may occur, and rejects the subsequent requests. Moreover, SMVisor checks the memory boundary (i.e. starting address and region range) that the driver tries to access to ensure that it can not write data outside of SMRAM. Furthermore, a driver may require more memory space during runtime (e.g. for DMA with devices), therefore SMVisor maintains a dynamic heap with a sanity-checking feature [25]. To avoid possible memory leaks, the manager frees all allocated memory for the driver before returning to the protected mode.

D. SMM Drivers

In this section, we describe how SMVisor safely reuses existing drivers. In modern monolithic systems, OS drivers are coupled with the kernel. These drivers lack of effective isolation from the rest of the untrusted systems, therefore we do not use them. Instead, since existing open-source UEFI firmware, such as Coreboot[2] and Project Mu[3], contain various drivers in their Driver eXecution Environment (DXE), and the code of these drivers are significantly scrutinized compared to the proprietary code, we reuse these drivers and forward the device interrupt for them to handle. This OS-neutral design allows AURORA to support different kinds of OS, e.g., Linux, Windows, or macOS.

Furthermore, we reuse UEFI drivers in a secure manner. At the booting stage, SMVisor calculates the hash checksum of each driver and stores its integrity signature inside SMRAM. When receiving an I/O request, SMVisor verifies the integrity of the corresponding driver to ensure it is not tampered with. When executing a driver, SMVisor puts its data, heap, stack segments inside SMRAM, and thus ensures them inaccessible to OS/HV. Moreover, SMVisor uses its sanitization module to validate the behavior of the driver, as described in § III-C.

[2]https://www.coreboot.org/
[3]https://microsoft.github.io/mu/

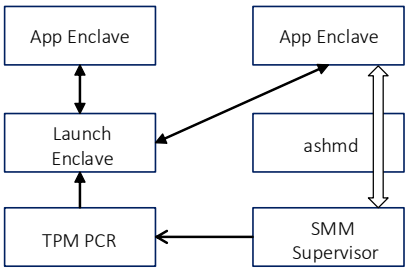

Fig. 3. Mutual attestation and key agreement between SMVisor and an application enclave. The single line arrows denote the attestation direction, the double line arrow denotes the following key agreement.

E. Kernel Module (ashmd)

SGX memory model is asymmetric: the processor prohibits code outside of enclave to access the enclave, whereas the enclave code can access addresses outside the enclave. AURORA leverages shared memory to bridge SMVisor and enclaves. For instance, we use a kernel module *ashmd* to allocate contiguous physical memory as shared memory. For an enclave program, Ulibaurora opens and mmaps this device into its address space. As a result, Tlibaurora can directly operate on this memory in enclave mode. If the kernel launches memory-based Iago attacks [10] such as mapping to an illegal location, Tlibaurora will verify whether the whole mmaped memory is outside of the enclave, otherwise the secure channel will not be established.

In order to distinguish interrupts to enclaves from others, ashmd module allocates an IRQ from the system. When ashmd receives an IPI from SMVisor, it knows this is a response to an enclave. Moreover, to prevent OS from modifying I/O redirection table, ashmd module spawns a kernel thread which holds a copy of I/O APIC table and continually check the status of I/O APIC table. Once it detects a modification by OS, it tries to restore it with the reserved one. If the attempt fails, ashmd immediately notifies the target enclave with an error code. We treat the denial of ashmd thread scheduling as a kind of DoS attack, which is beyond the scope of the paper.

F. Secure Session

We design a secure session that protects the message exchange between SMVisor and enclaves. The initial stage of the secure session is to ensure whether both parties are trusted or not. On one hand, the untrusted privileged system may launch SMI-specific fuzzing attacks on SMVisor. On the other hand, the privileged system may fake the identity as SMVisor since it can emulate an SMI and try to *handshake* with an enclave. To mitigate such a man-in-the-middle attack, we introduce *mutual attestation*. When each of both parties trusts the other, they can exchange a symmetric secret key using *key agreement*, as depicted in Figure 3.

Mutual Attestation. During a measured boot, Intel Boot Guard [26] hashes the firmware and stores its cryptographic hash in the TPM Platform Configuration Register (PCR) [27]. The final PCR value reflects the whole boot process. If the process is tampered with, the PCR value will differ.

In order to ease SMVisor attestation, we use the launch enclave provided by the Intel SGX Platform Software to attest SMVisor for one-time effort. Afterward, any application enclave running on the same machine can query the launch enclave to know if SMVisor attestation has succeeded. To attest SMVisor, the launch enclave needs to verify the PCR value by requesting a TPM quote, which includes a cryptographic signature over the PCR value alongside with a fresh nonce. This ensures the integrity of the PCR value and prevents replay attacks. Besides, an application enclave attests itself to the launch enclave using Intel's local attestation.

Key Agreement. After the mutual attestation, the SMVisor and an enclave establish an authenticated secure channel via an ephemeral Diffie-Hellman key exchange. We then use AES-GCM encryption scheme for further message exchange in order to prevent replay attacks. Intel processors with SGX feature support Advanced Encryption Standard New Instructions (AES-NI) to accelerate AES encryption and also can mitigate side-channel attacks [9].

Disconnection. When an enclave finishes its requests, its Tlibaurora logic will notify SMVisor to terminate the secure session and release resources. When there remains no live session, SMVisor will disable its interrupt routing and thereafter make no impact on the system.

G. Enhancement and Optimization

To provide better security and performance, AURORA introduces *hardware encryption*, *data obliviousness* and *batch mechanism for smcalls*.

Hardware Encryption. Intel extends x86 ISA with AES-NI and claims to prevent known side-channel attacks. We make use of it to address the same concern and use a constant-time algorithm to defeat cache timing attacks. This hardware acceleration also decreases the preemption time in SMM.

Data Obliviousness. In an established session, if an enclave requests the same I/O path twice and the results happen to be the same, the encrypted messages will also be identical because the session key is not changed. An adversary can infer secrets by observing such side channels. To prevent such secrecy leakage, AURORA pads all messages with random values to the same length (4KB, same size as one EPC page), which restricts possible information leakage at page-level.

Batched SMCALLs. To reduce the context switches between SMVisor and enclaves, AURORA supports a batched *smcalls* mechanism using two dedicated, lock-free ring buffers for input and output respectively. Enclaves can set a desired threshold, so Tlibaurora will coalesce these *smcalls*. For asynchronous I/O requests, the mechanism can benefit the enclave with higher throughput.

IV. TRUSTED I/O PATHS BETWEEN ENCLAVES AND DEVICES

As described in section § II-C, trusted I/O paths should assure that the users' data is transferred by a secure session. In this section, we illustrate how to build trusted I/O paths for data-provider/consumer devices, e.g. human-interface-device (HID) keyboards, serial printers, and hardware clocks, and data-storage/transmitter devices, e.g. portable USB disk.

A. Trusted HID Keyboard Input

Trusted input ensures that third-party software on the same computer has no access to the user's input intended for an enclave application. In other words, trusted input paths exclude other untrusted software including the underlying OS from sharing the input device. We use AURORA to secure user's private textual inputs from the keyboard to the enclave.

Trusted Input Mode. When an enclave issues a trusted input request, SMVisor routes the keyboard interrupt (IRQ 1 by default) to SMI. All of the subsequent keyboard scan codes are then cached inside SMRAM. We call this case *trusted input mode*. After an *enter* key is hit and released, SMVisor recovers the I/O APIC redirection table and exits trusted input mode. Finally, SMVisor encrypts the input and sends it to the secure channel. The desired enclave obtains it from the channel and decrypt it.

User Verification. Phishing attacks, where an adversary exploits social engineering tricks to allure a user to leak her privacy data, are a threat to trusted input. For example, a malware might present a fake login interface that prompts a user to enter her password. To mitigate this threat, we adopt an approach where PC speaker is used to indicate the trusted path has been established. When the system first boots, the network is disabled by the SMVisor, and we assume that the loaded kernel is clean due to TPM's measure boot. AURORA asks the user to store a short, arbitrary MIDI-format melody (around 5 seconds) inside SMRAM via an temporary enclave, so that every time when a trusted path is set up, the PC speaker will play the melody. Then the network is enabled by the SMVisor. Since the melody is a pre-shared secret only between the SMVisor and the user, it is impossible for the adversary to learn and mimic the process.

B. Trusted Serial Printer Output

Shared print services are very common today, by which colleagues in a unit or students in a college print their documents using the same physical machine. Users' private or sensitive data may also be printed using such infrastructures. Malware or compromised systems running on these shared machines can steal these data for malicious purposes like industrial espionage or illegal data acquisition. To mitigate this threat, we build trusted serial-port path for shared print services.

When an enclave requests the trusted printer service, it encrypts the output packet and sends the encrypted packet to SMVisor. SMVisor receives the packet and decrypts it to plaintext packet. As the packets are usually held with printer-specific format, SMVisor issues the corresponding serial port driver and adds this job into its task queue. Afterward, SMVisor returns the status code from the printer devices to the enclave end-point.

C. Trusted Hardware Clock

For the clock, its integrity and non-forgeability are much more vital than confidentiality. In this section, we describe how to extend AURORA for trusted, high-resolution absolute clock.

Multiple Sources. AURORA uses multiple clock sources available on x86 platforms, such as programmable interval timer (PIT) and advanced configuration and power interface/power management (ACPI/PM) timer. To estimate the latency of obtaining time from hardware and adjust their values, SMVisor references invariant time stamp counter (TSC) via *RDTSCP* instruction. The invariant TSC ensures that the duration of each clock tick is uniform (at the frequency relative to the crystal clock frequency of the processor core).

Absolute Value. We use Real-Time Clock (RTC) to provide the absolute wall-clock time (i.e. epoch) for enclaves. To avoid incorrect values due to hardware updating, SMVisor keeps obtaining the RTC values until the last two are consistent. After obtaining a valid wall-clock, SMVisor then obtains the rest timers. The order is critical because RTC time retrieval is the most expensive amongst others and will break the freshness of other timers' values.

High Resolution. When a time value with high resolution (e.g. micro-second) is required, AURORA uses the invariant TSC and High Precision Event Timer (HPET) to satisfy the need. For instance, AURORA uses the following formulae to compute the *tv_usec* value in *timeval* data structure: $tv_usec = (HPET_value/HPET_Hz)/1,000,000$; where $(HPET_value/HPET_Hz)$ computes the absolute time in micro-seconds.

Attack-Awareness. Though the hardware clocks can be controlled and modified by the malicious OS, diverse timers in Aurora offer enclaves the ability to validate the credibility of time values. Tlibaurora records last values read from all hardware clocks and obtains current values to calculate their differences respectively, and then uses clock frequencies to compute the actual elapsed time. When any of the measured time violates the monotonic rule, we assume a time attack.

For the case where the hardware clocks are altered in a consistent way, that is, all the timers are altered in the same offset, we propose a novel algorithm to detect such an attack. We use a dedicated counting thread [28] guarded inside an enclave occupying a logical thread on the same CPU core. Such a sibling thread will block the possibility of side-channel attacks when hyper-threading is active. The counting thread provides dT and the difference of hardware timers provides dt, we use first-order derivative dt/dT to detect the possible time attack. Currently, we set the confidence interval to 0.05, which denotes the possible altering in the timers' rising slope. If the slope changes much, we assume an attack.

D. Trusted USB Storage

Storage software contains block and file system. A compromised OS may silently discard data written by the application or return fabricated data during a read operation. It is a serious issue when secure data storage is necessary for ensuring correct operation (e.g., secure logging, APT monitoring and compliance). In this section, we extend AURORA to support secure USB disk. Note that AURORA's approach is also suitable and easy to support for other storage systems.

Secure Storage Protocol. When an enclave issues a request for a USB disk, SMVisor leverages I/O interrupt rerouting

mechanism to monitor and deal with every operation of the USB device, including transferring data and control commands via a secure session in AURORA. In Linux, the data is by default transferred using bulk mode and is exchanged based on DMA mechanism, which stores the DMA address and buffers location in a scatter-gather list. The ashmd module obtains the information from the USB driver.

After capturing the USB Request Blocks (URBs), SMVisor passes them to the USB device via a secure session. Note that SMVisor leverages AES-GCM scheme to encrypt transferred blocks between enclaves and devices III-A. All data blocks from the enclave are encrypted by default, and a message authentication code (MAC) is generated for each block. SMVisor checks the MAC of each block to validate its authenticity and integrity. If it checks an inconsistent MAC, SMVisor will return an error to the enclave.

V. IMPLEMENTATION

A. Components

We modified the SMI handler of CoreBoot to implement AURORA's SMVisor, and modified the drivers of CoreBoot project to export interfaces which can be invoked by SMVisor. We disable the caching mechanism in SMM and check the access permission using the memory type range registers (MTRR) to ensure SMVisor's protection. For the sake of compatibility, Tlibaurora supports standard POSIX APIs, so enclave developers need not write OCALLs.

To avoid machine check exception within SMM, we enable the Streaming SIMD Extensions (SSE) bit in control register CR0. With SSE and AES-NI, we boost encryption performance. For example, with AES-NI support, AES-256-GCM encryption and decryption on 4KB data in SMM costs 9us on average, for comparison, without AES-NI, AES-128-GCM implementation of Intel IPP Crypto library [29] costs 597us.

We implement a specific kernel model ashmd. Like Linux SGX driver, we use but do not trust them. the ashmd module is intended to relay the communications between hardware enclaves and SMVisor.

B. Code Base and Binary Size

AURORA's trusted components (i.e., SMVisor, ashmd, Tlibaurora, Cryptography) have 3393 lines of C code, and untrusted component (i.e., Ulibaurora) has 273 lines of C code. Compared to Wimpy kernel [30] which has 16K lines of code, it is smaller and simpler enough to facilitate formal verification. Both SMRAM and EPC RAM are scarce memory resource. For instance, the system-wide EPC limit is approximately 93MB and the SMRAM is 4MB by default on our platform. We measure the final size of the resulted stripped binary images. Our modification on CoreBoot only adds 3.9% on its total size (120.2KB V.S. 115.7KB). The enclave.so linked against Tlibaurora is 696KB in size and 1MB including runtime stack and heap manager. Smaller codebase denotes smaller TCB introduced.

TABLE I
MEASURING AURORA'S OVERHEAD BY CALCULATING PI.

Interval	Time cost (s)		Overhead ratio	
	70us	150us	70us	150us
Baseline	8.545	8.635	0	0
1000ms	9.045	9.025	5.85%	4.52%
100ms	9.605	9.590	12.40%	11.06%
10ms	10.180	10.455	18.90%	21.08%

C. Code Quality

To avoid exploitable vulnerabilities, we use well known static analysis tool Clang Static Analyzer[4] over AURORA's code base and fix all bugs we found. Besides, as AURORA is quite small and its complexity is obviously lower than that of the formally verified microkernel [31], we believe it is reasonable to put AURORA within reach of formal verification.

D. Limitation

Although SMM-based mechanism can be used to route many peripheral I/O events, it itself cannot be used to protect the framebuffers and therefore fall short of providing a trusted display. This is because SMRAM area by default starts at the same address as the VGA space, therefore SMVisor cannot obtain the frame buffer. It can be solved by redirecting SMRAM to another higher memory area without overlaying the VGA space. However, as SMM-based protection has performance implications [32], we recommend that users can use Intel PAVP (assisted by Intel ME) and SGX [33] for real-time scenarios such as an online-chatting conference.

VI. EVALUATION

In this section, we evaluate the performance of AURORA framework and the trusted I/O paths. Our experiments are carried out on an Intel Core i7-7700HQ 2.8GHz CPU with 16GB of memory, running Ubuntu 16.04 LTS and SGX SDK 2.4 and SGX driver 1.9.

A. Framework Overhead

We select pi_css5[5] program, which has no interaction with the external system, to measure the performance of AURORA with as little noise as possible. We ran the program till achieving 4,000,000 digits of precision, and used two durations (70us and 150us) to emulate different real-world environments.

Specifically, we ran two threads: one thread (T1) running Pi number calculation, the other thread (T2) requesting the ashmd module to trigger an SMI in a given interval. Firstly, we ran T1 without the interference of T2 and took the time cost as a baseline. Then we started T2 to see the slowdown of T1. From Table I, we observe that when the interval decreases, the overhead increases. The worst case of overhead is around 21%, where *smcalls* are requested too frequently. Such a situation is rare in real world applications because an enclave has to

[4]http://clang-analyzer.llvm.org/index.html
[5]http://myownlittleworld.com/miscellaneous/computers/piprogram.html

TABLE II
BREAKDOWN OF THE TRUSTED CLOCK SERVICE

Action Step	Time Cost(us)
EPC encryption	2
Copy to DRAM	2
Switch to SMM	13
Copy to SMRAM	0
SMM decryption	3
Clock Service	44
SMM encryption	3
Copy to DRAM	0
Return and enter SGX	12
Copy to EPC	3
EPC decryption	2

execute its own logic. We observe that intensive requests may impact the time-sensitive tasks on the same system. Since *smcalls* are forwarded by ashmd module, it can use a threshold to block a malicious enclave from abusing. In our current setting, we allow an enclave to request up 10,000 times per second, which introduces about 11% overhead to the system.

B. Trusted Clock Benchmark

For this experiment, we measured the complete trusted clock procedure for 1,000 times and used the average value. Table II shows the time cost for each step in a trusted clock path, as explained in § III-B. We can see that the clock service takes most of the time. This is because 1) the RTC driver has to read clock value twice to check if the clock is updating its time data; 2) The RTC involves several INS instructions to read each field of a calendar time, and costs 14us to obtain a complete wall-clock time in one request; 3) The other 4 timers cost roughly 10us in sum. The total time cost (84us) satisfies the requirement of real-world trusted timestamps.

For comparison, we measured the performance of other clock providers. The results are shown in Table III. Due to the fact that there are no input dependent branches in the secure channel (the channel simply transfers the I/O packets), we argue that our secure session is safe from side-channel attacks such as the timing attacks. Among existing approaches, AURORA outperforms remote clock (the 2nd row) and Intel's reference clock (the 3rd row) by introducing very low latency, while achieving the same resolution (nanosecond-level) as OS services (the 4th row).

C. Serial Port Output Benchmark

It is rather difficult to measure the overall time during which a printer accepts and finishes a print job, because we have to re-flash the printer firmware to hook its time function. Therefore, we redirected the serial port to a local file. To compare the serial output performance between native Linux and AURORA, we measured the time cost of writing the test data of different sizes to the serial-port address in Linux and in AURORA, respectively. Table IV shows the experimental results. AURORA performs better than native Linux because AURORA uses batch mechanism (§ III-G) to reduce the frequent mode transitions while Linux has more user/kernel mode transitions when writing large data to a serial port. Note that, for the larger outputted data, the speedup decreases due to cryptographic computations in AURORA.

D. Trusted USB Storage Benchmark

To compare the overhead introduced when applying AURORA's trusted I/O path on USB storage devices, we used *dd* program with options fsync and direct to write variable sizes of contents to a USB mass storage device on native Linux system as the baseline. To avoid the side-effect of any buffer mechanism, we use Linux raw device to mount and initialize the USB device. The throughput results are shown in Table V where the size of each block is set to 4KB. AURORA achieves approximately 90% of the baseline throughput when writing 1GB to the device. The major overheads are contributed by SMM/Protected mode transitions and cryptographic computations on each block.

E. Security Effectiveness

In this section, we evaluate AURORA's reliability with several security tests.

Keylogging Attack. To evaluate the effectiveness of AURORA's trusted input path, we deployed multiple spyware to get a user's inputs under trusted input mode, including a stealthy root keylogger[6], a rootless X11-based keylogger ixkeylog[7], a kernel-level rootkit keylogger[8], and a remote keylogger[9]. None of them can obtain the user's inputs.

Output Corruption Attack. We leveraged a DMA-based NIC device to launch output corruption attack when using Aurora's trusted serial printer service. Since SMRAM and EPC RAM are strongly isolated by architectural protections, only meaningless content (0xFF) is obtained. Therefore no secrets are leaked. We then conducted another DMA attack to corrupt SMM drivers outside of SMRAM. SMVisor detected its integrity tampered and rejected subsequent requests, then notified the enclave application. Moreover, we conducted another DMA attack to corrupt the content of shared memory of the secure session. Both SMVisor and Tlibaurora can verify the broken MAC and restart a new session.

Time Deception Attack. To evaluate AURORA's trusted clock, we intentionally modified the RTC when an enclave issued a request for trusted clock. Tlibaurora detected the attacks successfully and indicated a failure. For instance, gettimeofday() returns -1 and sets the global variable *errno* appropriately. Existing C library specification does not have a flag indicating time attacks, the enclave logic may keep requesting until obtaining a valid time value. We support failure handling in Tlibaurora to help enclaves deal with such situations.

Storage Deception Attack. We modified the kernel driver of SCSI device and randomly dropped several disk I/O requests intentionally. SMVisor detected such accidental conditions and notified the Tlibaurora of corresponding enclave.

[6]https://github.com/vim2meta/keylogger
[7]https://github.com/dorneanu/ixkeylog
[8]https://github.com/arunpn123/keylogger
[9]https://github.com/EinBaum/Totally-Not-A-Virus

TABLE III
COMPARISON OF EXISTING CLOCK SERVICES THAT CAN BE USED FOR SGX ENCLAVES. CLOCK SERVICES INCLUDE NETWORK TIME PROTOCOL (NTP), PRECISION TIME PROTOCOL (PTP), AND THE PLATFORM SOFTWARE (PSW) SUPPORTED BY INTEL MANAGEMENT ENGINE (ME)

Clock Provider	Approach	Type	Resolution	Request Cost	Latency	Security	Use Cases
Remote Clock	NTP/PTP	absolute	1s	>100ms	high	trusted	Town Crier [16]
Intel ME	PSW	relative	1s	10.3ms	medium	trusted	SGX-Tor [34]
OS Kernel	OCALL	absolute	1ns	6us	low	untrusted	Panoply [15]
Hardware Clock	*smcall*	absolute	1ns	69us	low	trusted	Aurora-OpenSSL VII-B

TABLE IV
SERIAL-PORT BENCHMARK COMPARISON BETWEEN LINUX AND AURORA.

Payload Size(KB)	Linux(s)	Aurora(s)	Speedup(%)
4	0.03	0.03	0.0
64	0.32	0.24	25.0
256	1.08	0.87	19.4
1024	3.95	3.43	13.2

TABLE V
STORAGE THROUGHPUT COMPARISON BETWEEN LINUX AND AURORA.

Payload Size(MB)	Linux (MB/s)	Aurora (MB/s)	Slowdown (%)
4	32.9	31.8	3.3
64	40.9	39.2	4.2
256	42.7	40.4	5.3
1024	53.2	47.5	10.7

In our current setting, the Tlibaurora will automatically try issuing the lost I/O requests three times so as to avoid storage failure. In our experiments, the enclave finally received the attack warning from the Tlibaurora and logged these events for further forensic analysis.

VII. CASE STUDIES

Aurora provides uniform abstractions (standard POSIX APIs) for the SGX applications, which need not be modified, to maintain platform-independence and thus achieve nice usability. We implemented trusted I/O paths for three real-world applications to illustrate the usability of AURORA.

A. Secure OpenSSH Login

Secure Shell (SSH) is widely used for shell access on UNIX-like systems. An SSH server uses a username and a password to authenticate an SSH client. If the client is infected with malware, the login credential can be stolen by keyloggers. To demonstrate the effectiveness of AURORA's trusted input path, we modified OpenSSH 7.7 to protect its client login process. Specifically, we ported passphrase related logic into an enclave, and used AURORA's *trusted input path* to get passwords which users input. We call the enhanced client as Aurora-OpenSSH client, as depicted in Figure 4.

Aurora-OpenSSH client first requests SMVisor to intercept the user's keyboard events. This interception adds around 13% overhead per keystroke. Only after SMVisor routes the keyboard interrupt into itself and acknowledges to the client, will

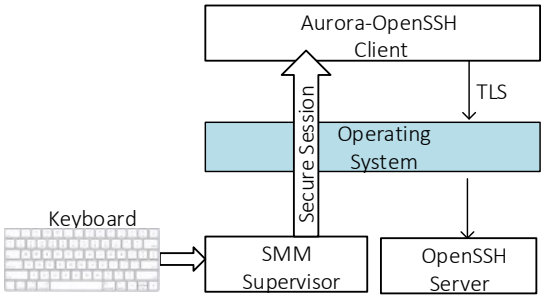

Fig. 4. Aurora-OpenSSH with trusted input path.

the prompt "username@hostname password:" be displayed on the screen. While the user is typing the passphrase, the client does not display any content on the screen, achieving the same effect as in the native OpenSSH client.

The user's input is buffered inside SMRAM. When the user releases Enter key, the password is then encrypted and sent to the secure channel, and SMVisor exits trust input mode. Aurora-OpenSSH client reclaims the password message and sends it to the server. Note that the plaintext password is only available in SMRAM and enclave. The path between SMRAM and enclave is protected by AURORA's secure channel and the path between Aurora-OpenSSH client and OpenSSH server is protected by TLS session.

B. Secure OpenSSL Session

SSL/TLS protocols are in widespread use in web browsing, email, instant messaging, and voice-over-IP, etc. An SSL/TLS session starts with SSL/TLS handshake protocol, including authentication, key exchange, etc. The procedures rely on system date and time. The SSL/TLS server needs to provide a certificate with a timestamp indicating the expiration time, and the SSL/TLS client needs to verify this certificate. Most of all, both parties require a reliable time source to detect possible timeout. For instance, both *ClientHello* and *ServerHello* messages use the system time to prevent replay attacks. If the time is emulated by an untrusted source, it may compromise the security of OpenSSL sessions.

One of the in-enclave SSL/TLS projects is SGX-OpenSSL[10] from SGX-Tor project [34]. It does not trust the system storage, therefore its server side creates the certificate inside the enclave each time it receives a new connection request from the client side. We enhanced the TLS handshake by

[10]https://github.com/sparkly9399/SGX-OpenSSL

TABLE VI
PERFORMANCE COMPARISON BETWEEN NATIVE SGX-OPENSSL AND AURORA-OPENSSL.

	SGX-OpenSSL	Aurora-OpenSSL
Certificate Generation	77.4ms	102.5ms
TLS Handshaking	2.8ms	3.4ms

TABLE VII
TPC-H BENCHMARK COMPARISON BETWEEN NATIVE SGX-SQLITE AND AURORA-SQLITE.

Query	SGX-SQLite(s)	Aurora-SQLite(s)	Slowdown(%)
02	4.68	5.10	8.97
11	1.29	1.42	10.08
16	1.08	1.10	5.30
17	91.26	93.30	2.23
18	24.98	25.91	3.72
19	93.15	98.25	5.47
21	39.68	43.16	9.04

using AURORA's trusted clock. Specifically, we replaced time-related OCALLs in the original project with AURORA's libaurora. We measured the time cost of certification generation at server side and TLS handshake at client side for 10,000 runs and take the average value. We also measured the native SGX-OpenSSL using original OCALLs. As shown in Table VI, in our LAN setting, Aurora-OpenSSL introduced about 32% latency in certificate generation and 21% in the TLS handshaking because both of them use AURORA's trusted clock. We anticipate the overhead ratio decreased in WAN environment.

C. Secure SQLite Database

Databases are widely used to store financial transaction records and other sensitive information. Some databases are built upon block devices, while maintaining its own caching mechanisms and storage policies without support of OS's file system, e.g. SQLite database.

We integrated AURORA's Tlibaurora into existing SGX-SQLite projects[11] and added code to support standard file system calls such as *open*, *read*, *write*, *stat*, *lstat*, *fstat*, *fsync*, *fcntl*, *ftruncate* and *unlink*. We then eliminated the file-related OCALLs for the untrusted system. To avoid password leak, we use AURORA's trusted input path to obtain users' password from keyboard devices. Moreover, AURORA's secure session protects the confidentiality and integrity of data between SQLite enclaves and SMVisor.

We evaluated the enhanced SQLite performance by running standardized TPC-H benchmark[12] over a large database. We make minor changes to these benchmark queries in order to make them possible to be executed in SQLite. Unfortunately, not all queries can be executed. To directly measure the overhead introduced by AURORA's infrastructure, we set the synchronize flag to FULL to avoid the uncertainty of I/O caching. When SQLite invokes Tlibaurora file APIs, it opens the USB storage device in direct I/O mode and reads/writes data using 4KB block size.

Table VII shows the successfully executed queries and their results of native SGX-SQLite and AURORA-SGLite respectively. In our experiments, no more than 10.08% overhead is introduced because of the extra encrypt/decrypt computation and mode transitions in AURORA. Note that these are the worst-case overheads (because we have set PRAGMA synchronous to FULL) as almost all databases have their own optimized caching mechanisms for better performance.

[11]https://github.com/yerzhan7/SGX_SQLite
[12]http://www.tpc.org/tpch/

VIII. RELATED WORK

Our technique was inspired by Scotch [35] which is the first work that combines SGX and SMM to audit VM resource usage. Its motivation differs from ours. Similar to AURORA's SMVisor, previous research such as HyperCheck [36], HyperSentry [37] and IOCheck [38], also employ a dedicated SMI handler to protect the integrity of the OS kernel, hypervisor or firmware, respectively. We next discuss related work of other trusted I/O architectures and trusted paths.

A. Trusted I/O Architectures

SGXIO [39] is a conceptual framework that discusses how to provide trusted generic I/O paths for SGX enclaves. It introduces a trusted hypervisor to assist the establishment of the trusted path and requires users to port drivers into enclaves. However, SGXIO is a conceptual design without any implementation and evaluation. Moreover, it is hard for users to port commodity drivers into an enclave because 1) enclave mode does not support privileged instructions like IN/OUT or RDMSR/WRMSR with which drivers read/write I/O ports; 2) it is unclear in the paper [39] how to correctly partition drivers. In comparison, AURORA's drivers are invoked in SMM without any instruction restricted. They are monitored and regulated by SMVisor protected inside SMRAM. This reusing technique allows AURORA easily deployed.

Zhou et al. [30] introduce a micro-hypervisor (named Wimpy) under OS to build trusted paths (TP) between program end-points (PE) and device end-points (DE). They require the PE of a TP includes the device drivers for DEs associated with the TP, and admit that *"running the PE in Ring 3 makes DE driver porting more difficult"*. Although AURORA and Wimpy share many common security goals, e.g. interrupt isolation and MMIO protection, AURORA exploits CPU features to protect the PEs and reuse DEs securely. As a result, AURORA has smaller TCB than Wimpy.

Intel SGX platform services (PSW) [17] uses management engines (ME) to provide trusted time and monotonic counters services by running a co-processor with integrated NIC, RTC and SPI flash, etc. It brings separated hardware that cannot be controlled by untrusted system. However, since Intel ME runs simultaneously with the main CPUs, we believe that it is difficult and insecure for Intel ME to implement secure human-interface input for enclaves as AURORA does. Because the CPU controlled by untrusted OS and the ME co-processor controlled by trusted software may race a DMA access to

the keyboard buffer, which cannot guarantee protection on user's confidential input. In comparison, AURORA's SMVisor in nature preempts the untrusted OS.

B. Specific Trusted Paths

Trusted Input Paths. On the desktop side, TrustLogin [40] uses SMM to protect user passwords. It caches the password inside the SMRAM; when the user releases the Enter key, TrustLogin places the password inside the packets of the NIC buffer. In contrast, AURORA does not need to intercept OS networking services, thus decreasing overall impact surfaces. Fidelius [41] leverages a Raspberry Pi to implement a secure channel between the keyboard and the hardware enclave. The specific LED is turned on when a secure channel is established. AURORA does not need any specialized I/O devices and reuse existing hardware devices. On the server side, SafeKeeper [13] leverages SGX to protect the password databases on untrusted clouds. It uses several strategies to mitigate attacks such as phishing. As Intel SGX is also available on personal laptops and mini PCs (i.e., NUCs), we take advantage of SGX to protect personal password when the user logs in on the client side, which differs from their scenarios. On the mobile side, TrustUI [42] exploits ARM TrustZone to build a trusted path between a user and a service provider, because ARM TrustZone can isolate physical memory and peripheral interrupts. In design, SMVisor is similar to the trusted OS inside TrustZone's secure world.

Trusted Clock Paths. Intel PSW [17] supports coarse-grained trusted time but does not provide a wall-clock time. AURORA provides high resolution and absolute clock. ShieldBox [43] achieves high-precision yet low-latency clock service by on-NIC PTP clock, however, the time source is not secure because enclaves cannot detect if NIC-Timer is tampered. By contrast, AURORA can detect time attack via a validation algorithm. Déjà Vu [44] implements a reference clock thread using transactional synchronization extensions (TSX) to protect a trustworthy source of time measurement. Déjà Vu's goal is to detect interrupt-based attacks, while AURORA can provide a general time service for enclaves. Compared to our prior work [45], which provides a trusted clock to enclaves, AURORA proposes a unified framework for different I/O devices and presents more evaluation on real-world applications. For distributed enclaves, ROTE [46] proposes a protocol to provide a monotonic counter, which has high latency than AURORA's trusted clock service.

Trusted Storage Paths. AuditedIO [47] leverages SGX and a kernel module to implement verifiable data storage for disk I/O operations. It requires a programmable SSD device and modifies the firmware. By contrast, AURORA aims for a trusted-path framework which can be used to support general storage devices. Jiang [48] builds a trusted path between a USB proxy device and an enclave. The proxy device uses LED display for user verification. It plays the role of AURORA's SMVisor while AURORA does not need to introduce dedicated hardware. BASTION-SGX [49] modifies the Bluetooth firmware and establishes trusted paths between Bluetooth devices and enclave programs. It has similar threat model with AURORA and rules the privileged software (OS, drivers, etc.) out of the TCB. Pesos [50] builds a trusted path between enclaves and cloud-based storage, and supports policy-based object protection. Still, Pesos requires a programmable storage HDD named Kinetic Open Storage, while AURORA does not.

IX. Conclusion

We present AURORA, a novel architecture which provides trusted I/O paths on client Intel SGX platforms. Based on AURORA, we design and implement several trusted I/O paths for SGX enclaves, including HID keyboard, serial-port printer, USB mass storage and the hardware clock. To the best of our knowledge, we are the first to provide these *realistic* trusted I/O paths for enclaves. Our implementation demonstrates that AURORA is extensible and transparent with underlying commodity systems. Security and performance evaluations with real-world applications show that AURORA can mitigate several I/O related attacks and provide trusted I/O paths with low overhead.

Acknowledgement

The authors would like to thank Kai Huang from Intel Corporation and Shweta Shinde from National University of Singapore for their generous help and constructive comments. The authors also thank the anonymous reviewers for their valuable feedback that help improve the article.

References

[1] E. W. Felten, "Understanding trusted computing: Will its benefits outweigh its drawbacks?" *IEEE Security & Privacy*, vol. 1, no. 3, pp. 60–62, 2003.

[2] F. McKeen, I. Alexandrovich, A. Berenzon, C. V. Rozas, H. Shafi, V. Shanbhogue, and U. R. Savagaonkar, "Innovative instructions and software model for isolated execution," in *HASP 2013, The Second Workshop on Hardware and Architectural Support for Security and Privacy, Tel-Aviv, Israel, June 23-24, 2013*, 2013, p. 10.

[3] A. Baumann, M. Peinado, and G. C. Hunt, "Shielding applications from an untrusted cloud with haven," *ACM Trans. Comput. Syst.*, vol. 33, no. 3, pp. 8:1–8:26, 2015.

[4] T. Hunt, Z. Zhu, Y. Xu, S. Peter, and E. Witchel, "Ryoan: A distributed sandbox for untrusted computation on secret data," in *12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016, Savannah, GA, USA, November 2-4, 2016.*, 2016, pp. 533–549.

[5] S. Arnautov, B. Trach, F. Gregor, T. Knauth, A. Martin, C. Priebe, J. Lind, D. Muthukumaran, D. O'Keeffe, M. Stillwell, D. Goltzsche, D. M. Eyers, R. Kapitza, P. R. Pietzuch, and C. Fetzer, "SCONE: secure linux containers with intel SGX," in *12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016, Savannah, GA, USA, November 2-4, 2016.*, 2016, pp. 689–703.

[6] H. Nguyen and V. Ganapathy, "Engarde: Mutually-trusted inspection of SGX enclaves," in *37th IEEE International Conference on Distributed Computing Systems, ICDCS 2017, Atlanta, GA, USA, June 5-8, 2017*, 2017, pp. 2458–2465.

[7] H. Nguyen, B. Acharya, R. Ivanov, A. Haeberlen, L. T. X. Phan, O. Sokolsky, J. Walker, J. Weimer, W. Hanson, and I. Lee, "Cloud-based secure logger for medical devices," in *2016 IEEE First International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*, June 2016, pp. 89–94.

[8] 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, SP 2015, San Jose, CA, USA, May 17-21, 2015*, 2015, pp. 38–54.

[9] I. Corporation, "Intel® 64 and ia-32 architectures software developer's manual, volume 3d," 2016.

[10] S. Checkoway and H. Shacham, "Iago attacks: why the system call API is a bad untrusted RPC interface," in *Architectural Support for Programming Languages and Operating Systems, ASPLOS '13, Houston, TX, USA - March 16 - 20, 2013*, 2013, pp. 253–264.

[11] P. Mittal, A. Khurshid, J. Juen, M. Caesar, and N. Borisov, "Stealthy traffic analysis of low-latency anonymous communication using throughput fingerprinting," in *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*, 2011, pp. 215–226.

[12] D. Silver, S. Jana, D. Boneh, E. Y. Chen, and C. Jackson, "Password managers: Attacks and defenses," in *Proceedings of the 23rd USENIX Security Symposium, San Diego, CA, USA, August 20-22, 2014.*, 2014, pp. 449–464.

[13] K. Krawiecka, A. Kurnikov, A. Paverd, M. Mannan, and N. Asokan, "Safekeeper: Protecting web passwords using trusted execution environments," in *Proceedings of the 2018 World Wide Web Conference on World Wide Web, WWW 2018, Lyon, France, April 23-27, 2018*, 2018, pp. 349–358.

[14] C. Tsai, D. E. Porter, and M. Vij, "Graphene-sgx: A practical library OS for unmodified applications on SGX," in *2017 USENIX Annual Technical Conference, USENIX ATC 2017, Santa Clara, CA, USA, July 12-14, 2017.*, 2017, pp. 645–658.

[15] S. Shinde, D. Le Tien, S. Tople, and P. Saxena, "Panoply: Low-TCB Linux Applications with SGX Enclaves." Internet Society, 2017. [Online]. Available: https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/panoply-low-tcb-linux-applications-sgx-enclaves/

[16] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, 2016, pp. 270–282.

[17] Intel. (2016) Trusted time and monotonic counters with intel sgx platform services. [Online]. Available: https://software.intel.com/sites/default/files/managed/1b/a2/Intel-SGX-Platform-Services.pdf

[18] ——. (2016) Intel sgxssl library. [Online]. Available: http://math.tntech.edu/rafal/cliff11/index.html

[19] P.-L. Aublin. (2017) Talos: Secure and transparent tls termination inside sgx enclaves. [Online]. Available: https://www.doc.ic.ac.uk/research/technicalreports/2017/DTRS17-5.pdf

[20] bl4ck5un. (2017) mbedtls-sgx: a sgx-friendly tls stack. [Online]. Available: https://github.com/bl4ck5un/mbedtls-SGX

[21] wolfssl. (2017) Embedded ssl/tls library for applications, devices, iot, and the cloud. [Online]. Available: https://www.wolfssl.com/

[22] I. Anati, S. Gueron, S. P. Johnson, and V. Scarlata, "Innovative technology for cpu based attestation and sealing," in *HASP 2013, The Second Workshop on Hardware and Architectural Support for Security and Privacy, Tel-Aviv, Israel, June 23-24, 2013*, 2013.

[23] G. Chen, S. Chen, Y. Xiao, Y. Zhang, Z. Lin, and T. H. Lai, "Sgxpectre attacks: Leaking enclave secrets via speculative execution," in *Security and Privacy (SP), 2019 IEEE Symposium*. IEEE, 2019.

[24] S. van Schaik, A. Milburn, S. Österlund, P. Frigo, G. Maisuradze, K. Razavi, H. Bos, and C. Giuffrida, "RIDL: Rogue in-flight data load," in *S&P*, May 2019.

[25] S. Silvestro, H. Liu, C. Crosser, Z. Lin, and T. Liu, "Freeguard: A faster secure heap allocator," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017*, B. M. Thuraisingham, D. Evans, T. Malkin, and D. Xu, Eds. ACM, 2017, pp. 2389–2403. [Online]. Available: https://doi.org/10.1145/3133956.3133957

[26] X. Ruan, "Platform embedded security technology revealed."

[27] TCG, "Trusted platform module library. part 1: Architecture. family 2.0. revision 01.16." TCG, 2014.

[28] M. Schwarz, S. Weiser, D. Gruss, C. Maurice, and S. Mangard, "Malware guard extension: Using SGX to conceal cache attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment - 14th International Conference, DIMVA 2017, Bonn, Germany, July 6-7, 2017, Proceedings*, 2017, pp. 3–24.

[29] *Intel ® Integrated Performance Primitives Cryptography*, 2nd ed., Intel, 2007.

[30] Z. Zhou, M. Yu, and V. D. Gligor, "Dancing with Giants: Wimpy Kernels for On-Demand Isolated I/O." IEEE, May 2014, pp. 308–323. [Online]. Available: http://ieeexplore.ieee.org/document/6956572/

[31] G. Klein, K. Elphinstone, G. Heiser, J. Andronick, D. Cock, P. Derrin, D. Elkaduwe, K. Engelhardt, R. Kolanski, M. Norrish, T. Sewell, H. Tuch, and S. Winwood, "sel4: formal verification of an OS kernel," in *Proceedings of the 22nd ACM Symposium on Operating Systems Principles 2009, SOSP 2009, Big Sky, Montana, USA, October 11-14, 2009*, 2009, pp. 207–220.

[32] B. Delgado and K. L. Karavanic, "Performance implications of system management mode," in *Proceedings of the IEEE International Symposium on Workload Characterization, IISWC 2013, Portland, OR, USA, September 22-24, 2013*, 2013, pp. 163–173.

[33] M. Hoekstra, R. Lal, P. Pappachan, V. Phegade, and J. del Cuvillo, "Using innovative instructions to create trustworthy software solutions," in *HASP 2013, The Second Workshop on Hardware and Architectural Support for Security and Privacy, Tel-Aviv, Israel, June 23-24, 2013*, 2013, p. 11.

[34] S. M. Kim, J. Han, J. Ha, T. Kim, and D. Han, "Enhancing security and privacy of tor's ecosystem by using trusted execution environments," in *14th USENIX Symposium on Networked Systems Design and Implementation, NSDI 2017, Boston, MA, USA, March 27-29, 2017*, 2017, pp. 145–161.

[35] K. Leach, F. Zhang, and W. Weimer, "Scotch: Combining software guard extensions and system management mode to monitor cloud resource usage," in *Research in Attacks, Intrusions, and Defenses - 20th International Symposium, RAID 2017, Atlanta, GA, USA, September 18-20, 2017, Proceedings*, 2017, pp. 403–424.

[36] J. Wang, A. Stavrou, and A. K. Ghosh, "Hypercheck: A hardware-assisted integrity monitor," in *Recent Advances in Intrusion Detection, 13th International Symposium, RAID 2010, Ottawa, Ontario, Canada, September 15-17, 2010. Proceedings*, 2010, pp. 158–177.

[37] A. M. Azab, P. Ning, Z. Wang, X. Jiang, X. Zhang, and N. C. Skalsky, "Hypersentry: enabling stealthy in-context measurement of hypervisor integrity," in *Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010*, 2010, pp. 38–49.

[38] F. Zhang, H. Wang, K. Leach, and A. Stavrou, "A framework to secure peripherals at runtime," in *Computer Security - ESORICS 2014 - 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11, 2014. Proceedings, Part I*, 2014, pp. 219–238.

[39] S. Weiser and M. Werner, "SGXIO: Generic Trusted I/O Path for Intel SGX." ACM Press, 2017, pp. 261–268. [Online]. Available: http://dl.acm.org/citation.cfm?doid=3029806.3029822

[40] F. Zhang, K. Leach, H. Wang, and A. Stavrou, "TrustLogin: Securing Password-Login on Commodity Operating Systems." ACM Press, 2015, pp. 333–344. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2714576.2714614

[41] S. Eskandarian, J. Cogan, S. Birnbaum, P. C. W. Brandon, D. Franke, F. Fraser, G. G. Jr., E. Gong, H. T. Nguyen, T. K. Sethi, V. Subbiah, M. Backes, G. Pellegrino, and D. Boneh, "Fidelius: Protecting user secrets from compromised browsers," 2019.

[42] W. Li, M. Ma, J. Han, Y. Xia, B. Zang, C. Chu, and T. Li, "Building trusted path on untrusted device drivers for mobile devices," in *Asia-Pacific Workshop on Systems, APSys'14, Beijing, China, June 25-26, 2014*, 2014, pp. 8:1–8:7.

[43] B. Trach, A. Krohmer, F. Gregor, S. Arnautov, P. Bhatotia, and C. Fetzer, "Shieldbox: Secure middleboxes using shielded execution," in *Proceedings of the Symposium on SDN Research, SOSR 2018, Los Angeles, CA, USA, March 28-29, 2018*, 2018, pp. 2:1–2:14.

[44] S. Chen, X. Zhang, M. K. Reiter, and Y. Zhang, "Detecting privileged side-channel attacks in shielded execution with déjà vu," in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, AsiaCCS 2017, Abu Dhabi, United Arab Emirates, April 2-6, 2017*, 2017, pp. 7–18.

[45] H. Liang and M. Li, "Bring the missing jigsaw back: Trustedclock for SGX enclaves," in *Proceedings of the 11th European Workshop on Systems Security, EuroSec@EuroSys 2018, Porto, Portugal, April 23, 2018*, 2018, pp. 8:1–8:6. [Online]. Available: https://doi.org/10.1145/3193111.3193119

[46] S. Matetic, M. Ahmed, K. Kostiainen, A. Dhar, D. M. Sommer, A. Gervais, A. Juels, and S. Capkun, "ROTE: rollback protection for trusted execution," in *26th USENIX Security Symposium, USENIX Security 2017, Vancouver, BC, Canada, August 16-18, 2017.*, E. Kirda and T. Ristenpart, Eds. USENIX Association, 2017, pp. 1289–1306. [Online]. Available: https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/matetic

[47] N. Balakrishnan, L. Carata, T. Bytheway, R. Sohan, and A. Hopper, "Non-repudiable disk I/O in untrusted kernels," in *Proceedings of the 8th Asia-Pacific Workshop on Systems, Mumbai, India, September 2, 2017*, 2017, pp. 24:1–24:6.

[48] Y. J. Jang, "Building trust in the user i/o in computer systems," 2017.

[49] T. Peters, R. Lal, S. Varadarajan, P. Pappachan, and D. Kotz, "BASTION-SGX: bluetooth and architectural support for trusted I/O on

SGX," in *Proceedings of the 7th International Workshop on Hardware and Architectural Support for Security and Privacy, HASP@ISCA 2018, Los Angeles, CA, USA, June 02-02, 2018*, 2018, pp. 3:1–3:9.

[50] R. Krahn, B. Trach, A. Vahldiek-Oberwagner, T. Knauth, P. Bhatotia, and C. Fetzer, "Pesos: policy enhanced secure object store," in *Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, April 23-26, 2018*, 2018, pp. 25:1–25:17. [Online]. Available: https://doi.org/10.1145/3190508.3190518