Reviewer Comments:

Reviewer: 1

Recommendation: AQ - Publish With Minor, Required Changes

Comments:

Thank you very much for the updated version of the document.

== Clarifications ==

Abstract: line 16 could give the impression to readers that other hardware manufacturers also provide SGX: "hardware manufacturers such as Intel released a new processor feature called Software Guard eXtension (SGX)".

I would suggest to make it clear that hardware vendors propose TEEs; Intel has implemented one called SGX.

Threat model:

-I would suggest to explicitly state that the attacker does not have access to the hardware. This would ease readability.

-page 7: "Such a sibling thread will block the possibility of side-channel attacks when hyper-threading is active.". Hyperthreading should be disabled for security reasons (see https://marc.info/?l=openbsd-tech&m=153504937925732&w=2for example).

Trusted time: Intel SGX v2 has access to trusted time (RDTSC), see section "39.6.1 Illegal Instructions" of the Intel® 64 and IA-32 Architectures Software Developer’s Manual. How does it affect your solution?

It would be interesting to see more details about Intel PVAP. Can it be integrated with Aurora? Can it provide additional guarantees?

== Evaluation ==

Table 4 (serial port performance), what is the performance with a larger payload (e.g. 1MB)?

TPC-H results, why are some requests not working?

== Minor comments ==

-Will the authors make the code available? It would be very beneficial for the community for building new secure systems with trusted I/O.

-introduction: rely \*on\* the clock value from untrusted systems

-p6, afterward\*s\*

Additional Questions:

1. Is the topic appropriate for publication in these transactions?: Adequate Match

1. Is the paper technically sound?: Yes

2. How would you rate the technical novelty of the paper?: Novel Enough for Publication

Explain: The problem of trusted I/O paths is an important problem for secure computing. The authors present an interesting and novel approach that combines Intel SGX with SMM. I believe the approach is worth being published.

3. Is the contribution significant?: Incremental

4. Is the coverage of the topic sufficiently comprehensive and balanced?: Yes

5. Rate the Bibliography: Satisfactory

1. How would you rate the overall organization of the paper?: Satisfactory

2. Are the title and abstract satisfactory?: Yes

3. Is the length of the paper appropriate? If not, recommend what should be added or eliminated.: Yes

4. Are symbols, terms, and concepts adequately defined?: Yes

5. How do you rate the English usage?: Satisfactory

Reviewer: 2

Recommendation: AQ - Publish With Minor, Required Changes

Comments:

Thank you for revising the draft. Most of my major comments seem to be addressed in the updated version. The paper needs some smaller edits, as listed in my review.

Additional Questions:

1. Is the topic appropriate for publication in these transactions?: Adequate Match

1. Is the paper technically sound?: Yes

2. How would you rate the technical novelty of the paper?: Novel Enough for Publication

Explain: The paper presents Aurora architecture for trusted I/O paths for enclave applications on Intel platforms with SGX and SMM support. Specifically, the paper outlines design for securing communication with a keyboard, printer clocks, and storage in the presence of an untrusted OS. By default, Intel SGX does not guarantee secure interface to devices, and Aurora bridges this gap for applications where it is essential to have a trusted path to one or more I/O devices. The authors make use of SMM which is protected from the OS to communicate with these devices over a trusted channel.

3. Is the contribution significant?: Incremental

4. Is the coverage of the topic sufficiently comprehensive and balanced?: Yes

5. Rate the Bibliography: Satisfactory

1. How would you rate the overall organization of the paper?: Could be improved

2. Are the title and abstract satisfactory?: Yes

3. Is the length of the paper appropriate? If not, recommend what should be added or eliminated.: Yes

4. Are symbols, terms, and concepts adequately defined?: Not always

5. How do you rate the English usage?: Needs improvement

\* Paper summary

- The paper presents Aurora architecture for trusted I/O paths for enclave applications on Intel platforms with SGX and SMM support. Specifically, the paper outlines design for securing communication with a keyboard, printer clocks, and storage in the presence of an untrusted OS. By default, Intel SGX does not guarantee secure interface to devices, and Aurora bridges this gap for applications where it is essential to have a trusted path to one or more I/O devices. The authors make use of SMM which is protected from the OS to communicate with these devices over a trusted channel.

\* Comments on the revision effort

- Thank you for revising the draft. Most of my major comments seem to be addressed in the updated version. Some of them need more clarifications as listed below.

\* Following is my feedback on the revised version of the paper draft:

- Missing citations for important points in the following sections:

+ time deception attacks (Section 1)

+ monotonic counters and NVRAM (Section 1)

+ Local attestation (Section 2A)

+ SMM mode (Section 2B)

+ swell the TCB and attack vector (Section 2C)

+ existing software stacks in a secure manner (Section 2C)

+ smaller TCB is better (Section 5B)

+ Fix name for Jiang [48] to Jang (Section 8C)

- The two types of I/O paths are not defined but referred to in the introduction and Section 2 first para.

- Clarify the security properties of the SMM enclave (Section 2B)?

- Before explaining the details of 2 categories of I/O, consider adding sentences which explain the main difference between them (Section 2C)

- Section 2C, should it be trust-but-verify or verify-then-use instead of distrust-but-verify?

- Section 2D

+ Does the UEFI driver have a standard security specification that Aurora verifies, if not, how did you decide what to check?

+ The attacker will learn the I/O size and request-response sizes. Should that be explicitly scoped out of the attacker model, or does Aurora prevent such leakage?

+ Even if the size of input and output is protected, the adversary will still learn the fact that the event occurred, is this considered a leakage under your threat model?

- How does Aurora hook on the events of output requests by an enclave (Section 3B)?

- The workflow in Section 3B can largely be moved to the figure caption. Try to keep the high-level details in the main text. In that text, specify that the driver is UEFI driver.

- Section 3E, Aurora seems to be susceptible to time-of-check to time-of-use (TOCTOU) attack, if not, please clarify why.

- Consider renaming disconnection to termination in Section 3F.

- Consider renaming Section 3G to 'Security Enhancement and Performance Optimization'.

- Is nonce used for encryption (Section 3G)?

- For data obliviousness, if the blocks are of 4KB, they will have no random padding. All 4K size blocks which happen to have the same content will still leak. Please double check your scheme and ensure this attack is not possible.

- Claims of Aurora solving phishing attacks in Section 4A are wrong. Please use a different example.

- The technique of using a pre-shared secret melody has a better entropy than the previous scheme, but the paper should clarify that it assumes that this pre-shared secret is not known by the adversary (Section 4B).

- How does aurora detect that the hardware clocks are being altered in a consistent way (Section 4C)?

- In Section 4D, Can you list which all other storage systems Aurora can be applied to?

- Consider combining Section 5B and 5C

- Limitations for trusted display are understandable, but can you check how Fidelius achieves/ side-steps this?

- Add one more column to show the percentage slowdown in Table 6

- Do not make any claims about how Aurora has side-channel protection in certain cases (Section 6B) if it is explicitly out of the scope of the paper.

- Consider adding a comparison table with checks and crossed to clarify design goals and choices with respect to related work such as ROTE, can be added to the evaluation.

- Clarify how the storage deception attack detects denial-of-service if the adversary drops requests, if it is not possible, please scope it out.

- Clarify the reasons why Aurora anticipates overhead ratio to decrease in WAN environment (Section 7B), or remove the claim.

- Clarify which types of SQL queries were executed (e.g., select, insert, delete), how many of them failed due to configuration challenges (Section 7C).

- Last para in Section 8A is not readable due to awkward English, please consider cleaning it up.

- Minor language and presentation issues

+ move table 3, 4, 5 to page 8 for ease of reading. better to position the tables where they are first referred to in the text.