*Department of Electrical and Computing Engineering*

UNIVERSITY OF CONNECTICUT

## CSE 5095-004 (15626) & ECE 6095-006 (15284)
## Secure Computation and Storage: Spring 2016

# Oral Exam: Hardware

There are two problem classes in this oral exam booklet. During your oral exam you will be given this booklet and the instructor will select problems out of each class for you to solve in front of the white board. You have **45 minutes** to answer all three questions.

**Be neat and legible.** If the instructor can't understand your answer, no credit is given! 20% of the grade for each question concerns clear exposition by using the white board and oral explanation.

**Write your name in the space below.** Write your initials at the bottom of each page.

**THIS IS A CLOSED BOOK ORAL EXAM**

*Do not write in the boxes below*

| 1 (xx/150) | 2 (xx/300) | Total (xx/450) |
|---|---|---|
| | | |

**Name:**

**Student ID:**

**1. [150 points]:** Memory Integrity Checking, ORAM, and Encryption: Explain (a) and (based on a random coin toss) one out of (b) and (c):

**(a)** Tree based memory integrity checking:

(a) Which properties does memory integrity checking verify?

(b) How does chash work?

(c) For reading/writing data blocks a whole path from root to leaf needs to be verified: Why is the performance overhead only $20\%$?

(d) Explain the chash type solution used in SGX: What is the main difference?

(e) Why did Intel not simply use chash, what benefit does their solution offer?

**Initials:**

**(b)** Memory integrity checking based on incremental multiset hash functions:

(a) What is multiset collision resistance?

(b) Give an example of a multiset collision resistant hash function.

(c) Describe the offline checker (when does Timer gets incremented)?

(d) Define:

- Let $x_1$ be the cycle fo the first incorrect get operation when, e.g., $(v_t, t_1)$ is read from address $a$.
- Let $x_2$ be the first cycle when $(v_1, t_1)$ is written to address $a$.
- Let $x_3$ be the cycle of the first read from $a$ after $x_2$.

Prove:

- $x_2 < x_1$,
- $x_3 < x_1$,
- the read at $x_3$ reads the same pair that was written at $x_2$,
- $(v_1, t_1)$ cannot be written after $x_3$,
- $(v_1, t_1)$ cannot be written before $x_2$,
- $(v_1, t_1)$ cannot be written between $x_2$ and $x_3$,
- the pair $(v_1, t_1)$ is written only once but is read at least twice,
- conclude that breaking the offline checker implies breaking the multiset collsion resistance of the underlying hash.

**(c)** Path ORAM & Encryption:

(a) Give the definition of an ORAM: What is its main goal?

(b) Explain the working of Path ORAM.

(c) What properties need to be proven in order to conclude the security of Path ORAM? Prove one of these properties.

(d) Is $\infty$-ORAM an ORAM?

(e) Explain how AES encryption is used by Aegis (what is the performance of a read and a write, can ciphertexts be linked)?

(f) Explain how AES encryption is used by SGX (what is the performance of a read and a write, can ciphertexts be linked)?

**Initials:**

**2. [300 points]:** SGX & Sanctum: Explain both (a) and (b):

**(a)** SGX:

(a) What are the two main security properties offered by SGX? What do they mean?

(b) What is an enclave? How does it work at a global level? Explain its life cycle.

(c) In multicore processors resources are shared for performance reasons. Does this conflict with an enclave's security posture? As an example name one attack to which SGX is vulnerable and explain how it works.

(d) When an enclave is created, what does it contain? Try to be as detailed as possible. Explain the role of each of the segments within an enclave.

(e) When the LP (logical processor) wants to access an address, what global checks are being performed?

(f) Who is signing the results computed by an enclave and with what key, and where does this key come from? Why did Intel make this design choice?

(g) What is synchonous enclave exit? Explain the main ingredients of how it works and why it is designed this way. Does the enclave writer still need to take care of something?

(h) Why do we need page swapping? What is address translation? What is an extended page table? With an extended page table how is a physical address retrieved? Why do page tables need to be isolated in HW?

(i) Name five attack scenarios to which SGX could be vulnerable (given the current literature on SGX).

(j) Why does an enclave have the least priviledge level?

**(b)** Sanctum:

(a) What small HW modifications does Sanctum require (you do not need to go into the finest detail)? What is the purpose/aim of each modification? Why did the Sanctum designers not choose other methods to reach these aims?

(b) Explain the working of the security monitor; Draw the main components of Figures 6-1 and 6-2 in Victor's thesis and explain (why is the monitor in sofware, isn't this risky)?

(c) Does the security model of secure processor technology fall apart when a processor's attestation key leaks? Can a certification authority resolve this problem?

# End of Oral Exam

Please double check that you wrote your name on the front of the quiz.

**Initials:**