Exp 3: secure data path

Both PDF and code submissions are required.

Convert to PDF before uploading.

Prerequisite

- Read the project description: https://fxlin.github.io/p3-tee/helloworld/#app-2-secure-data-path-sdp-basic
- Read the sdp example source code (both CA and TA) as mentioned in the description
- Follow the project description, compile and run the sdp example.

Reproduce

Show a screenshot of you successfully running the SDP example. It must be generated by yourself. (20)

Q&A

Describe what the following commands do: INJECT, TRANSFORM, and DUMP. Use your own word (not ChatGPT etc); one sentence for each command (10)

The INJECT command takes the values from the non-secure buffer and copies it into the secure buffer.

The TRANSFORM command modifies from and to the secure input and output.

The DUMP command copies the value of the secure input to the non secure output.

Measurement

Modify the given sdp example to implement the following: INJECT X bytes of data; TRANSFORM the data by flipping every bit; DUMP the results.

Change the CA code. No need to define new commands. Just modify the existing command(s) as you see fit.

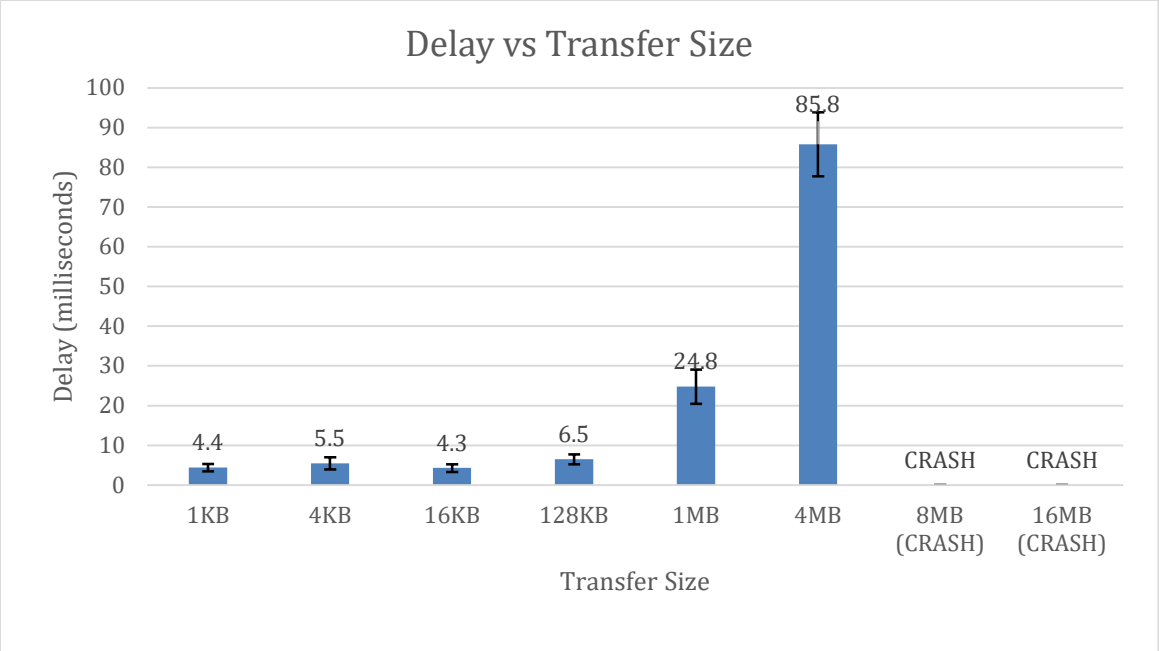
Change the TA code (which runs in the normal world), measure the end-to-end delay when X (transfer size) is: [1KB, 4KB, 16KB, 128KB, 1MB, 4MB, 8MB, 16MB]. Run 10 times for each value of X, report the average and standard deviations.

1. Upload a diff file showing your changes. (20)

   Just ONE diff file, no need to create a tarball. 50% penalty if the diff is larger than 50KB which must have contained some junk. 100% penalty if source file(s), instead of one diff file, are submitted. Create the diff early; do not wait until the last minute. Attempts to email instructors/TA for diff submissions will be ignored. Only one diff file is allowed; other diffs will be ignored.

2. Attach a plot below, showing your measurement results. (30)

   - Okay to use any software to generate the plot. Below is a sample which showcases how the plot should look. Note its data points do NOT represent the actual trends.



The bar reaches up to the average value and the error bars extend by one standard deviation above and below the average value.

- If for some X the program crashes (either CA or TA), states your observation and the possible cause. In the plot, show such data points with an annotation "CRASH".

  The programs crashes for X = 8MB and X = 16MB outputting that the program failed to allocate SDP buffer in ION heap. I think the possible cause is that the value of the size parameter is too high and there was too much data for CA and TA to process.

```
Secure Data Path basic access: NS invokes SDP TA
Allocate in ION heap 'unmapped_contiguous' (type=5, id=0)
[  252.724901] misc ion: ion_unmapped_allocate(75) err: alloc 0x00f43000 bytes f
ailed
Error: failed to allocate in target heap
Failed to allocate SDP buffer (16000000 bytes) in ION heap 5: -1
Test failed!
#
```