SGX Project Meeting #3

Agenda for July 14, 2016

What we have done

1. OpenSGX

   (a) Remote Attestation sample provided by OpenSGX team is implemented incorrectly. We fixed it and implemented provisioning on top of the fixed version.

2. NGINX + LibreSSL

   (a) Through use of valgrind we identified the following:

      i. Function callgraph during handshake

      ii. Private key handling functions

   (b) Implemented and tested a custom NGINX module

   (c) Identified the data structures that contain the private key and the ones used during certificate verification

   (d) Attempted to use crowbar, but we could not find the version of `pin` against which it is compiled and could not run the tool as a result.

3. Performance Evaluation

   (a) Tested Apache JMeter to measure end-to-end performance; however, we concluded that this tool may offer more than is required for our purposes.

   (b) Found a second tool called ApacheBench. This is a command-line utility included with Apache that can be used to specify things such as number of users and the url to test.

What we want to discuss

1. NGINX + LibreSSL

   (a) Regarding ciphers that implement forward secrecy, would they require us to change our partitioning? If so, could we disregard them for now?

2. Performance Evaluation

   (a) OpenSGX implements non-enclave to enclave communication through a pipe-like interface. The overhead of this is far greater than the model used by Intel (RPC-like).

   (b) Another possible metric for end-to-end performance is response time vs. number of users. It maybe an easier metric to measure than requests per second.

what we are planning to do next week

1. Some OpenSSL calls will have to happen within the enclave. This would entail either transferring the SSL context (used as an argument for all the function calls) into the enclave, or using an alternative set as functions provided in the enclave through a library called polarSSL.

2. Start working on integrating SGX+NGINX+LibreSSL