Storage

Design
Recovery from Intel SGX

SGX maintains there own key.
Operations about data

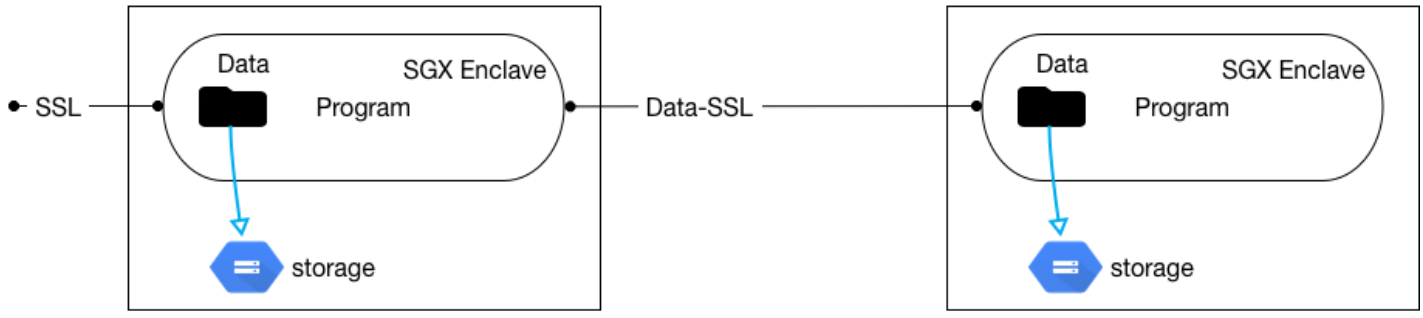
File search

Implementation:
how to secure control path and data path

Design Goal:

1. Target :防止黑入系统的黑客，或内部的某个员工在不惊动其他人的情况下，对文件进行窥探或者破坏。
2. Thread Model: 攻击者可以获得整个软件栈的权限，甚至OS和硬件。攻击者可以在任意时间终止Enclave的执行，但是不能获得Enclave内部的信息。
3. Program model:

Replic on Intel SGX



Data-AES(Key1) Key1-AES(Private Key2)

Data-AES(Key2) Key2-AES(Private key2)

Replica 过程：

init：三Replica，此处只画出两个。 Replica之间通过SGX Remote attestation建立可信的通信（SSL）

Write：数据通过传输到达SGX Enclave, SSL 解密后是明文。Enclave 生成一个Key，用Key对Data 进行加密以后，写入Storage 中，再将Key用Private key加密，放入storage 中。同时Data传递给对应的Replica，Replica做一样的操作。

Read：随便从一个Replica中解密数据。

Delete：

Recover：如何知道机器Crash了？Crash以后Object怎么找到新的Replica

Question：

如何选择三个Replica。加密的数据如何拷贝出来？Overhead有多大（哪些）？

Read的时候如何找到对应的Key，metadata的形式是什么样的，如何通过一个object找到Replica。