CS 628A: Computer System Security **25/02/2019**

Design Review

Reviewer: Harshit Gupta(18111020), Somesh Jaiswal(18111071)

Reviewee: Shivam Kumar(170668), Skand Rajmeet Upadhyay(170704)

User Creation and Authentication

Score: 3

Explanation: (Key,value) pair for storing the details of the user not specified properly. How is the User data structure being encrypted? What is the data being stored in User data structure? Asymmetric key pair is not stored in the User data structure.

Integrity preservation in the simple secure client

*Score:*4

Explanation: You should first sign and then encrypt. You can read here for the reason.

Confidentiality in the simple secure client

*Score:*3

*Explanation:*It is better to use RSA when there is communication between two clients. You are encrypting and decrypting using the same user's keys so why to use Asymmetric keys? Also you haven't stored Private Key anywhere(We can't find that in the design document).

AppendFile implementation and efficiency

Score: 2

Explanation: You're talking about blocks but we don't see blocks being created anywhere. So, this is a very inefficient implementation of append. Since this has been talked about again and again, I'm giving you a low rating.

Sharing implementation

Score: 3

Explanation: The location of file is not included in message. Also, while performing normal file operations, when user will decrypt to get the symmetric keys used for decryption and signing, how will he know whether to use his asymmetric keys to get the "original symmetric keys"(if he is the owner) or the keys received from the owner(is file has been shared with him).

Revocation implementation

*Score:*5

Explanation: Correct Implementation

Clarity of the design document

Score: 4

Explanation: Some parts of the documents were not explained properly, specifically how the locations of different entities on DataStore server are being generated.

Apart from the points mentioned above, the list of children that you are maintaining apparently has no use.