Computer Systems and Security(CS 628A): Design Review

REVIEWERS: Saket Harsh - 150617   Shashank Shekhar - 150662
REVIEWEE : Arunkumar Vediappan - 18111009   Supriya Suresh - 18111077

1. User Creation and Authentication

5 star.

2. Integrity preservation in the simple secure client

5 star.
HMAC check is ensured at each required level. Hence, safeguarded from length extension attack too.

3. Confidentiality in the simple secure client

5 star.
No information is leaked to unauthorized people.
Random number generation could have led to 2 files having same location, but the probability is 1 in 2^54. So this is a good assumption that there is no collision.

4. Append file implementation and efficiency

4 star.
Append is efficiently implemented. However, "there is a field of number of appends in the file which is saved in the userDS and is incremented". If A shares a file with B and B appends to the file, there is no way that A can change the number of appends in the file in its DS without communicating with B.

5. Sharing Implementation

5 star.

6. Revocation Implementation

5 star.
The idea of changing both E_k and X from one parameter (the random number) was appealing.

7. Clarity of the Design Document

3 star.
2 pages was a strict deadline. If we just reviewed page 1 and 2, essential parts like Load, Append, Sharing and Revoking could not have been reviewed. However, the document was quite explanatory (credits to the explanation given for Symbols used).