CS 1653: Applied Cryptography and Network Security
Term Project, Phase 4

Lindsey "Hellman" Bieda leb35@pitt.edu
Tucker "Diffie" Trainor tmt33@pitt.edu

April 5, 2012

Introduction: Cryptographic Techniques

(an introductory paragraph or two that broadly surveys the types of cryptographic techniques that your group has decided to use to address threats T5-T7)

Threat 5: Message Reorder, Replay, or Modification

Threat Description

Begin by describing the threat treated in this section. This may include describing examples of the threat being exploited by an adversary, a short discussion of why this threat is problematic and needs to be addressed, and/or diagrams showing how the threat might manifest in your groups current implementation.

Mechanism Description

The mechanism builds upon the protocols used in Threats 1-4 that establish a secure session key between a client and a server. Though messages passed in the session are secure from eavesdropping, they are not secure from reorder, replay, or modification. We use two methods to eliminate these new threats: sequence numbers and message authentication.

Sequence numbers are a simple yet effective tool that would alert either end of channel that a message has ben reordered or replayed. We modify our message format so that it includes an integer field to store the sequence number. Then, after receiving a message, the receiving party increments the sequence number by 1 and uses that value in their response. Replays and reordering of messages are easily detectable by either party, as the sequence number will reveal an inconsistency.

Message authentication is a cryptographic principal that is used to verify that a message has not been tampered with.

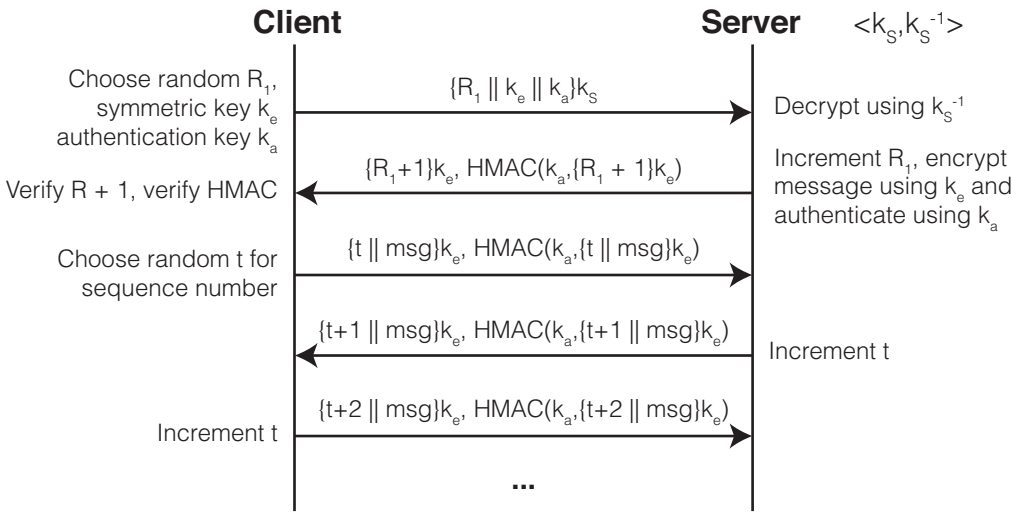

Figure 1: Threat 5 Mechanism

Correctness and Security of Mechanism

Lastly, provide a short argument addressing why your proposed mechanism sufficiently addresses this particular threat. This argument should address the correctness of your approach, as well as its overall security. For example, if your mechanism involves a key agreement or key exchange protocol, you should argue that both parties agree on the same key (correctness) and that no other party can figure out the key (security).

Threat 6: File Leakage

Threat Description

Begin by describing the threat treated in this section. This may include describing examples of the threat being exploited by an adversary, a short discussion of why this threat is problematic and needs to be addressed, and/or diagrams showing how the threat might manifest in your groups current implementation.

Mechanism Description

Next, provide a short description of the mechanism that you chose to implement to protect against this threat. For interactive protocols, it would be helpful to provide a diagram explaining the messages exchanged between participating principals. (See the notes from Lecture 10 for example diagrams.) Be sure to explain any cryptographic choices that your

group makes: What types of algorithms, modes of operation, and/or key lengths did you chose? Why? If shared keys are needed, how are they exchanged?

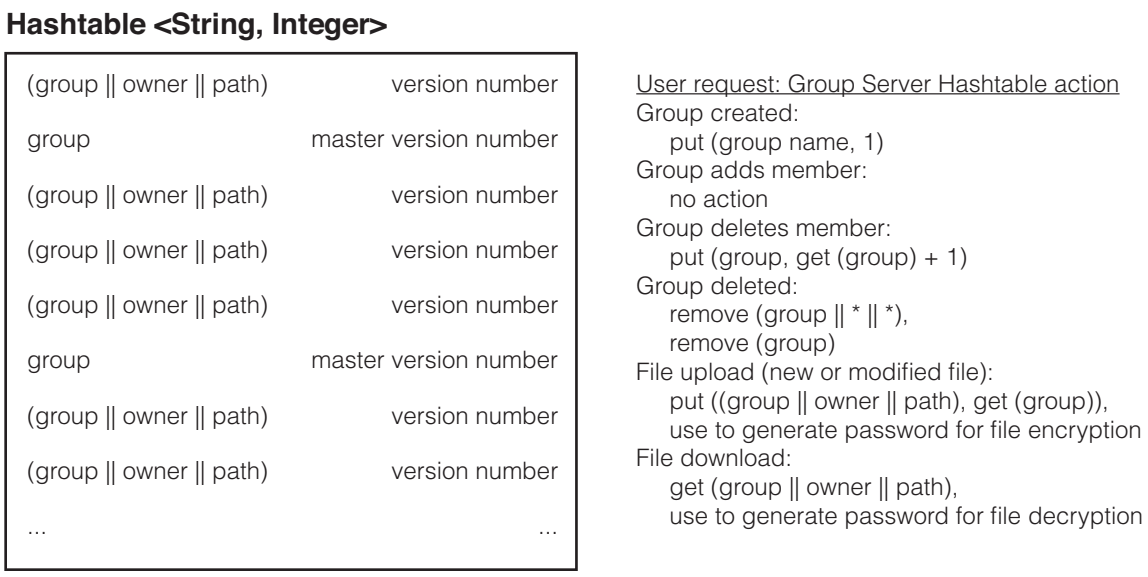

Figure 2: Threat 6 Mechanism: Hashtable and Operations

Correctness and Security of Mechanism

Lastly, provide a short argument addressing why your proposed mechanism sufficiently addresses this particular threat. This argument should address the correctness of your approach, as well as its overall security. For example, if your mechanism involves a key agreement or key exchange protocol, you should argue that both parties agree on the same key (correctness) and that no other party can figure out the key (security).

Threat 7: Token Theft

Threat Description

stub

Mechanism Description

stub

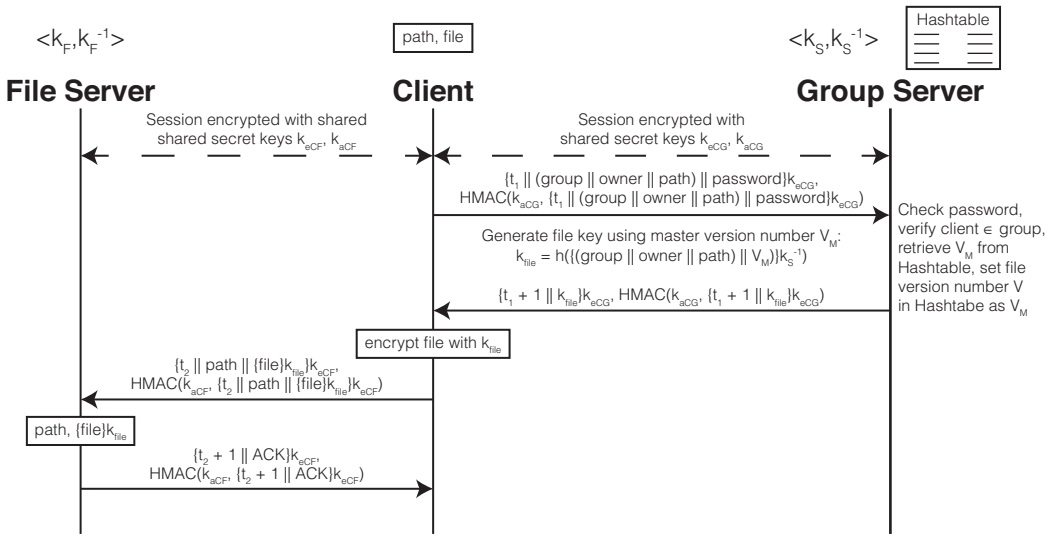

Figure 3: Threat 6 Mechanism: Upload Diagram

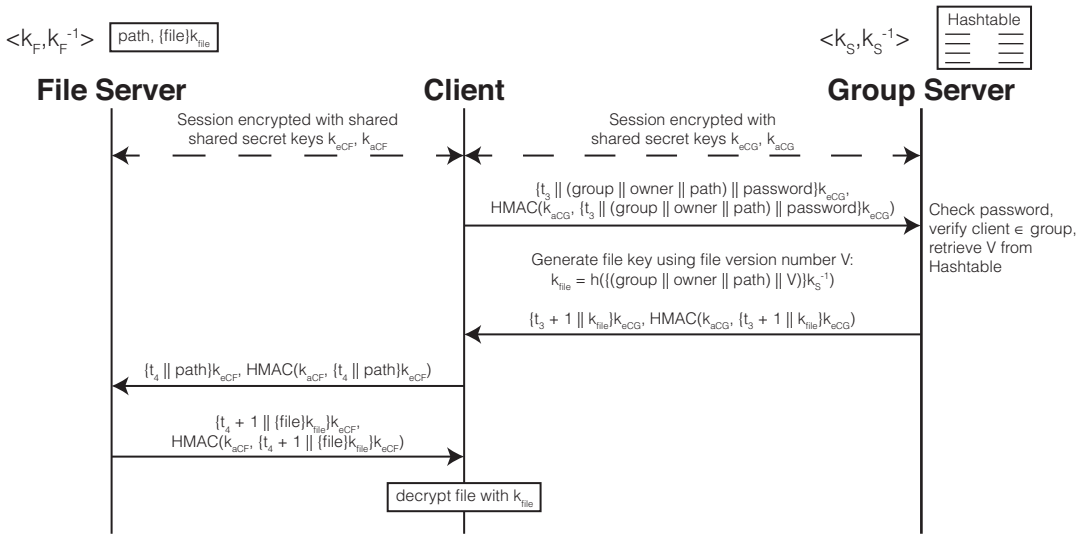

Figure 4: Threat 6 Mechanism: Download Diagram

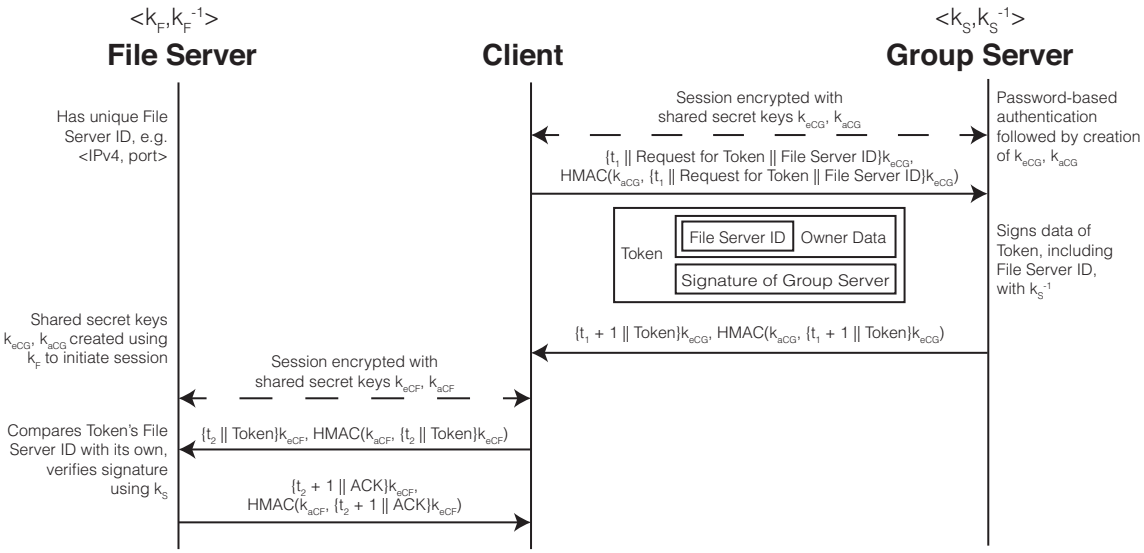

Figure 5: Threat 7 Mechanism

Correctness and Security of Mechanism

stub

Discussion and Commentary

After completing one section for each threat, conclude with a paragraph or two discussing the interplay between your proposed mechanisms, and commenting on the design process that your group followed. Did you discuss other ideas that didnt pan out before settling on the above-documented approach? Did you end up designing a really interesting protocol suite that addresses multiple threats at once? Use this space to show off your hard work!

Threats 1 through 4 revisited

Finally, spend about one paragraph convincing me that your modified protocols still address the threats T1-T4 described in Phase 3 of the project. Full credit for Phase 4 requires that all Phase 3 threats are still protected against.