

Problem Set 1 (due February 22, 2006). [100 points + 20 bonus points]

Problem 1 [50 points + 20 bonus points]: Broadcast Authentication.

Assume that a node wants to broadcast a real-time stream of data. Each receiver wants to verify that the data is generated by the source and was not modified, or replayed (i.e., integrity/data origin protection).



1. Why can't the source just use any message authentication code mechanism based on symmetric key crypto (e.g., HMAC) assuming that all the receivers share the same secret with the source?
2. If the receiving nodes do not have the capability to do a signature verification of each packet. Propose a technique to amortize signature verification and trades-off the computation with a delay in verification. Discuss potential DoS attacks on your approach.
3. Lamport hash technique allows protecting against both eavesdropping and database reading. First, briefly describe how Lamport hash can be used to provide broadcast authentication.
4. Conventional Lamport hash requires $O(n)$ computations or $O(n)$ memory storage. Propose a scheme that requires $O(\log n)$ computations and $O(\log n)$ memory storage for each authentication. In addition to the algorithm description, explain through a detailed example how the scheme works. *Hint: google for hash chains and carefully read "the" important paper on this topic!*
5. Assume that a set of nodes are loosely synchronized (i.e., we know a bound on the maximum time difference between the source and all other receiving nodes: T). How can the scheme described in (4) be used to provide data origin authentication of broadcast messages?
6. **BONUS (20 points):** Implement the broadcast authentication scheme, and the proposed algorithm.

Problem 2 [10 points]:

Assume that A and B share a secret key of length 64 bits. Does the following protocol have any major vulnerability? If yes describe an attack in detail.

1. $A \rightarrow B$: I am A , R_1
2. $B \rightarrow A$: R_2
3. $A \rightarrow B$: $\text{Hash}(K + R_2 \bmod 2^{64})$
4. $B \rightarrow A$: $\text{Hash}(K \oplus R_1)$

Assume that Hash is a cryptographically secure hashing function.

Problem 3 [10 points]:

Page 288, problem 4.

Problem 4 [10 points]:

Page 289, problem 8.

Problem 5 [10 points]:

Page 302, problem 14.

Problem 6 [10 points]:

Page 302, problem 15.