CSC/ECE 774 Network Security

Homework #2 (Topics 3 & 4, due by 10/03/11)

All submissions must be written with a word processor such as MS Word. Handwritten submissions will NOT be graded.

1. (10 points) Assume that the following packets are all received by a receiver using EMSS.

What should the receiver do to authenticate packet Pi? Please don’t include unnecessary steps that do not contribute to the authentication of Pi.

2. (10 points) The following figure illustrates the idea of the immediate authentication mechanism in the extension to TESLA.

Is it correct to say that once the packet for $M_{j+vd}$ is received, the receiver can immediately authenticate the entire packet? Why?

3. (10 points) TESLA is based on a one-way key chain of limited size. The key chain commitment is initially authenticated using a digital signature. When one key chain is completely used up, the sender will need to generate and use another key chain. For the later key chain, can you use keys in the previous key chain to authenticate its key chain commitments?

   (a) (5 points) Describe how exactly this should be done.

   (b) (5 points) Discuss the pros and cons of this approach.
4. (10 points) TESLA requires loose clock synchronization. In applications where such synchronization is not possible, TESLA cannot be used. Assume that we require a solution that is not vulnerable to compromised receivers for such applications. Further assume that the sender and each receiver share a pairwise symmetric key.

(a) (5 points) Describe a method for broadcast authentication that only uses symmetric cryptography.

(b) (5 points) Discuss the limitation of your solution.

5. (10 points) Compare the use of hash functions in BiBa signature scheme, BiBa broadcast authentication protocol, MicroMint, and TESLA. Consider both similarities and differences.

6. (10 points) Consider group key agreement protocols.

(a) (5 points) Describe the general form of the group key in the GDH protocols.

(b) (5 points) Describe the general form of the group key in the tree-based group key agreement protocol.

7. (10 points) In GDH.1, for the up flow, each member $M_i$, $i<n$, receives some intermediate values and forwards another set of values to $M_{i+1}$. Count the number of values in the message received by $M_i$. List the set of values received by $M_6$.

8. (10 points) Consider GDH.2. Denote the members as $M_i$, and the secret of $M_i$ as $N_i$. Assume there are totally 7 members in a group.

(a) (5 points) What is the set of messages $M_5$ receives in the upflow stage?

(b) (5 points) What is the message sent to $M_5$ in the downflow stage? What is needed by $M_5$ in this message?

9. (10 points) Consider the Tree-Based Group Key Agreement protocol and the following key tree:
Assume the prime defining the finite field is \( p = 11 \), and the generator is \( g = 2 \). Further assume the private key of \( M_1 \) through \( M_6 \) are 3, 4, 5, 6, 7, and 8. Compute the blind keys along the path from \( M_1 \) to the root.

10. (10 points) Consider the following network configuration, in which Iolus is used.

Assume the GSC is distributing a new group key to the group members using Iolus. How many times will this new key be encrypted and decrypted before A learns the value of the new key? Also describe what entity performs each of the encryption and decryption.
11. (10 points) Consider the basic LKH.

If R₃ is removed from the group, what keys must be changed? Give one way to distribute the updated keys to the other group members. (Please note that it’s R₃, not R₅, that is removed.)
12. (15 points) You need to read the following paper to answer this question:


Consider the following key tree.

(a) (5 points) If u₅ is removed from the group, what keys should be changed?

(b) (5 points) Assume key oriented rekeying is used. Describe the messages the group manager needs to send to the group members. Use the following convention to describe each message:

   GM → {set of users}: {Kx}Ky, {Kz}Kw, …

(c) (5 points) Assume group oriented rekeying. Redo (b).