Large Scale Multicast Key Distribution with Compromise Recovery

R. Poovendran/Advisor: J. S. Baras ---Systems Engineering and Integration Laboratory

**Project background and goals**
Providing security to large scale group communication is one of the difficult problems in information security. Nature of the group communication, time duration of the session, size of the group, number of senders, needs for message authentication, integrity and/or anonymity are often conflicting requirements. Among several possible models such as one-to-many, many-to-many, the commercial applications involving large scale groups belongs to the one-to-many type, which is the focus of our work.

Several key distribution schemes have recently been proposed. Among them, the rooted tree based schemes have been known to be relatively more scalable. However, there have been significant discrepancies among these tree based key schemes in terms of the needed keys to be stored by the group controller.

Our research presents a unified approach to the rooted tree based methods.

**Methodology/Procedure**
Each group member is assigned to a unique leaf. All the nodes of the rooted tree, including the root and the leaf nodes, represent a key. The keys along the path connecting a leaf to the root are assigned to the member at the leaf node.

By assigning revocation probabilities to each members, and adding the condition that the revocation of a member should not render the keys of another member invalid, we formulated a condition key updates as an optimization problem.

**Significance**
Our approach allows (a) security vulnerability analysis of the tree based schemes, (b) fast collusion detection for certain types of tree based schemes, (c) shows that the optimal Huffman coding techniques lead to member collusion, (d) show that the key length of the scheme is upper bounded by the number of members in the group by a logarithmic function.

**Project Results**
Showed that the optimal tree structure for key distribution is same as the Huffman trees. Optimal average number of keys per member was shown to be the entropy of the member revocation event. Further showed that some of the currently available schemes choose the worst case solution always.

**Future Work**
Analysis of dynamic group key distribution techniques.