Dynamic Elgamal Key Generation with Tight Binding

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

Project background and goals

Allowing a set of nodes to jointly generate a dynamic public key infrastructure with the group private key being the combination of the individual private keys and the group public keys being the combination of individual public keys.

This model allows a group initiator to set the initial group parameters and let the set of intermediate nodes compute the group security parameters, including the keys by a newly developed algorithm.

This approach also avoids the need for having a yellow page holder for specific groups. Once the members register their public keys with their registry, they can jointly generate their group key with the help of a trusted third party initialization.

Approach provides reliability up to the compromise of all but one member.

This work is an extension of the scheme developed in “A Shared Key Generation using Fractional Keys”.

Methodology/Procedure

1. Members generate the private public key pair and publish the public key.
2. Trusted third party generates the initial pads and the group parameter; each member is given a unique pad.
3. Each member adds the pad to its private key and generates a padded version; securely exchanges it with the other group members; all members combine the padded keys; remove the combined pad effect using the dynamic group binding parameter to generate the new group binding parameter; members generate the individual dynamic pad by removing their shares from the new group parameter.

Project Results

2. Filed a patent disclosure for the new method with OTL, UMD.

Significance

1. Allows a set of distributed nodes with no common CA to generate a group public key infrastructure that is dynamic.
2. Method has an in built non-cryptographic technique of increasing security without increasing key length.
3. Individual group members have no significant advantage over an external attacker. Model is based on “highly paranoid” mode.

Future Work

Use of the scheme in the group admission procedures.

Threshold cryptography.