Broadcast Encryption with Multiple Trust Centers and Dynamic Coalitions

In this paper we extend the topic of hierarchical identity-based encryption (HIBE) from the domain of a single Trusted Authority (TA) to a setting with multiple independent Trusted Authorities with their own HIBE's. Under this multi-TA HIBE a group of TA's form a coalition for secure communication. These coalitions may be be temporary in the sense that they a coalition may be formed and dissolved without compromising security of its members. Similarly the coalitions may be dynamic in the sense that individual coalition members may be added or removed at any time.. This scheme is then further extended to include one-to-many communication through the addition of broadcast encryption, a feature which also improves efficiency.

Secure communication across separated domains of trust has been solved in the past using pair-wise distribution schemes between all parties or through use of a public-key infrastructure (PKI). Pair-wise schemes work well for small numbers of TAs communicating but do not scale well as that number increases. Using a PKI would allow for scalable growth but requires transmission and verification of mutually trusted certificates. These constraints make the solutions ill-suited for a MANET or coalition environment. The multi-TA HIBE scheme proposed in this paper allows collaboration across domains of trust in a scalable manner while avoiding certificates.

Hierarchical identity-based encryption literature generally assumes the existence of a single root trusted authority. This root entity holds a master secret capable of decrypting all communications addressed within the hierarchy. This assumption holds within a single structured institution. Multiple trusted authorities collaborating would require a mutually trusted party to hold that root authority, giving this party the capability to compromise all communications in the hierarchy. This is undesirable in situations of mixed or uncertain trust. This paper offers a solution by allowing the creation of coalitions without a mutually trusted root administrator. Instead the participating TA's engage in collaborative key creation to achieve compatible keys for a particular coalition without jeopardizing security. Information related to a TA's coalition key may then be disseminated to subordinate nodes quickly and efficiently through one-to-many secure communications, allowing those nodes to adjust their keys to be compatible with the rest of the coalition.

One-to-many communication across domains is of particular interest for real-world implementation problems. In a MANETs setting it is much more expensive to transmit information than to perform computations. One-to-many communication allows for a single transmitted message to be read by a multiple valid recipients. In this paper the valid recipients for a one-to-many message are defined through the use of one or more "wildcards". A wildcard is a special character, usually "*", that may be used in an address in lieu of specifying that particular aspect of the recipient identity, allowing anyone matching the non-wildcard portion to read the message. For example a single recipient message to someone in a particular division's unit would be addressed to "name@unit.division", but to reach everyone in that unit could use a wildcard and address to "*@unit.division".

The scheme presented in this paper allows for members of a coalition to change over time and those changes do not compromise the security of any TA. Coalition members may be removed or added to the coalition with minimal configuration. Upon a change in coalition membership the participating TAs exchange public information, and based on non-public secret information they are able to communicate. The private keys of subordinate entities of each TA must be updated, but each TA can accomplish this through a single broadcast message exclusively readable to members of that TA. This flexible reconfiguration ability similarly allows a fixed set of TAs in coalition to schedule secure reconfigurations with minimal communication long before any secret key has a chance to become stale or compromised.

We offer an example instantiation of a broadcast enabled multi-TA HIBE based on the Boneh-Boyen HIBE as extended for wildcard encryption by Abdallah, et al. The original Boneh-Boyen HIBE is selective identity CPA secure in the standard model as is its wildcard counterpart. The multi-TA scheme in this paper maintains this level of security through a reduction to the Decisional Bilinear Diffie-Hellman problem. The scheme may then be made selective-identity CCA2 secure through a transformation as described by Canetti, Halevi, and Katz, or a transformation similar to that of Boyen, Mei, and Waters.