Università degli Studi di Salerno
Dipartimento di Informatica

DOTTORATO DI RICERCA IN INFORMATICA
CICLO XIV - NUOVA SERIE

Tesi di Dottorato in Informatica

New Insights on Cryptographic Hierarchical Access Control: Models, Schemes and Analysis

Abstract

Candidate
Arcangelo Castiglione

Tutor
Prof. Alfredo De Santis

Co-Tutor
Prof. Barbara Masucci

Coordinator
Prof. Gennaro Costagliola

2014/2015

Abstract

Nowadays the current network-centric world has given rise to several security concerns regarding the access control management, which ensures that only authorized users are given access to certain resources or tasks. In particular, according to their respective roles and responsibilities, users are typically organized into *hierarchies* composed of several disjoint classes (*security classes*). A hierarchy is characterized by the fact that some users may have more access rights than others, according to a top-down inclusion paradigm following specific hierarchical dependencies. A user with access rights for a given class is granted access to objects stored in that class, as well as to all the descendant ones in the hierarchy. The problem of *key management* for such hierarchies consists in assigning a key to each class of the hierarchy, so that the keys for descendant classes can be efficiently obtained from users belonging to classes at a higher level in the hierarchy.

In this thesis we analyze the security of hierarchical key assignment schemes according to different notions: security with respect to *key indistinguishability* and against *key recovery* [4], as well as the two recently proposed notions of security with respect to *strong key indistinguishability* and against *strong key recovery* [42]. More precisely, we first explore the relations between all security notions and, in particular, we prove that security with respect to strong key indistinguishability is *not stronger* than the one with respect to key indistinguishability. Afterwards, we propose a general construction yielding a hierarchical key assignment scheme that ensures security against strong key recovery, given any hierarchical key assignment scheme which guarantees security against key recovery.

Moreover, we define the concept of *hierarchical key assignment schemes supporting dynamic updates*, formalizing the relative security model. In particular, we provide the notions of security with respect to *key indistinguishability* and *key recovery*, by taking into account the dynamic changes to the hierarchy. Furthermore, we show how to construct a hierarchical key assignment scheme supporting dynamic updates, by using as a building block a symmetric encryption scheme. The proposed construction is provably secure with respect to key indistinguishability, provides efficient key derivation and updating procedures, while requiring each user to store only a single private key.

Finally, we propose a novel model that generalizes the conventional hierarchical access control paradigm, by extending it to certain additional sets of qualified users. Afterwards, we propose two constructions for hierarchical key assignment schemes in this new model, which are provably secure with respect to key indistinguishability. In particular, the former construction relies on both symmetric encryption and perfect secret sharing, whereas, the latter is based on public-key threshold broadcast encryption.