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

L'attuale mondo "*network-centrico*" ha dato origine a diversi problemi di sicurezza per quanto riguarda la gestione del controllo degli accessi, il quale assicura che solo gli utenti autorizzati possono accedere a determinate risorse o attività. In particolare, secondo i loro rispettivi ruoli e responsabilità, gli utenti sono in genere organizzati in gerarchie composte da più classi disgiunte (*classi di sicurezza*). Una gerarchia è caratterizzata dal fatto che alcuni utenti possono avere più diritti di accesso rispetto ad altri, secondo un paradigma di inclusione *top-down*, che segue specifiche dipendenze gerarchiche. Ad un utente con diritti di accesso per una determinata classe viene concesso l'accesso agli oggetti memorizzati in quella classe, così come a tutti quelli discendenti nella gerarchia. Il problema della gestione delle chiavi per tali gerarchie consiste nell'assegnare una chiave per ogni classe della gerarchia, in modo che le chiavi per le classi dei livelli inferiori possono essere efficientemente ottenute da parte degli utenti appartenenti a classi di un livello superiore nella gerarchia.

In questa tesi abbiamo analizzato la sicurezza degli schemi di assegnamento chiavi gerarchico in base a diverse nozioni: sicurezza rispetto a *key indistinguishability* e *key recovery*, così come rispetto alle due nozioni recentemente proposte di *strong key indistinguishability* e *strong key recovery*. Più precisamente, in primo luogo abbiamo esplorato le relazioni tra tutte le nozioni di sicurezza ed in particolare, abbiamo dimostrato che la sicurezza rispetto alla *strong key indistinguishability* è *non più forte* rispetto alla *key indistinguishability*. In seguito, abbiamo proposto una costruzione generale che permette di ottenere uno schema di assegnamento chiavi gerarchico che garan-

tisce sicurezza rispetto a *strong key recovery* a partire da un qualsiasi schema di assegnamento chiavi gerarchico che garantisce sicurezza rispetto a *key recovery*.

Inoltre, abbiamo definito il concetto di schemi di assegnamento chiavi gerarchico che supportano aggiornamenti dinamici, formalizzando il relativo modello di sicurezza. In particolare, abbiamo fornito le nozioni di sicurezza rispetto a *key indistinguishability* e *key recovery*, tenendo conto delle modifiche dinamiche alla gerarchia. Inoltre, abbiamo mostrato come costruire uno schema di assegnamento chiavi gerarchico che supporta aggiornamenti dinamici, utilizzando come building block *schemi di cifratura simmetrica*. La costruzione proposta è *dimostrabilmente sicura* rispetto alla *key indistinguishability*, fornisce procedure efficienti per la derivazione e l'aggiornamento della chiave, mentre richiede ad ogni utente di memorizzare una sola chiave privata.

Infine, abbiamo proposto un nuovo modello, che generalizza il tradizionale paradigma di controllo degli accessi gerarchico, estendendolo ad ulteriori insiemi di determinati utenti qualificati. Inoltre, abbiamo proposto due costruzioni per gli schemi di assegnamento chiavi gerarchico in questo nuovo modello, che sono *dimostrabilmente sicuri* rispetto alla *key indistinguishability*. In particolare, la prima costruzione è basata sia su *schemi di cifratura simmetrica* che su *schemi di perfect secret sharing*, mentre, la seconda costruzione è basata su schemi di *public-key threshold broadcast encryption*.