Dottorato di ricerca in Informatica e Ingegneria dell'Informazione

Abstract della Tesi di Dottorato

Studente di dottorato **FLORES Manuela**

Docente tutor: **Prof.ssa MASUCCI Barbara**

Ciclo **XXXI** Curriculum **Informatica** Area scientifica **Crittografia e Sicurezza**

Titolo della tesi: **On Provable Security of Entity Authentication Schemes**

Abstract in Inglese

Entity authentication is the process allowing a user, in a distributed system, to gain confidence in the identity of one (or more) communication user. Such a process may be either *unilateral* (the users are involved in a conversation in which only one of them, called the *verifier*, gains confidence that it is the other, called the *prover*, with whom he is speaking) or *mutual* (both users gain confidence about the identity of the communication partner). Moreover, the users might share some secret information, or might not.

A *one-message unilateral entity authentication scheme* allows one party, called the *prover*, to authenticate himself, i.e. to prove his identity, to another party, called the *verifier*, by sending a single *authentication message*. We consider schemes where the prover and the verifier do not share any secret information, such as a password, in advance.

We propose the *first theoretical characterization* for one-message unilateral entity authentication schemes, by formalizing the security requirements for such schemes with respect to different kinds of *passive* and *active* adversaries. More in details, we consider both *static* and *adaptive* adversaries for each kind of attack (passive/active). Afterwards, we explore the relationships between the security notions resulting from different adversarial behaviours for one-message unilateral entity authentication scheme.

Finally, we propose three different constructions for one-message unilateral entity authentication schemes and analyse their security with respect to the different security notions previously formalized in the work.

Dottorato di ricerca in Informatica e Ingegneria dell'Informazione

Abstract della Tesi di Dottorato

Studente di dottorato **FLORES Manuela**

Docente tutor: **Prof.ssa MASUCCI Barbara**

Ciclo **XXXI** Curriculum **Informatica** Area scientifica **Crittografia e Sicurezza**

Titolo della tesi: **On Provable Security of Entity Authentication Schemes**

Abstract in Italiano

L'*autenticazione utente* è il processo che consente ad un utente, in un sistema distribuito, di acquisire confidenza con l'identità di uno (o più) utente con cui è in comunicazione. Tale processo può essere *unilaterale* (gli utenti sono coinvolti in una conversazione nella quale solo uno di loro, chiamato *verificatore*, acquisisce la certezza di chi sia l'altro utente, chiamato il *provatore*, con il quale sta parlando) o *reciproca* (entrambi gli utenti guadagnano fiducia sull'identità del partner di comunicazione). Inoltre gli utenti potrebbero condividere alcune informazioni segrete o potrebbero non farlo.

Uno *schema di autenticazione utente unilaterale a messaggio singolo* consente a una parte, chiamata il *provatore*, di autenticarsi, ossia di provare la propria identità, ad un'altra parte, chiamata il *verificatore*, inviando un singolo *messaggio di autenticazione*. Consideriamo gli schemi in cui il provatore ed il verificatore non condividono in anticipo alcuna informazione segreta, come una password.

Proponiamo la *prima caratterizzazione teorica* per gli schemi di autenticazione utente unilaterale a messaggio singolo, formalizzando i requisiti di sicurezza per tali schemi rispetto a diversi tipi di avversari *passivi* e *attivi*. Più in dettaglio, consideriamo avversari sia *statici* che *adattivi* per ogni tipo di attacco (passivo/attivo). Successivamente, esploriamo le relazioni tra le nozioni di sicurezza risultanti dai comportamenti dei diversi avversari rispetto ad uno schema di autenticazione utente unilaterale a messaggio singolo.

Infine proponiamo tre diverse costruzioni per schemi di autenticazione utente unilaterale a messaggio singolo e analizziamo la loro sicurezza rispetto alle diverse nozioni di sicurezza precedentemente formalizzate nel lavoro.