Policy-Based Encryption Schemes from Bilinear Pairings (Fast Abstract)

Walid Bagga
Institut Eurécom
Sophia-Antipolis, France
walid.bagga@eurecom.fr

Refik Molva
Institut Eurécom
Sophia-Antipolis, France
refik.molva@eurecom.fr

Stefano Crosta
Institut Eurécom
Sophia-Antipolis, France
stefano.crosta@eurecom.fr

ABSTRACT

The concept of policy-based cryptography is a promising paradigm for trust establishment and authorization in large-scale open environments like the Internet and Mobile Networks. It aims at providing a framework for performing cryptographic operations with respect to policies formalized as monotone Boolean expressions written in standard normal forms. A policy involves conjunctions and disjunctions of conditions where each condition is fulfilled by a digital credential representing the signature of a specific credential issuer on a set of statements about a certain entity. Therefore, an entity fulfills a policy if and only if it has been issued a set of credentials fulfilling the combination of conditions specified by the policy.

In this work, we focus on policy-based encryption schemes which allow to encrypt a message according to a policy so that only entities fulfilling the policy are able to decrypt the message. More generally, policy-based encryption belongs to an emerging family of encryption schemes sharing the ability to integrate encryption with access control structures. This ability is mainly enabled by bilinear pairings over elliptic curves and allows for several interesting applications in different contexts.

A policy-based encryption scheme has to fulfill two primary requirements: on one hand, provable security under well defined attack models. On the other hand, efficiency, especially when dealing with the conjunctions and disjunctions of credential-based conditions.

The contributions of our research work are twofold:

1. The standard acceptable notion of security for public-key encryption schemes is indistinguishability against chosen ciphertext attacks. Hence, it is natural to require that a policy-based encryption scheme also satisfies this strong notion of security. However, the definition of this security notion must be adapted to the policy-based setting. Our first contribution is the definition of policy-oriented security model for policy-based encryption schemes as well as the development of an efficient policy-based encryption scheme that is provably secure under our security model in the random oracle model.

2. Policy-based encryption schemes may suffer from the key-escrow property i.e. in addition to the legitimate holder of the credentials fulfilling the encryption policy, any collusion of credential issuers who are able to issue a set of credentials fulfilling the policy can decrypt the message. Our second contribution is to address this issue through the notion of policy-based public-key encryption. The latter allows encrypting a message not only with respect to a policy but also according to a public-key so that only an entity fulfilling the policy and having access to the corresponding private-key is able to decrypt the message. We developed a policy-based public-key encryption scheme from bilinear pairings and proved its security under the corresponding security model. Our proposal improves related work in terms of both security and efficiency.

ASIACCS'06, March 21-24, 2006, Taipei, Taiwan.