A User Identity Based Authentication Mechanisms for Network Security Enhancement

Mots clés :

- **Directeur de thèse**: Hossam AFIFI
- **Co-encadrant(s)**:
- **Unité de recherche**: Services répartis Architectures MOdélisation Validation Administration des Réseaux
- **Ecole doctorale**: École Doctorale Informatique, Télécommunications, Électronique de Paris
- **Domaine scientifique principal**: Divers

**Résumé du projet de recherche (Langue 1)**

In this thesis, we study the use of the identity in the authentication mechanisms and improve the access control in different kinds of networks. The identity can be biometric public features, simple strings (email addresses, login...), etc. The goal of our work is to improve the security of the system using this identity without any compromise. We have two main parts in the thesis depending on the deployed identity. The first part is dedicated to systems using biometric features. We have studied the use of biometric and developed new algorithms for Home Network and e-Passports authentication mechanisms. The cryptographic parameters will be generated using the biometric templates and hence personalized for the user. The second part is dedicated to systems using simple string like email addresses as identifier to access to services. The study was done on IP Multimedia Subsystem (IMS). Our contribution in this context consists in a new authentication mechanism relying on Identity Based Cryptography (IBC) for the IMS architecture. The goal was to authenticate the users using their public and private identifiers to overcome known weakness in the Authentication and Key Agreement (AKA) protocol. In both cases, the use of identity in the authentication was helpful to the system from the perspectives of performance and security.