SOUTENANCE DE THESE

Amira BARKI

Unité de Recherche : **UMR 7253 Laboratoire Heudiasyc**

soutiendra sa thèse de **Doctorat**

sur le sujet :

Concilier authentification et protection de la vie privée dans le contexte du Machine-to-Machine (M2M)

A l'IMI - 62 Boulevard de Sébastopol - Paris III
Le vendredi 16 décembre 2016 à 9h

Devant le jury composé de :

M. AVOINE Gildas, Professeur des Universités, INSA de Rennes, Sécurité & Cryptographie
M. BOUABDALLAH Abdelmadjid, Professeur des Universités, Université de technologie de Compiègne, Laboratoire Heudiasyc
M. CHABANNE Hervé, Ingénieur de Recherche, Morpho 11, Issy-Les-Moulineaux
M. GHAROUT Saïd, Ingénieur de Recherche, Orange Labs, Châtillon
M. GOUBIN Louis, Professeur des Universités, Université de Versailles, Laboratoire PRiSM
Mme LAURENT Maryline, Professeur des Universités, TélécomSudParis,SAMOVAR, Evry
M. MOUKRIM Aziz, Professeur des Universités, Université de technologie de Compiègne, Laboratoire Heudiasyc
M. TRAORE Jacques, Ingénieur de Recherche, Orange Labs, Caen

Abstract

Machine to Machine (M2M) applications are increasingly being deployed so as to enable a better management of resources and provide users with greater comfort, convenience as well as peace of mind. Unfortunately, they also entail serious security and privacy concerns that users are either underestimating or unaware of. In this thesis, we focus on M2M security, and particularly on the authentication and privacy issues of M2M applications involving a SIM card.

In the first part of this thesis, we design five new cryptographic primitives, that are of independent interest, and formally prove that they meet the expected security requirements. More precisely, they consist of a partially blind signature scheme, a sequential aggregate Message Authentication Codes (MAC) scheme, an algebraic MAC scheme and two pre-Direct Anonymous Attestation (pre-DAA) schemes. Some of the proposed schemes aim to achieve a particular property that was not provided by previous constructions, as it is the case of our partially blind signature scheme which enables multiple presentations of the same signature in an unlinkable way, whereas others intend to improve the efficiency of state-of-the-art schemes. Furthermore, our five schemes do not require the user's device to compute pairings. Thus, they are suitable for resource constrained environments such as SIM cards.

In a second part, we rely on these primitives to propose new privacy-preserving protocols. More specifically, we design a private eCash system where the user can settle expenses of different amounts using a single reusable payment token. Its implementation on a standard NFC-enabled SIM card confirms that it is quite efficient, even for real world applications such as electronic Toll (eToll). In this particular use case, a payment can be performed in just 205 ms. We also propose a protocol enabling anonymous authentication and identification of an embedded SIM (eSIM) to a Discovery Server (DS), which is an MNO independent third party that allows linking of an eSIM to the relevant MNO. Thereby, eSIMs can be remotely provisioned with their new network profiles while protecting users' privacy against a malicious discovery server. Furthermore, we rely on our algebraic MAC scheme to build a practical Keyed-Verification Anonymous Credentials (KVAC) system which can be easily turned into an efficient public key anonymous credentials system. Finally, based on our sequential aggregate MAC scheme, we introduce a remote electronic voting system that is coercion-resistant and practical for real polls. The security of our protocols is formally proven in the Random Oracle Model (ROM) under classical computational assumptions.