N° d'ordre :

UNIVERSITE DE M'SILA
Faculté de Mathématiques et Informatique
Département d'Informatique

MEMOIRE

Présenté pour l'obtention du diplôme de :

MAGISTER

Spécialité : Informatique
Option : Ingénierie des systèmes d'informatique

Par :
CHIKOUCHE Noureddine

Thème :

PROBLÈMES DE SÉCURITÉ DANS LES SYSTÈMES EMBARQUÉS

Soutenu publiquement le 23/09/2010 devant le jury composé de:

Pr. Hocine Belouadah	**Prof. Université de M'sila**	**Président**
Pr. Mohamed Benmohammed	**Prof. Université de Constantine**	**Rapporteur**
Dr. Allaoua Chaoui	**M.C. Université de Constantine**	**Examinateur**
Dr. Azeddine Bilami	**M.C. Université de Batna**	**Examinateur**

Résumé :

Parmi les systèmes embarqués qui ont connu des évolutions rapides au cours des dernières années et qui sont utilisés dans plusieurs domaines (la santé, le transport, le logistique, etc.), on peut citer les systèmes d'identification par radiofréquence (RFID). Deux problèmes principaux restent toujours posés au niveau des systèmes embarqués communicants, notamment : la sécurité et la complexité (i.e. le coût).

La communication entre le tag et le lecteur est insécurisée, ce qui le rend ouvert devant toute attaque logique sur le protocole de sécurité. Dans ce mémoire, nous essayons de mettre l'accent sur les méthodes d'analyse des protocoles cryptographiques. Notre travail se focalise en particulier sur la vérification automatique des protocoles d'authentification des systèmes RFID sous la plateforme AVISPA. Les propriétés de sécurité vérifiées sont : *la confidentialité* et *l'authentification.* Notre étude comporte aussi une comparaison entre les différents protocoles étudiés en terme complexité d'implémentation des primitives cryptographiques et algébriques.

Mots-clés : Protocole d'authentification, RFID, vérification automatique, confidentialité, authentification.

Keywords: Authentication protocol, RFID, automatic verification, confidentiality, authentication.

TABLE DES MATIÈRES

CHAPITRE III :

LE LANGAGE DE SPECIFICATION HLPSL
ET LA PLATEFORME AVISPA

CHAPITRE IV :

CONTRIBUTION : VERIFICATION DES PROTOCOLES
D'AUTHENTIFICATION DES SYSTEMES RFID

CHAPITRE V :

ÉTUDE COMPARATIVE