

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

Pr. Mohamed Benmohammed

Dr. Allaoua Chaoui

Dr. Azeddine Bilami

Prof. Université de M'sila

Prof. Université de Constantine

M.C. Université de Constantine

M.C. Université de Batna

Président

Rapporteur

Examineur

Examineur

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

Table des matières	i
Liste des figures	iv
Liste des tables	v

1. Introduction générale.....	01
1.1. Cadre du travail.....	01
1.2. Objectifs du travail.....	02
1.3. Plan du travail.....	02

CHAPITRE I :

VÉRIFICATION AUTOMATIQUE DES PROTOCOLES CRYPTOGRAPHIQUES

1. Préface.....	04
2. principes cryptographiques.....	05
2.1. Les propriétés de sécurité	05
2.2. Les primitives cryptographiques.....	06
3. Protocoles cryptographiques.....	09
3.1. Notations.....	09
2.2. Les types de protocoles cryptographiques.....	09
4. Modélisation des Protocoles de sécurité.....	12
4.1. Modèles cryptographiques.....	12
4.2. Modèles formels.....	13
4.3. Lien entre modèles cryptographiques et formels	14
5. Les techniques des modèles formels	14
5.1. Modèle Dolev-Yao	14
5.2. Logique BAN	14
5.3. Model checking.....	15
5.4. Approche inductive.....	16
5.5. Système réécriture, et clause Horn.....	16
5.6. Algèbres de processus.....	16
6. Approches de vérification.....	17
6.1. Recherche d'attaque	17
6.2. Preuve d'un protocole	17
7. Les hypothèses de la modélisation.....	18
7.1. Les canaux de communication.....	18
7.2. Les agents.....	18
7.3. L'intrus.....	18
7.4. Chiffrement parfait.....	20
8. Outils de vérification.....	21
8.1. Outils basé sur la recherche d'attaque	21
8.2. Outils basé sur le Preuve	21

CHAPITRE II :

LA SÉCURITÉ DES SYSTÈMES RFID

1. Les systèmes RFID.....	24
1.1. Les catégories des RFID.....	24
1.2. Les applications des RFID.....	27
1.3. Les normes de RFID.....	28
2. Implémentation des primitives cryptographiques et algébriques.....	30
2.1. Chiffrement symétrique.....	30
2.2. Chiffrement asymétrique.....	30
2.3. Fonction de hachage.....	31
2.4. Les nonces.....	31
2.5. Ou exclusif (xor).....	31
3. Propriétés de sécurité.....	32
3.1. Propriétés classique.....	32
3.2. Propriétés spécifique.....	33
4. Attaques contre RFID.....	33
4.1. Attaque contre tag RFID.....	34
4.2. Attaque contre lecteur RFID.....	34

CHAPITRE III :

LE LANGAGE DE SPECIFICATION HLPSL ET LA PLATEFORME AVISPA

Rappel.....	35
1. Le langage de spécification HLPSL.....	36
1.1. Rôles basiques.....	37
1.2. Rôles de composants.....	40
1.3. Les prédicats et les propriétés à vérifier.....	41
2. Langage IF.....	42
3. La plateforme AVISPA.....	42
3.1. OFMC.....	43
3.2. CL-Atse.....	43
3.3. SATMC.....	44
3.4. A4SP.....	44
4. La correspondance entre la spécification et le protocole.....	44
5. Comparaison aux autres outils.....	45
6. Synthèse.....	46

CHAPITRE IV :

CONTRIBUTION : VERIFICATION DES PROTOCOLES D'AUTHENTIFICATION DES SYSTEMES RFID

1. Introduction.....	47
2. Les propriétés à vérifier.....	48
3. Les scénarios de la vérification.....	48
4. Résultats de la vérification.....	49
5. Les protocoles de la cryptographie symétrique.....	51
5.1. Protocole FDW (Question/Réponse).....	51
5.2 Protocole FDW (Mutuelle).....	52
6. Les protocoles de la fonction de hachage.....	53
6.1. Protocole RLHS.....	54
6.2. Protocole HMNB.....	55
6.4. Protocole CRAP.....	57
6.5. Protocole LAK.....	58
7. Les protocoles qui exigent des primitives non cryptographiques.....	60

7.1. Protocole LRMAP.....	60
7.2. Protocole CH.....	62
8. Synthèse	63
CHAPITRE V :	
ÉTUDE COMPARATIVE	
1. Analyse de résultats.....	64
2. Travaux existants.....	66
2.1. Protocole FDW (Question/Réponse)	66
2.2. Protocole FDW (Mutuelle)	66
2.3. Protocole RLHS.....	67
2.4. Protocole HMNB.....	67
2.5. Protocole CRAP.....	67
2.6. Protocole LAK.....	68
2.7. Protocole LRMAP.....	68
2.8. Protocole CH.....	68
2.9. Comparaison les résultats obtenus aux travaux existants	69
3. La performance et la complexité du tag	69
4. Synthèse	71
Conclusion et Perspective.....	72
Bibliographie.....	74
Annexe A : Spécification du protocole FDW (Question/Réponse)	79
Annexe B : Spécification du protocole FDW (Mutuelle)	80
Annexe C : Spécification du protocole RLHS	81
Annexe D : Spécification du protocole HMNB.....	82
Annexe E: Spécification du protocole CRAP.....	83
Annexe F: Spécification du protocole LAK.....	84
Annexe G: Spécification du protocole LRMAP.....	85
Annexe H: Spécification du protocole CH.....	86