

# INTRODUCTION

## **Contexte général :**

L'identification par radiofréquence (RFID) a connu des évolutions rapides au cours des dernières années et qui sont utilisés dans plusieurs applications, tels que la santé, le logistique, le transport, le contrôle d'accès ...etc. Parmi les caractéristiques importantes dans les tags des systèmes RFID on trouve la limitation des ressources (mémoire, énergie, ...), ce qui rend des problèmes au niveau de sécurité. Les différentes couches du système RFID sont: la couche physique, la couche réseau-transport et la couche application. Les protocoles d'authentification des systèmes RFID se trouve dans la couche de réseau-transport.

Les protocoles d'authentification des systèmes RFID représentent un cas particulier des protocoles cryptographiques qui assurèrent la propriété d'authenticité. Donc, le protocole cryptographique est un ensemble de règles d'échange entre les participants d'un réseau, basé sur les notions de crypto-systèmes qui permettent de sécuriser les communications dans un environnement hostile afin de réaliser une certaine fonctionnalité (Confidentialité, Authentification,...). Les participants du système RFID sont : serveur, lecteur et tag.

Souvent des tels protocoles ne sont qu'en cours de spécification et leurs réelles performances ne sont que théoriques. C'est ainsi pour évaluer les performances d'un protocole, la manière la moins coûteuse est l'implémentation dans un simulateur. La simulation est un outil d'aide à la décision très utilisé par les concepteurs et les gestionnaires des systèmes complexes, Elle consiste à construire un modèle d'un système réel (physique, économique, humain ... etc.) et à conduire des expériences sur ce modèle afin de bien comprendre le comportement de ce système et d'en améliorer les performances.

## **Objectifs du travail :**

Dans ce mémoire, nous allons étudier des récents protocoles d'authentification des systèmes RFID. Les protocoles sélectionnés basés sur deux primitives cryptographiques, la fonction de hachage et le générateur des nombres pseudo-aléatoire.

L'objectif de cette étude est de simuler ces protocoles d'authentification RFID et simuler ses attaques si se trouve en développant un simulateur « SimRF-Auth » pour assurer le fonctionnement des protocoles et pour représente réellement des protocoles et des traces d'attaque s'il existe. Notre simulateur assure l'évaluation de performance des protocoles étudiés.

## **Plan du mémoire :**

Ce mémoire est organisé de la façon suivante:

### **Chapitre I : La cryptographie.**

Dans ce même chapitre sont exposées les notions de base de la cryptographie et les propriétés de sécurité qui peuvent être assurées dans ces systèmes . Nous présentons les primitives cryptographiques exigés dans les protocoles tels que : fonction de hachage cryptographique, générateur des nombres pseudo-aléatoire (PRNG) et l'opérateur Ou-exclusif.

### **Chapitre II : Protocoles d'authentification RFID**

Ce chapitre est divisé en deux sections: la section 1 consiste à définir les systèmes d'identification par radio- fréquence (RFID), ses composants, ses applications. La section 2 consiste à décrire les protocoles d'authentification RFID étudiés dans ce mémoire.

### **Chapitre III : Spécification des besoins et conception du simulateur**

Le chapitre 3 porte sur la spécification des besoins de l'implémentation du simulateur des protocoles d'authentification RFID ainsi que les différentes étapes de conception d'un tel simulateur.

### **Chapitre IV : Implémentation du simulateur**

Le chapitre 4 est consacré au développement et l'expérimentation du simulateur : En effet, en premier lieu, ce chapitre présente les différents outils (Java, Net Beans IDE 6.9, JCE et MySQL) et les différentes interfaces de l'outil mis en place. Et dans un second lieu, une expérimentation des protocoles étudiés à travers le simulateur développé.

Finalement, nous clôturons ce mémoire par une conclusion et des perspectives.