heig-vd
Haute Ecole d'Ingénierie et de Gestion
du Canton de Vaud
http://www.heig-vd.ch

Travail de diplôme 2006

HEIG-VD
Route de Cheseaux 1
CH - 1401 Yverdon-les-Bains

Sécurité RFID et préservation de la sphère privée

Technologie RFID

L'identification par radiofréquence (RFID) est une technologie qui permet d'identifier à distance des objets sans contact physique ni visuel. Elle nécessite pour cela des transpondeurs à bas coût, appelés tags qui sont apposés sur les objets à identifier ; des lecteurs qui permettent d'interroger ces tags par radiofréquence ; et un système de traitement de données, qui peut être centralisé ou distribué dans chaque lecteur. On l'utilise pour la traçabilité dans les chaînes logistiques, pour les abonnements aux transports publics, pour les clefs de démarrage des voitures, pour les badges de contrôle d'accès, pour les passeports électroniques, etc.

Problématique

La RFID fait face à de nombreux problèmes de sécurité, difficiles à résoudre en raison des faibles ressources des tags. Elle doit se prémunir des dénis de service, des fuites d'information, des problèmes de vie privée et de l'usurpation d'identité. L'une des technique permettant d'usurper l'identité d'une personne (par exemple dans le cadre d'un contrôle d'accès physique) est de pratiquer une attaque relais, c'est-à-dire de faire croire à un lecteur qu'un tag légitime est à sa proximité, alors qu'il est en fait en dehors de son champs opérationnel. Pour cela, le pirate, avec l'aide d'un complice, joue le rôle d'une rallonge entre le lecteur et le tag : il suffit que le pirate soit proche du lecteur et son complice proche du tag au moment même de l'attaque.

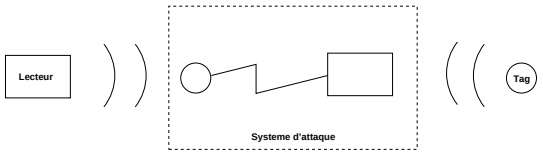

FIGURE 1 : Attaque relai

L'attaque est totalement transparente pour la victime car le tag répond à toute sollicitation sans demander l'accord de son porteur. Les conséquences d'une telle attaque peuvent être très importantes, en particulier dans le cadre du contrôle d'accès ou du paiement électronique. Les techniques pour éviter ce type d'attaques reposent sur la mesure du temps de réponse du tag : un temps de réponse trop important implique le rejet du tag. Ces techniques sont appelées *distance bounding protocols*.

But du travail

Le but est d'analyser les protocoles de *distance bounding* existants. Ces protocoles ajoutent à l'authentification usuelle une preuve de proximité, permettant ainsi de parer aux attaque par relais. Ils se basent sur le fait qu'il existe une vitesse causale indépassable (la vitesse de la lumière c) et qu'un éventuel relai entre le tag et le lecteur implique forcément un retard dans un échange entre les deux entités.

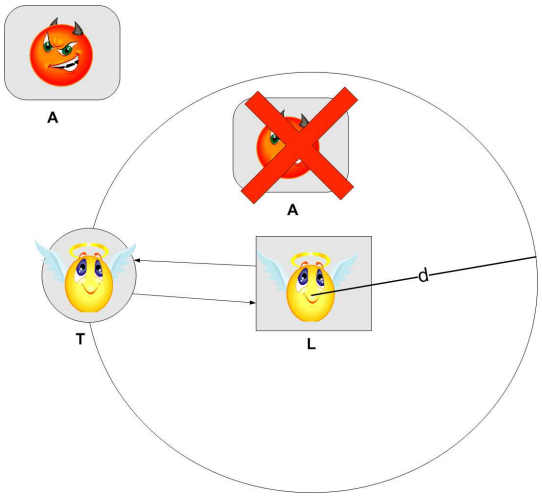

FIGURE 2 : Principe de la borne sur la distance

Un échange de bits rapide est opéré entre le tag et le lecteur afin de mesurer le temps d'aller retour et ainsi déterminer une borne supérieure d en deça de laquelle aucun attaquant ne peut se trouver. L'autre partie de l'authentification se fait à l'aide d'une clé secrète partagée.

Auteur : Léonard GROSS
Répondant externe : Gildas AVOINE
Prof. responsable : Stephan ROBERT
Sujet proposé par : Gildas AVOINE

Hes·so
Haute Ecole Spécialisée
de Suisse occidentale