Mécanismes de Restauration de Privacy pour les Systèmes RFID Offlines

Gildas Avoine, Iwen Coisel et Tania Martin

Dans le domaine de la RFID, les protocoles d'authentification sont développés pour faire face à des adversaires capables d'écouter et de réorganiser à souhait les communications entre les lecteurs et les étiquettes. Dans la plupart des modèles de sécurité, l'adversaire a de plus la capacité de corrompre une ou plusieurs étiquettes RFID afin d'en obtenir les secrets. En revanche, aucun de ces modèles ne donne la possibilité à un adversaire de corrompre un lecteur afin de récupérer l'intégralité des données que celui-ci stocke. Toutefois, dans certaines applications RFID à grande échelle (e.g. système de transport, tickets électroniques...), cette menace n'est plus une fiction.

Si le protocole d'authentification utilise des lecteurs offlines, ces derniers doivent contenir l'ensemble des informations permettant d'authentifier/identifier les étiquettes du système. Par conséquent, la corruption d'un lecteur peut être lourde de conséquences entraînant par exemple la possibilité d'usurper l'identité des utilisateurs du système ou encore la possibilité de les tracer. L'unique moyen de restaurer la sécurité des systèmes actuels est de renouveler la totalité des tags et des lecteurs, ce qui en pratique est évidemment irréalisable. Nous avons introduit un protocole d'authentification d'étiquettes RFID assurant le respect de la vie privée des utilisateurs capable de restaurer la propriété de privacy suite au vol d'un lecteur compromis. De plus, l'obtention des secrets d'un lecteur ne permet pas à l'adversaire d'usurper l'identité des utilisateurs auprès des autres lecteurs légitimes du système.

Dans notre protocole d'authentification, un identifiant unique est associé à chaque couple (lecteur,tag). Chaque tag est capable de recalculer cet identifiant à l'aide de sa clé secrète et de l'identité du lecteur auprès duquel il souhaite s'authentifier. Le lecteur ne connaît pas les clés secrètes des étiquettes et doit par conséquent stocker l'ensemble de ces identifiants. Lors de la corruption d'un lecteur, l'adversaire récupère l'ensemble des données stockées et pourra par la suite temporairement tracer les tags à l'aide des identifiants uniques obtenus. Toutefois, il est dans l'incapacité de calculer les identifiants uniques correspondants à d'autres lecteurs.

Lorsque le vol du lecteur a été détecté, celui-ci est remplacé par un autre lecteur et la procédure de restauration de privacy est activée. Lorsqu'un tag tentera de s'authentifier auprès du lecteur, ce dernier informera le tag qu'un lecteur a été compromis en lui transmettant de nouveaux identifiants certifiés visant à remplacer ceux du lecteur compromis. Lorsque le tag mis à jour communiquera avec d'autres lecteurs il propagera cette information aux autres lecteurs qui feront de même avec les autres tags etc. La restauration de la privacy se déroule ainsi comme la propagation d'un virus dans un réseau informatique.

Nous avons appliqué de manière théorique notre protocole en utilisant les logs d'un évènement sportif de trois jours utilisant des tickets électroniques. Le système était composé de 55 lecteurs offlines et plus de 100.000 tags RFID. La restauration de la privacy est analysée dans différents cas dépendant du moment où les lecteurs ont été compromis.