تحسين بروتوكول التوثيق الخفيف لأنظمة RFID الكامنة

عائشة علي عسيري

المشرف الرئيسي على الرسالة

د.أميمه عمر بامسق

المستخلص

انتشرت تقنية التعريف بالتردد اللاسلكي (Radio Frequency Identification-RFID) و تطبيقاتها في الآونة الأخيرة عبر العديد من مجالات حياتنا اليومية. و حيث أن انخفاض تكلفة البطاقة هو أحد العوامل الهامة لإنتشارها، فإن هذا يقتضي أهمية تصميم بروتوكول للتوثيق الخفيف بحيث يكون آمن وفعال لمقاومة كل الهجمات الممكنة. إن معظم بروتوكولات (RFID) القائمة حاليا للتوثيق الخفيف تبني تصميماتها على أوليات مكلفة قد تتجاوز قدرات الشرائح من أجل كسب المزيد من الأمان.

اكتسبت عائلة بروتوكولات التوثيق الخفيف (HB- Hopper and Blum) أكبر قدر من الاهتمام في السنوات القليلة الماضية مقارنة بغيرها من البروتوكولات خفيفة الوزن، نظرا لاستخدامها الواسع في التطبيقات الخاصة بالأجهزة ذات التكلفة المنخفضة، الواسعة الانتشار. و قد وجد أن معظم اصدارات عائلة (HB) هي عرضة لهجوم (Gilbert, Robshaw, and Seurin attack)-GRS، نوع من هجومات Man-in-the-Middle.

في هذه الأطروحة، تم اقتراح و تصميم بروتوكول جديد و آمن لعائلة (HB)، اسمه (HB-MP*)، باستخدام تقنيات الدوران العشوائي. و قد تم اثبات أمان البروتوكول المقترح باستخدام الاثبات المنهجي. بعد ذلك، تم إجراء نموذج أولي للبروتوكول للتحقق من إمكانية تطبيقه، اختبار مدى أمانه أثناء التنفيذ و مقارنة أداؤه بالبروتوكول الأكثر صله به. و قد تم التوصل إلى أن (HB-MP*) هو بروتوكول آمن ضد الخصوم الغير مباشرة والنشطة، وهو أيضا قابل للتنفيذ ضمن القيود المشددة للموارد في شرائح (RFID) اليوم من نوع (EPC). تبعا لذلك ، يوفر بروتوكول (HB-MP*) أمانا أفضل من بروتوكولات (HB) السابقة من دون أي خسارة في جانب الأداء.

Enhancing A Lightweight Authentication Protocol For Passive RFID-Tagged Systems

Aisha Ali Aseeri

Thesis Advisor

Dr. Omaima Omar Bamasak

Abstract

RFID technology and its applications have recently spread across many aspects of our daily life. The low cost of the tag is one of the important factors to their proliferation, which of course restricts storage and computation capabilities on tags. This implies the importance of designing a secure and efficient light-weight authentication protocol to resist all feasible attacks using only low cost primitives. Most of the existing light-weight RFID authentication protocols based their designs on expensive primitives which is beyond tags capabilities in order to gain more security. HB family lightweight authentication protocols have gained most attention in the past few years among other lightweight protocols due to its broad spectrum of application in low-cost pervasive devices. Most of HB variants are vulnerable to a GRS man-in-the-middle attack.

In this thesis, a new and secure variant of HB family protocols named HB-MP* is proposed and designed, using the techniques of random rotation. Then, the security of the proposed protocol is proven using formal proofs. After that, a prototype of the protocol is conducted to check its applicability, test the security in implementation and to compare its performance with the most related protocol. The HB-MP* protocol is found secure against passive and active adversaries and is implementable within the tight resource constraints of today's EPC-type RFID tags. Accordingly, HB-MP* protocol provides higher security than previous HB-like protocols without sacrificing performance.