Research Article, 2021, Volume 8, Number 2
http://www.jcomsec.org

Journal of Computing and Security

طرح احراز هویت سبک وزن برای RFID با عملیات جایگشت روی برچسب‌های غیرفعال

علیرضا عبدالهی خوراسگانی[آ]، مهدی سجادیه[آ،*]، محمد روح الله یزدانی[آ]

[آ] گروه مهندسی برق، واحد خوراسگان (اصفهان)، دانشگاه آزاد اسلامی، اصفهان، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 23 June 2021
اصلاح: 22 January 2022
پذیرش: 30 January 2021
انتشار آنلاین: 22 February 2022

کلمات کلیدی:
RFID، حملات بازپخش، جعل هویت خواننده، ردیابی برچسب.

چکیده

توسعه سریع و روزافزون اینترنت اشیا (IoT) امیدواری فراوانی در ارتقاء کیفیت زندگی انسان به ارمغان آورده است. فناوری شناسایی فرکانس رادیویی (RFID) به عنوان فناوری پشتیبان در اینترنت اشیا به طور گسترده در حوزه‌های مختلف زندگی در حال استفاده است. بنابراین مسائل امنیتی و حفظ حریم خصوصی کاربران باید در اولویت مباحث این بخش قرار گیرد. اما محدودیت توان محاسباتی و منابع ذخیره‌سازی در برچسب‌های غیرفعال RFID اجرای مسائل امنیتی را دشوار ساخته است. بطوریکه طراحی پروتکل‌های احراز هویت سبک وزن برای سامانه‌های RFID کماکان یکی از اصلی‌ترین مسائل در حوزه امنیت RFID محسوب می‌شود. در سال‌های اخیر Liu، پروتکل احراز هویت سبک وزنی مناسب برای برچسب‌های غیرفعال پیشنهاد دادند. آنها در پروتکل IOLAS از عملیان Invers بخصوصی استفاده کرده‌اند و چنین ادعا کردند که این عملیات بیتی سبک وزن این پروتکل را در برابر حملات شناخته شده و قابل وقوع در سامانه‌های rRFID مقاوم کرده است. در مقاله فعلی ما نشان می‌دهیم که همین عملیات Invers مشکل اساسی این پروتکل است بطوریکه این پروتکل نمی‌تواند امنیت روبه عقب را تضمین کند. همچنین نشان داده شد که پروتکل IOLAS در برابر پخش مجدد، جعل هویت خواننده، حملات ردیابی برچسب و حمله افشای اطلاعات مخفی آسیب‌پذیر است. در نهایت، پروتکل IOLAS را بهبود دادیم و پروتکل POLAS را پیشنهاد کردیم که در برابر حملات شناخته شده فعلی مقاوم است. ما سطح امنیتی پروتکل پیشنهادی را تجزیه و تحلیل می‌کنیم و امنیت طرح پیشنهادی را با استفاده از منطق BAN (Burrows-Abadi-Needham) اثبات می‌کنیم. همچنین با استفاده از ابزار شبیه‌سازی Scyther، امنیت پروتکل پیشنهادی را به طور رسمی تایید کردیم. با توجه به تحلیل‌های امنیتی، می توان مشاهده کرد که این پروتکل از امنیت بالایی برخوردار هستند. مقایسه عملکرد پروتکل Scyther نشان می‌دهد که این پروتکل از نظر هزینه‌های محاسباتی، هزینه‌های ذخیره‌سازی و هزینه‌های ارتباطی با پروتکل‌های مشابه قابل مقایسه است.

* نویسنده مسئول.
آدرس‌های رایانامه: alireza.abdellahi@khuisf.ac.ir (ع. عبدالهی خوراسگانی)، m.sajadieh@khuisf.ac.ir (م. سجادیه)، m.sajadieh@khuisf.ac.ir (م. ر. یزدانی)

ISSN: 2322-4460