عنوان مقاله:
تحلیل محرمانگی و امنیت پروتکل احراز هویت دوسویه در سامانه های RFID مبتنی بر توابع چکیده ساز

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 1, شماره 2 (سال: 1392)

تعداد صفحات اصل مقاله: 0

نویسندگان:
سید محمد علوی - *دانشگاه جامع امام حسین*

بهزاد عبدالملکی - *دانشگاه شاهد*

کریم باقری - *دانشگاه شاهد*

خلاصه مقاله:
فناوری شناسایی با استفاده از امواج رادیویی (RFID)، یک فناوری نوینی است که در زمینه های متفاوت، جهت شناسایی و احراز هویت مورد استفاده قرار می گیرد. نظر به اینکه در اکثر کاربردها، امنیت این سامانه ها مورد اهمیت است، لذا برای حفظ این امنیت پروتکل های رمزنگاریی برای احراز هویت این سامانه ها مورد استفاده قرار می گیرد. در این مقاله، به تحلیل امنیتی یک پروتکل احراز هویت متقابل سامانه های RFID می پردازیم. این پروتکل توسط آقای کیم در سال ۲۰۱۳ ارایه شده است. نشان می دهیم بر خلاف اینکه طراح سعی کرده است که پروتکل امنی را طراحی کند، همچنان ضعف هایی بر این پروتکل وارد است و این پروتکل نمی تواند امنیت و محرمانگی کاربر را فراهم کند. در ادامه، حمله های جعل برچسب، ردیابی و ردیابی پسرو را روی این حمله انجام می دهیم. برای ارزیابی قابلیت ردیابی این پروتکل از مدل اوفی-فانی استفاده شده است، و حمله های ردیابی و ردیابی پسرو در قالب این مدل انجام شده است. در ادامه، نسخه ی بهبود یافته از پروتکل کیم پیشنهاد شده است، که ضعف های پروتکل قبلی حذف شده است. امنیت و محرمانگی پروتکل بهبود یافته با برخی از پروتکل های پیشنهاد شده در سال های اخیر مقایسه می شود و مشاهده می شود که پروتکل پیشنهاد شده از امنیت خوبی برخوردار است.

کلمات کلیدی:
امنیت سامانه های RFID, پروتکل های احراز هویت سامانه های RFID, پروتکل های احراز هویت دوسویه