Journal of Computing and Security

January 2019, Volume 6, Number 1
http://www.jcomsec.org

حمله کشف تمام مقادیر مخفی به یک پروتکل احراز اصالت منطبق بر EPC-C1 G2

معصومه صفخانی[آ،*]

[آ] دانشکده مهندسی کامپیوتر، دانشگاه تربیت دبیر شهید رجایی، تهران ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 16 March 2018
اصلاح: 8 August 2018
پذیرش: 23 September 2019
انتشار آنلاین: 25 November 2019

کلمات کلیدی:
RFID، EPC-C1 G2، پروتکل احراز اصالت، حمله‌ی کشف مقادیر مخفی، منطق GNY.

چکیده

تحلیل امنیتی یک پروتکل گام مهمی در جهت جلب اعتماد عمومی به امنیت آن است. اخیراً در سال ۲۰۱۸، مرادی و همکاران امنیت پروتکل احرازاصالت منطبق بر EPC-C1 G2 ونگ و ژنگ را بررسی کردند و حمله غیر همزمان‌سازی و همچنین حمله جعل هویت سرور/قرائتگر را علیه آن ارائه دادند. آنها سپس یک نسخه بهبود یافته از آن پروتکل را ارائه نمودند. اما در این مقاله، تا آن جایی که اطلاع داریم و به عنوان اولین تحلیل شخص ثالث، ما یک حمله کشف مقادیر مخفی کارا با پیچیدگی تنها اجرای $O(۲^{۱۶})$ بار ارزیابی‌های برون‌ـخط PRNG را ارائه می‌دهیم. از آنجایی که به نظر طراحی یک پروتکل امن با استفاده از CRCهای ۱۶بیتی و PRNGهای ۱۶ بیتی در چهارچوب استاندارد EPC-C1 G2 ممکن نیست و تغییر این استاندارد به گونه‌ای که اجازه استفاده از توابع رمزنگاری سبک‌وزن را بدهد، اجتناب‌ناپذیر است، توصیه می‌شود از این توابع با هدف رسیدن به یک پروتکل امن استفاده نشود. در همین راستا ما نسخه بهبود یافته پروتکل مرادی و همکاران را ارائه می‌دهیم و امنیت آن را هم به روش غیرصوری و هم به روش صوری از طریق منطق GNYاثبات می‌نماییم.

* نویسنده مسئول.
آدرس رایانامه: Safkhani@sru.ac.ir (م. صفخانی)
ISSN: 2322-4460