Journal of Computing and Security

January 2018, Volume 5, Number 1 (pp. 51--51)

http://www.jcomsec.org

بهبودی بر پروتکل تبادل کلید لی و همکاران

حسین اورعی [آ]، محسن پورپونه [ب]، رسول رمضانیان [ج،*]

[آ] دانشکده ریاضی دانشگاه علم و صنعت، تهران، ایران.

[ب] دانشکده علوم ریاضی دانشگاه صنعتی شریف، تهران، ایران.

[ج] دانشکده ریاضی دانشگاه فردوسی مشهد، مشهد، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 16 July 2017
اصلاح: 01 October 2018
پذیرش: 03 October 2018
انتشار آنلاین: 26 December 2018

کلمات کلیدی:
پروتکل تبادل کلید، محرمانگی رو به جلو، محرمانگی رو به عقب، تحلیل صوری.

چکیده

در سال ۲۰۰۴ هووآنگ و همکاران یک پروتکل تبادل کلید گروهی جهت به اشتراک گذاشتن یک کلید امن در یک گروه پیشنهاد کردند. پروتکل آن‌ها یک توسعه از پروتکل تبادل کلید دو عاملی به تبادل کلید گروهی است. اخیراً جونگ‌ـسن لی و همکاران به وجود دو ضعف امنیتی در پروتکل هووآنگ و همکاران اشاره نموده‌اند. آن‌ها نشان دادند که پروتکل ارائه‌شده محرمانگی روبه‌جلو در زمانی که یک عضو جدید به گروه می‌پیوندد را برقرار نمی‌کند. همچنین درصورتی‌که یکی از اعضای گروه از پروتکل خارج شود محرمانگی رو به عقب با مشکل مواجه می‌شود.همچنین آن‌ها یک پروتکل مبادله کلید جدید به‌منظور رفع نواقص گفته‌شده ارائه نموده‌اند. در این مقاله ما بهبود دیگری برای پروتکل ارائه‌شده مطرح می‌کنیم که نه‌تنها محرمانگی روبه‌جلو و رو به عقب را حفظ می‌کند بلکه از نظر محاسباتی نیز از پروتکل داده شده توسط لی و همکاران کاراتر می‌باشد. در نهایت، با استفاده از ابزار صوری اسسایتر به تحلیل رسمی جهت بررسی صحت پروتکل پیشنهاد شده می‌پردازیم.

* نویسنده مسئول.

آدرس‌های رایانامه: hossein_oraei@mathdep.iust.ac.ir (ح. اورعی)، mohsen.pourpoune1@student.sharif.ir (م. پورپونه)، rramezanian@um.ac.ir (ر. رمضانیان)

ISSN: 2322-4460