Journal of Computing and Security

July 2018, Volume 5, Number 2
http://www.jcomsec.org

تحلیل امنیت دو طرح امضا فاقد گواهینامه سبک‌وزن

نصراله پاک‌نیت [آ,*]،

[آ] پژوهشکده علوم اطلاعات، پژوهشگاه علوم و فناوری اطلاعات ایران (ایرانداک)، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 20 May 2018
اصلاح: 25 February 2019
پذیرش: 13 March 2019
انتشار آنلاین: 27 November 2018

کلمات کلیدی:
رمزنگاری فاقد گواهینامه، تحلیل امنیت، امضا، اینترنت اشیا صنعتی، شبکه‌های حسگر بیسیم سلامتی.

چکیده

رمزنگاری فاقد گواهینامه راه‌حلی میانی است که به طور همزمان بر مشکلات موجود در سیستم‌های رمزنگاری سنتی و سیستم‌های رمزنگاری مبتنی بر شناسه غلبه می‌کند. بررسی پیشینه نشان می‌دهد که طرح‌های امضا فاقد گواهینامه زیادی در گذشته ارائه شده اما کارایی هیچ یک از این طرح‌ها به اندازه‌ای نیست که بتوان از آن‌ها در محیط‌هایی با محدودیت منابع مانند "اینترنت اشیا" یا "شبکه‌های حسگر بیسیم سلامتی" استفاده کرد. اخیرا دو طرح امضا فاقد گواهینامه سبک‌وزن توسط Karati و همکاران، و Kumar و همکاران به ترتیب برای استفاده در اینترنت اشیا و شبکه‌های حسگر بیسیم سلامتی ارائه شده است. علی‌رغم ادعای ارائه‌دهندگان هر دو طرح مبنی بر دستیابی به سطح امنیت جعل‌ناپذیری وجودی، در این مقاله خلاف این ادعاها را اثبات کرده و نشان خواهیم داد که جعل امضا در هر یک از این دو طرح به راحتی ممکن است. به بیانی دقیق‌تر، در این مقاله نشان خواهیم داد که ۱) در طرح ارائه شده توسط Karati و همکاران، متخاصم نوع اول در نظر گرفته شده در رمزنگاری فاقد گواهینامه می‌تواند برای هر کاربر دلخواهی کلید خصوصی جزئی معتبر ایجاد کرده و با استفاده از آن امضا آن کاربر را بر روی هر پیامی جعل کند، و ۲) در طرح Kumar و همکاران، هر دو نوع متخاصم در نظر گرفته شده در رمزنگاری فاقد گواهینامه قادر به جعل امضا هر کاربری بر روی هر پیام دلخواهی هستند.

* نویسنده مسئول.
آدرس رایانامه: pakniat@irandoc.ac.ir (ن. پاک‌نیت)
ISSN: 2322-4460