July 2019, Volume 6, Number 2
http://www.jcomsec.org

Journal of Computing and Security

CSE: یک مبهم‌سازی پویا جدید مبتنی بر ترکیب سیگنال، کنترل جریان و رمزگذاری

بهاره هاشم زاده [آ]، مجید عبدالرزاق نژاد [ب،*]

[آ] .دانشکده برق و مهندسی کامپیوتر، دانشگاه تربت حیدریه، تربت حیدریه، ایران
[ب] .گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بزرگمهر قائنات، قائن، ایران

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 1 February 2019
اصلاح: 26 January 2020
پذیرش: 26 January 2020
انتشار آنلاین: 8 April 2020

کلمات کلیدی:
مبهم‌سازی پویا، کنترل جریان، سیگنال، رمزگذاری، جدول مدیریت، Spritz، توابع ارزیابی.

چکیده

مبهم‌سازی که به عنوان یک استراتژی تهاجمی محسوب می‌شود را می‌توان به عنوان یک استراتژی تدافعی در حوزه‌ی حفاظت از نرم‌افزارهای و اطلاعات حیاتی نیز در نظر گرفت. در این مقاله، براساس ترکیب سه گانه جریان کنترل و سیگنال‌ها و رمزگذاری جدول مدیریت (MT) ، یک روش مبهم‌سازی پویا جدید، که آن‌را CSE خطاب می‌کنیم ، پیشنهاد می‌شود. این سه گانه پیشنهادی، برنامه‌ی کنترل نمودار را نخست تغییر و سپس پنهان می‌نماید و MT را که شامل آدرس‌ها است برای هدایت ارتباط بین دستورالعمل‌ها تولید می‌کند. یک نوع رمزگذاری متقارن جریان حروف (Spritz) برای رمزگذاری MT به کار گرفته شده است. همچنین، یک تابع چندهدفه (توانایی و تاب‌آوری) مبتنی بر شش معیار اجرای و دو تابع هدف کلاسیک (هزینه و میشرا) در ارزیابی روش مبهم‌سازی پیشنهادی در نظر گرفته شده است. روش مبهم‌سازی سه‌گانه پیشنهادی و این توابع چند هدف برروی یک برنامه کوچک و یک مجموعه داده معیار در بخش نتایج تجربی اجرا شده است. مقایسه نتایج تجربی روش‌های انسداد موجود نشان می دهد که CSE مزایای رقابتی دارد. مقایسه این پیاده‌سازی با سایر روش‌های مبهم‌سازی موجود نشان می‌دهد که روش CSE دارای مزیت‌های رقابتی با سایر روش‌های مبهم‌سازی موجود می‌باشد.

* نویسنده مسئول.
آدرس‌های رایانامه: b.hashemzadeh@profs.torbath.ac.ir (ب. هاشم زاده)، abdolrazzagh@buqaen.ac.ir (م. عبدالرزاق نژاد)
ISSN: 2322-4460