عنوان مقاله:
ترکیب الگوریتم RSA و الگوریتم AMEA برای رمزنگاری هویت ها در SOA

محل انتشار:
همایش جامع بین المللی کامپیوتر، فناوری اطلاعات و مهندسی برق (سال: 1396)

تعداد صفحات اصل مقاله: 6

نویسنده:
پردیس کله سری - *دانشجوی دکتری تخصصی در گروه کامپیوتر دانشگاه آزاد اسلامی واحد رشت*

خلاصه مقاله:
معماری های سرویس گرا به ارایه یک الگوی معماری می پردازد که به ساده سازی ادغام سرویس ها و برنامه های کاربردی مختلف کمک می کند. پیاده سازی معماری سرویس گرا برگرفته از ایده اولیه ای از یک سرویس بوده است. برای اجرای معماری سرویس گرا سه مولفه نقش اساسی دارد: ارایه دهنده خدمات، درخواست کننده خدمات و ثبت و پیگیری. هدف از ایجاد امنیت به حداقل رساندن تخریب داده ها در ارتباطات و جلوگیری از حملات بالقوه است. هرچه تعداد مصرف کنندگان معماری سرویس گرا افزایش می یابد، نیاز آن به امنیت نیز بالاتر رفته و افراد بیشتری تلاش خواهند کرد تا به اطلاعات ارزشمند در سیستم هایی با معماری سرویس گرا رخنه کنند. از این رو محققین در تلاشند تا امنیت معماری سرویس گرا را افزایش دهند. برای حفاظت بیشتر از هویت ها در SOA از مهر زمانی و رمزنگاری بهره می گیرند که این کار می تواند سربار ذخیره سازی رموز در سیستم را تا حدی چشمگیر افزایش دهد، اما برای اینکه این مشکل بر طرف شود می توان از الگوریتم رمزنگاری RSA بهره برد که سرباری کمتر را با خود به همراه دارند. الگوریتمی که در مقاله پیشنهاد شده تا با الگوریتم RSA ترکیب شود الگوریتم AMEA بوده که می توان از آن برای سیستم های SOA بهره گرفت، الگوریتم AMEA یک الگوریتم تولید کلید تصادفی است که مشکلاتی را که برملا شدن یکی از کلیدها می تواند در سیستم به وجود بیاورد را با ایجاد کلیدهایی جدید در هر دور کاملا از بین خواهد برد. این الگوریتم می تواند در هر دور کلیدی جدید و امن را برای RSA ایجاد کند. این تغییر کلید در هر دور باعث می شود که افراد غیر مجاز نتوانند کلیدها را در دور بعدی حدس بزنند و با استفاده از ترکیب این دو الگوریتم دستیابی به کلید رمزگشایی غیر ممکن خواهد بود و سیستم هم از سربار اضافی در امان خواهد بود.

کلمات کلیدی:
معماری سرویس گرا، رمزنگاری، هویت، AMEA، RSA

لینک ثابت مقاله در پایگاه سیویلیکا: