عنوان مقاله:
تعریف و بررسی نامتغیرهای امنیتی روی توصیف ماشین حالت پروتکل های رمزنگار

محل انتشار:
سومین کنفرانس انجمن رمز ایران (سال: 1384)

تعداد صفحات اصل مقاله: 12

نویسندگان:
بهروز ترک لادانی - *گروه کامپیوتر دانشکده مهندسی دانشگاه اصفهان*

سعید جلیلی - *گروه کامپیوتر دانشکده مهندسی دانشگاه تربیت مدرس*

خلاصه مقاله:
در این مقاله روشی برای تحلیل پروتکل های رمزنگاری بر اساس مدل سازی پروتکل و نفوذی در قالب مجموعه ای از ماشین های حالت محدود تعمیم یافته (EFSM) مرتبط با یکدیگر ارائه شده است. برای وارسی پروتکل ها ابتدا ویژگی های امنیتی مورد نظر در قالب برخی نامتغیرهای ویژه توصیف شده، سپس صحت یا عدم صحت این نامتغیرها روی توصیف ماشین حالت پروتکل بررسی میشود. توصیف برخی ویژگی های امنیتی در پروتکل ها به کمک نامتغیرهای تعریف شده و الگوریتم هایی برای بررسی صحت یک نامتغیر داده شده روی EFSM ارائه شده است. به کمک الگوریتم های ارائه شده علاوه بر ارزیابی نامتغیر می توان سناریوی حمله متناظر با شکست یک نامتغیر Liveness یا موفقیت یک نامتغیر Safety را نیز ایجاد نمود. یک ویژگی خاص روش ارائه شد به دلیل استفاده از روش هاو ابزارهای متعار توسعه پروتکل های ارتباطی، کم کردن فاصله موجود بین تخصص لازم برای تحلیل درحوزه خاص پروتکل های رمزنگاری و تحلیل و طراحی در حوزه عام تر پروتکل های ارتباطی است.

کلمات کلیدی:
وارسی پروتکل های رمزنگاری ، بررسی مدل ، بررسی نامتغیرها ، SDL