عنوان مقاله:
تشخیص نفوذ مبتنی بر ناظر، براساس رویکرد سیستم های ایمنی مصنوعی

محل انتشار:
هشتمین کنفرانس انجمن رمز ایران (سال: 1390)

تعداد صفحات اصل مقاله: 8

نویسندگان:
رضا عزمی - *عضو هیئت علمی گروه آموزشی مهندسی کامپیوتر دانشگاه الزهرا(ع) تهران*

بشری پیشگو - *دانشکده فنی مهندسی دانشگاه الزهرا(ع) تهران*

حامد نعمتی - *دانشکده فنی مهندسی دانشگاه الزهرا(ع) تهران*

خلاصه مقاله:
یکی از چالشهای اساسی در مبحث امنیت سیستمهای کامپیوتری تشخیص فعالیتهای خرابکارانه ونفوذی به سیستم می باشد در این راستا روشهای گوناگونی بکار گرفته می شوند که از آن جمله می توان به مدلسازی رفتار پردازه ها اشاره نمود مدلسازی رفتار نیازمند الگویی مناسب از چگونگی رفتار پردازه ها و نیز روشی کارا برای تولید مدلرفتاری مبتنی بر این الگوها می باشد فراخوان های سیستمی الگوی مناسبی از چگونگی رفتار را فراهم می آورند به همین دلیل رویدادنگاری فراخوان های سیستمی به عنوان ابزاری متداول برای پیاده سازی مکانیزم های امنیتی شناخته می شود همزمان با پیشرفت این مکانیزم نفوذگران سعی کردند تا با تغییر در شیوه ی رویدادنگاری فراخوان ها حضور خود در سیستم و نوع فعالیتی که انجام می دهند را پنهان سازند. از این رو در این مقاله با بهره گیری از یک معماری مبتنی بر مانیتور ماشین مجازی به تضمین سلامت رویدادنگاری فراخوان های سیستمی می پردازیم.

کلمات کلیدی:
سیستم تشخیص نفوذ، رویدادنگاری فراخوانهای سیستمی ، مانیتور ماشین مجازی، سیستمهای ایمنی مصنوعی، الگوریتم انتخاب غیرخودی