عنوان مقاله:
مدل سازی تهدیدات داخلی در گراف های جهت دار و برچسب دار

محل انتشار:
دومین کنفرانس ملی رویکردهای نو در مهندسی برق و کامپیوتر (سال: 1395)

تعداد صفحات اصل مقاله: 9

نویسندگان:
حمیدرضا حسینی - *کارشناس فناوری اطلاعات، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه زابل، زابل، ایران،*

احسان سرگلزایی - *عضو هیات علمی، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه زابل، زابل، ایران،*

فاطمه کیخا - *عضو هیات علمی، گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه زابل، زابل، ایران*

خلاصه مقاله:
ارزیابی امنیت و تحلیل مخاطرات امنیتی سیستم ها جهت بهبود عملکرد آنها باید مورد توجه قرار گیرد. یکی از حملاتی که می تواند سیستم های اطلاعاتی را مورد هدف قرار دهد، تهدیدات داخلی است. مدل سازی تهدید رویکردی برای تحلیل امنیت سیستم های اطلاعاتی است. این نوع مدل سازی، رویکردی ساخت یافته است که طراحان را قادر به شناسایی، سنجش و تصحیح خطرات مرتبط با سیستم های اطلاعاتی می سازد. مدل سازی تهدید بر مبنای این نگرش استوار است که هر سیستم یا سازمان دارای منابع و دارایی های ارزشمندی است که این دارایی ها در معرض تهدیدات داخلی و خارجی قرار دارد. متناسب با این تهدیدات، اقدامات متقابل امنیتی نیز برای کاهش اثرات آن ها وجود دارد. علاوه بر این، مستندات تولید شده در مدل سازی تهدید می تواند درک بهتری از سیستم های اطلاعاتی مهیا کند. در این پژوهش این مشکل از منظر مجوزها در بستر کنترل دسترسی مورد بررسی قرار می گیرد. مجوزهای حساس در سیستم های امنیتی و ایجاد یک بستر مناسب برای کاهش سوءاستفاده کاربران مخرب، محدودیت های امنیتی و همچنین روابط کاربران باید در نظر گرفته شود. در تفکیک وظایف سعی بر این است نقش هایی که به گونه ای مستعد سوءاستفاده هستند، به افراد مختلف اعطا شوند تا یک فرد نتواند از مجموعه مجوزهای بدست آمده، سوء استفاده کند. بنابراین کاربری که قصد انجام حمله ای را دارد، نیاز به مهندسی اجتماعی و تبانی با کاربران دیگر دارد. در این پژوهش اینکه چگونه خطر تقلب را تا پایین ترین سطح ممکن کاهش دهیم، مورد بررسی قرار گرفته است.

کلمات کلیدی:
تهدید داخلی، آسیب پذیری امنیتی، ارزیابی کاربران، گراف تاثیر کاربر، الگوی سوءاستفاده، شاخص تضاد علاقه