عنوان مقاله:
اصول طراحی و معماری ماژول امنیت سخت افزاری

محل انتشار:
اولین همایش ملی رویکردهای نوین در مهندسی کامپیوتر و بازیابی اطلاعات (سال: ۱۳۹۲)

تعداد صفحات اصل مقاله: ۸

نویسندگان:
روح اله ییلاقی اشرفی - کارشناسی ارشد

فرهاد فرخ پناه کلاش - کارشناسی ارشد

خلاصه مقاله:
باوجود گسترش روزافزون سامانه های فن اوری اطلاعات این تکنولوژی دارای نقاط ضعف بسیاری درخصوص امنیت و محرمانگی است تلاشهای بسیاری جهت ارتقای سطح امنیتی سیستم های it صورت گرفته که حاصل آن افزایش امنیت درزمینه الگوریتم های رمزنگاری تکنیکهای تصدیق اصالت پروتکلهای ارتباطی و... بود هاست ناامن ترین نقطه درسیستم ها الگوریتم ها نیستند بلکه این خود سیستم های محاسباتی اند که باعث افشای اطلاعات میشوند همانطور که دراستانداردهای امنیتی مطرح است برای کلیدرمزباید حفاظت اضافی درنظر گرفته شود میدریت من چرخه حیات کلیدها و محافظت مداوم آنها منجر به ایجادچالشها و مسائلی درمدیریت امنیت میشود تا زمانی که کلیدرمز درداخل سیستم میزبان ذخیره شده و محاسبات رمزنگاری توسط واحدها یمحاسباتی معمول اجرا گردد فردمهاجم می تواند با الوده نمودن سیستم به یک تروجان به اطلاعات ذخیره شده درآن دسترسی یابد این امربسیارساده تروخطرنااک تر ازتحلیل الگوریتم رمزنگاری جهت استخراج کلیدهای رمز میب اشد زمانی که یک مهاجم کلیدرمزنگاری را دراختیارداشته باشد تمام امنیت سیستم ازبین خواهد رفت دراین شرایط یک راه حل مناسب استفاده ازماژول امنیتی است که چیزی نیست جز یک سخت افزاریانرم افزارضدمداخله که تمام اعمال رمزنگاری را اجرا نموده و داده های حساس مانند کلیدهای رمز یادیگراطلاعات محرمانه کاربررادرمحیط امن خود ذخیره و نگهداری می کند هدف ازاین مقاله ارایه یک معماری پیشنهادی جهت طراحی ماژول امنیت سخت افزاری HSM می باشد

کلمات کلیدی:
امنیت اطلاعات، ماژول امنیت سخت افزاری، کلیدرمزنگاری، استاندارد#PKCS۱۱، استاندارد FIPS۱۴۰