عنوان مقاله:
ارائه یک روش جدید برای شناسایی بدافزارها در سطح مجازی ساز در ماشین های مجازی

محل انتشار:
فصلنامه پدافند الکترونیکی و سایبری, دوره 2, شماره 3 (سال: 1393)

تعداد صفحات اصل مقاله: 12

نویسندگان:
سیدمحمدرضا فرشچی - *فردوسی مشهد*

حسین شیرازی - *مالک اشتر*

خلاصه مقاله:
امروزه از ماشین های مجازی برای مدیریت بهینه و اثربخش منابع سیستمی درسطح وسیعی استفاده می شود. مجازی سازی، تکنیک ایجاد چندین ماشین مجازی بر روی یک سخت افزار است که امکان استفاده بهینه از منابع سیستمی و سهولتدرنگهداری را فراهممی نماید. اخیرا، با گسترشبدافزارها در ماشین هایمجازی، صدماتجبران ناپذیری به سیستم های میزبان وارد شده است. یکبدافزار در ماشینمجازی، اشیاءسیستمی را تغییر داده، و در زمان اتمام کار ماشین مجازی به سیستم عامل میزبان نفوذ، و مقاصد خود را انجام می دهد. این مقاله برای اولین بار به ارائه یک روش امن، برای شناسایی، دسته بندی و امحاء بدافزارها در ماشین مجازی پرداخته است. روش پیشنهادی به نام، SSM، در مرحله اول با استفاده از پروفایل رفتاری و بررسی تغییرات، اقدام به شناسایی رفتارهای پرخطر می نماید. SSM، در مرحله بعد با اعمال یک الگوریتم جدید، به طبقه بندی گروه های رفتاری مرحله قبل اقدام می نماید. در مرحله آخر نیز، دسته های سالم شناسایی شده و به ماشین میزبان منتقل می شود. استفاده از جریان های اطلاعاتی فرآیندها در ماشین مجازی، دقت بسیار مطلوبی را برای مکانیزم پیشنهادی فراهم کرده است. با استفاده از روش پیشنهادی، اولا برخلاف روش های کنونی، تنها قسمتی از اطلاعات سیستمی مورد پردازش قرار می گیرد. ثانیا، برخلاف کلیه ضدبدافزارهای موجود، روش پیشنهادی، بجای بررسی تک به تک اشیاء سیستمی، گروه های تشکیل شده توسط طبقه بند را بررسی می کند. بنابراین، سربار بسیار کمی به لایه مجازی ساز اعمال می شود. نهایتا اینکه، با استفاده از مدل رفتاری مضاعف، نرخ نمونه غلط منفی، به شدت کاهش پیدا کرده است. دراین تحقیق نمونه واقعی مکانیزم پیشنهادی بر روی مجازی ساز Xen، در لینوکس پیاده سازی شده است. با انجام بررسی های دقیق، و مقایسه SSM با ضدبدافزارهای تجاری کنونی، عملکرد بسیار مناسب در تشخیص و حذف بدافزارها و همچنین کاهش نرخ نمونه های غلط منفی به خوبی محرز شده است.

کلمات کلیدی:
امنیت مجازی ساز, طبقه بندی بدافزار, امنیت در لینوکس, مدل رفتاری