پایان‌نامه‌ی کارشناسی ارشد: هاشم ایزدخواه، ۱۳۹۷

جلوگیری از حملات در ابر با استفاده از سیستم تشخیص نفوذ (IDS)

امروزه استفاده از اینترنت و برنامه‌های مختلف آن از قبیل شبکه‌های اجتماعی به‌سرعت در بین تمام اقشار مردم گسترش یافته است. همزمان حجم داده‌های ذخیره‌شده در سرورهای ابر در حال افزایش است. همین امر بستر مناسبی را برای هکرها ایجاد می‌کند تا با روش‌های مختلف سعی در نفوذ به سیستم‌های موبایلی و یا پایگاه داده داده‌های حساس مردم نموده و سعی در جاسوسی و یا سوءاستفاده از آن داده‌ها برای اهداف مختلف بنمایند.

سیستم‌های تشخیص نفوذ در سال‌های اخیر با توجه بسیار زیادی از طرف محققان در سرتاسر دنیا مواجه شده است. با استفاده از این سیستم‌ها سعی می‌شود تا بتوان نفوذ گران را در لحظات اولیه و قبل از وارد آوردن صدمه جدی به سیستم شناسایی نموده و از فعالیت آن‌ها جلوگیری نمود. عمده مشکل این سیستم‌های تشخیص نفوذ پیشنهادشده توسط محققان مختلف، دقت کم این سیستم‌ها در تشخیص نفوذ می‌باشد. در این پایان‌نامه سعی کرده‌ایم تا روش جدید ترکیبی پیشنهاد نماییم که از سه روش رده‌بندی (شامل: درخت تصمیم، بردار پشتیبانی و الگوریتم ژنتیک) استفاده شده است. ارزیابی روش پیشنهادی نشان داد که در مقایسه با روش‌های دیگر توسعه‌یافته توسط محققان دیگر دارای دقت بالاتری در شناسایی نفوذها می‌باشد.

کلیدواژه‌ها: سیستم‌های تشخیص نفوذ ، الگوریتم ژنتیک، بردار پشتیبان ، درخت تصمیم .

شماره‌ی پایان‌نامه: ۱۲۷۴۱۰۰۶۹۵۲۰۱۳
تاریخ دفاع: ۱۳۹۷/۱۱/۱۰
رشته‌ی تحصیلی: مهندسی کامپیوتر- نرم‌افزار
دانشکده: فنی و مهندسی
استاد راهنما: مهندس علی‌اکبر نقابی
استاد مشاور: مهندس حسام حسن‌پور

M.A. Thesis:

Prevent attacks in the cloud using intrusion detection systems (IDS)

Nowadays, the use of the Internet and its various programs, such as social networks, has spread rapidly across Different masses of people. At the same time, the amount of data stored on cloud servers is increasing. This provides a good platform for hackers to try to penetrate mobile systems or data storage databases with different methods and try to spy or

misuse these data for various purposes.
Intrusion detection systems in recent years have been faced with great attention from researchers around the world. Using these systems, they try to identify the attackers at early moments of attacks before they cause serious damage to the system and prevent their activity. The major problem with these intrusion detection systems proposed by various researchers is the low accuracy of these systems in detecting infiltrations. In this thesis, we have tried to propose a new hybrid method using three classification methods (including decision tree, vector support machine and genetic algorithm). The evaluation of the proposed method showed that, compared to other methods developed by other researchers, it has a higher accuracy in detecting infiltrations.