بخشی از ترجمه مقاله

عنوان فارسی مقاله :

طرح تشخیص نفوذ ناهنجاری مبتنی بر برنامه با استفاده از ابزارهای تشخیص چندگانه و استنباط فازی

عنوان انگلیسی مقاله :

A program-based anomaly intrusion detection scheme using multiple detection engines and fuzzy inference

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

5. Conclusions and future work

In this paper, we presented a fuzzy-based scheme for the integration of HMM anomaly intrusion detection engine and normal-sequence database detection engine for program anomaly intrusion detection using system calls. Instead of using crisp conditions, or fixed thresholds, fuzzy sets are created to represent the space of sequence parameters. A set of fuzzy rules is created, which combine multiple sequence parameters and determine the sequence status through a fuzzy reasoning process. In order to address the issue of prohibitive computational cost of HMM model training, an incremental HMM training method and an initial optimization scheme have been proposed. Experimental results have shown that the proposed detection scheme reduced false positive alarms by 48% and 28%, compared to the normal-sequence database scheme (Forrest et al., 1996) and the two-layer scheme (Hoang et al., 2003a), respectively. The proposed detection scheme also generated much stronger anomaly signals, compared to the normal-sequence database scheme (Forrest et al., 1996) and the two-layer scheme (Hoang et al., 2003a). The HMM training time was reduced by four times and the memory requirement was also decreased significantly. These improvements have made a good progress towards online and real-time intrusion detection. However, on-going effort is needed before anomaly IDS technology can be deployed for real-life online intrusion detection. In a most recent work, a data pre-processing scheme has been proposed to reduce the load of training (Hu et al., 2009). Our future work is to investigate how to integrate these approaches together and conduct real-life data test.

5- نتایج و فعالیت‌های آتی

در این مقاله، طرح فازی محور را برای ترکیب ابزار تشخیص نفوذ ناهنجاری HMM و ابزار استنتاجی تشخیص پایگاه داده با توالی نرمال برای برنامه تشخیص نفوذ ناهنجاری با استفاده از فرامین سیستمی ارائه کردیم. به جای استفاده از شرایط جدید یا آستانه‌های ثابت، مجموعه‌های فازی برای ارائه فضای پارامترهای متوالی ایجاد شده است. مجموعه ای از قوانین فازی ایجاد شده که در آن پارامترهای توالی چندگانه ترکیب شده و شرایط توالی از طریق فرآیند استنتاجی فازی تعیین شده است. به منظور پرداختن به موضوع هزینه محاسباتی پیشگیرانه آموزش مدل HMM یک روش آموزشی HMM همگرایی و یک طرح بهینه سازی آغازین پیشنهاد شده است. نتایج تجربی نشان داده است که طرح تشخیص پیشنهادی آلارمهای مثبت کاذب را به ترتیب تا 48% و 28 % در مقایسه با طرح پایگاه داده توالی نرمال و طرح دولایه(هوآنگ و همکاران، 2003) کاهش داده است (فورست و همکاران، 1996). طرح تشخیص پیشنهادی نیز سیگنالهای ناهنجاری قوی‌تری را در مقایسه با طرح پایگاه داده توالی نرمال (فورست و همکاران، 1996) و طرح دولایه (هوآنگ و همکاران، 2003) تولید کرده است. زمان آموزش HMM تا چهار برابر کاهش یافته و الزامات حافظه نیز به طور چشمگیری کاهش یافته است. این بهبودها پیشرفت مناسبی در قبال تشخیص نفوذ زمان واقعی و آنلاین ایجاد کرده است. با وجود این، تلاش مداومی پیش از اینکه فن‌آوری IDS ناهنجاری بتواند برای تشخیص نفوذ آنلاین واقعی گسترش دهد مورد نیاز است. در اکثر فعالیت‌های اخیر، یک طرح پیش پردازشی داده برای کاهش بار آموزشی پیشنهاد شده است (هو و همکاران، 2009). فعالیت پژوهشی آتی ما بررسی نحوه ترکیب این رویکردها با یکدیگر و انجام آزمون داده زندگی واقعی است.