بخشی از ترجمه مقاله

عنوان فارسی مقاله :

سیاست تشخیص سو استفاده در شبکه های ارتباطی با مدل های پنهان مارکوف

عنوان انگلیسی مقاله :

Policy Misuse Detection in Communication Networks with Hidden Markov Models

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. Conclusion

Our approach worked in high accuracy for the detection of protocols. Most of the time, training *HMM*s may be problematic since there is not always enough information. Rare data problems may arise and *HMM*s may be trained unbalanced. We tried to train the models equally except login protocol. User behaviour needs to be modelled with more parameters than duration and packet size. Clustering the data in more than two dimensions may cause memorization of the cases for *HMM*. Our approach focuses on network based intrusion detection. Another alternative may be to detect intrusions computer based. Different threads may be used to detect ip based packet flows. This approach needs support by system administrator because users may change ip numbers if shut down happens in a period of time and restart later. System administrator may assign static ip numbers to each computer to pursue this case. Our approach is only restricted to protocol detection via information level data. Multistage attack patterns can also be detected with *HMM*s and multiple training methods can be developed for paralelizing *HMM* training procedure.

5. استنتاج

روش ما با دقت بالا برای تشخیص پروتکل ها کار می کند. اکثر اوقات، آموزش HMM ها ممکن است مشکل ساز باشد، از آنجاییکه همواره اطلاعات کافی وجود ندارد. ممکن است مسائل نادر داده ها بوجود آید و ممکن است HMM ها بصورت نامتعادل آموزش داده شوند. سعی می کنیم مدل‌ها بجز پروتکل ورود به سیستم را بطور برابر آموزش دهیم. لازم است رفتار کاربر با پارامترهای بیشتری از اندازه بسته و مدت زمان مدلسازی شود. دسته بندی داده ها در بیش از دو بعد ممکن است باعث حفظ حالت ها برای HMM شود. رویکرد ما بر تشخیص نفوذ مبتنی بر شبکه تمرکز می کند. پیشنهاد متناوب دیگر ممکن است تشخیص نفوذهای مبتنی بر کامپیوتر باشد. ممکن است از برنامه های مختلف برای تشخیص جریان های بسته مبتنی بر Ip استفاده شود. مدیر سیستم از این روش حمایت می کند زیرا ممکن است کاربران شماره های Ip را تغییر دهند اگر خاموش کردن سیستم در دوره ای از زمان صورت گیرد و بعدا مجددا راه اندازی شود. ممکن است مدیر سیستم برای اتخاذ این مورد شماره های استاتیک Ip را به هر کامپیوتر اختصاص دهد. روش ما تنها به تشخیص پروتکل از طریق داده های سطح اطلاعات محدود شده است. الگوهای حمله چندمرحله ای را نیز می توان با HMM تشخیص داد و روشهای آموزشی متعدد را می توان برای تشبیه کردن روند آموزشی HMM بسط داد.