تحسين تحليل تنبيهات كشف الاختراق في الزمن الحقيقي للتعرف على الهجمات الالكترونية متعددة المراحل

فاطمة أحمد باحارث

د. أميمة عمر بامسق

المستخلص

انتشار ظاهرة الهجمات الالكترونية على شبكات وأنظمة الحاسوب جعل أنظمة كشف الاختراق تتبوأ الصدارة في التدابير الوقائية لمراقبة أمن الشبكات والأنظمة الحاسوبية. تولد أنظمة كشف الاختراق كمية هائلة من التنبيهات مما جعل عملية تحليلها وإدارتها يشكل صعوبة على مسؤول الشبكة، كما ومن جهة أخرى لا تستطيع أنظمة كشف الاختراق اكتشاف الهجمات متعددة المراحل. كان ذلك سببًا في أن أصبحت عملية تحليل وإدارة هذه الكميات الهائلة من التنبيهات قضية حرجة وصعبة. تعتبر عملية الربط بين هذه التنبيهات نهجًا مفيدًا للحد من حجم التنبيهات واكتشاف سيناريوهات الهجوم متعدد المراحل. في هذه الأطروحة، تم اقتراح نظام التعرف على الهجوم متعدد المراحل في الوقت الحقيقي (RMARS) للكشف عن سيناريوهات هجوم متعدد المراحل مع مستوى خطورتها. يتألف هذا النظام من جزئين: جزء لا يعمل في الوقت الحقيقي وهو الذي يتم فيه بناء أنماط وسيناريوهات الهجوم متعدد المراحل باستخدام خوارزمية للتنقيب عن المتسلسلات والأنماط المتكررة. والجزء الآخر يتلقى التنبيهات في الزمن الحقيقي ويقوم بدوره باكتشاف الأنماط متعددة المراحل وكذلك التنبؤ بالهجمات المقبلة باستخدام الأنماط التي تم بناؤها مسبقًا. هدفنا هو تحسين الكشف والتنبؤ عن طريق تحديد مستوى خطورة سيناريوهات الهجوم متعدد المراحل في الوقت الحقيقي، وذلك بإجراء تحسين في عملية اختيار سلاسل المرشح "Candidate Sequences" التي تُعد مدخلات خوارزمية التنقيب عن الأنماط المتكررة. يتم التحسين باستخدام طريقة "التحقق المرشح Candidate Verification" التي تقوم بحساب مدى الترابط بين التنبيهات عند تكوين المرشح للتأكد من أن جميع التنبيهات في المرشح المختار تنتمي إلى سيناريو الهجوم نفسه. وقد تم تنفيذ النظام المقترح وتقييم مدى فاعليته من خلال سلسلة من التجارب باستخدام البيانات DARPA 2000. وتبين من النتائج أن سيناريوهات الهجوم متعدد المراحل التي تم بناؤها من سلاسل الترشيح أكثر دقة وفاعلية عند استخدام "التحقق المرشح Candidate Verification". وعلاوة على ذلك، توقع الخطوة التالية من الهجوم مع مستوى الخطورة أى إلى زيادة كفاءة نظام تحليل التنبيهات وإعطاء مدير الشبكة معلومات أكثر قيمة لاتخاذ القرار ووقف هجوم متعدد المراحل قبل استمرار مراحله التي قد تسبب ضرر وإتلاف في الشبكة والبيانات.

Improving Real Time Intrusion Detection Alerts Analysis for Recognizing Multi-Stage Attacks

Fatmah Ahmed Bahareth

Dr. Omaima Bamasak

Abstract

With the rise of cyber-attacks, the amount of audited security data such as alerts produced from Intrusion Detection Systems (IDSs) are increased dramatically. IDSs have become one of the most common countermeasures for monitoring safety in computer systems and networks. IDSs generate a massive amount of low-level alerts, in which the information on multi-stage attack scenario is missing. The analysis and management of these massive amounts of alerts have become a critical and challenging issue. Alert correlation is a very useful approach to reduce the volume of alerts and discover multi-stage attack scenarios.

In this thesis, a Real-time Multi-stage Attack Recognition System (RMARS) is proposed to recognize multi-stage attack scenarios with their associated severity level in real time. It consists of two parts: offline part which builds attack patterns using the sequential pattern mining algorithm GSP, and online part which receives alerts and predicts upcoming attacks using patterns built in offline part.

RMARS presents improvement in the detection and prediction by identifying severity level of discovered multi-stage attack scenarios in real time. In addition, it uses a new method "Candidate Verification" in offline part that calculates alerts correlativity while generating candidate attack sequences to insure that all alerts in selected candidate belong to the same attack scenario.

The proposed system has been implemented and evaluated against the specified requirements by a series of experiments using DARPA 2000 data sets. The results show that using "Candidate Verification" method increases the efficiency of generating attack scenario patterns in offline and detecting multi-stage attack in real-time. Moreover, predicting the next step of attack with severity level increases the efficiency of alert analysis system and gives network administrator valuable information to take a decision and deter a serious multi-stage attack to be completed and, hence, protecting the system from getting damaged.