نظام كشف التسلل الهجين على الشبكات اللاسلكية IEEE 802.11

إسحاق سيد إكرام سيد عبدالله

بحث مقدم لنيل درجة الماجستير في العلوم

(تقنية المعلومات / أمن الشبكات)

تحت إشراف

أ. د. محمد اشرف اسماعيل مدكور

كلية الحاسبات وتقنية المعلومات
جامعة الملك عبد العزيز
جدة – المملكة العربية السعودية
شعبان ١٤٣٨هـ – مايو 2017 م

نظام كشف التسلل الهجين على الشبكات اللاسلكية IEEE 802.11

إسحاق سيد إكرام سيد عبدالله

المستخلص

بروتوكول IEEE 802.11i هو معيار الأمان الحالي للشبكات المحلية اللاسلكية. ويقدم هذا البروتوكول آليات أمنية قوية مثل معيار التشفير المتقدم AES للقيام بالتشفير وبروتوكولات المصافحة رباعية الاتجاه للمصادقة، إلا أنه لا يزال عرضة لعدد من الهجمات الخطيرة مثل فيضان الغاء المصادقة والانفصال. تم اقتراح العديد من تقنيات كشف التسلل من قبل المجتمع البحثي للكشف عن هجمات الشبكات المحلية اللاسلكية المعروفة والغير معروفة. ومع ذلك، هناك حاجة لبذل مزيد من الجهود لتحسين أداء الكشف باستخدام مجموعة بيانات قياسية لبروتوكول ٨٠٢,١١ والتي تحتوي على كل من بيانات حركة انتقال البيانات العادية وحركة انتقال البيانات المتسللة لجميع الهجمات المعروفة. يبدأ البحث الحالي من خلال التعرف على جميع الهجمات الخطيرة ومواطن الضعف في شبكات IEEE 802.11i. بعد ذلك نقدم مسح شامل لأنظمة كشف التسلل المقترحة في الأدبيات لمعرفة مزاياها وقيودها. ويلي ذلك تصميم وتنفيذ نموذج أولي لنظام كشف تسلل هجين يعمل في الزمن الحقيقي ويستخدم أساليب الكشف عن البصمة والكشف عن السلوك المستغرب. استخدام أسلوب الكشف عن البصمة يمكن أن يحسّن أداء نظام الكشف عن التسلل الذي طورناه من خلال زيادة المعدل الإيجابي الحقيقي في حين يمكن لأسلوب الكشف عن السلوك المستغرب إيجاد الهجمات الغير معروفة. بالإضافة إلى قواعد بصمة الهجمات، أخذنا بعين الاعتبار كلا من خوارزمية التصنيف C4.5 وخوارزمية معدل التقدير أحادي الاعتماد (AODE) للكشف عن السلوك المستغرب. تم تقييم النظام المطّور من حيث دقة اكتشاف الهجمات (Precision) وشموليتها (Recall)، مقدمين بذلك ثلاث مساهمات. أولا تم تطوير خوارزمية جديدة لاختيار خواص فعالة بالاعتماد على نموذج التصفية ومعرفة الآثار التي تتركها هجمات الشبكات اللاسلكية. وثانيا، فإن الخوارزمية المطورة تحسن دقة التصنيف والاكتشاف، مقارنة مع النتائج المنشورة مؤخراً، وتقلل بشكل كبير من وقت التصنيف عن طريق تقليل وقت التدريب وعدد الخواص. ثالثاً، فإن البحث يقدم نظام كشف تسلل هجين عالي الأداء للشبكات اللاسلكية يعمل في الزمن الحقيقي. تم تنفيذ النموذج الأولي واختباره على حاسب شخصي ١,٧ جيجاهرتز i5 مع ١٢ جيجابايت من ذاكرة الوصول العشوائي. وأظهرت النتائج التجريبية أن النظام المنفذ لديه وقت تعلم سريع قدره ٤٥ ثانية وأداء تصنيف عالي بدقة ٩٩,٦٪، وشمولية ٩٨,١١٪، ودقة شاملة قدرها ٩٩,٨٢٪.

A Hybrid Intrusion Detection Systems Approach for IEEE 802.11 Wireless Networks

Ishaque Sayedikram Sayedabdullah

A thesis submitted for the requirements of the degree of Master of Science in Information Technology / Networks Security

Supervised By
Prof. Dr. Mohamed Ashraf Ismail Madkour

Faculty of Computing and Information Technology
KING ABDULAZIZ UNIVERSITY
JEDDAH-SAUDI ARABIA
Shaaban 1438 H – May 2017 G

A Hybrid Intrusion Detection Systems Approach for IEEE 802.11 Wireless Networks

Ishaque Sayedikram Sayedabdullah

ABSTRACT

The IEEE 802.11i protocol is the current security standard for WLANs. While it has strong security mechanisms such as Advanced Encryption Standard for encrypting and the four-way handshake protocol for authentication, it is still vulnerable to a number of serious attacks such as deauthentication and disassociation flooding. Various intrusion detection techniques are proposed by the research community to detect known and zero-day WLAN attacks. Nevertheless, further efforts are needed to improve the detection performance using a benchmark 802.11 dataset that contains both normal traffic and intrusive traffic of all known attacks. The present research starts by investigating all serious attacks and vulnerabilities in IEEE 802.11i networks. Next we provide a comprehensive survey of the proposed intrusion detection systems in the literature to find out their merits and limitations. This is followed by designing and implementing a prototype for a hybrid real-time network based WLAN intrusion detection system that employs signature and anomaly detection methods. Using signature detection can improve the performance of the developed intrusion detection system by increasing the true positive rate while anomaly detection can detect zero-day attacks. In addition to the signature rules, we considered both C4.5 classifier and Averaged One-Dependence Estimator (AODE) for anomaly detection. The developed system is evaluated in terms of precision and recall, providing three contributions. Firstly a novel technique is developed for effective feature selection based on filtering model and knowledge of WLAN attack footprints. Secondly, it improves classification accuracy, compared with recently published results, and dramatically increases the classification speed by minimizing the training time and the classification attributes. Thirdly, it offers a high performance real time hybrid WLAN intrusion detection system. The prototype is implemented and tested on 1.7 GHz i5 PC with 12 GB RAM. The experimental results show that the implemented system has a fast learning time of 45 seconds and a high classification performance of 99.6% precision, 98.11% recall, and an overall accuracy of 99.82%.