أسلوب إدارة أمنية الشبكات المبني على طريقة تمثيل المفاهيم باستخدام الوكيل المتنقل

عبد الله مارش محمد علي

إشراف
أ.د. محمد أشرف مدكور
د. عمر عبد الله باطرفي

المستخلص

شبكات الحاسب الآلي ، والإنترنت على وجه الخصوص ، أمر لا غنى عنه في الحياة اليومية في كافة النواحي تقريبا ، وتشمل ذلك العملية التعليمية والتجارية والحكومية والاجتماعية ، وغيرها. ولذا فإن أمنية الشبكات لها أهمية كبيرة جدا في حماية البيانات المهمة والوصول الموثوق إليها حينما وحيثما تطلب. الطرق اليدوية لإدارة أمنية الشبكة تتطلب اهتماما متواصلا من مدير الشبكة ، وتكون غير قابلة للتطبيق وعرضة للخطأ كلما زاد حجم الشبكة. وبالتالي ، فإن الشبكات الكبيرة والمتوسطة سيكون استخدام إدارة أمنية الشبكات NSM Network Security Management الآلي أمرلا مفر منه ، والذي ينبغي أن يكون مرن ومستقل عن مدير الشبكة وعن تدخل أناس آخرين.

يوجَه هذا البحث لدراسة إمكانية تطوير نظام أتوماتيكي في ادارة أمنية الشبكات بطريقة تحقق كلا ممن المرونة في تحديد أهداف النظام ، والكفاءة في استخدام النطاق الترددي bandwidth المتاح للشبكة مع أعباء نقل منخفضة نسبيا. هناك عدة تقنيات من الممكن استخدامها في تطوير هذا النظام ، ولكن عند الأخذ في الاعتبار المرونة والكفاءة فإنه يتم الحصول عليهما بشكل مفيد باستخدام (أ) الوكيل المتنقل (MA Mobile Agent لجمع المعلومات الأمنية المطلوبة من أجهزة الشبكة المختلفة . (ب) علم علاقات المفاهيم Ontology التي تستخدم في تمثيل السياسات الأمنية Security policies المطلوبة في طريقة تكون مفهومة من قبل الوكيل المتنقل.

في هذا العمل نحاول إثبات جدوى نظام إدارة أمنية الشبكات بالإعتماد على الوكيل المتنقل وعلم علاقات المفاهيم من خلال تطوير نموذج أولي prototype بسيط ، وتنفيذه واختباره عمليا في شبكة محلية.

تم تصميم وتنفيذ النموذج الأولي لمراقبة إعدادات مكونات الشبكة عن طريق إنشاء منصة platform مناسبة تسمح للوكيل المتنقل بالانتقال في هذه الشبكة وجمع المعلومات

اللازمة باستخدام السياسات الأمنية الممثلة باستخدام علم علاقات المفاهيم . وتم تصميم هذا النظام ليقوم بتنفيذ مهمتين رئيسيتين :

1. جمع المعلومات من مكونات الشبكة مثل أجهزة التوجيه Routers ،خادمات الشبكة Servers ، والعملاء Host، وغيرها. وكمثال على هذه المعلومات ، الوكيل المتنقل يقوم بجمع معلومات برامج مكافحة الفيروسات ، ومعلومات عن سياسات كلمة المرور لنظام التشغيل ويندوز. بعد جمع المعلومات المطلوبة من أجهزة الشبكة المحددة ، يعود الوكيل المتنقل بهذه المعلومات لمدير الشبكة ويترك له اتخاذ القرار و تطبيق الإجراءات المناسبة.

2. . اتخاذ القرارالمناسب من الممكن أيضا أن يقو به الوكيل المتنقل عند ما يجد أن المعلومات التي تم جمعها من جهاز المستخدم لا تتطابق مع السياسة الأمنية المحددة. في هذه الحالة فإنه يقوم بإظهار رسالة على شاشة المستخدم يطلب منه إعادة عمل الإعدادت لجهاز الكمبيوتر الخاص به وفقا للسياسة الأمنية المطلوبة. بعد ذلك يقوم الوكيل المتنقل ، بحفظ هذه القرارات وإرجاعها في نهاية المطاف إلى مدير الشبكة.

تم تنفيذ النموذج الأولي باستخدام البرامج التالية :

- لغة جافا التي استخدمت لتصميم واجهات المستخدم ، وغيرها من التعليمات التي استخدمت مثلا في استرجاع سياسات كلمة المرور لنظام ويندوز.
- المكتبة Aglet والتي استخدمت في انشاء الوكلاء والتي تمثل المنصة التي تسمح للوكيل المتنقل للإنتقال في الشبكة وتنفيذ المهام المطلوبة.
- المكتبة Jena والتي تستخدم لاسترجاع السياسات الأمنية الممثلة بعلم علاقات المفاهيم.
- مكتبة JNIRegistry والتي تستخدم للوصول إلى سجل Registry الويندوز .

شملت عملية التطوير ثلاث مراحل رئيسية.**المرحلة الأولى** ، تحديد السياسات المطلوبة لمعلومات محددة لبعض مكونات الشبكة ، مثل برنامج مكافحة الفيروسات وكلمة المرور للويندوز. تم استخدام علم علاقات المفاهيم لتمثيل هذه السياسات. **المرحلة الثانية** هي تحديد منصة مناسبة ، تقوم بالسماح وخدمة الوكيل المتنقل ليقووم بالمهام المطلوبة و ذلك باستخدام Aglet . **المرحلة الأخيرة** هي كتابة الكود الفعلي للوكيل المتنقل ليقوم بجمع المعلومات والعودة بها إلى مدير الشبكة.

تم اختبار هذا النموذج الأولي لدراسة وظائفه باستخدام شبكة صغيرة تتكون من ثلاثة أجهزة من الكمبيوترات بإعدادت مختلفة. الكمبيوتر الأول تم عمل إعداداته بشكل صحيح ومطابقة للسياسات الأمنية المطلوبة ، وتم عمل إعدادت الكمبيوتر الأخربحيث تطابق بعض السياسات الأمنية المطلوبة فقط ، والكمبيوتر الثالث تم عمل إعداداته بحيث لا تتطابق أي واحدة من السياسات الأمنية. الوكيل المتنقل كان قادرا على فهم السياسات الأمنية الممثلة باستخدام علم علاقات المفاهيم والتحرك في جميع أنحاء الشبكة. واكتشف الوكيل المتنقل الأجهزة التي اعدادتها غير صحيحة. و على الرغم من إجراء الاختبار العملي باستخدام شبكة صغيرة، إلا أنه قابل للتوسع ويمكن تطبيقه مباشرة على أكثر من جهازكمبيوتر في شبكة محلية أو حتى في شبكة واسعة.

ONTOLOGY-BASED NEWTORK SECURITY MANAGEMENT USING MOBILE AGENT

By
Abdullah Marich Mohammad Ali

Supervised By
Prof. Dr. Mohammed Ashraf Madkour
Dr. Omar Abdullah Batarfi

ABSTRACT

Computer networks, and in particular the Internet, is indispensible in the everyday life of almost all aspects including commercial, educational, governmental, social, etc. Network security is therefore of extreme importance to protect the valuable data and to provide reliable access to it whenever and wherever requested. Manual techniques for managing network security require continuous attention of the network administrator, and it tends to be infeasible and error prone as the network size increases. Consequently, for moderate and large network sizes it would be inevitable to consider the use of an automatic network security management (NSM) system that should be flexible and independent of the network administrator and other human intervention.

This research is directed to investigate the possibility of developing an automatic NSM system in such a way that provides both flexibility in deciding the system's objectives and efficiency in using the valuable network bandwidth with a relatively low transmission overhead. Several techniques are possible to develop a NSM system, but it is considered that the required flexibility and efficiency could be advantageously obtained using (a) mobile agents (MA) to collect the required security information from various network devices, and (b) ontology to specify the required security policies in such a way understandable by the MA's software.

The present work attempts to prove the feasibility of a NSM system based on mobile agents and ontology by developing a simplified NSM prototype, and implementing and testing it practically in a typical local area network.

The prototype is designed and implemented to monitor the configuration of the network components by establishing a suitable platform that allows the mobile agent to travel through the network and collect the necessary information using an ontology-based security policy. The developed system is designed to perform two main tasks:

1. Collecting information from network components such as routers, servers, hosts, and etc. As an example of such information the developed MA is concerned with the antivirus program information, and windows password policies. After collecting the required information from the specified network devices, the MA returns back to the network administrator and let him decide and perform the suitable actions.
2. An alternative behavior is also possible when examining user hosts by allowing the mobile agent itself to take the appropriate decision if it realizes that the collected information does not match the specified security policy. In this case it shows a message on the host's monitor requesting the user to reconfigure his host computer according to the required security policy. Next, the MA stores and eventually returns these decisions to the network administrator.

The developed prototype is implemented using the following software:

- The Java libraries that is used to develop the user interface windows , and other Java statements to retrieve the windows password policies.
- The Aglet library that creates the agents and provides the necessary platform for agents traveling through the network.
- The Jena that is used to retrieve the policies represented by ontology.
- The JNIRegistry library which is used to access the windows registry

The development process included three major phases. The first phase is concerned with the specification of the required policies for the selected information, namely the antivirus program and the windows password. Ontology is written to represent these policies. The second phase is the establishment of the proper platform, using Aglet, to allow for the MA travels. The last phase is the actual coding of the MA logic to collect the information and return back to the administrator.

This prototype is tested to examine its functionality using a minimum network consisting of three computers with different configurations. One computer is properly configured to match the required security policies, the other is configured to match some required security policies and the last one does not match any one of the considered security policies. The developed MA was able to understand the ontology and move around the network. It has properly detected the components that are wrongly configured. It should be made clear that although the practical test was carried out using a minimal network, yet the design is scalable and can be directly applied to more computers in a local area network or even in a wide area network.