الخلاصة

نظراً للتطور الكبير الذي حصل في مجال تكنولوجيا تبادل المعلومات وكثرة عدد المستخدمين لشبكات الحاسبات الذي يزداد يومياً، فقد اصبح التعامل مع هذه المعلومات يتم بأساليب متطورة تتطلب استخدام مختلف التقنيات للحفاظ عليها والتقليل من إمكانية التطفل عليها. ومن تلك التقنيات استخدام اسلوب تحديد الوصول لمصادر المعلومات كوسيلة للحفاظ عليها.

في هذا البحث تم تصميم وتنفيذ منظومة حماية مرنة لتحديد الوصول الى ملفات الحاسبة بالاعتماد على لغة الجافة و التي يمكن استخدامها ضمن تطبيقات لغة جافة المختلفة. وذلك بالاعتماد على تطبيع خصائص المدير الأمني الى Java 2 بما يلائم الخوارزمية المقترحة. و لتحقيق هذا الهدف تم دراسة وتحليل الاحترازات الأمنية التي توفرها معمارية اللغة. حيث تتوفر في لغة جافا وبيئة عملها العديد من وسائل الحماية التي تستعمل لتحقيق متطلبات امنية التطبيقات. ومن أهم مميزات هذه اللغة المرونة والمتانة بالإضافة إلى الأمنية.

برنامج النموذج الأمني في هذا العمل يَتضمَنُ على صنفين رئيسيين : برنامج المدير الأمني للسيطرة على عملية ترخيص الوصول إلى ملفات الحاسبة ، والذي تم اشتقاقه من صنف (Java.security).اما البرنامج الثاني صمّم لتعريف قاعدةِ معلومات المدير الأمني والتي تتألف من ثلاث قوائم تعَرّفَ أسماء المسارات (Paths) والملفات لتحديد ترخيص قراءة ، كتابة و حَذف ملفات الحاسبة. أيضاً تم تَزويد البرنامج بكلمات سر مختلفة إلى كل فعالياتِ وضع وتَحْديثُ أسماء الملفات الموجودة في قاعدةِ أولويةِ الوصل بحيث لا يسمح التحديث للأشخاص الغير مخوّلين بذلك.

PDF created with pdfFactory trial version www.pdffactory.com

ABSTRACT

The Java programming language and its runtime environment provides several valuable aspects to use it for the realization of security demanding applications. The language enforces robust and reliable programs, adding to security.

In this thesis an information accessing protection software is developed in the Java environment, by creating a file access control security manager class. This is based on the security architecture of the Java 2 platform. To achieve this goal, The security mechanisms of the Java 2 platform are analyzed. Based on this analysis a flexible, reusable and easy-to-use file access security manager model developed to be reused with any Java application.

In Java, access rights for resources are modeled using the security manager class hierarchy. The root of the class hierarchy is the abstract class java.security. The security model in this work consists of two main classes: file access control security manager class. It is a subclass of the Java abstract class java.security, and will perform the file access permission checks. The second class designed to maintain three lists that define what paths and files are accessible for the security manger. The first list controls read access, the second controls write access, and the third controls delete access.

To test this security model, a simple "*test.java*" application program is built, which installs an instance of the FAC security manager. Besides the security restriction, further protection is provided to the application by assigning a different password to each file setting action taking place within the computer stored files. This password is given on a priority basis so that no further file accessing for unauthorized persons can occur.

PDF created with pdfFactory trial version www.pdffactory.com