JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Working Sets for the Principle of Least Privilege in Role Based Access Control (RBAC) and Desktop Operating Systems

DISSERTATION

zur Erlangung des akademischen Grades

Doktor

im Doktoratsstudium der

Technischen Wissenschaften

Eingereicht von:
Dipl.-Ing. Christian P. Praher

Angefertigt am:
Institut für Informationsverarbeitung und Mikroprozessortechnik (FIM)

Beurteilung:
em. o. Univ.-Prof. Dr. Jörg R. Mühlbacher (Betreuung)
a. Univ.-Prof. Dr. Josef Küng

Linz, März, 2013

Abstract

The central topic of this thesis is the the access control principle of least privilege, which states that every user and every program should run with the least privileges necessary required to complete an intended task. Adherence of users and programs to this principle can protect a system from serious damage in case of attacks. However, as will be shown, it is in practice very hard to follow this principle. The focus of consideration of the mentioned least privilege security principle in this thesis lies on Role Based Access Control (RBAC) and operating systems.

At first, the two access control models Role Based Access Control (RBAC) and Domain and Type Enforcement (DTE), which were fundamental for the development of the models presented in this thesis, are described. This is followed by a description and critical discussion of selected security extensions for the Linux and Windows operating systems. The presented security frameworks are evaluated and analyzed according to their least privilege properties.

After that the two models Dynamic Sessions in Role Based Access Control (DSRBAC) and Working Set Model for General Purpose Operating System Least Privilege Access Control (WSACOS), which were developed as part of this thesis, are described and presented in detail. Although the two models are different due to their different fields of application, they share the concept of working sets for approximating least privilege access control. In short, this approach tries to limit the directly available permissions to those that have been needed in the recent past. An important assumption of this approach is that users exhibit a locality of application and thus resource usage, which allows to remove unnecessary permissions from the session of a user. In addition, it incorporates a fault handling mechanism for allowing the user to access permissions that are not contained in the automatically created working set.

DSRBAC is a direct extension of the RBAC ANSI standard model. It adds activity information to roles to be able to expire those roles that are not needed in a running session. It is shown that the extensions of the RBAC

core features by DSRBAC are designed such, that they do not have any negative side effects on the optional RBAC components of hierarchies and separation of duties.

The DSRBAC model was implemented prototypical inside the Linux Kernel as Linux Security Module (LSM) based on Linux capabilities. An overview of this prototype together with a performance analysis of it is also presented.

Finally, the WSACOS model is introduced which is not an extension of RBAC but targeted at stand-alone un-administrated single user machines. It introduces the concept of "application roles", which are automatically learned least privilege policies for applications. The resources captured by these application roles are parent-/child process relation, file system access, network communication and loaded modules. Additionally, WSACOS extends the concept of working set based access control introduced in DSRBAC.

The performance and behavior of WSACOS in respect of real world data was evaluated on basis of an empirical analysis. The results of this study together with its interpretation is also presented in this thesis.

Kurzfassung

Das zentrale Thema dieser Dissertation ist das wichtige Zugriffskontroll-Prinzip des Principle of Least Privilege, das verlangt, dass jede/r Benutzer/in eines Systems, sowie jedes Programm mit nur jenen Berechtigungen läuft, die notwendig sind um eine geplante Aufgabe zu erledigen. Eine Einhaltung dieses Prinzips durch Benutzer und Programme kann schlimmere Folgen beim Angriff auf ein System verhindern. Wie gezeigt wird, ist dieses Prinzip aber in der Praxis schwierig umzusetzen. Der Fokus der Betrachtung des Principle of Least Privilege im Rahmen dieser Dissertation liegt auf Role Based Access Control (RBAC) und Betriebssystemen.

Zunächst werden die beiden Zugriffskontrollsysteme Role Based Access Control (RBAC) und Domain and Type Enforcement (DTE) präsentiert, die für die im Zuge dieser Dissertation entwickelten Modelle von zentraler Bedeutung sind. Danach folgt eine Beschreibung und kritische Betrachtung von ausgewählten Sicherheitserweiterungen für das Linux und Windows Betriebssystem. Weiters erfolgt eine Bewertung der "Least Privilege Eigenschaften" der vorgestellten Frameworks.

Danach werden die beiden Modelle Dynamic Sessions in Role Based Access Control (DSRBAC) and Working Set Model for General Purpose Operating System Least Privilege Access Control (WSACOS), die im Rahmen dieser Arbeit entwickelt wurden, ausführlich beschrieben und vorgestellt. Obwohl die Anwendungsszenarien dieser beiden Modelle unterschiedlich sind, teilen sie doch das gemeinsame Konzept des Working Sets zur Approximation einer Least Privilege Zugriffskontrolle. Kurz gesagt versucht dieser Ansatz automatisch die aktuellen Berechtigungen eines/r Benutzers/in auf jene zu beschränken, die auch in der Vergangenheit benötigt wurden. Eine wichtige diesem Ansatz zu Grunde liegende Annahme ist, dass Benutzer eine Lokalität an Programm und somit Ressourcen-Nutzung aufweisen, was ermöglicht, aktuell nicht benötigte Berechtigungen aus der aktiven Benutzersitzung zu entfernen. Zusätzlich baut dieses Modell auf so genannte Fault Handling Mechanismen, die es einem/r Benutzer/in erlauben, Berechtigungen die aktuell nicht im automatisch generierten Working Set sind wieder zu aktivieren.

DSRBAC ist eine direkte Erweiterung des RBAC ANSI standard Modells. Es fügt den Rollen Aktivitätsinformationen hinzu, die es erlauben, nicht benötigte Rollen in einer laufenden Sitzung automatisch zu deaktivieren. Es wird gezeigt, dass die nötigen Erweiterungen des RBAC Core Standards keinerlei negativen Effekte auf die optionalen ANSI RBAC Komponenten Hierarchies und Separation of Duties haben.

Ein Prototyp des DSRBAC Modell als Erweiterung des Linux Kernels wurde mit Hilfe von Linux Security Modules (LSM) und Linux capabilities implementiert. Dieser Prototyp wird ebenfalls ausführlich in der Arbeit beschrieben und sein Laufzeitaufwand anhand einer Performance Analyse bewertet.

Schließlich wird das WSACOS Modell vorgestellt, das nicht auf RBAC basiert, sondern speziell für "stand-alone" Computer-Systeme ohne administrative Betreuung entwickelt wurde. Dieses Modell führt das Konzept der "Application Roles" ein, die automatisch erstellte Least Privilege Security Policies für Programme darstellen. Bei der Bildung dieser Policies werden die Ressourcen Vater-/Kind Prozessbeziehung, Datei System Zugriff, Netzwerkkommunikation sowie die geladenen Module berücksichtigt. Zusätzlich erweitert WSACOS auch das Konzept der Working Set, das bereits im DSRBAC Modell eingeführt wurde.

Das Verhalten des WSACOS Modells auf der Basis von echten Benutzerdaten wurde anhand von einer empirischen Studie analysiert. Die Ergebnisse dieser Studie sowie deren Interpretation werden zum Abschluss ebenfalls in dieser Dissertation präsentiert.