Institut für Systemsoftware

O.Univ.-Prof. Dr. Hanspeter Mössenböck

JOHANNES KEPLER
UNIVERSITÄT LINZ
Netzwerk für Forschung, Lehre und Praxis

Sicherheit in Webanwendungen

Diplomaufgabe für Hubert Grininger
Matr.Nr.: 9956174

Theoretische Betrachtungen und praktische praktischer Einsatz von Sicherheitstechnologien für das Web unter besonderer Betrachtung feingranularer Berechtigungen.

Ziel

Das Ziel der Diplomarbeit soll sein, eine Übersicht über das Thema Sicherheit im Kontext von Web-Anwendungen zu geben. Der Blick wird dabei aber nicht auf low-level Sicherheit, wie Firewalls, Hardwarenahe Sicherheitstechnologien o. Ä. gerichtet. Stattdessen sollen die Aspekte und Technologien vorgestellt und wenn möglich auch bewertet werden, die für den Auftraggeber und den Entwickler von Web-Anwendungen interessant sind.

Aufbau

Im ersten Teil sollen die theoretischen Grundlagen erläutert werden (Klärung wichtiger Begriffe wie z.B.: „Webanwendung“, „Computersicherheit“). Ein Schwerpunkt soll auf Authentisierung und Autorisierung liegen, die wichtigsten Methoden zur Benutzerauthentisierung sollen vorgestellt werden.

Der zweite Teil soll sich mit Berechtigungsmodellen beschäftigen, somit liegt hier der Schwerpunkt auf der Frage der Autorisierung. Die wichtigsten Berechtigungsmodelle sollen beschrieben werden, wie z.B.: MAC (Mandatory Access Control), DAC (Discretionary Access Control) und besonders RBAC (Role-based Access Control).

Im dritten Teil soll auf die sicherheitsrelevanten Aspekte von konkreten Web-Anwendungs-Frameworks (J2EE, CORBA, .NET, …) eingegangen werden. Bei CORBA soll im Speziellen die Idee des RAD-Dienstes (Ressource Access Decision Service) näher betrachtet werden. Die Fragen, die hier beantwortet werden sollen, sind z.B.: „wie unterstützt das Framework die Vergabe von Berechtigungen?“, „wie flexibel sind die Lösungen?“. Es soll auch kritisch hinterfragt werden, ob die Möglichkeit dieser Frameworks für die Entwicklung von Web-Anwendungen wirklich eingesetzt werden können.

Im vierten und letzten Teil sollen die Probleme aufgezeigt werden, die ein ideales Sicherheits-Framework abdecken muss. Konkret soll u. A. beschrieben werden, welche Granularitätsstufen in Systemen vorhanden sein können/müssen (Klassen, Objekte, Methoden ...) und wie Berechtigungsmodelle darauf eingehen können/sollten. Weiters soll dargestellt werden, welche Abläufe abzuarbeiten sind, wenn Berechtigungs-Überprüfungen durchgeführt werden (z.B.: Unterschied bei Create/Read/Update/Delete-Methoden). Abschliessend soll ein Lösungsansatz präsentiert werden, der die Vergabe von Berechtigungen auf sehr fein-granularer Ebene erlaubt und für J2EE-Anwendungen eingesetzt werden kann.

Der Fortgang der Arbeit ist in 14-tägigem Abstand mit dem Betreuer zu besprechen. Für die Ausarbeitung der schriftlichen Diplomarbeit sind die Richtlinien der Abteilung Systemsoftware zu beachten.

Nähere Auskünfte: Dipl.-Ing. Markus Löberbauer
Ausgabe: August 2004