INFORMATION SECURITY WITH SPECIAL REFERENCE TO DATABASE INTERCONNECTIVITY

by

MARIJKE COETZEE

DISSERTATION

submitted in compliance with the requirements for the degree

MAGISTER SCIENTIAE

in the subject of

COMPUTER SCIENCE

in the

FACULTY OF SCIENCE

at the

RAND AFRIKAANS UNIVERSITY

Supervisor:

PROF. J.H.P. ELOFF

NOVEMBER 2001

Vir Johan

ERKENNINGS

In erkenning aan my Skepper, vir die genade waaruit ek leef, wat ek elke dag ervaar.

Met dank aan prof. Jan Eloff vir sy leiding, waardevolle insette en tyd, wat hierdie studie laat vorm aanneem het.

Dankie aan my ouers, vir die liefde, motivering en ondersteuning wat hulle altyd aan my gee.

Laastens, dankie aan my kinders, Jeanne en Marnus vir hulle geduld met ‘n soms ongeduldige ma.

TITEL:	Information security with special reference to database interconnectivity
OUTEUR:	M. Coetzee
PROMOTOR:	Prof. J.H.P. Eloff
GRAADKURSUS:	M. Sc.
DEPARTEMENT:	Rekenaarwetenskap
TAAL:	Engels

OPSOMMING

Inligting kan beskou word as maatskappye se mees waardevolste bate en moet beskerm word as sulks. Voorheen het maatskappye baie beperkte toegang tot hierdie korporatiewe inligting toegelaat. Die koms van die Internet het hierdie situasie dramaties omgekeer. Dit word al meer belangrik vir maatskappye om hulle korporatiewe inligting in databasisse met gebruikers te deel. Dit is egter uiters belangrik om toegang tot webtoeganklike databasisse te beheer, veral as sensitiewe inligting soos kredietkaartnommers gestoor word.

Die sekuriteit van webtoeganklike databasisse word uitgedaag, wanneer groot getalle gebruikers toegang aan inligting gegee word, sonder die normale korporatiewe beheer. ‘n Beveiligde webtoeganklike databasis is nie net eenvoudig ‘n beveiligde databasis met ‘n paar dinamies veranderende web bladsye vooraan nie. Die webtoeganklike databasis is geweldig gesofistikeerd en bestaan uit ‘n aantal komplekse applikasies wat voor die databasis geplaas word. Aangesien die meeste aanvallers die webtoeganklike databasis van binne die maatskappy binnedring, gee grensbeskerming soos “firewalls”, “intrusion detection tools” en virus beheer sagteware beperkte beskerming.

Die doelwit van hierdie studie is om sekuriteitsdienste en meganismes te ondersoek wat beskerming aan webtoeganklike databasisse sal verleen. Aangesien databasissekuriteit reeds vir jare deur navorsers bestudeer is, is besluit om te bepaal of hierdie tradisionele sekuriteitsdienste en meganismes as raamwerk gebruik kan word om ‘n veilige webtoeganklike databasis omgewing te skep.

Nege tradisionele databasissekuriteitsdienste en meganismes is ondersoek. Addisionele sekuriteitsdienste en meganismes is gevind wat meer beskerming aan webtoeganklike databasisse in die Internet omgewing sou verleen. Daarna is elke sekuriteitsdiens geïntegreer soos dit vesprei is oor die komponente van die webtoeganklike databasis, met die doel om die geïntegreerde diens te vegelyk met die diens wat voorsien word deur tradisionele databasissekuriteit. ‘n Model is ontwikkel wat illustreer hoe hierdie sekuriteitsdienste en meganismes toegepas kan word in ‘n veilige webtoeganklike databasis.

Die studie is afgesluit met ‘n gevolgtrekking oor die sekuriteit wat behaal kan word in webtoeganklike databasisse, met huidige sekuriteitsdienste en meganismes. Verdere probleemareas, waarin navosing moontlik gedoen kan word is kortliks toegelig.

ABSTRACT

Information can be considered a company's most valued asset and should be protected as such. In the past, companies allowed very limited access to corporate information. Today, the rapid growth of the Internet increases the importance of connecting to existing databases. Access to such web-enabled databases, containing sensitive information such as credit card numbers must be made available only to those who need it.

The security of web-enabled databases is challenged, as huge user populations access corporate information, past traditional perimeters. Providing a secure web-enabled database environment is not as simple as creating a few dynamic pages linked to a secured database. As a web-enabled database is very sophisticated, consisting of various applications in front of the database, it is vulnerable to attack. Furthermore, since most malicious intrusions occur from inside, defences such as firewalls, intrusion detection and virus scanning provide limited protection.

The principle aim of this study was to consider security services and mechanisms that would provide protection to web-enabled databases. As database security has been a well-researched topic ever since the first databases were used, it was decided to investigate whether traditional database security could possibly provide a basic framework to be used when approaching the security of web-enabled databases.

An investigation was made into nine current state database security services and their associated mechanisms. Additional services and mechanisms were identified, that could provide protection in the new environment. The integrated service provided by web-enabled databases was contrasted to the service provided by current state database security. A model was developed that illustrated how these services and mechanisms could be applied to create a secure web-enabled database.

The study was brought to an end with a conclusion on the security that can be attained by web-enabled databases. Further problem areas, which could be researched in the future, were touched upon briefly.

CONTENTS

Chapter 3

Database security

Chapter 4

Can current state-of-the-art database security services and mechanisms protect against virtual web database environment threats?

Chapter 5

Information security services to be provided by a web server in a virtual web database environment

Chapter 6

Information security services to be provided by an application server in a virtual web database environment

Chapter 7

Information security services to be provided by a database server in a virtual web database environment

Chapter 8

A secure virtual web database environment

LIST OF FIGURES

LIST OF TABLES