

**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**



## 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 versprei is oor die komponente van die webtoeganklike databasis, met die doel om die geïntegreerde diens te vergelyk 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 navorsing 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 1

### Introduction

1.1	Introduction.....	2
1.2	Terminology.....	4
1.3	Problems and issues to be addressed.....	6
1.4	Overview.....	8

## Chapter 2

### Virtual web database environments

2.1	Introduction.....	12
2.2	Web environments.....	13
2.2.1	Intranets.....	13
2.2.2	Extranets.....	14
2.2.3	Internet.....	15
2.3	The virtual web database environment.....	16
2.3.1	Interconnectivity between servers of the virtual web database environment.....	18
2.3.2	Definition of servers of the virtual web database environment.....	18
2.3.3	Functionality of servers of the virtual web database environment.....	19
2.3.4	Virtual web database environment protocols and technologies.....	21
2.4	Information security risks of a virtual web database environment.....	23
2.4.1	The two-tier client/server environment.....	24
2.4.2	The virtual web database environment.....	25
2.4.3	Information security threats faced by each server of the virtual web database environment.....	26
2.5	Conclusion.....	32

## Chapter 3

### Database security

3.1	Introduction.....	34
3.2	Database information security policy.....	34
3.3	Database information security services.....	35
3.3.1	Identification and authentication.....	35
3.3.2	Authorization.....	36
3.3.3	Confidentiality.....	47
3.3.4	Integrity.....	51
3.3.5	Accountability.....	54
3.3.6	Availability.....	55
3.3.7	Manageability.....	57
3.3.8	Assurance.....	58
3.3.9	Physical security.....	59
3.4	Conclusion.....	60



## Chapter 4

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

4.1	Introduction.....	63
4.2	Information security services and mechanisms investigated in current state database security and virtual web database environment threats.....	63
4.3	Analysis of results.....	65
4.3.1	Can current state database security services and mechanisms protect against threats posed by network risks.....	65
4.3.2	Can current state database security services and mechanisms protect against web server threats.....	65
4.3.3	Can current state database security services and mechanisms protect against application server threats.....	67
4.3.4	Can current state database security services and mechanisms protect against database server threats.....	68

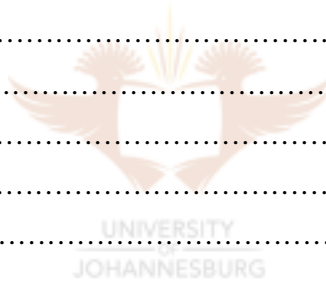


4.3.5	Can current state database security services and mechanisms protect against employees and facilities threats.....	69
4.4	Conclusion.....	70

## Chapter 5

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

5.1	Introduction.....	72
5.2	Information security services of a web server in a virtual web database environment.....	73
5.2.1	Identification and authentication.....	74
5.2.2	Authorization.....	78
5.2.3	Confidentiality.....	80
5.2.4	Integrity.....	82
5.2.5	Accountability.....	85
5.2.6	Availability.....	87
5.2.7	Manageability.....	89
5.2.8	Assurance.....	90
5.2.9	Physical security.....	92
5.3	Web server information security services and the threats facing the web server of ABC Bids.....	92
5.3.1	Network threats.....	92
5.3.2	Web server threats.....	93
5.3.3	Employees and facilities threats.....	94
5.4	Conclusion.....	95



## Chapter 6

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

6.1	Introduction.....	98
6.2	Application server component models.....	99
6.2.1	The Enterprise JavaBeans (EJB) component model on J2EE platform.....	99
6.2.2	The COM+ component model on Windows DNA platform.....	100
6.2.3	A comparison of EJB and COM+ in terms of security.....	101
6.3	Database access technologies.....	101
6.3.1	Data access technologies on the J2EE platform.....	102
6.3.2	Data access technologies on the Windows DNA platform.....	102
6.3.3	Security considerations of data access technologies.....	103
6.4	Information security services to be provided by an application server in a virtual web database environment.....	104
6.4.1	Identification and authentication.....	105
6.4.2	Authorization.....	107
6.4.3	Confidentiality.....	109
6.4.4	Integrity.....	110
6.4.5	Accountability.....	112
6.4.6	Availability.....	114
6.4.7	Manageability.....	116
6.4.8	Assurance.....	117
6.4.9	Physical security.....	118
6.4.10	Non-repudiation.....	118
6.5	Application server information security services and the threats facing the application server of ABC Bids.....	120
6.5.1	Network threats.....	120
6.5.2	Application server threats.....	120
6.5.3	Employees and facilities threats.....	121
6.6	Conclusion.....	122

## **Chapter 7**

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

7.1	Introduction.....	125
7.2	Information security services to be provided by a database server in a virtual web database environment.....	126
7.2.1	Identification and authentication.....	128
7.2.2	Authorization.....	129
7.2.3	Confidentiality.....	132
7.2.4	Integrity.....	134
7.2.5	Accountability.....	136
7.2.6	Availability.....	137
7.2.7	Manageability.....	139
7.2.8	Assurance.....	140
7.2.9	Physical security.....	141
7.3	Database server information security services and the threats facing the database server of ABC Bids.....	142
7.3.1	Network threats.....	142
7.3.2	Database server threats.....	142
7.3.3	Employees and facilities threats.....	144
7.4	Conclusion.....	144

## **Chapter 8**

### **A secure virtual web database environment**

8.1	Introduction.....	147
8.2	Database security services integrated in the virtual web database environment.....	147
8.2.1	Identification and authentication.....	148
8.2.2	Authorization.....	150
8.2.3	Confidentiality.....	152
8.2.4	Integrity.....	153

8.2.5	Accountability.....	155
8.2.6	Availability.....	157
8.2.7	Manageability.....	158
8.2.8	Assurance.....	160
8.2.9	Physical security.....	161
8.2.10	Non-repudiation.....	163
8.3	Summary of all security services and mechanisms to be provided by the virtual web database environment.....	164
8.4	A high-level model of respective virtual web database environment responsibilities.....	166
8.5	Conclusion.....	167

## **Chapter 9**

### **Conclusion**

9.1	Introduction.....	169
9.2	The dissertation.....	169
9.3	Limitations and future expandability.....	171

<b>List of sources consulted.....</b>	<b>173</b>
---------------------------------------	------------

### **Appendix A**

ABC Bids case study.....	A-1
--------------------------	-----

### **Appendix B**

A description of data access technologies employed by application servers.....	B-1
--	-----

### **Appendix C**

A paper titled “Secure virtual web databases for an e-commerce environment”.....	C-1
--	-----

### **Appendix D**

A paper titled “Secure database connectivity and the WWW”.....	D-1
--	-----

## LIST OF FIGURES

Figure 1.1:	Database access in a corporate environment.....	2
Figure 1.2:	Database access through the Internet.....	3
Figure 1.3:	Chapter layout.....	8
Figure 2.1:	A web-enabled database environment.....	16
Figure 2.2:	A virtual web database environment with its servers.....	17
Figure 2.3:	Integration of the functionality of each server in the virtual web database environment.....	19
Figure 2.4:	A detailed view of the virtual web database environment.....	21
Figure 2.5:	Employee creating an item in the database server.....	25
Figure 2.6:	Customers directly interacting with the virtual web database environment of ABC Bids.....	26
Figure 3.1:	An access control matrix.....	38
Figure 3.2:	DAC allows unlawful access control.....	40
Figure 3.3:	MAC protection – data cannot flow to a lower level.....	42
Figure 3.4:	Records of ITEMS.....	42
Figure 3.5:	Flat RBAC.....	45
Figure 5.1:	A web server in a virtual web database environment.....	72
Figure 6.1:	A virtual web database environment on the J2EE platform.....	102
Figure 6.2:	A virtual web database environment on the Windows DNA platform.....	103
Figure 7.1:	A database server in a virtual web database environment.....	125
Figure 8.1:	Database identification and authentication.....	148
Figure 8.2:	Virtual web database environment identification and authentication.....	148
Figure 8.3:	Database authorization.....	150
Figure 8.4:	Virtual web database environment authorization.....	151
Figure 8.5:	Database confidentiality.....	152
Figure 8.6:	Virtual web database environment confidentiality.....	153
Figure 8.7:	Database integrity.....	154
Figure 8.8:	Virtual web database environment integrity.....	154
Figure 8.9:	Database accountability.....	155
Figure 8.10:	Virtual web database environment accountability.....	156
Figure 8.11:	Database availability.....	157
Figure 8.12:	Virtual web database environment availability.....	158

Figure 8.13:	Database manageability.....	159
Figure 8.14:	Virtual web database environment manageability.....	159
Figure 8.15:	Database assurance.....	160
Figure 8.16:	Virtual web database environment assurance.....	161
Figure 8.17:	Database physical security.....	162
Figure 8.18:	Virtual web database environment physical security.....	162
Figure 8.19:	Virtual web database environment non-repudiation.....	163



## LIST OF TABLES

Table 2.1:	Threats as a result of network protocol vulnerabilities.....	28
Table 2.2:	Threats as a result of data and software vulnerabilities.....	28
Table 2.3:	Threats when employees and facilities are vulnerable.....	30
Table 3.1:	Database security services and mechanisms.....	60
Table 4.1:	Current state database security services and mechanisms with virtual web database environment threats?.....	64
Table 4.2:	Can current state database security services and mechanisms protect against network threats?.....	65
Table 4.3:	Can current state database security services and mechanisms protect against web server threats?.....	66
Table 4.4:	Can current state database security services and mechanisms protect against application server threats?.....	67
Table 4.5:	Can current state database security services and mechanisms that can protect against database server threats?.....	68
Table 4.6:	Can current state database security services and mechanisms protect against employees and facilities threats?.....	69
Table 5.1:	Additional web server authentication mechanisms.....	77
Table 5.2:	Additional web server authorization mechanisms.....	80
Table 5.3:	Additional web server confidentiality mechanisms.....	82
Table 5.4:	Additional web server integrity mechanisms.....	84
Table 5.5:	Additional web server accountability mechanisms.....	87
Table 5.6:	Additional web server availability mechanisms.....	89
Table 5.7:	Web server manageability mechanisms.....	90
Table 5.8:	Additional web server assurance mechanisms.....	91
Table 5.9:	Web server physical security mechanisms.....	92
Table 5.10:	Web server threats and services that can protect against them.....	92
Table 5.11:	All web server security services and mechanisms.....	95
Table 6.1:	Application server identification and authentication mechanisms.....	106
Table 6.2:	Authorization mechanisms employed by an application server.....	109
Table 6.3:	Additional application server confidentiality mechanisms.....	110
Table 6.4:	Additional application server integrity mechanisms.....	112
Table 6.5:	Additional application server accountability mechanisms.....	113

Table 6.6:	Additional application server availability mechanism.....	115
Table 6.7:	Additional application server manageability mechanisms.....	116
Table 6.8:	Additional application server assurance mechanisms.....	118
Table 6.9:	Application server physical threat mechanisms.....	118
Table 6.10:	Application server non-repudiation mechanisms.....	120
Table 6.11:	Application server threats and security services that can provide protection....	120
Table 6.12:	All application server security services and mechanisms that can provide protection.....	122
Table 7.1:	Additional database server authentication mechanisms.....	129
Table 7.2:	Database server authorization mechanisms.....	132
Table 7.3:	Additional database server confidentiality mechanisms.....	133
Table 7.4:	Additional database server integrity mechanisms.....	135
Table 7.5:	Additional database server accountability mechanisms.....	137
Table 7.6:	Additional database server availability mechanisms.....	138
Table 7.7:	Database server manageability mechanism.....	140
Table 7.8:	Database servers at TCSEC C2 level are assured for commercial environments.....	140
Table 7.9:	Database servers at ITSEC EAL4 level are equal to TCSEC C2 assurance.....	140
Table 7.10:	Additional database server assurance mechanisms.....	141
Table 7.11:	Database server physical threat mechanisms.....	141
Table 7.12:	Database server threats and security services that can provide protection.....	142
Table 7.13:	All database server security services and mechanisms.....	144
Table 8.1:	All services and mechanisms to be provided by the virtual web database environment.....	164
Table 8.2:	Security responsibilities taken by the servers of the virtual web database environment.....	166