A methodology for accrediting a commercial distributed database

J.H.P. Eloff and R. Körner

Department of Computer Science

Rand Afrikaans University, P.O. Box 524, Auckland Park,

Johannesburg 2006, South Africa

Eloff@rkw.rau.co.za, Korner@iafrica.com

Abstract

This paper proposes a process through which a commercial distributed database could be accredited. The said process could be executed in order to ensure that the database product used in the operational environment, of an organisation is best suited to provide security safeguards and countermeasures to meet the unique security requirements of such environment. In addition, the framework of accreditation evaluation could provide a basis for the comparison of security criteria implementation in various commercial distributed database products.

Keywords

‘information security’, ‘Common Criteria’, ‘accreditation framework’, ‘replicated distributed database environment’, ‘operational security environment’ and ‘certification’

1 INTRODUCTION

Buying off-the-shelf products, each with its own security classification, is all very well, but what do you have to show at the introduction of your computer system? Are you sure that you are fully utilising all the security services provided by these products? Are you confident that you are aware of all the features the certified products have to offer? Is the classification of your most important data product, the DBMS, relevant to you? The answers to these questions may even give rise to more pertinent questions, such as: ‘Do you know which security services you need in your database environment?’, and ‘Do you know how to fully utilise the services provided by your suite of products in order to meet your needs?’.

The increasing use of client-server driven computer systems, as well as the geographic distribution of branches, has led to many companies’ implementation of distributed database

systems. In this paper, the authors will endeavour to provide all developers, database administrators and managers of distributed databases with a high-level framework for security. In the first section an overview will be given of the certification and accreditation processes. The second section will be devoted to the identification of all the security needs and requirements for your distributed database in your own operational environment. After having identified your needs, you may want to determine to what extent your current (or potential) distributed database meets these needs. The evaluation framework is set up in a very generic way, using the security functions specified in the 'Common Criteria' (Common, 1994). Oracle 7.2 will be evaluated in terms of the security services it provides for a symmetrical replication distributed database. Although Trusted Oracle 7 is classified as an NCSC B1 product, and Oracle 7.2 as an NCSC C2 product (Oracle 7, 1994), the authors believe in using a widely used commercial product to illustrate the workings of the framework.

The evaluation framework may also be used to accredit non certified products, or to compare the same product in two different operational environments. It is the generic nature of the framework, that contributes to making it a very important tool when evaluating and comparing products for a specific operational environment. The scope of this paper restricts the authors to accrediting one product (Oracle 7.2) in one environment (symmetrical replicated distributed database).

2 CERTIFICATION AND ACCREDITATION

Currently, there are many definitions for the processes of certification and accreditation. The following constitute the definitions selected by the authors for the purpose of this paper. Certification is the process of classifying a product according to a standard, generally known as Security Criteria, like the ITSEC, CTCPEC and NCSC standards. Accreditation is the process of certifying a product according to the specific needs of the operational environment in which it will be used. In this paper, Oracle 7.2 will not be certified (as it has already been certified by the NCSC as a C2 product, and by ITSEC as an E3 product), but rather accredited in terms of the security needs of a commercial symmetrical replication distributed database environment. The authors hold the view that the certification of a commercial product is very useful for the prospective buyer comparing database products, but that it is only once the buyer has gone through the accreditation process, as suggested in this paper, that the most suitable database product for his/her specific operational environment could be selected. A strong case will be made out for this view throughout the paper.

One of the weak points of or hot spots in the existing certification criteria (Pfleeger, 1989) is that the criteria are focused on commercial *products*, especially operating systems, at the expense of application systems. It might, however, be unfair to blame the standards, as this perception may have been created owing to the fact that the standards are currently only being applied to products (by the industry). The reality is that several computer products combine to form an operational computer system. These products may work in such synergy that the effect the security functions provided by a product, may be far more profound than anticipated merely from its certification classification. On the other hand, the product may behave very differently in its operational environment and in combination with other products than in clinical tests during its certification period. Used as a case in point is the example of an Oracle 7.2 database and the UNIX operating system combined with a front-end development tool such as SQL*Windows to form an operational environment. The Oracle 7.2 database and the UNIX operating system may be jointly responsible for the identification and authentication of users. The combination of the Oracle 7.2

database with the UNIX operating system enhances the function of identification and authentication of users in that true synergy is created. The user in such an environment, therefore, receives a better identification and authentication service from the combined products than from either product on its own. It may, however, also be possible that the SQL*Windows applications do not require the user to provide a password, but keeps a flat file containing passwords, against which it matches the user's log-on ID and password, and sends this information to the database. The identification and authentication service provided in the Oracle 7.2 database will, therefore, only be cosmetic, for any user may gain access to the client PC and log into the database by supplying a user log-on ID only. The uniqueness of an operational environment is, therefore, of vital importance when it comes to security services and their importance in the operational environment. The challenge for all of those managing an application system is to identify the best security services provided by the products and the optimal combinations of these services to act as safeguard for the application system as a whole. This process is known as accreditation.

The authors would, therefore, define the term accreditation as the assurance the user of an application system will have that the products combined in the application system are individually suited to the specific operational environment, and that they combine in an optimal manner to provide the best possible security safeguard for the system. The accreditation process will involve the evaluation of the potential products in terms of the security needs in the specific operational environment. In this paper, the core of the application system, i.e. the database, will be evaluated against the security needs of a distributed database environment, using the proposed accreditation framework. Some of the functional security services of the 'Common Criteria' (Common, 1994) will be used in the next section to act as a guideline for the identification of the security needs and requirements of a distributed database. These needs and requirements will help to define an ideal operational security environment for a distributed database system. Only five of the nine security functions of the 'Common Criteria' (Common, 1994) are used in this paper. The security functions were selected because they are, in the authors' minds, the most relevant to a distributed database system. The security criteria are used not to certify the database product, but to accredit the product in the operational environment of the organisation. The accreditation process can be seen as complementary to the certification process, and will be the responsibility of the organisation aiming to provide a secure computer system.

The long term goal of the research currently conducted by the authors, is to be able to accredit a database application, consisting of many products, for a specific operational environment. In order to complete such a methodology, additional criteria to the ones used for the purpose of this paper, will be developed. The said criteria may include aspects influencing the security policy, for instance the ownership of data. In this paper the first step towards accrediting a database application is taken in accrediting the database management system.

The authors will endeavour to use existing commercial products to illustrate the workings of the proposed accreditation framework. Although Trusted Oracle 7 boasts more security features than most other database products currently available, Oracle ver 7.2 has been chosen as an exemplar because of its widespread commercial use. Whilst all the exemplars used and all the technical information given may also be applicable to other commercial products, the focus of this paper will be on Oracle 7.2. Oracle 7.2 (Oracle 7 (TM), 1995) provides mechanisms for various types of data replication, depending, of course, on the need of the organisation implementing it.

3 IDENTIFYING SECURITY REQUIREMENTS

von Solms et al. (von Solms, et al, 1994) defines the operational security environment (OSE) of a computer system as the operational environment plus the countermeasures provided by the computer system. The ideal OSE will depict the ideal security environment for the computer system. This will be the environment that the system owner will endeavour to establish throughout the life-cycle of the system (von Solms, et al, 1994).

The very first step in evaluating a product for accreditation is, therefore, to identify security requirements and to weight them in the operational environment. The authors would suggest that an ideal OSE must first be compiled and evaluated for each component of the application, and then for the application system as a whole. When product evaluations are done, strong and weak points will be identified, where after the component evaluations could be used to combine these strong and weak points to produce a strong synergy in the application system. In this paper, the authors will define an ideal OSE for a traditional distributed database environment, as well as the symmetrical replication distributed database environment. This is done to illustrate the differences in the ideal OSE for different environments. The proposed framework will only be used to accredit Oracle 7.2 in the symmetrical replication database environment.

3.1 The ideal OSE for a distributed database

When administrators, users or managers want to assure themselves of the security provided by their computer system, it is logical to start at the core of the system, which is the database. The first step in accrediting a database application in a distributed environment, will be an attempt to identify the ideal operational security environment (OSE) for a distributed database.

In Table 1, the applicability of five of the main security functions, as defined in the 'Common Criteria' (Common, 1994), is plotted against the two main types of distributed database environments, namely the traditional and the replicated environment. The former criteria were chosen because of their applicability to the database environment, and in particular to the distributed database environment. The scaling method, as developed by Eloff (Eloff, 1983), will be used throughout this framework (Appendix A). This method weights the identified security requirements in terms of the relevance to the considered environment, as well as the degree to which they are implemented by the product to be accredited.

Table 1 The importance of security criteria in a distributed database environment

<i>Security requirements</i>	<i>Traditional distributed database environment</i>	<i>Replicated distributed database environment</i>
Trusted path	4	4
Identification and Authentication	3	4
Audit	2	4
Communication	4	3
Privacy	3	4

Where: 0 - Not applicable
 1 - Necessary
 2 - Important
 3 - Very important
 4 - Of critical importance

As it can be seen from Table 1 the ideal OSE for a traditional distributed database environment differs slightly from that of a replicated database environment. Only the ideal OSE for the replicated environment will be discussed in this paper. The generic accreditation framework may, however, be used to evaluate the same product in both environments.

Some of the high-level security requirements can be broken down into more specific security services that need to be provided in the operational database environment. In the following sections, the authors will break down these requirements and evaluate to what extent Oracle 7.2 provides these services in a replicated database environment. Only the security mechanisms provided in Oracle 7.2, and not all possible mechanisms, will be used for the evaluation.

3.1.1 Trusted path

The concept of a trusted path is that communication between a user and the database will be trusted in the sense that the user will be sure that he or she is talking directly to the database, and that the database is sure that data will be returned only to trusted applications (Common, 1994). The trusted path is used to ensure that the information used for authentication supplied by the user will be protected at all times (Common, 1994). Symmetrical replication supports updates on any and every copy of the data, as well as the distribution of such an update through to other copies, therefore, there should also be a trusted path between the various copies of data. The master table must be sure that it is sending data across the network to a trusted node to keep copies of the data. Both of the aforementioned security services are of critical importance to the secure implementation of a trusted path in the replicated distributed database environment. Table 2 shows the degree to which Oracle 7.2 implements this criteria.

Table 2 Oracle implementation of trusted path

<i>Trusted path security services</i>	<i>Log-on protocol</i>
Trusted path between client and server	0
Protecting user authentication data	2

Where:

- 0 - Not applicable
- 1 - Partially implemented
- 2 - Fully implemented

Oracle 7.2 does not have the ability to ensure a trusted path between client and server, or between server and server (Harris, et al, 1994). This means that there is no way in which the client could be certain that he/she is responding to the trusted server when passing user IDs and passwords in an attempt to log onto the database. It is, therefore, also not possible for the server to be sure that it is passing a result set back to a trusted client. There is also no way in which any one server could be certain that it is sending data to be copied onto another server (as in the case of a snapshot) to a trusted server.

Oracle 7.2 provides encrypted password-passing across the network. A special log-on protocol is used for communications between the client and the server. This protocol makes use of a different encryption key for each session. Every session the client opens with the server will, therefore, have the same password encrypted to different values (Harris, et al, 1994), making it very difficult for an eavesdropper to try and decrypt the encrypted password.

It may be argued that the log-on protocol should be seen as an implementation of the secure communication function and not of the trusted-path function. A possible solution may be to include

the log-on protocol as an implementation of both the trusted path and the communication functions. In this case, the authors chose to keep the log-on protocol as part of the trusted-path function, for this arrangement satisfies one of the most important trusted-path security requirements as specified in the Common Criteria, namely that of protecting user authentication data.

3.1.2 Identification and authentication

Table 3 Oracle implementation of identification and authentication

<i>Identification and authentication security services</i>		
	<i>User log-on Ids</i>	<i>Password verification</i>
Identification	2	0
Authentication	0	2

Where:

- 0 - Not applicable
- 1 - Partially implemented
- 2 - Fully implemented

As is shown in Table 3, Oracle 7.2 implements identification and authentication through the use of user log-on identifications and passwords. Oracle 7.2 provides the facility of twofold identification: either the identification can be left up to the operating system or every user requesting a session with the database will have to provide a username and password. In case the identification and authentication process is left up to the operating system, users' IDs and passwords will be validated by the operating system mechanisms, and database roles may be mapped to operating system groups (Harris, et al, 1994). The user will, therefore, receive the database privileges associated with the operating system group for which it was authenticated. This means that access will be granted to a user to use applications without having to provide a separate database ID and password (Oracle 7, 1994). This will be done where it can be ensured that all users requiring access to the database will have only one path to the database, namely through the operating system. In case of database authentication, every user or program trying to gain access to the database will have to supply a user ID and password (Oracle 7, 1994). The latter case would probably be more often used in a replicated distributed database environment.

In the authors' minds, the mechanisms Oracle 7.2 provides fully satisfies the identification and authentication security service requirements. There are, however, some deficiencies in the current password mechanisms Oracle 7.2 is using. Oracle does not manage a minimum password length and suitable time periods requiring password changes (Harris, et al, 1994). This may, however, be overcome by educating staff members to keep their passwords secret, to choose them carefully and to change them regularly.

3.1.3 Security audit

The security audit of a database involves the recording, storing and analysis of information recognised as information regarding security-related activities (Common, 1994). Oracle 7.2 (Oracle 7 (TM), 1995) does provide an automated audit trail facility that will record information on relevant actions. The audit trail may be kept on database activity, prompted by a user using a system privilege, or only of actions relevant to certain objects or attributes, or actions performed by individual users (Oracle 7, 1994). A specific database activity may be audited through Oracle's audit facility without the additional overhead that is normally associated with audit keeping (Oracle

7, 1994). The audit trail may be switched on or off, and the scope and granularity of the trail may be changed, as the administrator sees fit. The audit trail records are kept in an Oracle table, available for viewing (Oracle 7, 1994). This table will be seen as a normal access control object, and rights to this table will be granted to users. The audit trail table is, therefore, protected against malicious changes.

All of the above is true for each and every node in the replicated database environment, the audit functions on each local database will function separately. Oracle 7.2 does not provide a distributed audit function that will allow a central audit function to manipulate audit functions on various geographical nodes. Every node will have full control of the audit function at local database level, but no control over the audit function at another node. The audit trail of a specific object will, therefore, be scattered over as many nodes as there are copies of the object. Database triggers and stored procedures may be used to partially implement a consolidated audit trail for an object (Oracle 7, 1994).

Table 4 Oracle implementation of audit criteria

<i>Audit security services</i>	<i>Audit trail</i>
Audit	1
Where:	0 - Not applicable 1 - Partially implemented 2 - Fully implemented

The extensive audit facility offered in Oracle 7.2 satisfies the audit security service requirement but, ideally, the database containing the master object should be able to manipulate audit trails on the various local databases where copies of the object occur. As indicated in Table 4, the implementation of the audit function in Oracle 7.2 is only partial, as it lacks the distributed option that would be required in a replicated distributed database environment.

3.1.4 Communication

Secure communications should support mechanisms to prove that data was either created, transmitted or received by a specific party (Chii-Ren, 1995). This service will be provided by implementing proof of sender, submission, delivery and receipt. These services form part of a secure communication system and do not fall within the scope of a database. The distributed database should, however, provide data protection on the communication of the data object itself. Trusted communication services regarding data objects ought to provide non-repudiation of origin and receipt (Common, 1994). Proof of origin and receipt will supplement the normal secure communication non-repudiation services. Proof-of-origin mechanisms will provide acceptable proof regarding the originator of the data object. The originator will not be able to deny preparing or creating the data object. The originator and sender of a data object need not be the same party. On the other hand, proof of receipt mechanisms will provide acceptable proof that the data object was received, and that the receiver will not be able to deny the receipt of the data object (Chii-Ren, 1995).

In the replicated distributed database environment, proof of origin and receipt should be implemented between the servers housing various copies of the data. In this way, the replicated database will have proof that the master database was the originator of the replicated data, and the master database will have proof that the replicated database had received data transmitted to it.

Oracle 7.2 does not provide any mechanisms to ensure proof of origin or receipt. This is the one component in which Oracle 7.2 does not even begin to achieve what is expected of it in terms of security services provided.

3.1.5 Privacy (confidentiality)

In the replicated distributed database environment, there are many copies of the same data stored over many geographical nodes, thus increasing the risk of an unauthorised subject (user or program) reading data. The implementation of access control in the replicated distributed environment is, therefore, of critical importance to the security of such a system. Another critical component is to ensure that the data that is read will not be tapped into covert channels. This environment also requires a more complex implementation of object re-use mechanisms than other database environments. Object re-use deals mainly with memory protection mechanisms in the operating system (Pfleege, 1989). The mechanisms of the operating system will ensure that each user's program runs in a specific piece of memory, inaccessible to unauthorised users (Pfleege, 1989). In the replicated distributed database environment, each geographical node may run on a different hardware platform, leading to diverse implementations of the object re-use, or memory protection, mechanisms in this environment. The unobservability and unlinkability of communication events are not that important for the implementation of security, but protect the privacy of users.

Table 5 Breakdown of privacy criteria

<i>Privacy security services</i>	<i>Symmetrical replicated distributed database environment</i>
Read control (access control)	4
Unobservability of communication events	1
Unlinkability of communication events	1
Object re-use	3
Covert channel handling	4
Where:	
0 -	Not applicable
1 -	Necessary
2 -	Important
3 -	Very important
4 -	Of critical importance

The access control mechanisms provided by Oracle, as discussed earlier, are well defined and implemented (Oracle 7 (TM), 1995). Oracle provides insert and update privileges up to attribute level. It does not, however, provide row level access and selective select privileges. These can be achieved through snapshots on horizontal or vertical subsets of tables. Row level access is the responsibility of the developers and administrators of the database schema, and may be implemented through application-specific database triggers. A database encryption facility is offered by Oracle 7.2 to supplement the access control measures when it comes to read control. Access to sensitive data may be limited by encrypting such data. The decryption privileges may then only be granted to the functional user of the sensitive data. This will ensure that developers and users in other functional areas cannot read the sensitive data in clear text format. At this point in time, table encryption facilities are provided and not column or row level encryption (Oracle 7, 1994).

Plotted in Table 6 are the security services and corresponding mechanisms through which the services are achieved .

Table 6 Oracle implementation of privacy

<i>Privacy security services</i>	<i>Access control (discretionary)</i>	<i>Database encryption</i>	<i>Snapshot</i>	<i>Deleted objects</i>
Read control	2	2	2	0
Unobservability of communication events	0	0	0	0
Unlinkability of communication events	0	0	0	0
Object re-use	0	0	0	1
Covert channel handling	1	1	0	0

Where: 0 - Not applicable
1 - Partially implemented
2 - Fully implemented

Oracle 7.2 does not provide for the unlinkability and unobservability of communication sessions with the database. This is not critical for the secure working of the replicated distributed database system. Object re-use will be achieved when Oracle only allocates space for use by an object (memory) once all traces of deleted data have been removed (Oracle 7, 1994).

This discussion has clearly shown how interdependent some of the security criteria are. The *Privacy criteria* is dependent on the *Identification and authentication criteria*, as are the *Communications* and *Trusted Path criteria*. Not only are the criteria interrelated, but some security mechanisms may satisfy security services in more than one criteria. The mechanism of access control, for instance, implements security services both in the *Identification and authentication* and *Privacy criteria*. In the following section, Eloff's (Eloff, 1983) model will be used to give Oracle 7.2 an accreditation score on each of the criteria, as discussed.

The five criteria used for the illustration of the model are by no means the only criteria applicable when doing accreditation. Two other criteria contained in the 'Common Criteria' (Common, 1994), namely *Protection of user data* and *Resource utilisation* may be included. The model will be extended ultimately to award Oracle 7.2 a global accreditation score for providing the security services needed in the ideal operational security environment of a replicated distributed database.

4 MEASURE OF ACCREDITATION

After identifying and discussing the security requirements of the ideal OSE in section 3, Oracle 7.2 can now be accredited in the symmetrical replicated distributed database environment. Each criterion will be evaluated separately using the formula as shown in Appendix A. The accreditation score will be determined by taking the product of the importance of the requirement and the degree of implementation thereof, multiplied by a constant value of 50, all divided by the weighted importance of the requirement. The calculations for the accreditation score achieved for the *Privacy criteria* is shown as an example.

Table 7 Accreditation score for the privacy criteria

<i>Security services</i>	<i>Implementation Scale</i>	<i>Importance of Requirement</i>	<i>Product (implementation and importance)</i>
Read control	2	4	8
Unobservability of communication events	0	1	0
Unlinkability of communication events	0	1	0
Object re-use	1	3	3
Covert channel handling	2	4	8
		13	19

Evaluation for privacy:

$$S \text{ Privacy} = (50.19) / 13 = 73,08 \%$$

Table 8 Accreditation scores

<i>Security requirements</i>	<i>Accreditation score</i>
Trusted path	$S \text{ Trusted Path} = (50.8) / 8 = 50\%$
Identification and authentication	$S \text{ I \& A} = (50.8) / 4 = 100\%$
Audit	$S \text{ Audit} = (50.4) / 4 = 50\%$
Communication	$S \text{ Communication} = (50.0) / 3 = 0\%$
Privacy	$S \text{ Privacy} = (50.19) / 13 = 73,08 \%$

The accreditation scores obtained by Oracle 7.2 for the five security criteria used are summarised on a high level in Table 9.

Table 9 High level accreditation scores

<i>Criteria</i>	<i>Accreditation score</i>	<i>Implementation scale</i>	<i>Importance of requirement</i>	<i>Product (implementation and importance)</i>
Trusted path	50%	1	4	4
Identification and authentication	100%	2	4	8
Audit	50%	1	4	4
Communications	0%	0	4	0
Privacy	73%	1	4	4
			20	20

Where: 0 - 49% = 0
 50 - 89% = 1
 90 - 100% = 2

Overall evaluation for Oracle 7.2:

$$S \text{ Oracle 7.2} = (50.20) / 20 = 50\%.$$

The accreditation model we used indicates that Oracle 7.2 achieves an accreditation score of 50% of the security services required in a replicated distributed database environment, based on the five chosen criteria. The framework makes it possible to determine what percentage Oracle achieves for each criterion, making comparison between products easy. It can be derived that Oracle 7.2 is very strong on the *Privacy* and *Identification and authentication criteria*. This enables the prospective database manager to evaluate several products with the same model and to obtain scores for each product. The accreditation scores for each product may then be compared to support a decision on which product to buy. It may be possible that the overall score is lower than that of other evaluated products, but its score obtained in one of the criterion is much higher than that of other products. If the specific criterion is very important to the potential database manager, the product may even be chosen over a product with a higher aggregate score. This framework, therefore, supports business orientated information systems decisions.

5 CONCLUSION

Every organisation serious about its data and application systems, should strive towards accreditation and peace of mind (regarding the security safeguards provided by their company). In this paper, the emphasis was placed on understanding how operational security needs and requirements for a distributed database can be satisfied by the mechanisms provided in the database. The proposed accreditation framework may be seen as an exciting development in achieving a better understanding of accrediting products for a specific operational environment. Distributed database managers can use this framework first of all to help answer the question: What security needs exist in the immediate operational environment of the distributed database, and how important are they? The second question that will have to be answered is: How well, if at all, does the current database mechanisms satisfy these security needs.

This framework will help the manager of the database system to identify the current security needs existing in the database's environment, and to evaluate the current or potential database's ability to satisfy these security needs. The framework also provides the manager with a yardstick with which to compare various database products in the same manner, so as to reach the best possible decision regarding a database product for the organisation. Although the framework provided primarily focused on the distributed database, it is sufficiently generic to allow for the evaluation of any component in an application system.

6 REFERENCES

- Chii-Ren Tsai (1995) Extending Distributed Audit to Heterogeneous Audit Subsystems, in *Proceedings of the IFIP Sec '95* (ed. J.H.P. Eloff, S.H. von Solms).
- Common Criteria (1994) *Preliminary draft*.
- Eloff, J.H.P. (1983) Selection Process for Security Packages. *Computers & Security*, 2, 256-260.
- Harris, D. and Sidwell, D. (1994) Distributed Database Security. *Computers & Security*, 13, 547-557.
- Kaijser, P. (1995) Data Protection in Communication and Storage, in *Proceedings of the IFIP Sec '95* (ed. J.H.P. Eloff, S.H. von Solms).
- Oracle 7 (1994) Database Security in Oracle 7 (Release 7.1).

- Oracle 7 (TM) (1995) Server Distributed Systems, Volume II: Replicated Data, Release 7.2.
- Pfleeger, C.P. (1989) Security in Computing. Prentice-Hall, Inc., London.
- von Solms, R., van de Haar, H., von Solms, S.H. and Caelli, W.J. (1994) A Framework for Information Security Evaluation. *Information & Management*, 3.

BIOGRAPHY

Jan Eloff holds a Ph.D (Computer Science) specialising in Information Security. He worked for a number of years in industry, since 1988 he is a Professor in Computer Science at the Rand Afrikaans University, South Africa. He has published widely on various aspects of information security. He has delivered papers at leading information security conferences on an international level. He is chairman of the South African Special Interest Group in Information Security which is affiliated to the Computer Society of South Africa. He is also chairman of an international working group on Small System Security. He serves as a professional advisor on various aspects on information security to industry.

Renita Körner is currently studying towards her Ph.D (Computer Science) specialising in the field of database security. She works as a Computer Consultant for Q Data Consulting, one of South Africa's leading consulting firms. In her capacity as a computer consultant she is often called upon to advise clients in the intricacies of computer security, and more specifically database security.