

Security im Oracle-Umfeld

Johannes Kebeck
Senior Systemberater
ORACLE Deutschland GmbH

ORACLE

Nicht-Verfügbarkeit - oder schlimmer - Manipulation von

- Einsatzleitsystemen der Rettungsdienste oder der Polizei
- Führungsinformationssystemen bei Großschadenslagen oder militärischen Einsätzen
- Operativen Systemen im Bereich der Flugsicherheit
- ...

news 30.03.2004 16:32
Datenleck bei der japanischen Polizei
Die Polizei von Kyoto musste zugeben, dass Akten mit Ermittlungsdaten im Internet verfügbar sind

„The Air Force alone noted over 300,000 attempts of unauthorized intrusion last year ... We are insufficiently manned and very poorly prepared to deal with what's ahead ...“ (Richard Clark, 26.09.2000)

ORACLE

- 90% der Befragten gaben an, in den letzten 12 Monaten Sicherheitsvorkommnisse registriert zu haben
- 80% der Befragten gaben zu aufgrund der Sicherheitsvorkommnisse finanzielle Verluste hingenommen zu haben
 - \$455,848,000 in quantifizierbaren Verlusten
 - \$170,827,000 durch Diebstahl urheberrechtlich geschützter Informationen
 - \$115,753,000 durch Betrug
- 74% stellten den Internet-Zugang als häufigen Angriffspunkt fest
- 33% nannten interne Systeme als häufigen Angriffspunkt

ORACLE

Quelle: 2002 CSI/FBI Computer Crime and Security Survey

- Die Anzahl der sicherheitsrelevanten Vorkommnisse nimmt dramatisch zu.
- Die Zeit zwischen dem Entdecken einer Schwachstelle und der Entwicklung erster Angriffsmethoden wird immer kürzer.
- Alle Bereiche sind betroffen.
- Automatisierte Werkzeuge ermöglichen auch wenig versierten Nutzern das Schreiben von Viren und Würmern oder das Hacken.

ORACLE

Quelle: http://www.symantec.com/region/de/PressCenter/Threat_Reports.html

Security im Oracle-Umfeld

- **Ein kurzer Rückblick**
- **Bedrohungen und Gegenmaßnahmen**
- **Die Leiden der IT-SichhBeauftr**

ORACLE

Ein kurzer Rückblick

ORACLE

'Caesar Cipher'



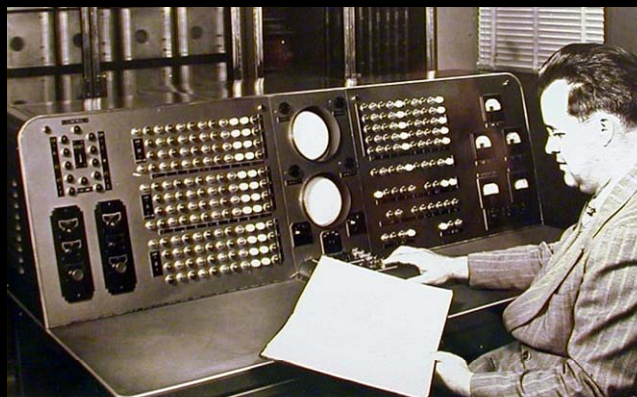
Selective Data Encryption

XYZABCDEFGHIJKLMN**OP**QRSTUVWXYZ
ABCDEFGHIJKLMN**OP**QRSTUVWXYZ

Vhohfwlyh Gdwd Hqfubswlrq

ORACLE

Die Wache an der Tür und ein Ausweis für den Benutzer










ORACLE



- Robert Morris, Jr., Sohn des Chef-Wissenschaftlers des NCSC
- Erster Zwischenfall
- selbst replizierendes und selbst propagierendes Programm
- Nutzt fingerd und sendmail
- Geschätzter Schaden \$100 Mio
- **Folgen: Steigendes Problembewusstsein und Gründung des CERT**



ORACLE

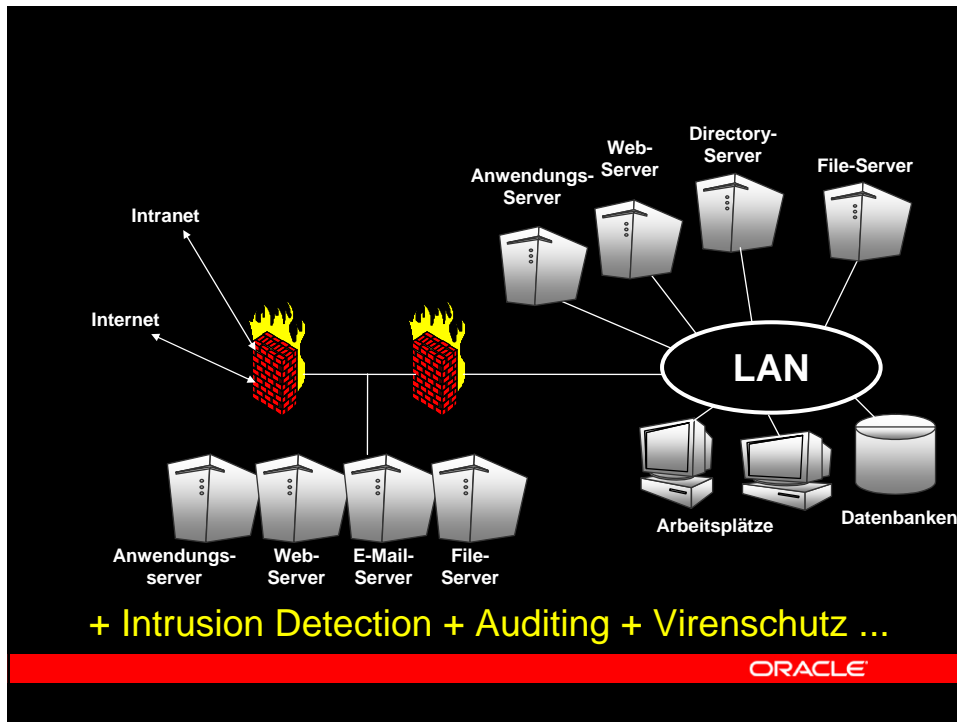


- Ziele:
 - Verfügbarkeit
 - **Vertraulichkeit**
 - Verbindlichkeit
 - Integrität
- Maßnahmen
 - organisatorisch
 - personell
 - **technisch**
 - infrastrukturell

ORACLE

Bedrohungen und Gegenmaßnahmen

ORACLE



Viren und Würmer

Adresse <http://www.hnc3k.com/viruscreationprogramz.htm> Wechseln zu Links >

Adresse http://www.hacker-archiv.de/page/viren/construction_kits.html Wechseln zu Links >

Adresse http://web.zdnet.de/itsupport/virencenter/dict/cat9_0-wc.html Wechseln zu Links >

Adresse http://wizard.ae.krakow.pl/~wasylsp/txt/Virus_Writing_HOWTO/ Wechseln zu Links >

The Linux Virus Writing HOWTO

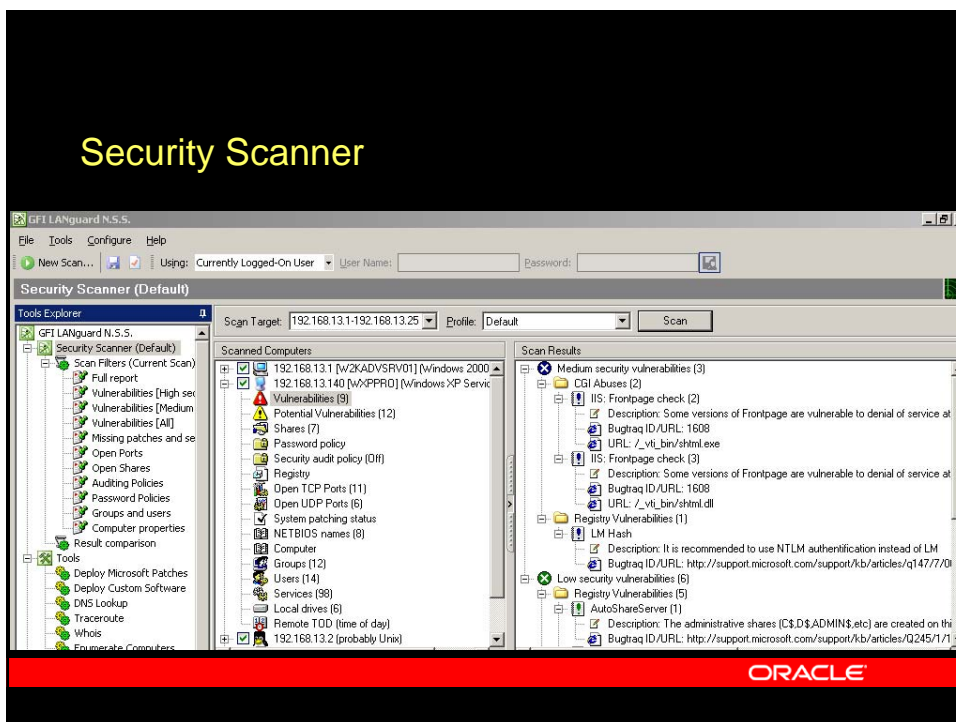
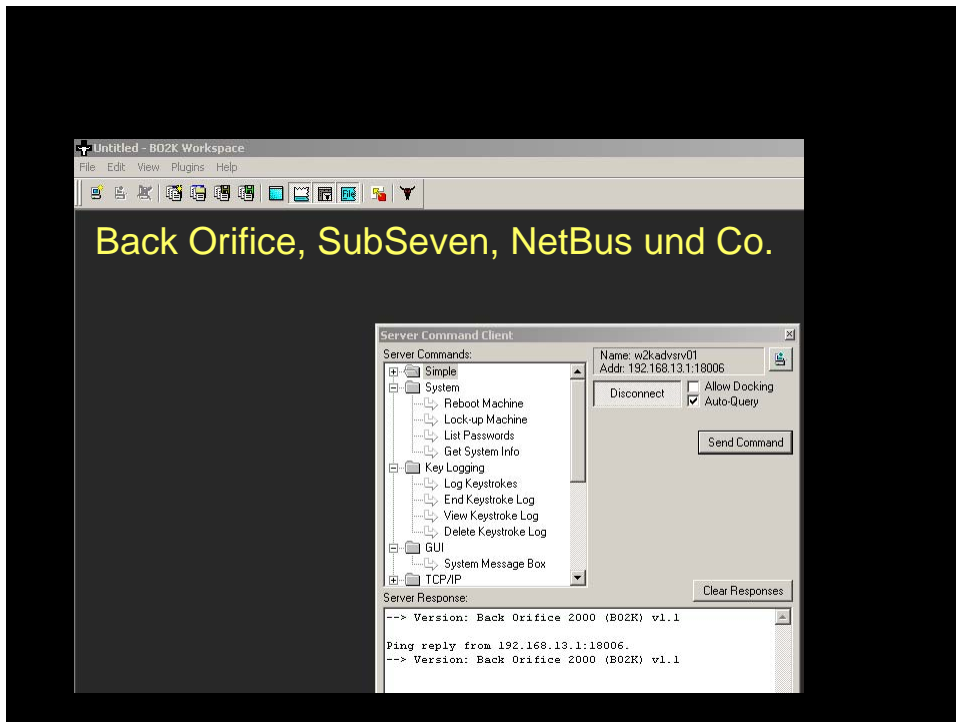
post-link-time code modification of ELF executables under Linux/i386

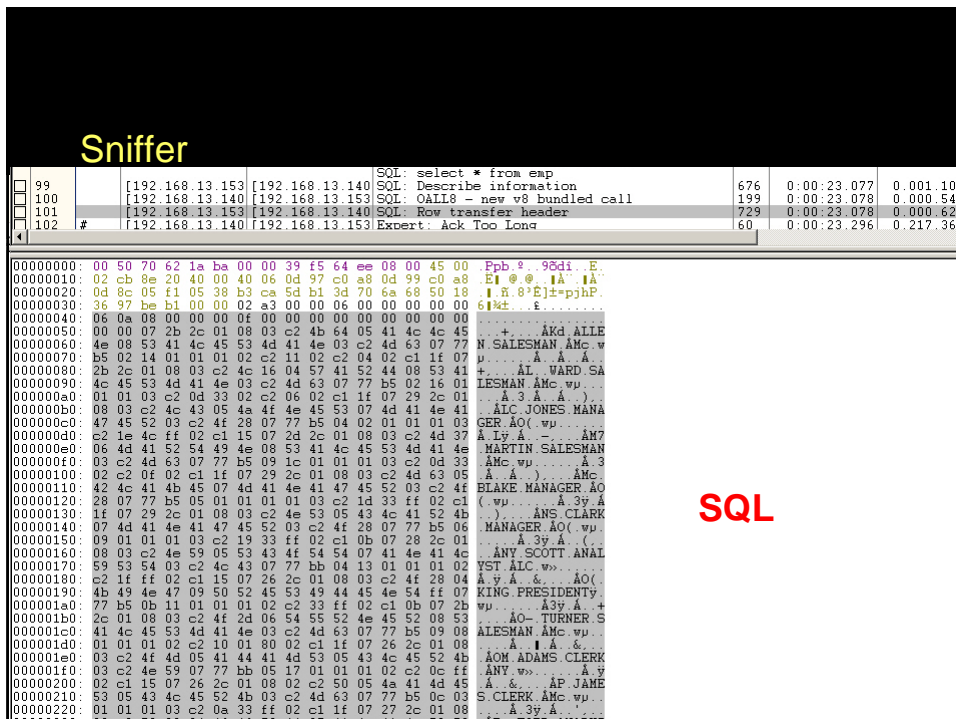
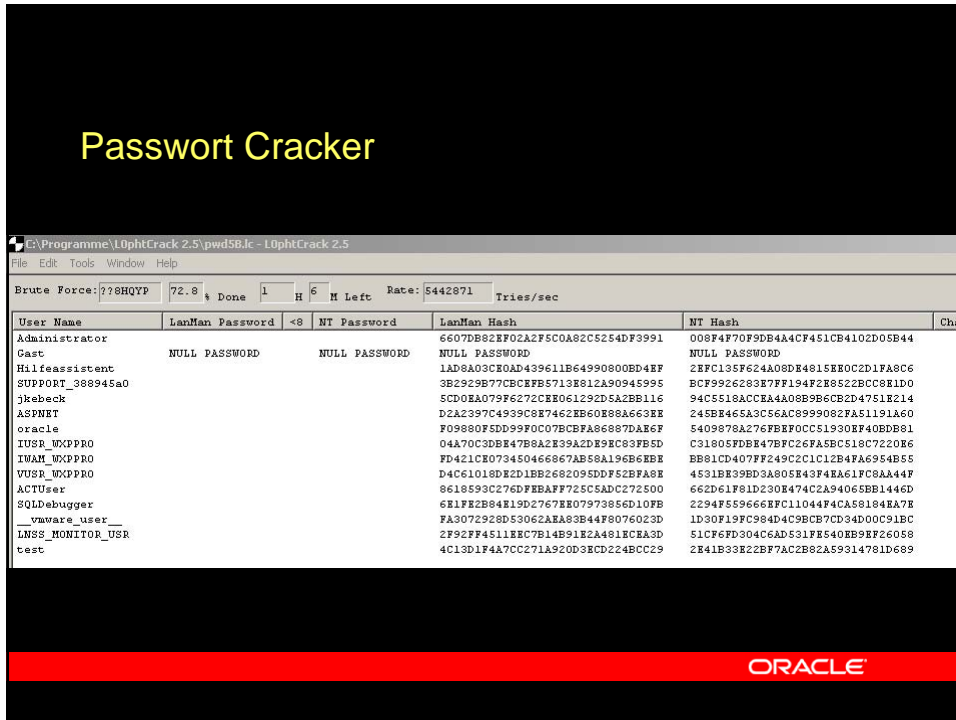
Abstract
This document describes how to write parasitic file viruses infecting ELF executables on Linux/i386. Though it contains a lot of source code, no actual virus is included.

Unfinished snapshot taken on 2002-03-14. Genie escaped the bottle.

Table of Contents
[Introduction](#)
[The magic of the Elf readelf](#)
[One step closer to the edge](#)
[The entry point](#)

Introduction





- Denial of Service (DoS bzw. DDoS)
- Keylogger
- Mailbomber
- Wireless Hacking
- Buffer Overflows
- Social Engineering

ORACLE

The screenshot displays the Norton AntiVirus 2002 interface with several overlapping 'Viruswarnmeldung' (Virus warning) dialog boxes. The background shows the 'Virendefinitionsdienst' (Virus Definitions Service) status window.

Viruswarnmeldung Details:

- Objektname: G:\Steganos Hacker
- Virename: [Hacktool.PWcrack](#)
- Aktion: Die Datei konnte nicht repariert werden.

- Objektname: E:\Daten\Oracle
- Virename: [Hacktool](#)
- Aktion: Die Datei konnte nicht repariert werden.

- Objektname: C:\Dokumente und Einstellungen\jkebeck\Desktop\...bo2k.exe
- Virename: [BackOffice2K_Trojan](#)
- Aktion: Die Datei konnte nicht repariert werden.

Virendefinitionsdienst Status:

<input checked="" type="checkbox"/> Virendefinitionen	28.03.2004
<input checked="" type="checkbox"/> Abonnement-Dienst	17.02.2005
<input checked="" type="checkbox"/> Automatisches LiveUpdate	Aktiviert

Norton AntiVirus 2002

- Firewalls
- Digitale Signaturen
- Verschlüsselung
- Virtual Private Network
- Intrusion Detection
- Honeypot-Netze
- Zugriffskontrolle
- Passwortpolicies
- Verzeichnisdienste
- Single Sign-On
- Biometrische Verfahren
- Sicherheitsrichtlinien von Geschäftsführung erlassen
- Regelmäßige Überprüfungen
- Schulungen und Weiterbildungen

ORACLE

1997 wurde die OpenPGP Working Group innerhalb der Internet Engineering Task Force gebildet (IETF Proposed Standard ([RFC 2440](#)))

The screenshot shows a Microsoft Internet Explorer browser window displaying the OpenPGP Alliance website. The address bar shows the URL <http://www.openpgp.org/resources/downloads.shtml>. The website has a blue header with the text "OpenPGP Alliance" and a navigation menu with links for "Home", "About OpenPGP", "News & Events", "Members", and "Technical". On the left side, there is a "Resources" sidebar with links for "FAQs", "Links", "Books & Media", "Mailing Lists", "Newsgroups", and "Downloads". The main content area is titled "Downloads" and contains the following text:

The best place to go for downloading free software that implements the OpenPGP standard is [The In Page](#). This site in Norway has been run by PGP activist Stale Schumacher since before PGP Inc was

To download PGP, you can rely on these trusted sites:

- [Where to find PGP](#)
Detailed information by Phil Zimmermann on where to find PGP, and what versions are available
- [www.pgpi.org](#)
International PGP home page, for freeware versions of PGP outside of US, including source code, foreign language translations of PGP and manuals.

To download source code for other OpenPGP-compliant products, try these:

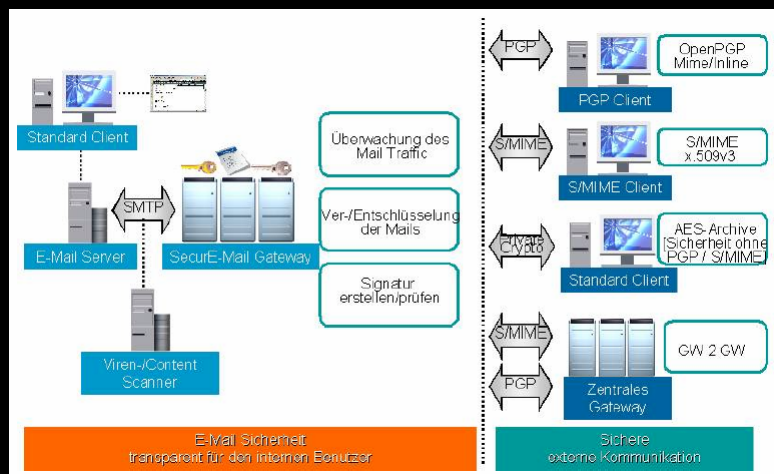
- [Gnu Privacy Guard](#)
Source code is available for this well-known open source OpenPGP-compliant product.
- [HushMail](#)
Web based encrypted email implemented as a Java applet, with free source code downloads.

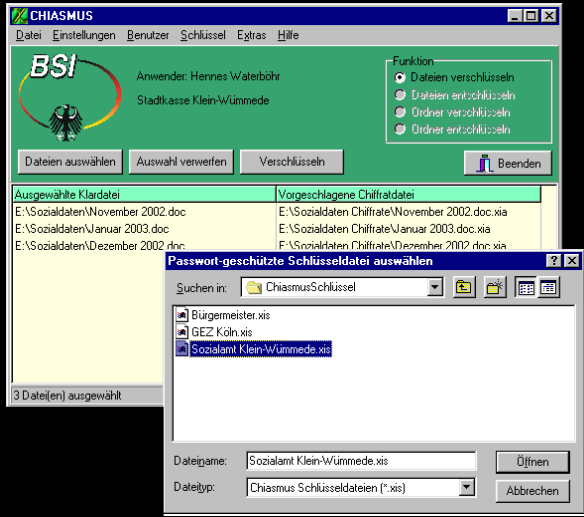
[S/MIME Version 2 Message Specification](#)
[S/MIME Version 2 Certificate Handling](#)

Achtung: Stark unterschiedliche Formate und Zertifikate

ORACLE

**Übergreifende Lösungen wie SecureE-Mail Gateway
Von Utimaco**

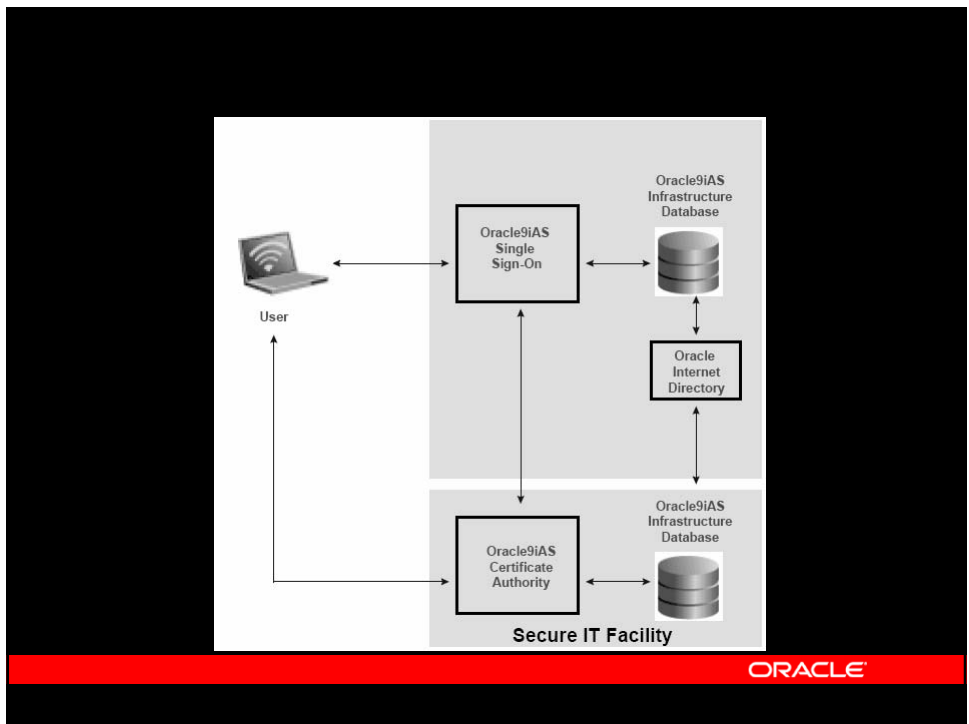




The screenshot shows the CHIASMUS application window with a menu bar (Datei, Einstellungen, Benutzer, Schlüssel, Extras, Hilfe) and a BSI logo. The main area displays a list of files and folders to be encrypted, with a 'Passwort-geschützte Schlüsseldatei auswählen' dialog box open, showing a file selection process. The dialog lists files like 'Bürgermeister.xls', 'GEZ Köln.xls', and 'Sozialamt Klein-Wümmede.xls'.

Der CHIASMUS für Windows darf grundsätzlich nur dort eingesetzt werden, wo ein öffentliches Interesse für die Nutzung besteht.

ORACLE



Oracle Advanced Security

The screenshot displays the Oracle Advanced Security configuration interface. It is divided into two main sections: Encryption (Verschlüsselung) and Integrity (Integrität). Both sections are currently configured for the 'CLIENT' user.

Encryption (Verschlüsselung) Settings:

- Integrität: CLIENT
- Checksum-Ebene: obligatorisch
- Verfügbare Methoden: AES256, RC4_256, AES192, 3DES168, RC4_128, 3DES112
- Ausgewählte Methoden: AES128

Integrity (Integrität) Settings:

- Integrität: CLIENT
- Checksum-Ebene: obligatorisch
- Verfügbare Methoden: SHA1
- Ausgewählte Methoden: MD5

ORACLE

```
00000000: 00 50 70 62 1a ba 00 00 39 f5 64 ee 08 00 45 00  Ppb 9 98di E
00000010: 02 e4 fc e9 40 00 40 06 9e b4 c0 a8 0d 99 c0 a8  aae @ | A | A
00000020: 0d 8c 05 f1 05 46 91 65 f0 df 6d 94 9e 2c 50 18  . | R F e58n | | P
00000030: 40 74 e2 b6 00 00 02 bc 00 00 06 00 00 00 00 00  @tA% . % . . . .
00000040: af 51 a1 21 4e 08 f3 df 9a 50 34 a0 00 fc 41 51  Q i N 68 P4 uAQ
00000050: 41 73 9f dc e8 7b 52 4b 92 e9 31 1e 7e c7 62 9e  A s I U e { R K e l ^ C b |
00000060: 10 b3 ac 06 0b c8 8a 20 9f 95 58 80 34 d9 51 ff  . . . | | | X | 4 U q
00000070: c6 44 1b bd 55 3b 2e 51 c1 9f a2 63 0b 7e d2 ea  ED . H U . Q A | c c ^ O e
00000080: e7 b6 e1 3a f6 ce ad 1a 6d 05 40 b5 38 fc 69 c9  c A : o I . n . @ p u i E
00000090: ec 00 7c a6 60 53 4d 8b cd 57 8a e6 93 5e 81 c1  i | | | S H | U | e | | A
000000a0: 31 16 53 7e ae 15 0a e9 8f e4 8d 5b fe ee e8 0d  i S ^ e | a | | p | e
000000b0: fd 1d bf cc 55 d3 f0 cd f0 5f 84 0b bb 45 0f 28  v . + I U O 6 | E . | . > E . (
000000c0: d2 d5 02 2b e0 4b 01 13 7c a1 0d e0 37 48 de 7a  O O + a K . | | . a 7 H b z
000000d0: 30 5d d8 13 c9 44 d8 d3 a6 63 29 ac f9 da 50 30  0 | 0 . E D 0 0 | c ) - u P 0
000000e0: 2f d7 7a aa 3e 45 5c 6f 03 e9 f2 d7 4a 87 19 07  ^ x z ^ E n o . e b x J | . .
000000f0: f4 1f fb 14 92 5a 3f b0 3f a6 3f 78 1c 52 b4 fe  o u ^ Z ? ? ? | x . R | b
00000100: ae e9 d5 9c 21 c4 80 90 33 c2 5e 26 3a 90 cf 24  @ e O | | A | | 3 A k . | | S
00000110: 47 18 72 fd e3 6d 67 29 7f ca e7 eb ba 3f be 89  G . r y a g | | E c e 8 ? % |
00000120: c4 d0 6e 0f 61 a0 02 31 77 fd 45 51 17 a0 e1 d2  AD n . a . l v y E Q . a 0
00000130: 26 e7 a4 fe 18 a2 c7 ce 1a bc 24 5f 82 af 92 90  & c h b . c c | . k 8 . | _ |
00000140: 39 fc 8b bc a4 6e 12 26 06 e4 18 7f 51 ee 66 67  9 u | k n . & a . | Q i f g
00000150: dc ec 2f 01 e9 1d a8 cc 43 5c f0 2f 08 85 8a 14  U | / e . | | C 8 / | | .
00000160: c5 ae 4c 6d 70 3c 15 6e 8c 86 ac c6 ec 02 88 f1  A 0 | L a p . n | | - E i . | R
00000170: e1 00 c7 4f 15 43 41 1d 05 8b e4 88 38 55 e6 42  a . C O C E A . O i a | 8 U e B
00000180: c0 1a 4e 60 2d 62 8c e6 12 3b d7 54 db f9 84 1a  A . N - b | e . : x T O u | .
00000190: ec 93 8e a2 2a e2 03 da 49 bd b7 df 35 bf fb 45  i | | c . a . U | % B 5 c a E
000001a0: 0b 1d e1 8a 80 63 05 e3 0f 95 be c6 41 42 62 d5  . a | | c . a . | B a R A B B o
000001b0: 77 61 24 eb e6 d6 da 3a eb 2d 44 79 d7 91 c1 95  w a s e s O U . e - D y x ^ A |
000001c0: bd 10 98 78 49 7d 84 c3 c3 d3 54 7a e1 b5 73 cf  k . | x | | | A A O T z a u s I
000001d0: 7e 4e e8 6f 32 9e 5d dc 09 8a 75 96 f9 57 cf b6  ~ N e o 2 | | U . u | u a W I M
000001e0: 58 57 54 63 83 40 ab 9d 2a 0b 70 f9 bf 94 f6 6f  X U T c | | @ * | * . p a c | c o
000001f0: 7e f0 98 7f 24 7a ce c7 2d 00 cd 04 38 af 82 71  ^ 8 | | s | z | c - l . 8 | | q
00000200: 71 37 a3 63 32 6a 09 bb ea 93 99 42 d9 58 52 94  q | f c 2 | | e | | | E U E R |
00000210: 5e 08 9d 4f 65 58 55 5c ed 3d e1 20 4e 56 90 81  | | O e R U N | e . N V | |
00000220: 5e 40 6d 31 b6 8b 23 44 c7 43 51 45 e6 32 68 80  V a | | | | U | D C C O U 2 h |
```

ORACLE

In der Oracle Datenbank: DBMS_OBFUSCATION_TOOLKIT oder DBMS_CRYPT

```

select customer_id,cust_last_name,cust_first_name,credit_card_no,
expiry_date
from customers where customer_id = 1015;

```

Ausführen Skript laden Skript speichern Abbrechen

```

select customer_id, cust_last_name, cust_first_name
into t_customer_id, t_cust_last_name, t_cust_first_name
from customers
where customer_id = 1015;
customer_encrypt.decrypt_credit_info(unencrypted_credit_card_no,
unencrypted_expiry_date, t_customer_id);
dbms_output.put_line(' ');
dbms_output.put_line('Customer First Name Customer Last
Name Customer Credit Card Expiration Date');
dbms_output.put_line(t_cust_first_name || ' ' ||

```

Ausführen Skript laden Skript speichern Abbrechen

Encryption Demonstration ----- Customer Listing and Credit Card Numbers

CUSTOMER_ID	CUST_LAST_NAME	CUST_FIRST_NAME	CREDIT_CARD_NO	EXPIRY_DATE
1015	Constantin	Velles	1234567890123411	07032000

Before select statement from customer_keys table :
Unencrypted Credit_card_no is :1234567890123411
Unencrypted expiry_date is :07032000
Customer First Name Customer Last Name Customer Credit Card Expiration Date
Constantin Velles 1234567890123411 07032000
PL/SQL procedure successfully completed.

Verschlüsselung in der Datenbank

- Datenbank-Package:
DBMS_OBFUSCATION_TOOLKIT oder
DBMS_CRYPT
- Algorithmen: Data Encryption Standard DES,
3DES, AES, RC4
- MD5-Checksummen
- GetKey-Funktion zur sicheren Erzeugung
zufälliger Schlüssel – Nicht DBMS_RANDOM
verwenden (liefert vorhersagbare Ergebnisse)

ORACLE

■ Verschlüsseln

```
dbms_obfuscation_toolkit.DES3Encrypt(
  input_string      => customer_encrypt.unencrypted_credit_card_no,
  key_string        => customer_encrypt.customer_key,
  encrypted_string  => encrypted_credit_card_no);
```

■ Entschlüsseln

```
dbms_obfuscation_toolkit.DES3Decrypt(
  input_string      => encrypted_credit_card_no,
  key_string        => incustomer_key,
  decrypted_string  => unencrypted_credit_card_no);
```

ORACLE




■ Verschlüsseln

```
raw_no :=
  UTL_RAW.CAST_TO_RAW(CONVERT(customer_encrypt.unencrypted_credit_card_no,'AL32
  UTF8','US7ASCII'));
raw_key :=
  UTL_RAW.CAST_TO_RAW(CONVERT(customer_encrypt.customer_key,'AL32UTF8','US7AS
  CII'));
encrypted_credit_card_no_raw := dbms_crypto.Encrypt(
  src => raw_no,
  typ => DBMS_CRYPTO.DES_CBC_PKCS5,
  key => raw_key);
```

■ Entschlüsseln

```
raw_no :=
  UTL_RAW.CAST_TO_RAW(convert(encrypted_credit_card_no,'AL32UTF8','US7ASCII'));
raw_key := UTL_RAW.CAST_TO_RAW(convert(incustomer_key,'AL32UTF8','US7ASCII'));
unencrypted_credit_card_no_raw := dbms_crypto.Decrypt(
  src => raw_no,
  typ => DBMS_CRYPTO.DES_CBC_PKCS5,
  key => raw_key);
```

ORACLE

Package Feature	DBMS_CRYPTO 	DBMS_OBFUSCATION_TOOLKIT
Cryptographic algorith.	DES, 3DES, AES, RC4, 3DES_2KEY	DES, 3DES
Padding forms	PKCS5, zeroes	none supported
Block cipher chaining modes	CBC, CFB, ECB, OFB	CBC
Cryptographic hash Algorithms	MD5, SHA-1, MD4	MD5
Keyed hash (MAC) Algorithms	HMAC_MD5, HMAC_SH1	none supported
Cryptographic pseudo-random nr. gen.	RAW, NUMBER, BINARY_INTEGER	RAW, VARCHAR2
Database types	RAW, CLOB, BLOB	RAW, VARCHAR2

DBMS_CRYPTO wird das DBMS_OBFUSCATION_TOOLKIT ablösen

ORACLE

Verschlüsselung ist nicht alles

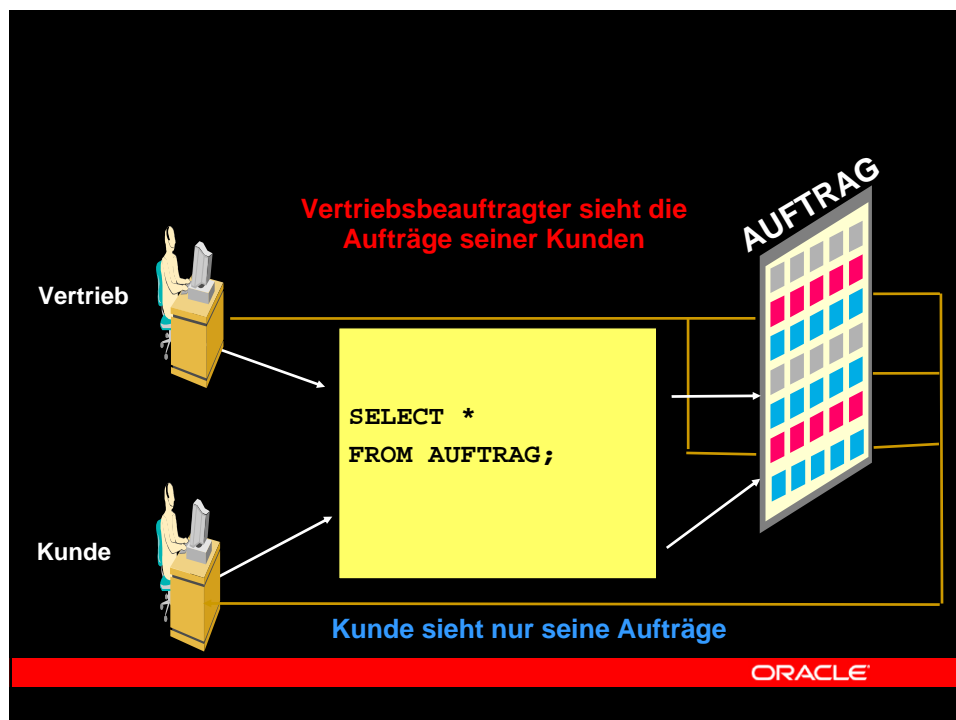
- Verschlüsselung hat nichts mit Zugangskontrolle zu tun
- Der Schutz der Vertraulichkeit von Daten gegenüber Administratoren erfordert ein sehr einfaches oder sehr komplexes Schlüsselmanagement
- Verschlüsselung kann zu einem Verfügbarkeitsproblem werden

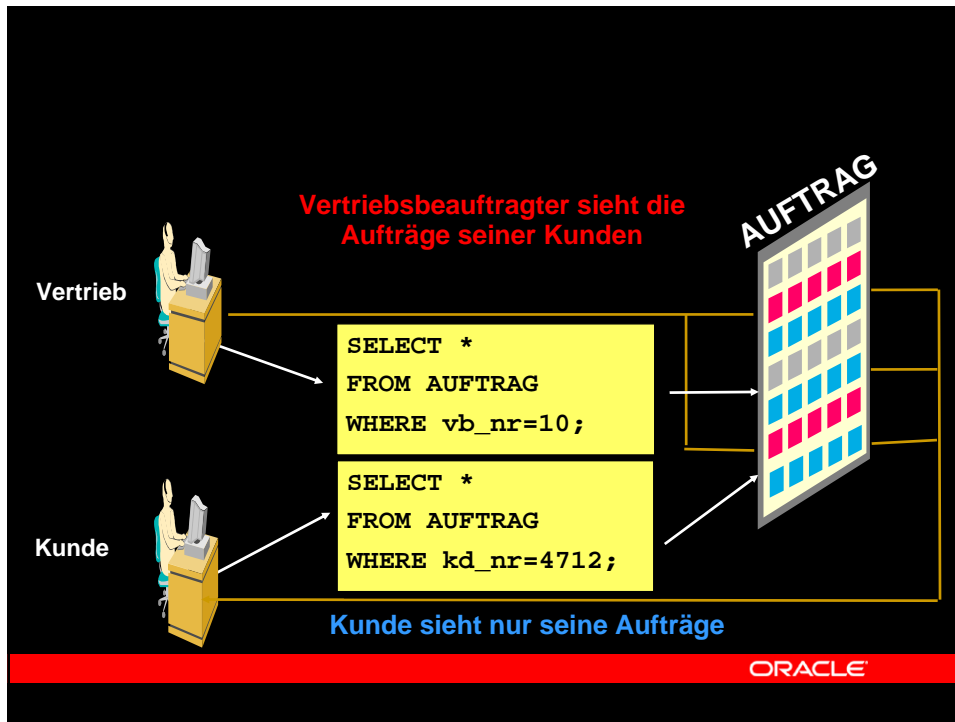
ORACLE

Herausforderungen

- Verschlüsselung indizierter Daten
- Keymanagement
 - Erzeugen
 - Verteilen
 - Speichern
 - in der Datenbank
 - im Filesystem
 - beim User
 - Wechsel
- BLOBs (bei DBMS_CRYPTO unproblematisch)

ORACLE





ORACLE

KING

Virtual Private Database

EMPNO	ENAME	JOB	MGR	HIREDATE	SAL	COMM	DEPTNO
7839	KING	PRESIDENT	-	17.11.81	5000	-	10

ORACLE

SCOTT

Virtual Private Database

EMPNO	ENAME	JOB	MGR	HIREDATE	SAL	COMM	DEPTNO
7788	SCOTT	ANALYST	7566	19.04.87	3000	-	20

Die Regelwerke können je nach Anwendung unterschiedlich sein.

ORACLE

Ein einfaches Beispiel

Sicherheitsfunktion

```
CREATE OR REPLACE FUNCTION user_only (
  p_schema IN VARCHAR2 DEFAULT NULL,
  p_object IN VARCHAR2 DEFAULT NULL)
  RETURN VARCHAR2
AS
BEGIN
  RETURN 'ename = nvl(v(''APP_USER''),USER)';
END;
```

Policy

```
BEGIN
  DBMS_RLS.add_policy
    (object_schema => 'Hannes02',
     object_name   => 'EMP',
     policy_name   => 'EMP_SEL_POL',
     function_schema => 'Hannes01',
     policy_function => 'USER_ONLY',
     statement_types => 'SELECT');
END;
```

ORACLE

Column-level VPD

```
BEGIN
  DBMS_RLS.add_policy
    (object_schema => 'Hannes02',
     object_name   => 'EMP2',
     policy_name   => 'EMP2_SEL_POL',
     function_schema => 'Hannes01',
     policy_function => 'USER_ONLY',
     sec_relevant_cols => 'sal,comm',
     statement_types => 'SELECT');
END;
```

ORACLE



neue

Arbeitsbereich
Geben Sie SQL-, PL/SQL- und SQL*Plus-Anweisungen ein.
select * from Hannes02.emp2

Ausführen Skript laden Skript speichern Abbrechen

EMPNO	ENAME	JOB	MGR	HIREDATE
7788	SCOTT	ANALYST	7566	19-APR-87

Arbeitsbereich
Geben Sie SQL-, PL/SQL- und SQL*Plus-Anweisungen ein.
select empno, ename, mgr from Hannes02.emp2

Ausführen Skript laden Skript speichern Abbrechen

EMPNO	ENAME	MGR
7369	SMITH	
7499	ALLEN	
7521	WARD	
7566	JONES	
7654	MARTIN	
7698	BLAKE	
7782	CLARK	

Column Level VPD

ORACLE

neue

Column-level VPD mit Spaltenmaskierung

```

BEGIN
  DBMS_RLS.add_policy
    (object_schema      => 'Hannes02',
     object_name        => 'EMP3',
     policy_name        => 'EMP3_SEL_POL',
     function_schema    => 'Hannes01',
     policy_function    => 'USER_ONLY',
     sec_relevant_cols  => 'sal,comm',
     sec_relevant_cols_opt => dbms_rls.ALL_ROWS,
     statement_types    => 'SELECT');
END;
    
```

ORACLE

neu

Column-level VPD mit Spaltenmaskierung

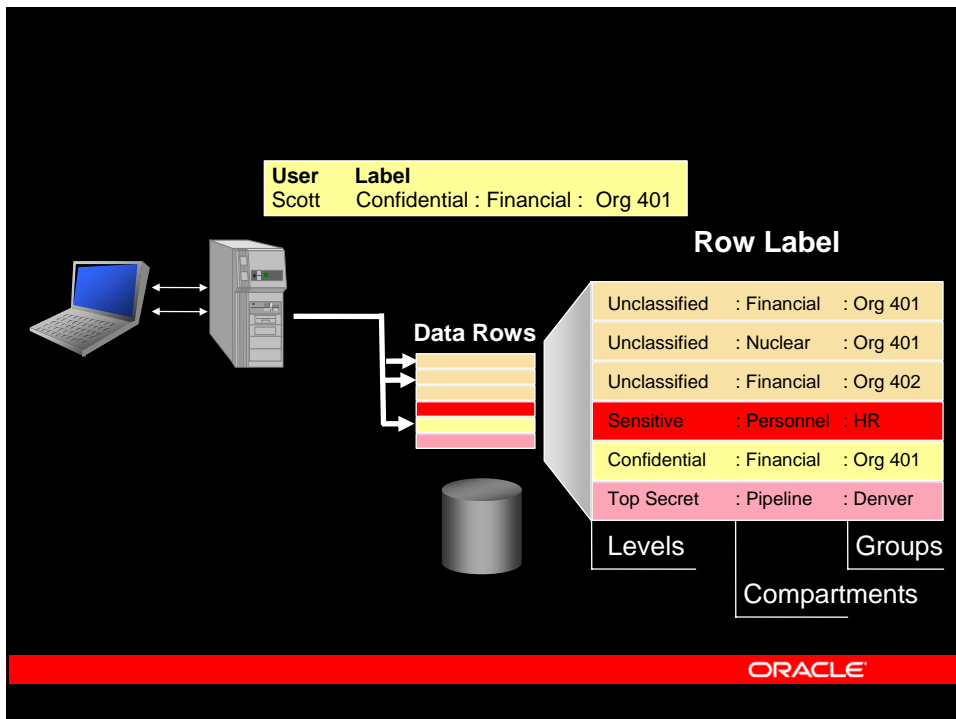
Arbeitsbereich

Geben Sie SQL-, PL/SQL- und SQL*Plus-Anweisungen ein.

```
select * from Hannes02.emp3;
```

Ausführen Skript laden Skript speichern Abbrechen

EMPNO	ENAME	JOB	MGR	HIREDATE	SAL	COMM	DEPTNO
7369	SMITH	CLERK	7902	17-DEC-80			20
7499	ALLEN	SALESMAN	7698	20-FEB-81			30
7521	WARD	SALESMAN	7698	22-FEB-81			30
7566	JONES	MANAGER	7839	02-APR-81			20
7654	MARTIN	SALESMAN	7698	28-SEP-81			30
7698	BLAKE	MANAGER	7839	01-MAY-81			30
7782	CLARK	MANAGER	7839	09-JUN-81			10
7788	SCOTT	ANALYST	7566	19-APR-87	3000		20



Levels Compartments Groups Labels

Specify the levels contained in this policy. Hit ENTER after entering a numeric value, or changing the short and long forms:

Short	Long	Numeric
U	Unclassified	100
C	Confidential	200
S	Sensitive	300
HS	Highly Sensitive	400

ORACLE

- Label Security
- Oracle Internet Directory (LDAP v3-konformer Verzeichnisdienst)
- Single Sign-On Server (Radius, Kerberos, WNA)
- Certification Authority
- Fine Grained Auditing
- Proxy Authentication
- Standardkonformität (JAAS, OASIS ...)

ORACLE

Die Leiden der IT-SichhBeauftr

ORACLE

- Die Bedeutung der IT-Sicherheit wächst beständig
- ...und immer mehr Menschen sorgen sich darum
- ...aber sie wird durch eine Vielzahl von Faktoren untergraben:
 - der Druck des time-to-market
 - kürzere product life cycles
 - neue Sicherheitsmodelle
 - Zunahme der Hacker und der automatisierten Hacking-Tools
- Wenn IT-Sicherheit so wichtig ist, warum ist sie dann nicht besser?

ORACLE

- Time-to-market
 - "Wir müssen am ... fertig sein"
- Ignoranz
 - "Das würde doch niemand tun oder?"
- Schwierigkeitsgrad
 - "Es gibt keine absolute Sicherheit"
- Einstellung
 - "Ihr Sicherheitsleute seit paranoid"

ORACLE

- "Wir müssen am ... fertig sein"
 - "Zahlt jetzt oder zahlt später!"
 - "Wie viel ist der gute Ruf wert?"
- "Das würde doch niemand tun, oder?"
 - "Doch, sie würden, sie haben es getan und sie werden es wieder tun"
- "Es gibt keine absolute Sicherheit"
 - „Es muss nicht perfekt sein, um wertvoll zu sein“
- "Ihr Sicherheitsleute seit paranoid"
 - „IT-Sicherheit ist Risikomanagement. man muss sich immer auf das schlimmste Vorbereiten und auf das Beste hoffen“

ORACLE

■ Sicherheit in der Programmierung

- Sichere Coding-Standards
- „Hacker-Tests“
- Zentrale Gruppen von Sicherheitsexperten
- Zentralisieren von querschnittlichen Sicherheits-Funktionen (z.B. Kryptographie)
- Sicherheitsregeln in der Spezifikation von Funktionen, von Design und von Tests
- Reviews des Security-Designs

■ Qualitätssicherung

- Test-Suites zur Überprüfung der Sicherheit laufen jeden Tag

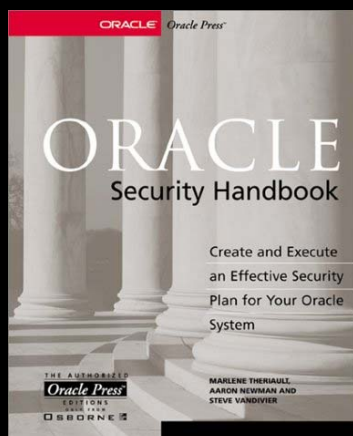
ORACLE

	Product	Release	Level	Criteria	Platform	Status
Common Criteria	OLS 9i	9.2.0.1.0	EAL4	DBMS PP	Solaris 8, NT 4.0	Evaluated
	Oracle9i	9.2.0.1.0	EAL4	DBMS PP	Solaris 8, NT 4.0	Evaluated
	OLS 8i	8.1.7	EAL4	DBMS PP	Solaris 8	Evaluated
	Oracle8i	8.1.7	EAL4	DBMS PP	Solaris 8, NT 4.0	Evaluated
	Oracle8	8.0.5	EAL4	DBMS PP	NT 4.0	Evaluated
	Oracle7	7.2.2.4.13	EAL4	C.DBMS PP	NT 3.51	Evaluated
ITSEC	Oracle7	7.3.4.0.0	E3 / F-C2	E3/F-C2	NT 4.0	Evaluated
	Oracle7	7.2.2.4.13	E3 / F-C2	E3/F-C2	NT 3.51	Evaluated
	Oracle7	7.0.13.6	E3 / F-C2	E3/F-C2	Solaris 2.2	Evaluated
	Trusted Oracle7	7.2.3.0.4	E3 / F-B1	E3/F-B1	HP-UX CMW 10.16	Evaluated
	Trusted Oracle7	7.1.5.9.3	E3 / F-B1	E3/F-B1	Trusted Solaris 1.2	Evaluated
	Trusted Oracle7	7.0.13.6	E3 / F-B1	E3/F-B1	Solaris CMW 1.0	Evaluated
TCSEC	Oracle7	7.0.13.1	C2	C2	HP-UX BLS 8.0.4	Evaluated
	Trusted Oracle7	7.0.13.1	B1	B1	HP-UX BLS 8.0.4	Evaluated
Russian	Oracle8	8.0.3	IV	Russian Criteria	HP-UX 10.20	Evaluated
	Oracle7	7.3.4	III	Russian Criteria	NT 4.0	Evaluated
FIPS	Oracle9iAS	9.0.4	2	FIPS 140-2	Solaris 8	In Evaluation
	Oracle Advanced Security	8.1.6	2	FIPS 140-1	Solaris 2.6 SE	Evaluated

ORACLE

- Oracle Technology Network
<http://otn.oracle.com/deploy/security>
- Oracle By Example
<http://otn.oracle.com/obe>
- Oder bei mir:
johannes.kebeck@oracle.com

ORACLE

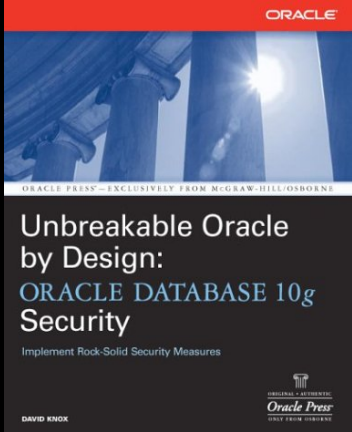


Oracle Press™ Books

Oracle Security Handbook
by Marlene Theriault and
Aaron Newman
ISBN: 0-07-213325-2, US \$59.99

A comprehensive guide to
implementing a sound security
plan in your Oracle environment.

ORACLE



Oracle Press™ Books

**Unbreakable Oracle by Design:
Oracle Database 10g Security**

by David Know
ISBN: 0-07-223130-0, US \$59.99

ORACLE

- Digitale Signatur
Deutsche Post Signtrust, Smarttrust, Entrust, Baltimore, ...
- Verschlüsselung in der Datenbank
Protegrity, Siemens
- SSL Hardware
nCipher
- Policy Management
Netegrity
- Consulting, Konzepte, PenTest
@stake

ORACLE

