© 2003 Michael Heitkötter, Oracle Corporatio

Have you been reading the news lately???

© 2003 Michael Heitkötter, Oracle Corporatio

In the news

- 3/15/03 – Former Employees Allegedly Hacked Company System Through Old Accounts
- 3/13/03 - Memory Stick Contained Patient Data
- 3/06/03 - University of Texas Cyber Security Breach Exposed Information About 55,000 People
- 3/06/03 - Bank Account Access Problem Exposes Princeton University's Accounts
- 2/28/03 - Company Shuts Down After Serious Security Breach
- 2/21/03 - Banks Cancel Cards After Security Breach
- 2/17/03 - Confidential Canadian Documents Exposed
- 2/12/03 - FTD.com Exposes Customer Data
- 2/06/03 - Website Tells How to Hack London's Traffic Signals

Source: http://www.sans.org/newsletters/newsbites/

© 2003 Michael Heitkötter, Oracle Corporatio

This just in…

(17/18 February 2003)
-- Millions of Credit Card Numbers May Have Been Compromised
A hacker broke into the computer system of a company that processes credit card transactions, gaining access to more than 8 million Visa, MasterCard, American Express and Discover accounts…

This is the largest known credit card compromise to date…

(29/30 January 2003)
Attorneys have filed a class action lawsuit against Tri-West Healthcare after hard drives containing personal information about more than 500,000 customer were stolen. The lawsuit seeks monetary damages and asks that Tri-West pay for monitoring the credit reports of all those affected by the theft for the next twenty years.

Source: http://www.sans.org/newsletters/newsbites/

© 2003 Michael Heitkötter, Oracle Corporatio

Big Brother is listening

Every word of every message intercepted at each station gets automatically searched - whether or not a specific telephone number or e-mail address is on the list.

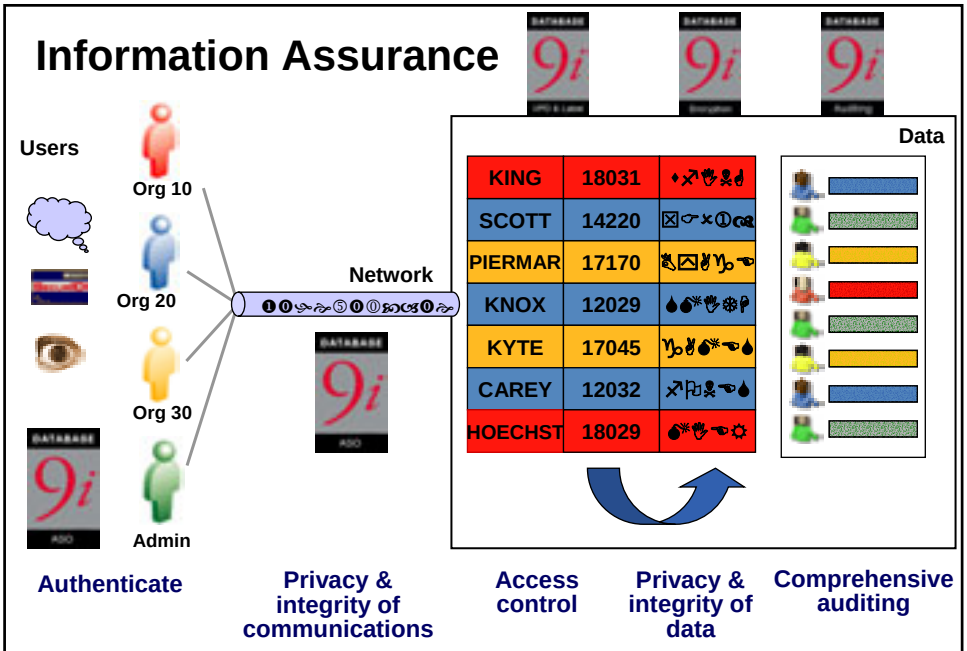
© 2003 Michael Heitkötter, Oracle Corporatio

Top Security Myths

- Myth: Hackers cause most security breaches.
- *Fact: 80% of data loss is to insiders.*
- Myth: Encryption makes you secure.
- *Fact: Security includes access control, data integrity, encryption, and auditing.*
- Myth: Firewalls make you secure.
- *Fact: 40% of Internet break-ins occur where there is a firewall in place.*

© 2003 Michael Heitkötter, Oracle Corporatio

Information Assurance



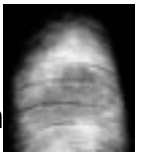
© 2003 Michael Heitkötter, Oracle Corporatio

AUTHENTICATION

© 2003 Michael Heitkötter, Oracle Corporatio

Oracle9*i* Authentication

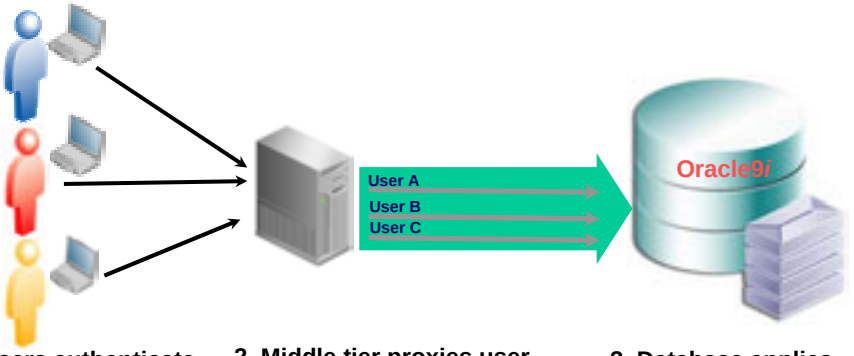
- Password-based authentication
- Strong authentication with 3rd party industry leaders
  - Kerberos, CyberSafe, DCE
  - Token cards (SecurID), biometrics
  - RADIUS: *any* auth vendor can integrate (sm cards, fingerprints, voice, etc.)
- Strong authentication within digital certificates
  - X.509v3 certificates and SSL in a PKI
- Single sign-on functionality



© 2003 Michael Heitkötter, Oracle Corporatio

Identity Preservation – Proxy Authentication

Security cannot be based on anonymity!



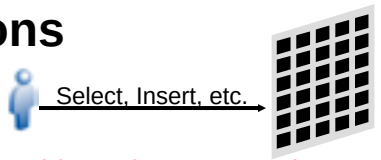
1. Users authenticate to middle tier

2. Middle tier proxies user identity to database

3. Database applies authorizations, access control, and auditing for real end user

© 2003 Michael Heitkötter, Oracle Corporatio

Database Authorizations



- Object or system privileges granted to roles
- Roles granted to users for ease of administration
- Roles enabled by default or “turned on” by application
- Protected by password
- Challenges
  - Application controls database privileges
  - Sharing password among applications is not easy, practical, or secure

© 2003 Michael Heitkötter, Oracle Corporatio

Oracle9*i* Secure Application Role

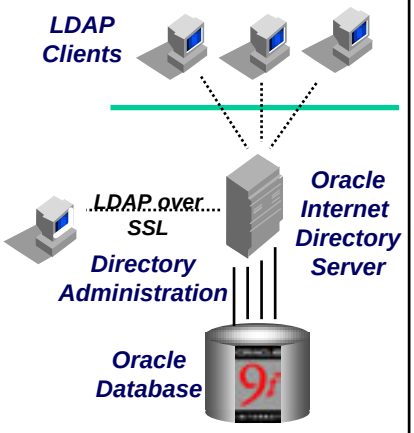
- Secure application role is a role enabled by security code
- Application asks database to enable role (can be called transparently)
- Security code performs desired validation before setting role (privileges)

© 2003 Michael Heitkötter, Oracle Corporatio

Oracle Internet Directory

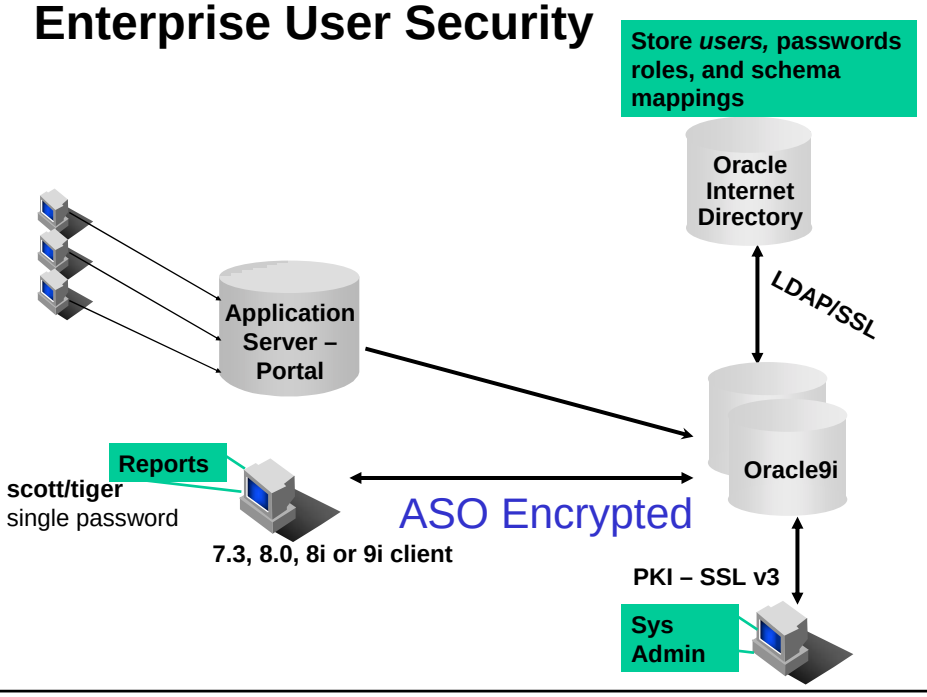
Scalable and Secure Enterprise User Management

- Directory backbone for Oracle Advanced Security
- Native LDAP v.3
- Synchronize data between various directories and OID
- Interoperable with third party LDAP products such as Novell Directory Services (NDS)
- Centralize user credentials and database privileges for single sign-on
- 500+ million users, 1000's of concurrent clients on a single server

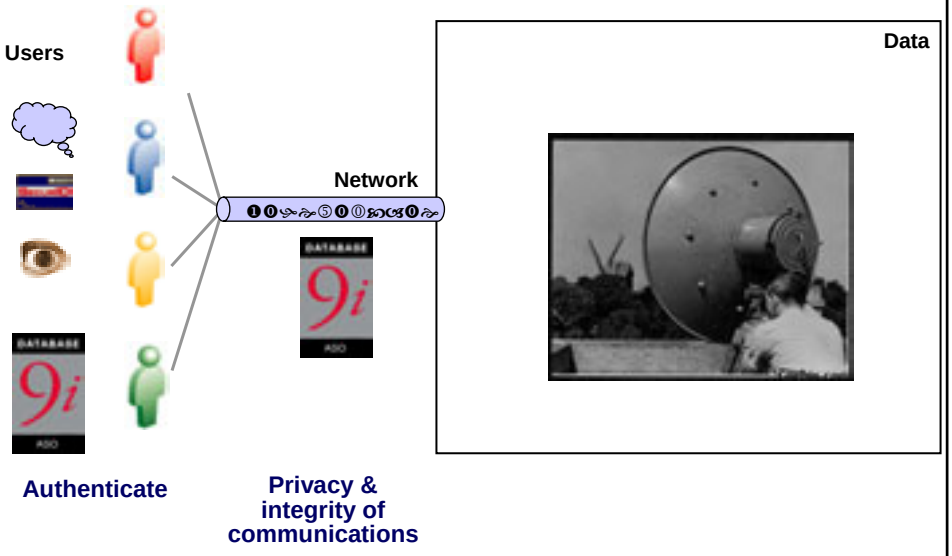


© 2003 Michael Heitkötter, Oracle Corporatio

Enterprise User Security

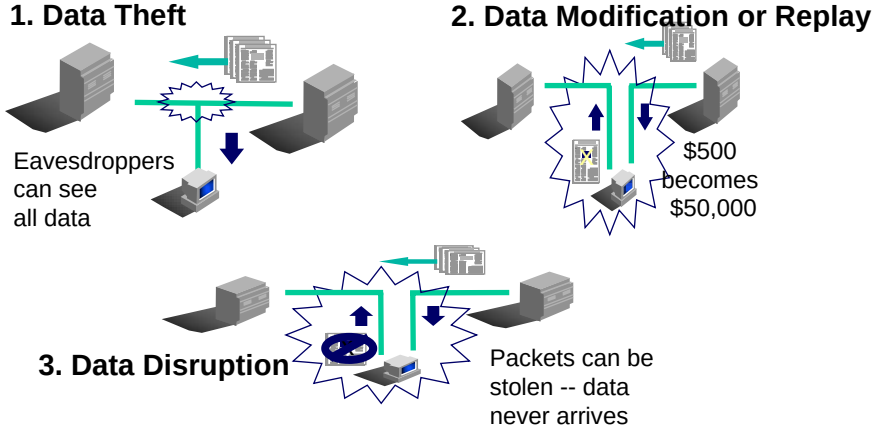


Secure in Transmission



© 2003 Michael Heitkötter, Oracle Corporatio

Threats to Networks and Internet



© 2003 Michael Heitkötter, Oracle Corporatio

Oracle Advanced Security

1. Network encryption & integrity
   - Includes AES and SSL
   - FIPS140-1 level 2 evaluated
2. Strong authentication of end users, clients and servers
   - Kerberos, biometrics, tokens, RADIUS
3. Identity management/Centralized users
   - Lowers cost of user administration
   - LDAP-standard
   - Extensible
   - Protected by SSL

ORACLE
© 2003 Michael Heitkötter, Oracle Corporatio

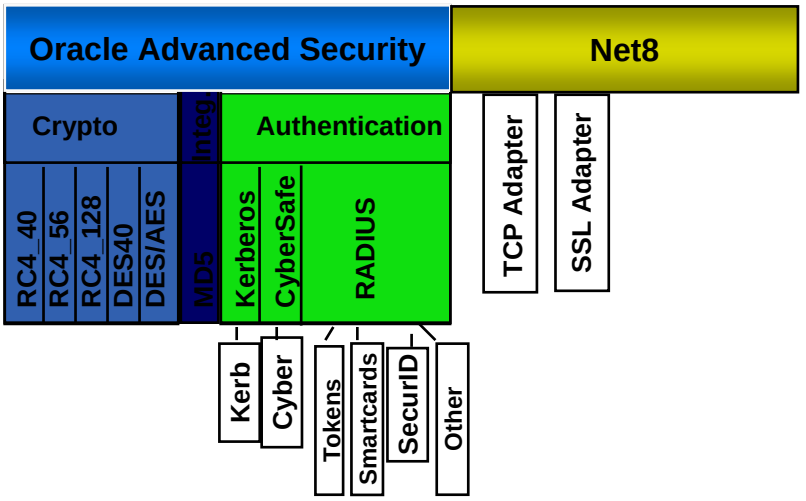
"Native" Net8 Encryption

worldwide available

- Advanced Security Option (ASO) encrypts all communications with the database using standard algorithms
  - RSA RC4 (40-, 56-, 128- and 256-bit Key)
  - DES (40-, 56-bit) and 3DES
  - AES (256-bit)
  - Diffie-Hellman for key exchange
  - The strength of cryptography depends on keymanagement
  - By default, no keymanagement when using encryption

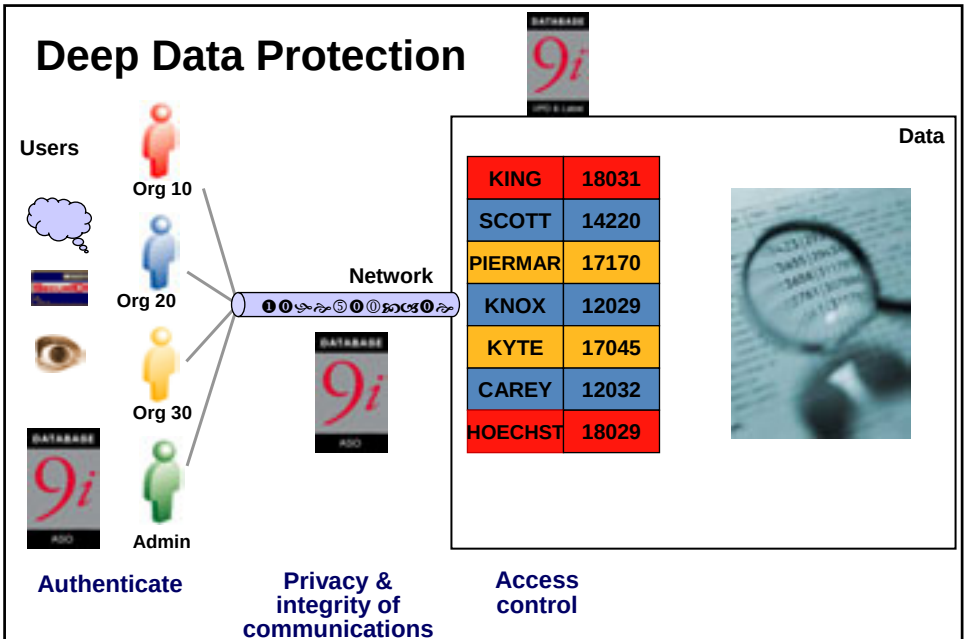
ORACLE
© 2003 Michael Heitkötter, Oracle Corporatio

ASO Architecture



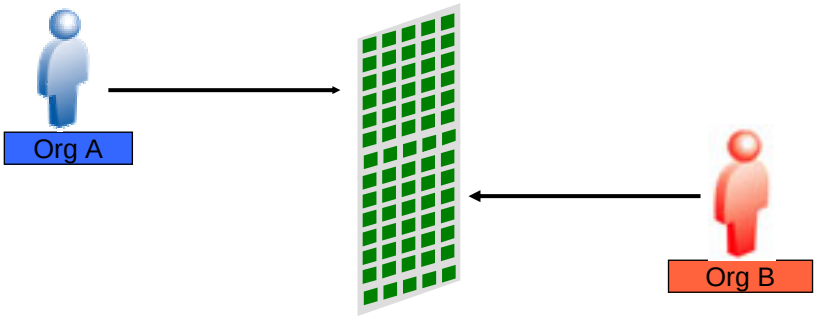
© 2003 Michael Heitkötter, Oracle Corporatio

Deep Data Protection



© 2003 Michael Heitkötter, Oracle Corporatio

Object Access Control

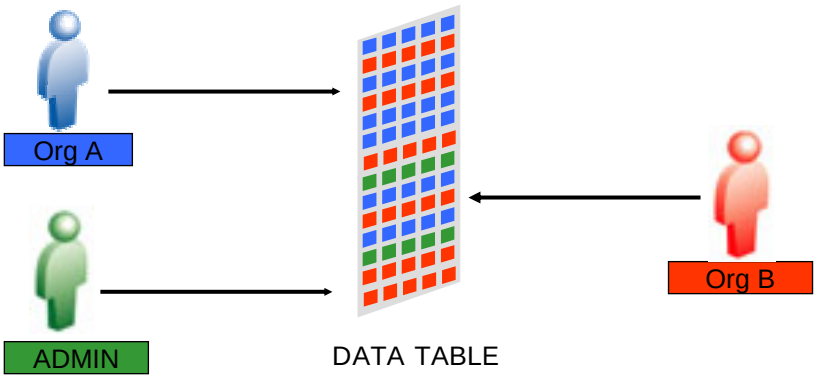


DATA TABLE

ORACLE
© 2003 Michael Heitkötter, Oracle Corporatio

Fine Grained Access Control

A.K.A. Row-level Security



DATA TABLE

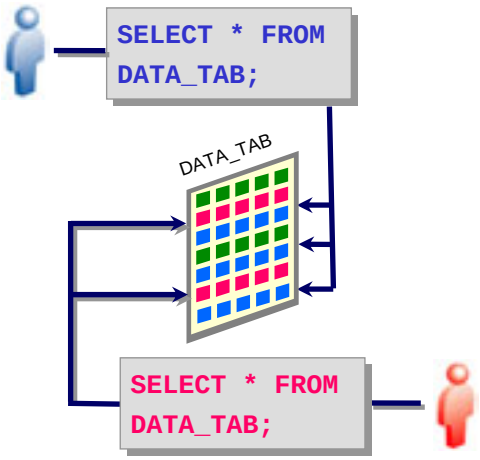
ORACLE
© 2003 Michael Heitkötter, Oracle Corporatio

Fine-Grained Access Control: Enforcement Mechanisms

- Application Enforcement
  - Subject to errors
  - Enforced within application only
  - Requires changes to all applications when policy changes
  - Expensive to maintain
- Server Enforcement
  - Well-defined
  - Strictly enforced, no exceptions
  - No changes to applications when policy changes
  - Easy to manage/verify

© 2003 Michael Heitkötter, Oracle Corporatio

Virtual Private Database (RLS)

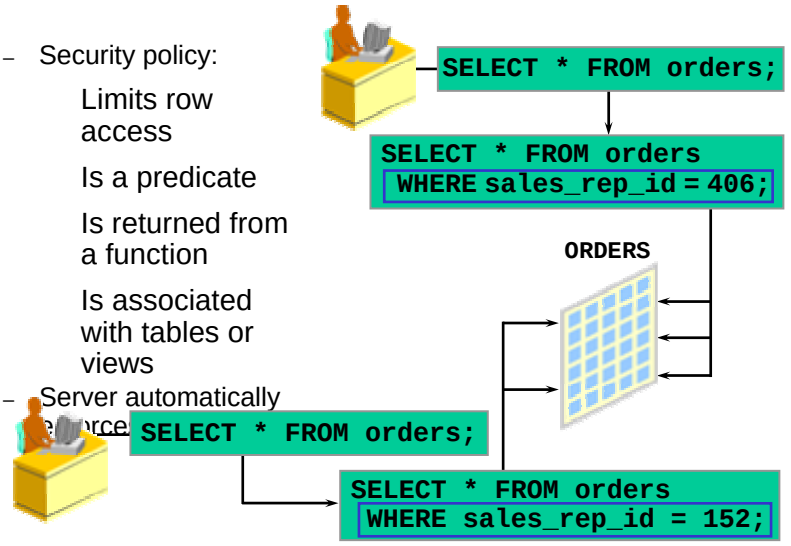


- Multiple policies
- Different policies for different operations
- Simplifies application development
- Security cannot be by-passed
- Scalable via secure attribute cache
- Better manageability
  - Better than Views
  - Better than multiple applications

© 2003 Michael Heitkötter, Oracle Corporatio

VPD - Overview

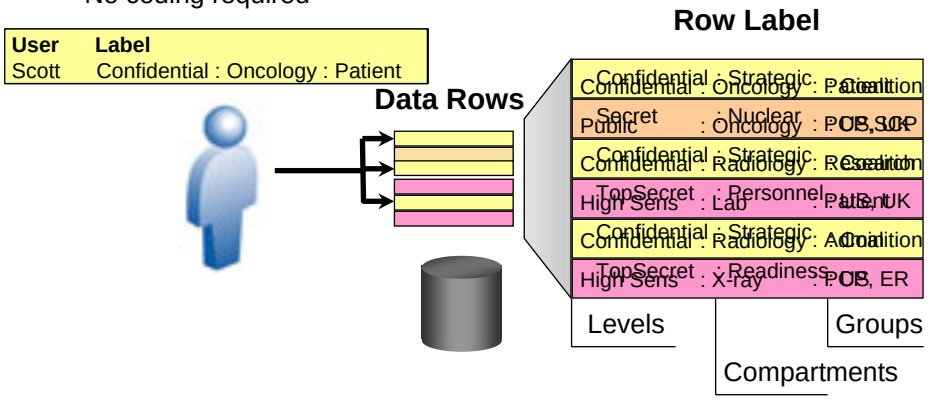
- Security policy:
  - Limits row access
  - Is a predicate
  - Is returned from a function
  - Is associated with tables or views
- Server automatically enforces



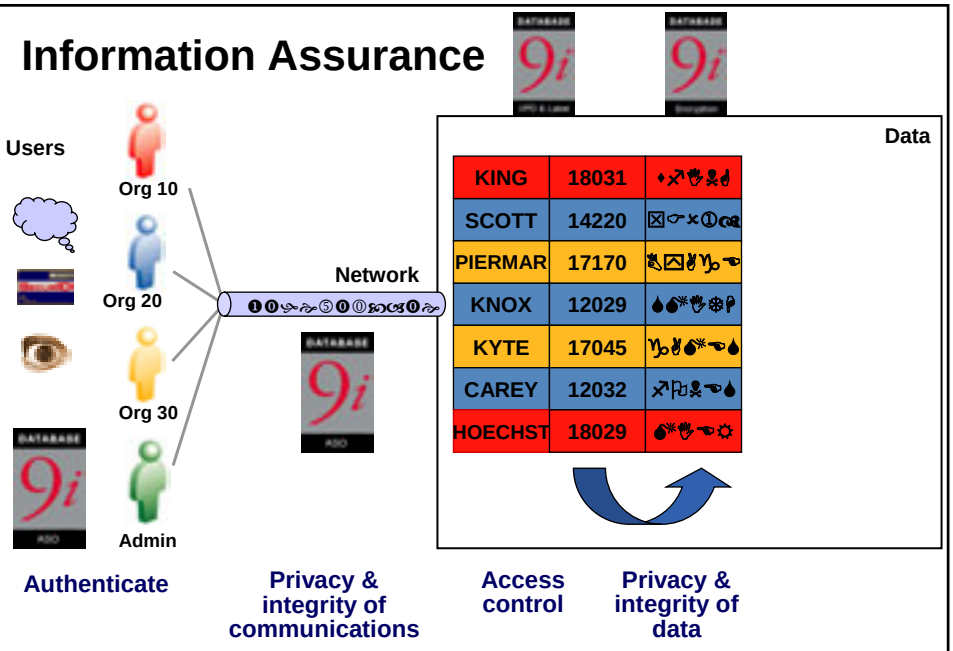
© 2003 Michael Heitkötter, Oracle Corporatio

Oracle Label Security

- Based on VPD, grew out of accredited consulting work and over seven years of MLS efforts
- Off-the-shelf label based RLS system
- GUI for administration
  - No coding required



Information Assurance



© 2003 Michael Heitkötter, Oracle Corporatio

Stored Data Encryption

- Requirement
  - Selective encryption of sensitive data (e.g., ssn, ccn, diagnosis)
  - hackers compromising the operating system and reading database/log files
  - malicious DBA
- Features
  - Data Encryption Standard (DES)
  - Triple-DES
  - MD5 cryptographic checksum

		Encrypted SALARY
KING	10	♦➚✋✌
SCOTT	20	☒☞✕①♋
BLAKE	30	✍🖂✌♍☜
SMITH	20	♠💣✳✋❄☤
JAMES	30	♍✌💣✳☜♠
JONES	20	➚⚐✌☜♠
MILLER	10	💣✳✋☜☼

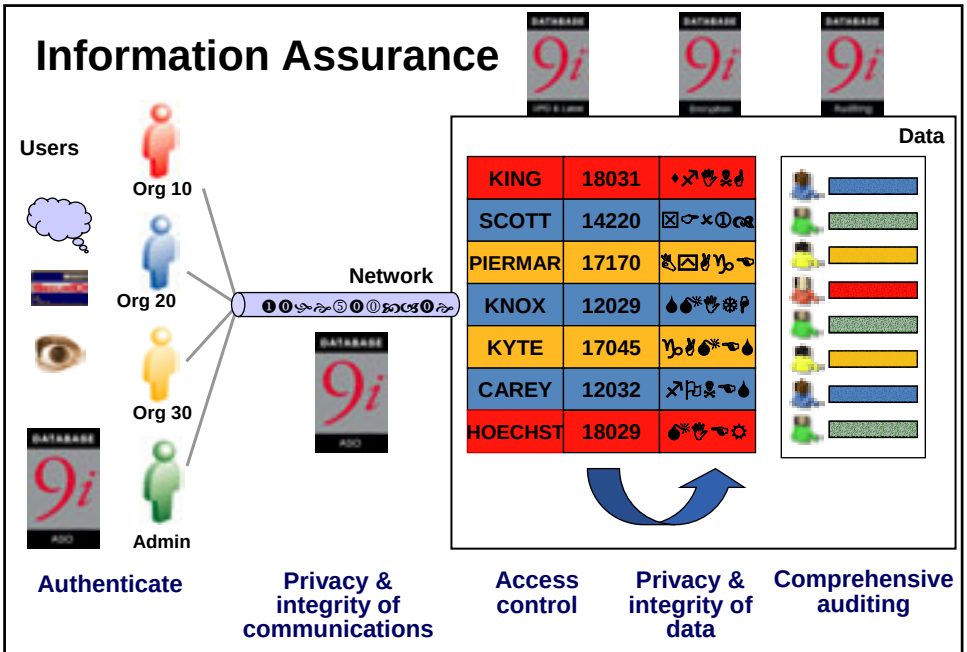
© 2003 Michael Heitkötter, Oracle Corporatio

DBMS_OBFUSCATION_TOOLKIT Package

- Functionality
  - Random number generation for encryption keys
  - Encryption and decryption using Data Encryption Standard (DES)
  - Encryption and decryption using triple DES (3DES)
  - Hashing using the MD5 cryptographic hash
- Procedures and functions in the package include:
  - `DESGetKey` and `DES3GetKey` create random keys
  - `DESEncrypt` and `DES3Encrypt` encrypt columns
  - `DESDecrypt` and `DES3Decrypt` decrypt columns
  - `MD5` creates a checksum on a column
- Routine are overloaded for maximum flexibility

© 2003 Michael Heitkötter, Oracle Corporatio

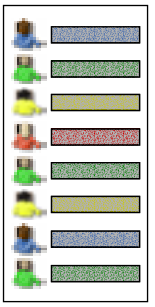
Information Assurance



© 2003 Michael Heitkötter, Oracle Corporatio

Security Processes: Prevention, Detection and Response

- Prevention
  - Authentication, Access Controls
- Detection and Response
  - Database Auditing
  - Audit by user, by object, by privilege
  - Capture Successful and Unsuccessful actions
- Audit Improvements
  - Minimize audit data
  - Capture user's intent (query)
  - See resulting data set



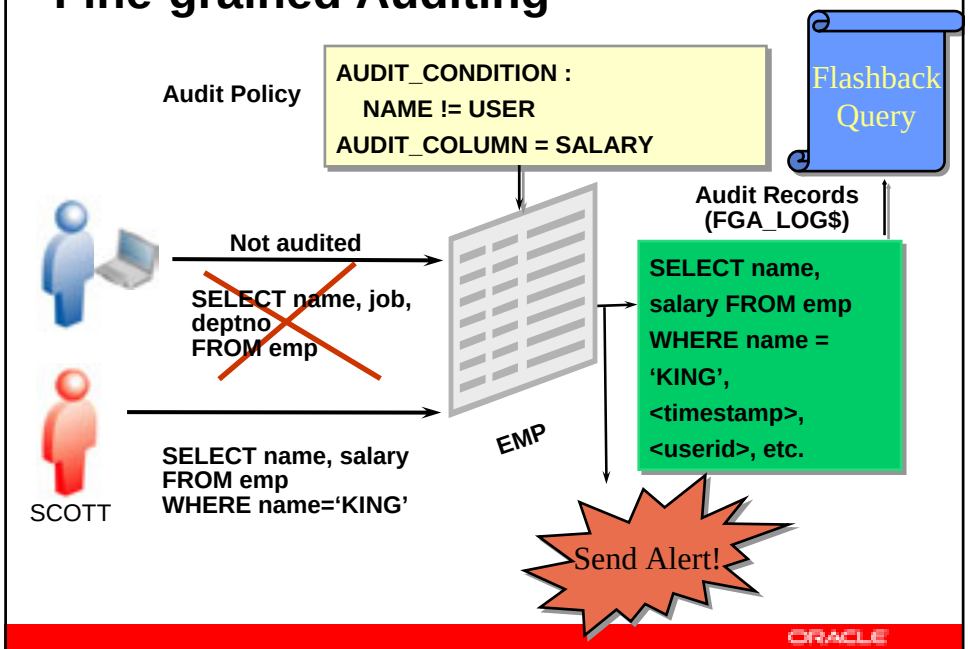
© 2003 Michael Heitkötter, Oracle Corporatio

Auditing Guidelines

- Define what you want to audit
  - Audit users, statements, or objects
  - Statement executions
  - Successful statement executions, unsuccessful statement executions or both
- Manage your audit trail
  - Monitor the growth of the audit trail
  - Protect the audit trail from unauthorized access

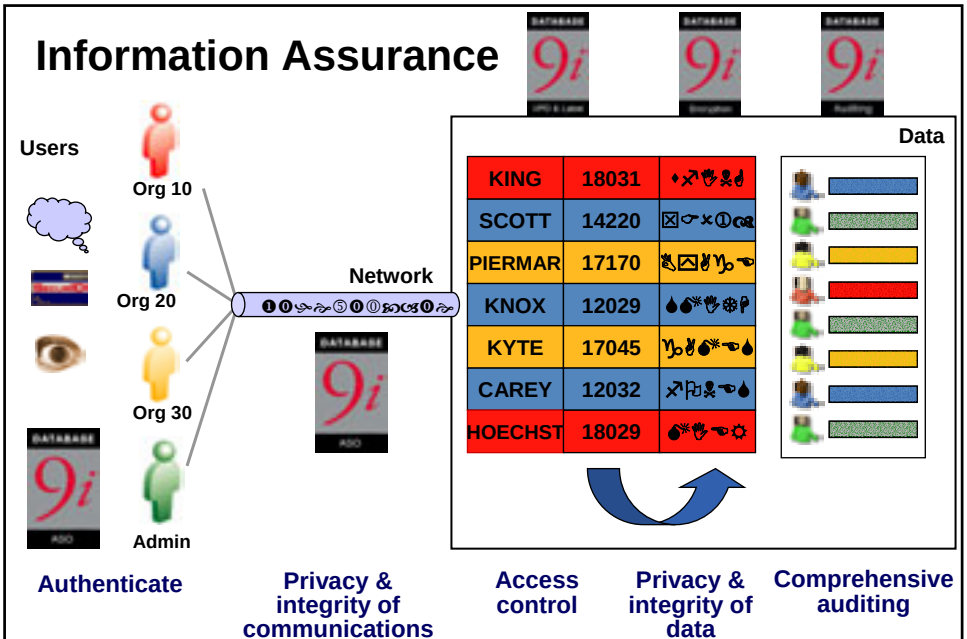
© 2003 Michael Heitkötter, Oracle Corporatio

Fine-grained Auditing



© 2003 Michael Heitkötter, Oracle Corporatio

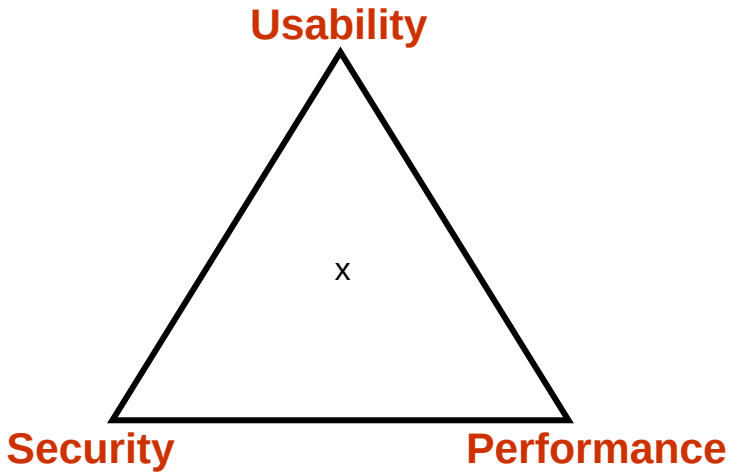
Information Assurance



© 2003 Michael Heitkötter, Oracle Corporatio

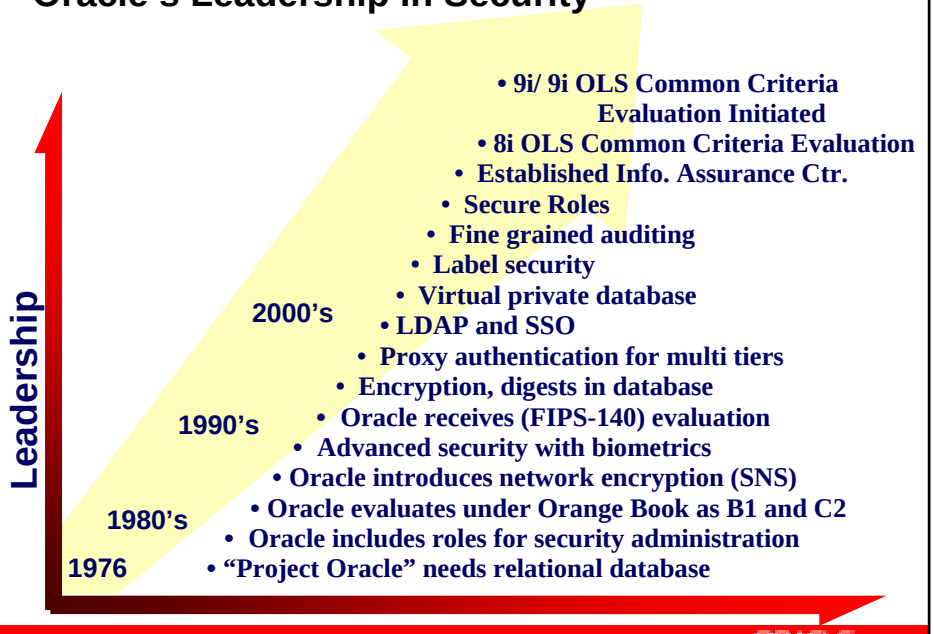
Balancing Requirements

Need flexibility to adjust to current situation



© 2003 Michael Heitkötter, Oracle Corporatio

Oracle's Leadership In Security



© 2003 Michael Heitkötter, Oracle Corporatio

Security Certification

	Product	Release	Level	Criteria	Platform	Status
Common Criteria	Oracle9*i*, 9*i* OLS	9.2.0.1.0	EAL4	ISO 15408	Solaris 8, NT 4.0	Started
	OLS 8*i*	8.1.7	EAL4	ISO 15408	Solaris 8	Evaluated
	Oracle8*i*	8.1.7	EAL4	ISO 15408	Solaris 8, NT 4.0	Evaluated
	Oracle8	8.0.5	EAL4	ISO 15408	NT 4.0	Evaluated
	Oracle7	7.2.2.4.13	EAL4	C.DBMS PP	NT 3.51	Evaluated
	Oracle7	7.2.2.4.13	*Trial* EAL3	C.DBMS PP	NT 3.51	Completed
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	Oracle Advanced Security	8.1.6	2	FIPS 140-1	Solaris 2.6 SE	Evaluated

© 2003 Michael Heitkötter, Oracle Corporatio

How important is security?

- „A survey by Forrester Group showed that the average company‘s percentage revenue spend on IT security was 0.025%.

  This is less than they spend on coffee.“

Richard Clarke, president George W Bush‘s advisor on Internet Security

© 2003 Michael Heitkötter, Oracle Corporatio

“If you spend more on coffee than on IT security, then you will be hacked
…what's more, you deserve to be hacked!”

Richard Clarke, 2002
Special Advisor to the President, Cyberspace Security

© 2003 Michael Heitkötter, Oracle Corporatio

Security Vulnerabilities

with Oracle9i you can…

- ✓ Be confident your security solution is proven
- ✓ Protect data across the infrastructure
- ✓ Manage and scale user accounts efficiently
- ✓ Control access to sensitive information
- ✓ Track user activity
- ✓ Securely share applications and information within the same database
- ✓ Enforce compliance of privacy laws

© 2003 Michael Heitkötter, Oracle Corporatio

Oracle Security Resources

for more information:

- Security alert
  - http://otn.oracle.com/deploy/security/alerts.htm
- Security patches
  - http://metalink.oracle.com
- Oracle Partner information
  - http://partner.oracle.com/DIReview
- Oracle Partner Resource Network
  - http://opn.oracle.com
- Oracle Technology Network
  - http://otn.oracle.com
- Oracle home page
  - http://www.oracle.com

© 2003 Michael Heitkötter, Oracle Corporatio

© 2003 Michael Heitkötter, Oracle Corporatio