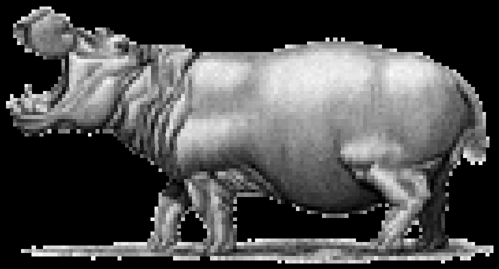
ORACLE®

SOFTWARE POWERS THE INTERNET

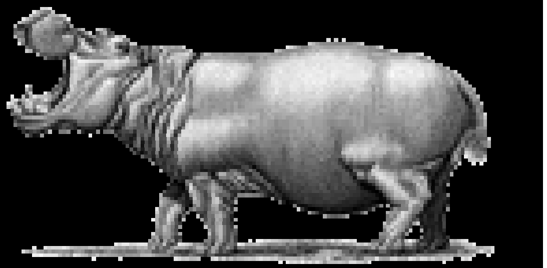
HIPAA Privacy and Security



Richard Wark
Product Technologist - Security Technologies

“Nothing is more private than someone's medical or psychiatric records. And, therefore, if we are to make freedom fully meaningful in the Information Age, when most of our stuff is on some computer somewhere, we have to protect the privacy of individual health records.”

- Bill Clinton



ORACLE

Agenda

- Overview of Privacy/Security HIPAA issues, and the “threat”
- Technologies:
  - Authentication/User Management
  - Access Control and Encryption
- Product Evaluations
- Summary
- Q & A

HIPAA Issues - Privacy and Security

- Privacy & integrity of communications
- Strong user authentication
- Access control and audit
- User account management
- Formal Product Evaluations

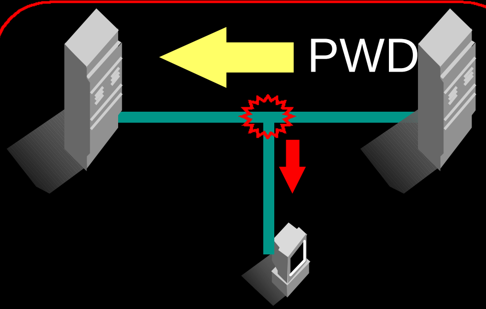
The Threat:

Fortune 1000 Survey

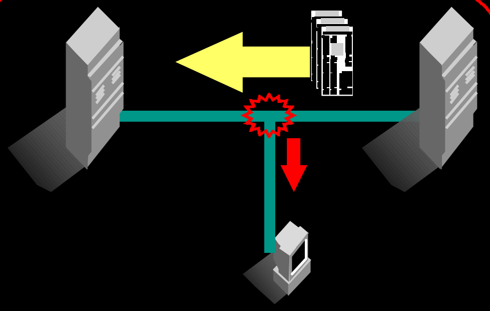
- 90% detected security breaches
- 60% External, 40% Internal
- 71% detected unauthorized access by insiders
- Average loss per intrusion:
  - External : $57,000
  - Internal: $2,700,000

Source: 2000 Computer Security Institute and FBI Survey

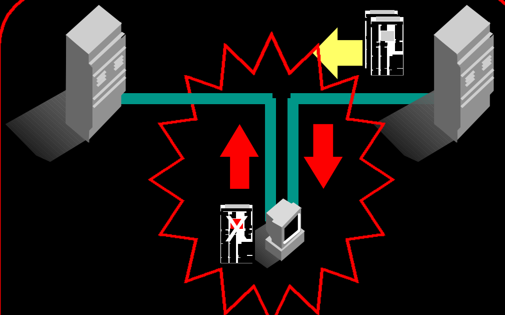
Common Security Breaches



PASSWORD SNOOPING



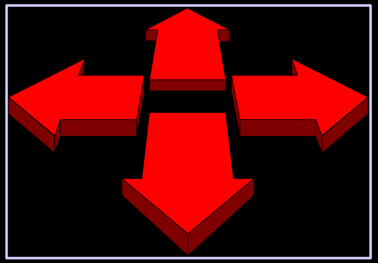
DATASTREAM SNOOPING



DATASTREAM MODIFICATION

ESTABLISHING USERS & AUTHORIZATIONS

USERS HAVE TOO MANY PASSWORDS



DISTRIBUTED SECURITY ADMINISTRATION

Federal Security Directives

- **Critical Infrastructure Protection**
  - Banking & Finance
  - Communications & Utilities
  - Government Operations
- **Security Evaluations**
  - Common Criteria
  - FIPS 140-1
  - NSTISSC Policy # 11
- **Public Key Infrastructure**
  - Digital Certificates
  - LDAP
- **HIPAA**
  - Health Information Privacy

Efficiency Through Standardization

Electronic Processes

- claims: ASC X12N 837
- claims: NCPDP
- enrollment: ASC X12N 834
- eligibility: ASC X12N 270/271
- remittance: ASC X12N 835
- premium: ASC X12N 820
- referrals: ASC X12N 278
- claim status: ASC X12N 276/277

Identifiers

- providers (NPI)
- plans (Payer ID)
- individuals (UHID)
- employers (EIN)

Security Standards

- access control
- authorization control
- data authentication
- entity authentication
- network safeguards
- physical safeguards

Medical Codes

- hospital (ICD-9-CM)
- physician (CPT-4)
- non-institutional (HCPCS)
- dental (CDT-2)
- drugs (NDC)

Language/Terminology

- including electronic signature
- medical terminology
- reporting (CDE)
- practitioner classifications

Security Standardization

Security Standards

- **access control - Label Based Access**
- **authorization control - LDAPv3 ACLs**
- **data authentication - MD-5 or SHA-1**
- **entity authentication - PKI or Biometric**
- **network safeguards - Firewalls and IDS**
- **physical safeguards - Plan and Follow**

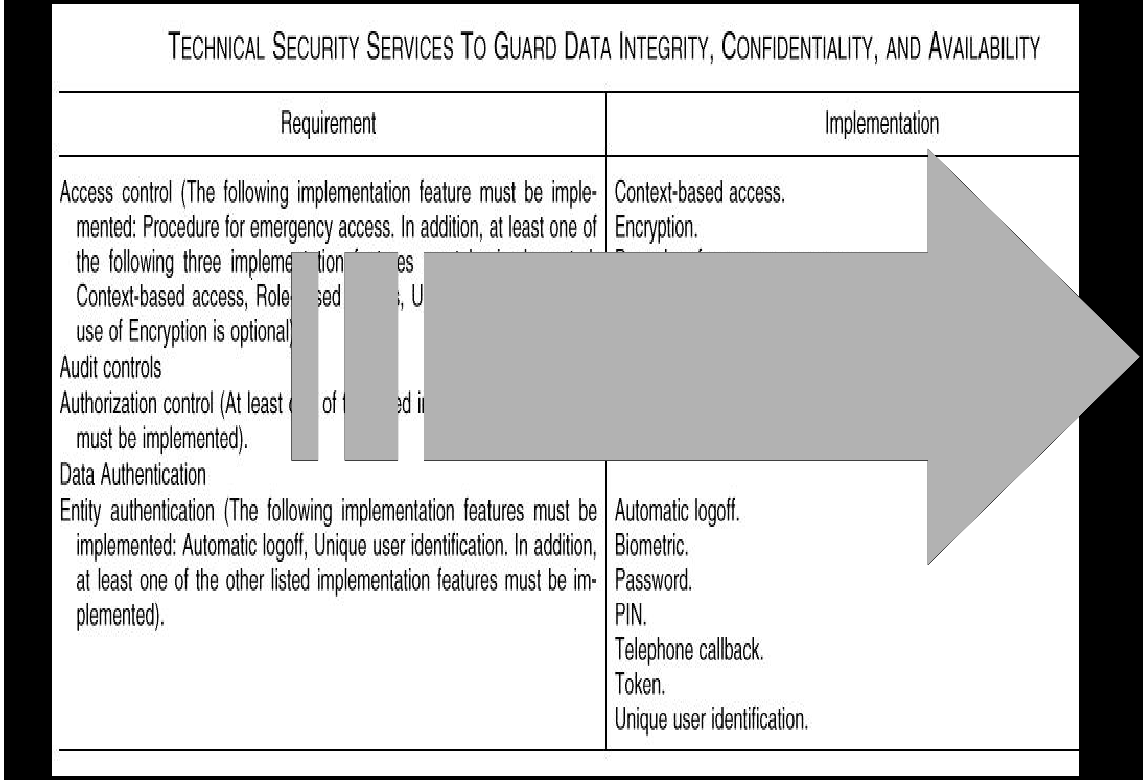
Key benefits: interoperability and assurance

Enterprise Security Issues

- Strong user authentication → *Smartcards, biometrics, - PKI (X.509v3 Certificates)*
- Privacy & Integrity of communications → *Encryption (RC4, DES, MD5, etc.)*
- Access control → *Fine-grained Access Control Policies-Auditing*
- User Account Management → *LDAP Directory Integration*
- Flexibility & Cost Avoidance → *Security Standards (FIPS 140, Common Criteria)*

Oracle and HIPAA

Mandates



TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY

Requirement	Implementation
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three impleme tion es Context-based access, Role sed , U use of Encryption is optional)	Context-based access. Encryption.
Audit controls	
Authorization control (At least of ed i must be implemented).	
Data Authentication	
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented).	Automatic logoff. Biometric. Password. PIN. Telephone callback. Token. Unique user identification.

Solutions

- Oracle8i
- Oracle Advanced Security
- Oracle Label Security
- Oracle Internet Directory

Oracle8*i* Security Features

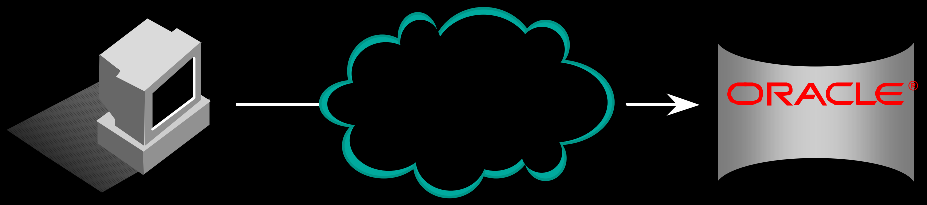
- Identification & Authentication
  - OS or DBMS Login
  - Password Management
- Access Control and Confidentiality
  - Privileges and Roles, Views, Triggers
  - Fine-grained Access Control
  - Database Encryption
- User / Resource Management
  - LDAP / Enterprise Domains (via Oracle Internet Directory and Advanced Security)
- Auditing
  - 200+ auditable events, triggers, etc.
  - New custom “Fine-grained Audit Policy” *

* New with release 9*i*

Identification and Authentication

Know your Users

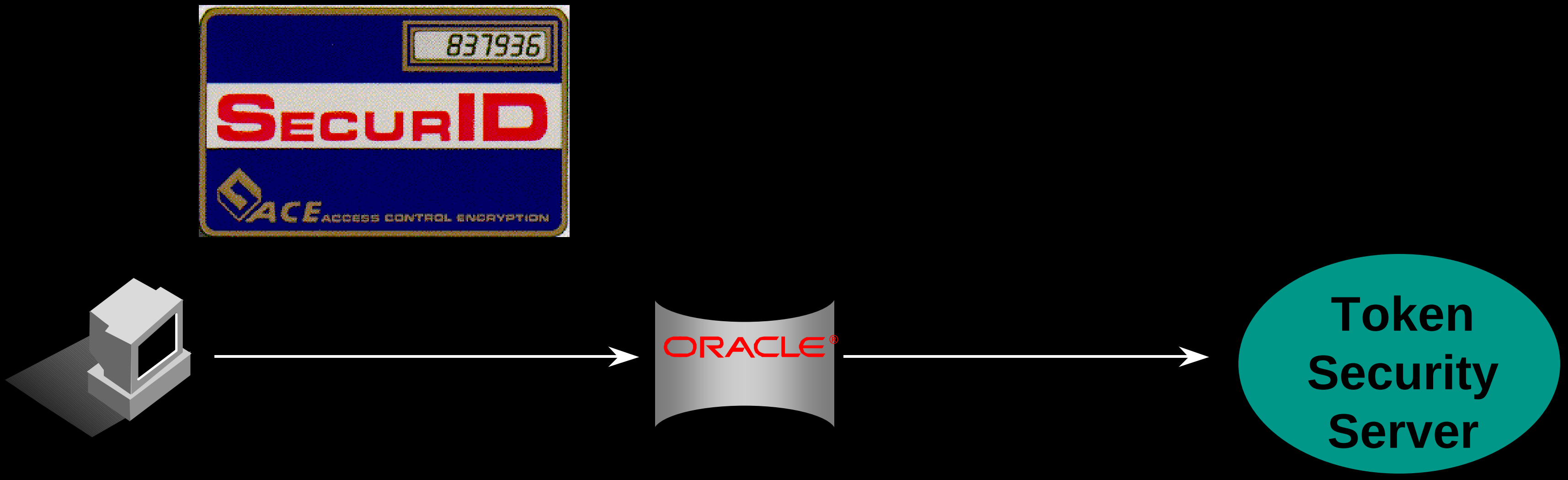
Integration with Biometric Devices



Step One:
User enters username
and provides fingerprint.
validates fingerprint
and authenticates login.

Step Two:
Server provides
login to user on the
basis of fingerprint
authentication.

Integration with Tokens



Step One:
User enters username and token information

Step Two:
verifies supplied token with token security server

Step Three:
token security server authenticates users and allows login.

PKI - Public Key Infrastructure using Secure Socket Layer (SSL)

SSL provides :

- Server authentication (checks that the server is who it claims to be)
- Secure data transmission (encryption)
- Data integrity

VeriSign™

www.verisign.com

User Identification & Authentication

The client is Identified & authenticated

Certificate

Issued by Verisign

The server checks if the certificate was issued by a known & trusted authority

This certificate belongs to :

Richard Wark
DN=Richard.Wark@oracle.com

Security Solutions

Oracle Corporation

San Antonio Texas, USA

This certificate was issued by :

Secure Server Certification Authority

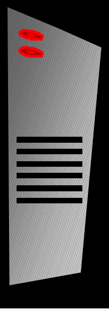
Verisign Inc.

Serial number : 02:78:00:09:AE

This certificate is valid from jan 10,1999 to jan 10, 2001

Certificate Fingerprint:

42:18:B0:1E:51:6C:28:9c:D4:AE:1D:F4:8D:F4:8D:F4:0B



List of Trustpoints

- Verisign
- GTE
- ...

Advanced Security - Features

Enhanced Authentication

- Mechanisms Supported
  - X.509 Certificates (PKI)
  - Card/Token: SecurID, ActiveCard, SafeWatch, CryptoCard, others
  - Centralized: DCE, CyberSAFE, Platinum, Bull (Kerberos, SESAME-based)
  - Biometric: Identix (fingerprint reader)
  - RADIUS

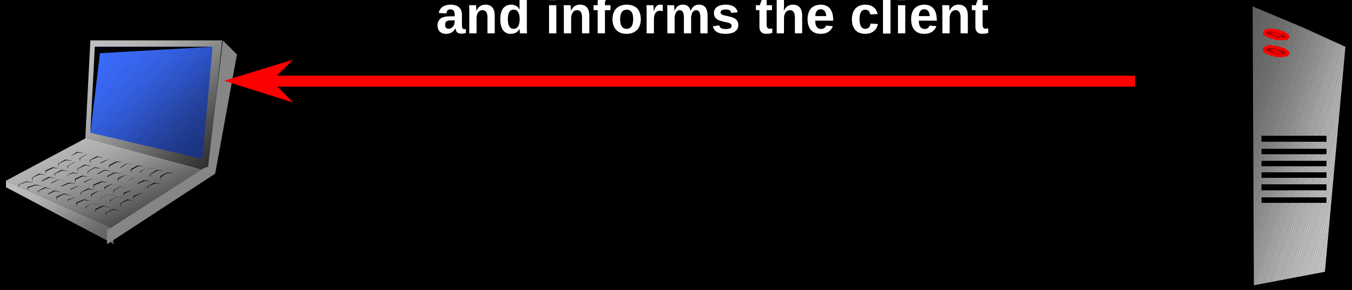
Privacy and Integrity

Protect Data “on-the-move”

Advanced Security

- Data Privacy and Integrity (Encryption & Checksumming)
  - All Oracle8*i* Protocols (SQL*Net, Net8, IIOP, Thick JDBC, Thin JDBC)
  - RSA RC4 (40, 56, 128 bit keys)
  - DES (40 and 56 bit keys), 3DES
  - MD5 & SHA-1 Hashing
- Complements database encryption
- Requires No Application changes!

Encryption



The server selects

the strongest common cypher

and informs the client

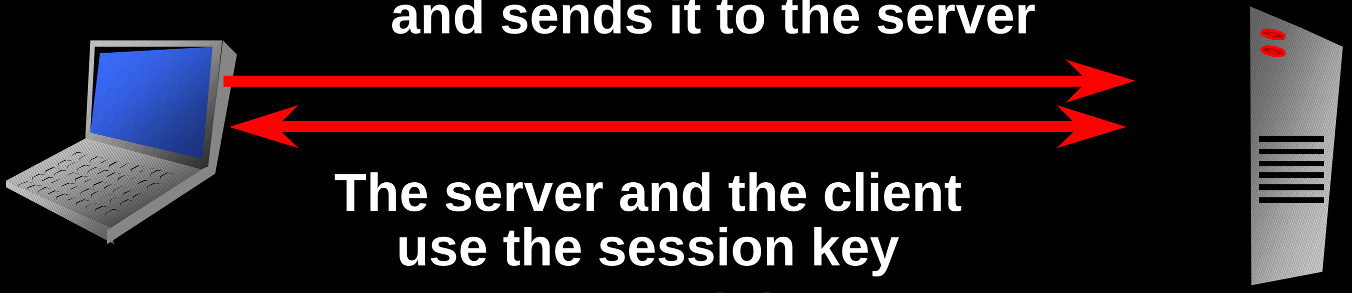
Encryption

The communication is encrypted!

The client uses the selected cypher

to create a session key

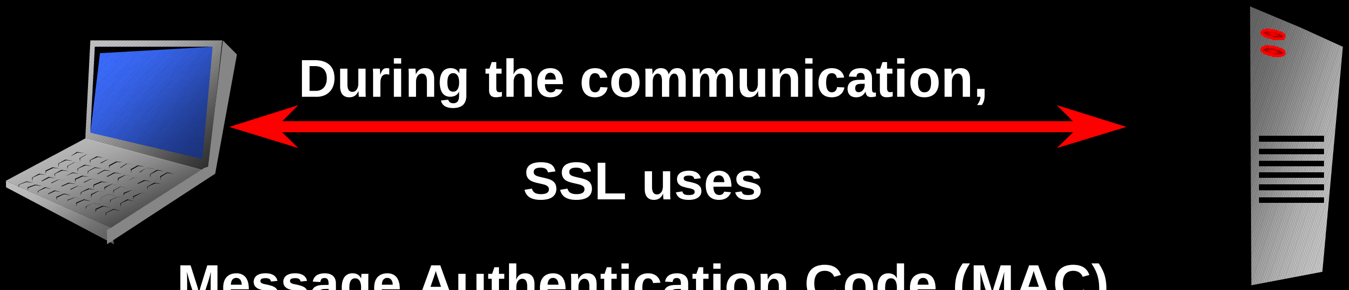
and sends it to the server



The server and the client
use the session key
to encrypt and decrypt
the information they send and receive

Data Integrity

Cannot
Hijack or
“SPOOF”
the data



During the communication,

SSL uses

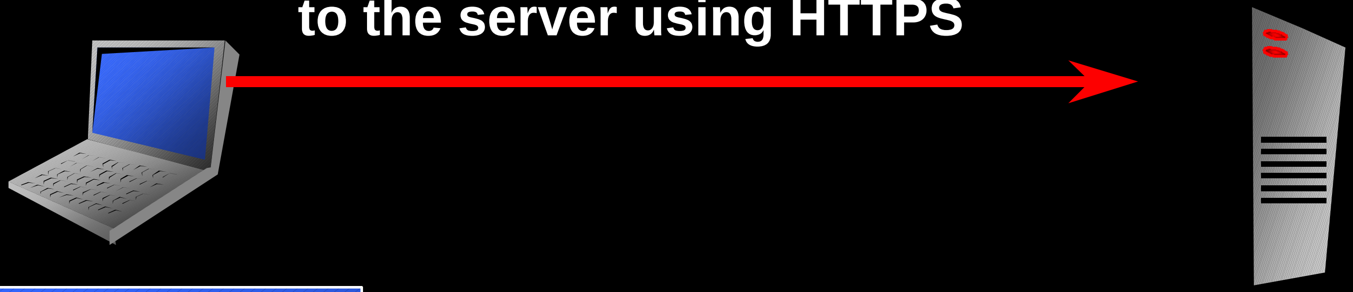
Message Authentication Code (MAC)

to ensure that there has been

no tampering

with the transferred data.

Server Authentication



The client sends a request

to the server using HTTPS

List of Trustpoints

- Verisign
- GTE
- ...

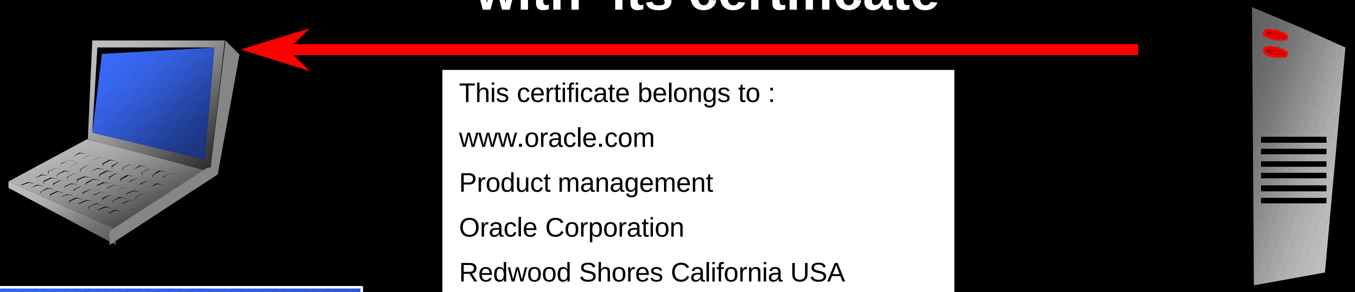
Certificate

Issued by Verisign

Server Authentication

The server responds

with its certificate



List of Trustpoints

- Verisign
- GTE
- ...

This certificate belongs to :

www.oracle.com

Product management

Oracle Corporation

Redwood Shores California USA

This certificate was issued by :

Secure Server Certification Authority

Verisign Inc.

Serial number : 02:78:00:09:AE

This certificate is valid from jan 10,1999 to jan 10, 2001

Certificate Fingerprint:

42:18:B0:1E:51:6C:28:9c:D4:AE:1D:F4:8D:F4:8D:F4:0B

Certificate

Issued by Verisign

Server Authentication

The server is authenticated

The client checks if the certificate was issued by a known & trusted authority

List of Trustpoints

- Verisign
- GTE
- ...

This certificate belongs to :

www.oracle.com

Product management

Oracle Corporation

Redwood Shores California USA

This certificate was issued by :

Secure Server Certification Authority

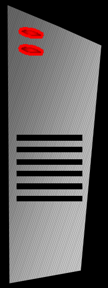
Verisign Inc.

Serial number : 02:78:00:09:AE

This certificate is valid from jan 10,1999 to jan 10, 2001

Certificate Fingerprint:

42:18:B0:1E:51:6C:28:9c:D4:AE:1D:F4:8D:F4:8D:F4:0B



Certificate

Issued by Verisign

Access Control

Protect Data at-rest

Access Control: Enforcement Mechanisms

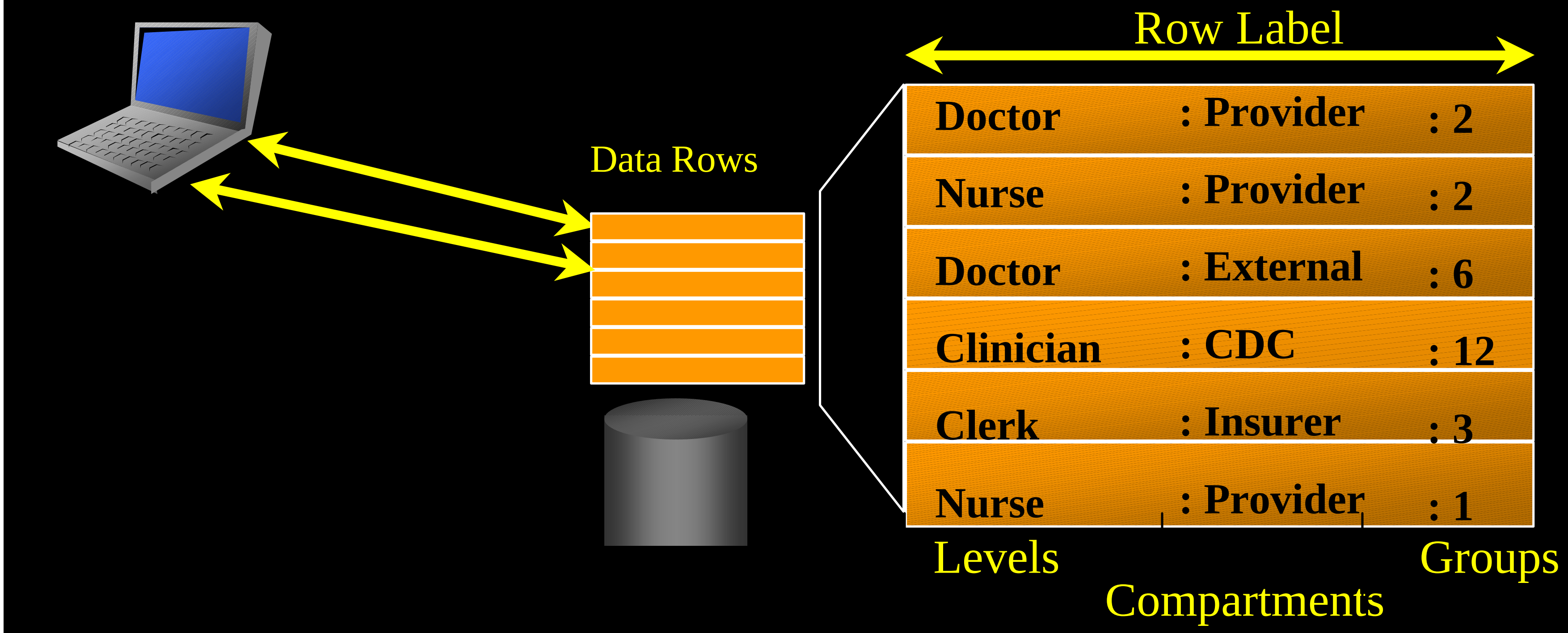
- Application Enforcement
  - Subject to errors
  - Enforced within application only
  - Requires changes to applications when policy changes

- **Server Enforcement**
  - **Well-defined**
  - **Strictly enforced, no exceptions**
  - **No changes to applications when policy changes**
  - **Flexible policy management**

Label Security

Protecting "data-at-rest"

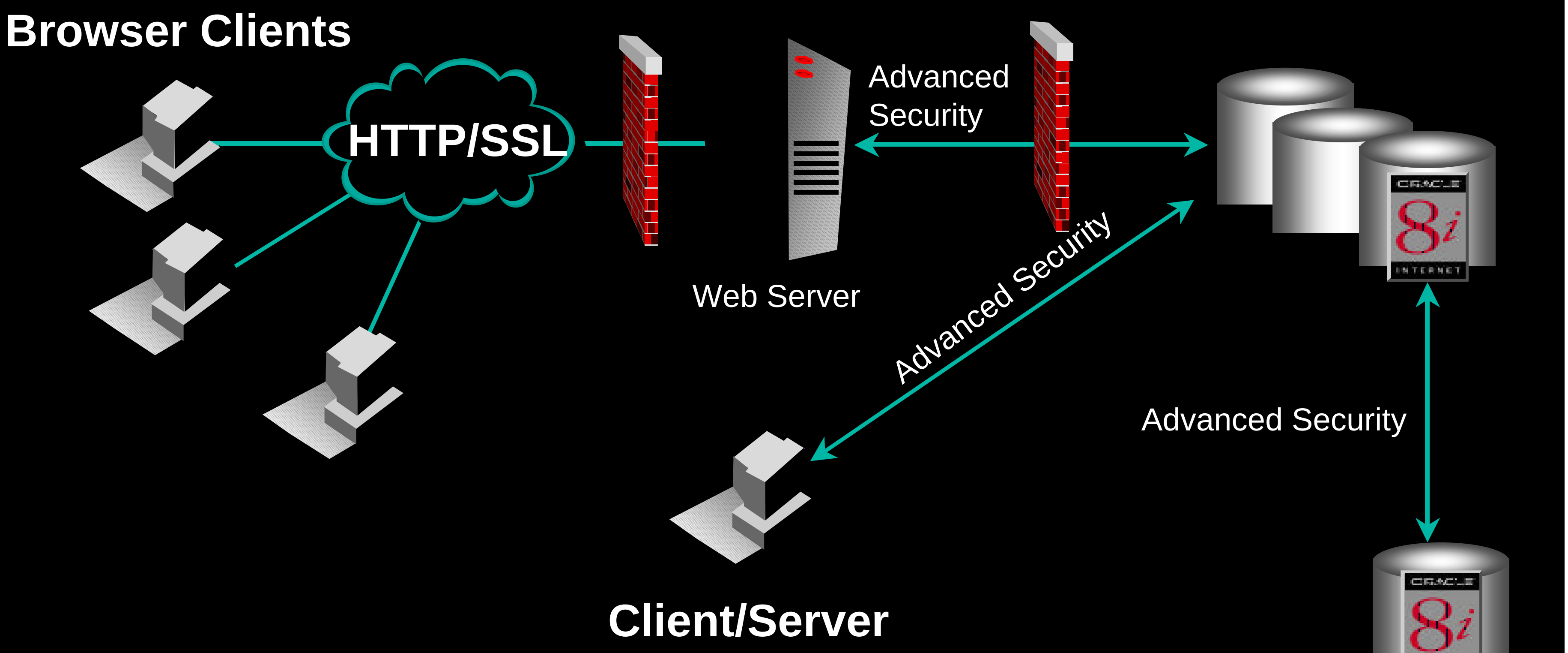
Example Label: **Doctor : Provider : Region-2**



Levels	Compartments	Groups
Doctor	: Provider	: 2
Nurse	: Provider	: 2
Doctor	: External	: 6
Clinician	: CDC	: 12
Clerk	: Insurer	: 3
Nurse	: Provider	: 1

Protect Data Confidentiality:

Protecting “data on-the-move”



Client/Server

User Management

Entries Identified by Distinguished Names

```
dn:uid=ddavis, ou= Orthopedics, o=uhsc,
c=us
uid:ddavis
password:secret
emailAddress: ddavis@uhsc.edu
mailhost:pop1.uhsc.com
homeTelephoneNumber:210-555-1212
employeeNumber:13974
```

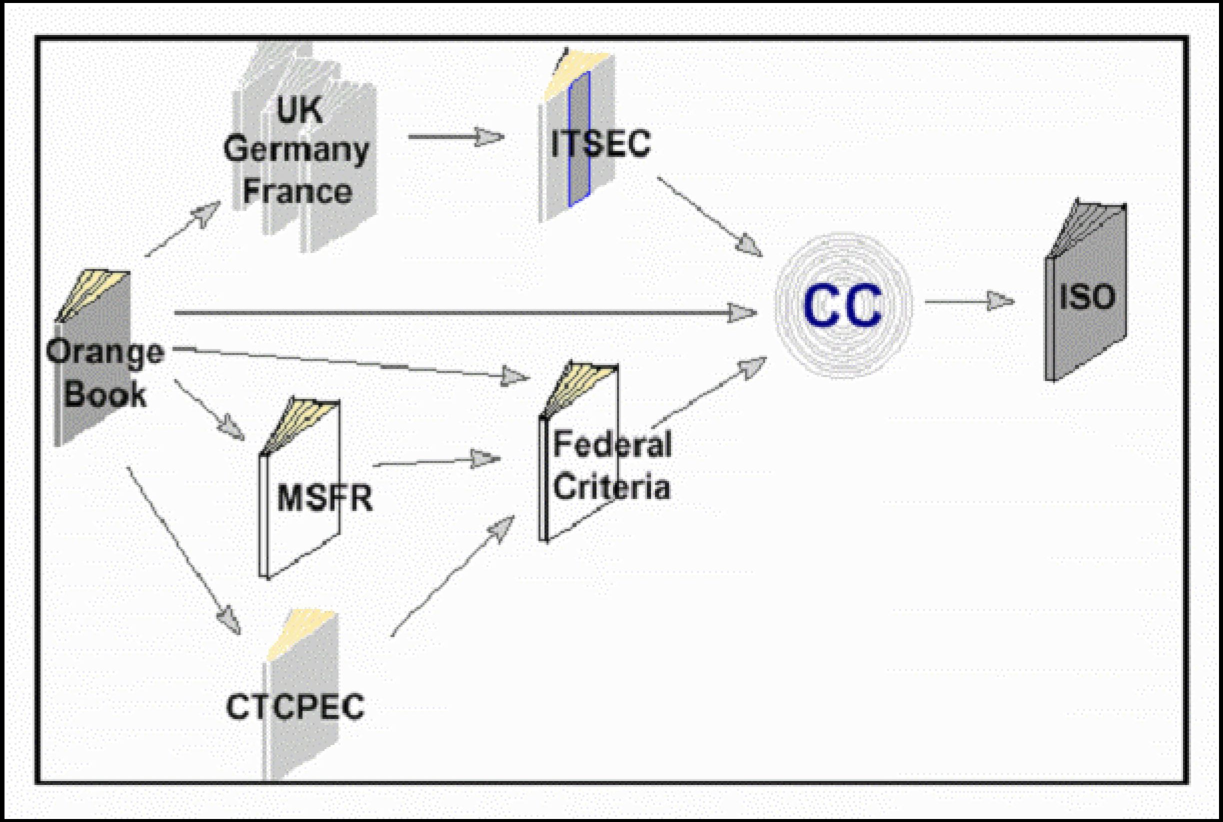
●
●
●

LDAP Directory Service

Users/Rolls
Employees
Network Resources
Rooms
Devices
Services
●
●
●

Formal Product Evaluations

Why Common Criteria ?



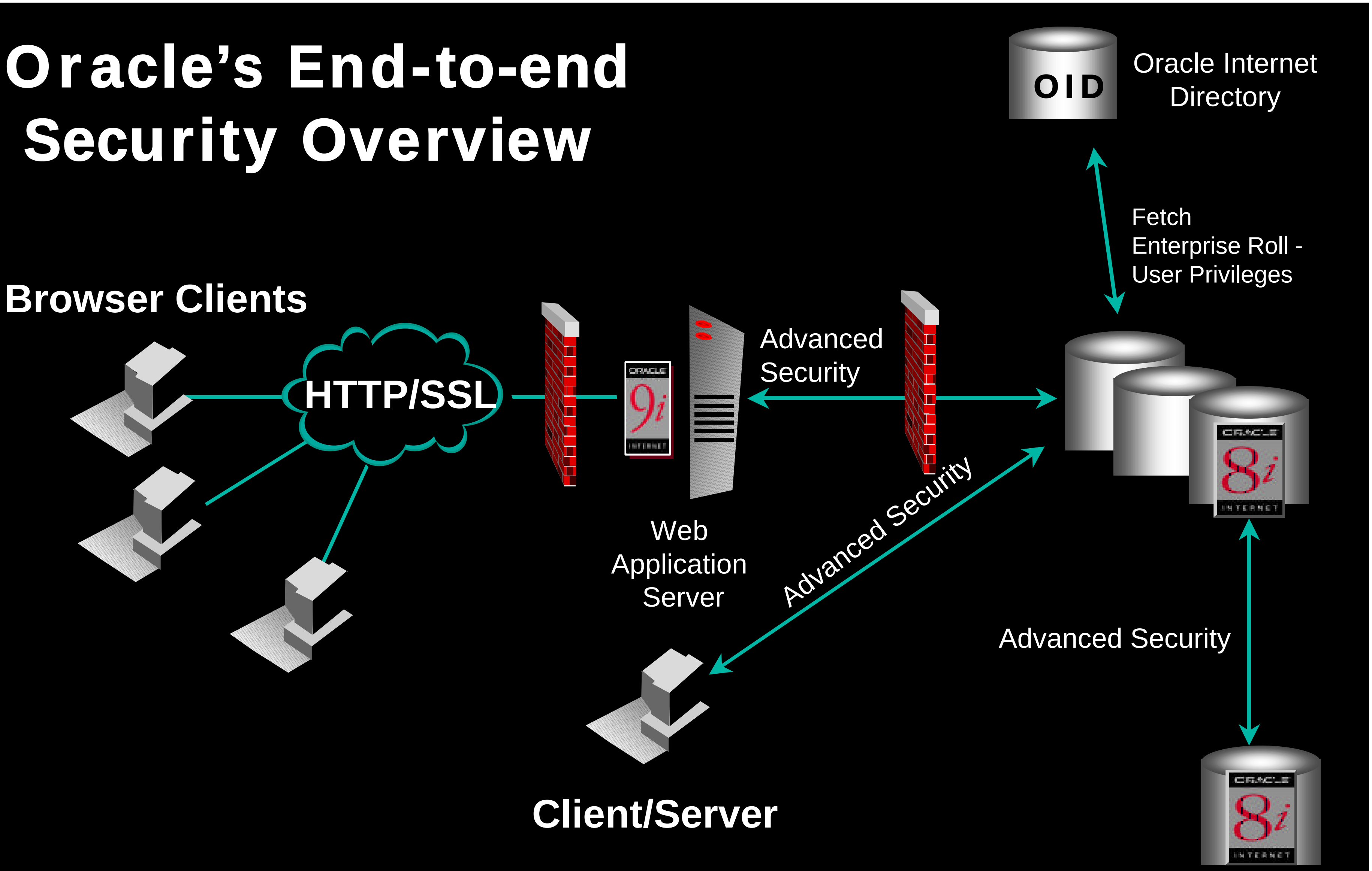
ISO Standard 15408 - Common Criteria
for Information Technology Security Evaluation

History of Oracle Security Evaluations

	Product	Release	Level	Criteria	Platform	Status
Common Criteria	Oracle8	8.0.5	EAL4	G.DBMS PP	Solaris, NT	Evaluated
	Oracle8*i*	8.1	EAL4	G.DBMS PP	Solaris, NT	In Evaluation
	Trusted Oracle8*i*	8.1	EAL4	G.MLS.DBMS PP	Trusted Solaris, NT	Pre-Evaluation
	Oracle7	7.2.2.4.13	EAL4	C.DBMS PP	NT	Evaluated
	Oracle7	7.2.2.4.13	*Trial* EAL3	C.DBMS PP	NT	Evaluated
ITSEC	Oracle7	7.3.4	E3 / *F-C2*	E3/F-C2	NT	Evaluated
	Oracle7	7.2.2.4.13	E3 / *F-C2*	E3/F-C2	NT	Evaluated
	Oracle7	7.0.13.6	E3 / *F-C2*	E3/F-C2	Solaris	Evaluated
	Trusted Oracle7	7.2.3	E3 / *F-B1*	E3/F-B1	HP-UX CMW	Evaluated
	Trusted Oracle7	7.1.5.9.3	E3 / *F-B1*	E3/F-B1	Trusted Solaris	Evaluated
	Trusted Oracle7	7.0.13.6	E3 / *F-B1*	E3/F-B1	Trusted Solaris	Evaluated
TCSEC	Oracle8	8.0.5	C2	C2	NT	CC Evaluation
	Trusted Oracle8	8.1	B1	B1	TBD	CC Evaluation
	Oracle7	7.0.13.1	C2	C2	HP-UX BLS	Evaluated
	Trusted Oracle7	7.0.13.1	B1	B1	HP-UX BLS	Evaluated
Russian	Oracle8	8.0.3	1V	Russian Criteria	HP-UX	Evaluated
	Oracle7	7.3.4	III	Russian Criteria	NT	Evaluated

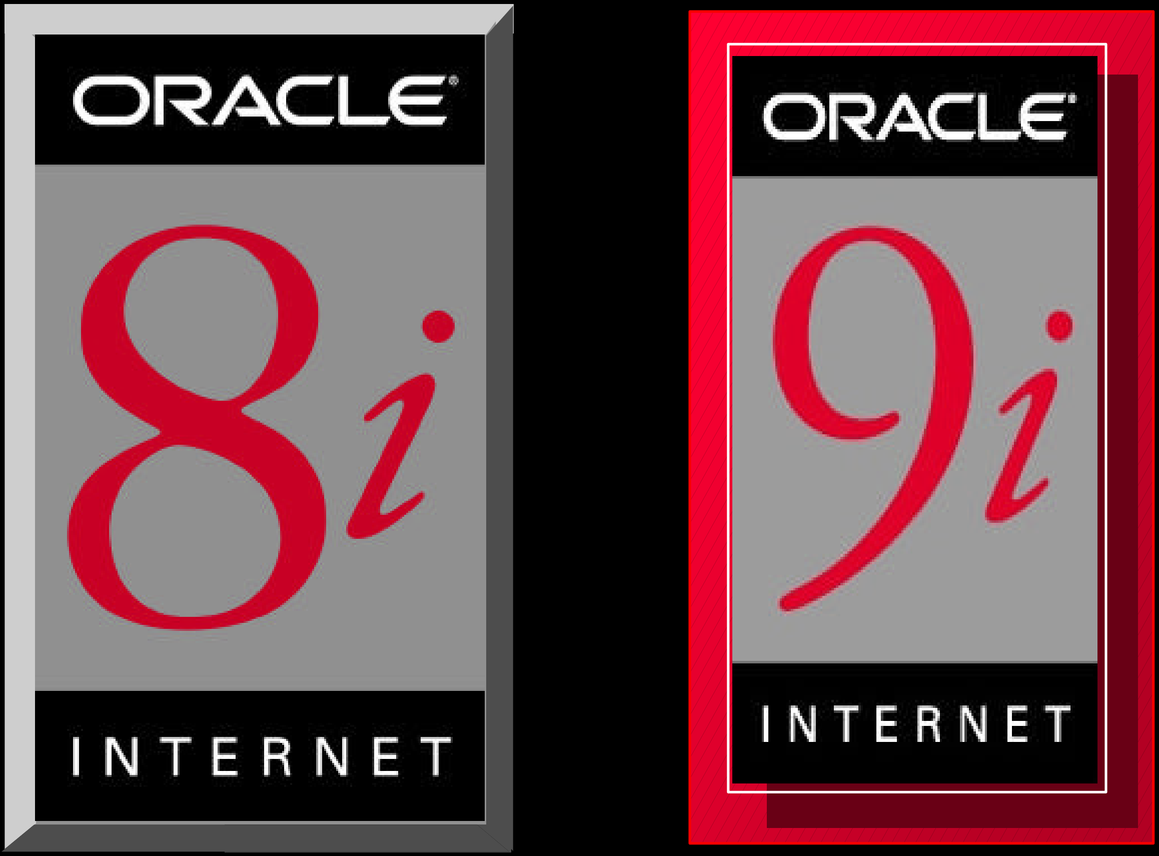
Note: ITSEC Evaluations are all E3, and when used in conjunction with an evaluated Operating System, achieve the functionality class claimed, either F-C2 or F-B1.

Oracle's End-to-end Security Overview



QUESTIONS
ANSWERS

Oracle8*i Security Technologies*



http://technet.oracle.com/products