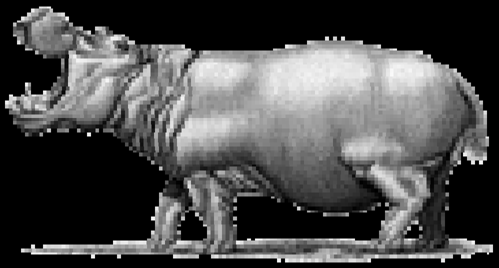
ORACLE®

SOFTWARE POWERS THE INTERNET

HIPAA Security
What’s Real, What’s Practical



Richard Wark
Security Technologist - Oracle Corporation

“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.”

- President Bill Clinton

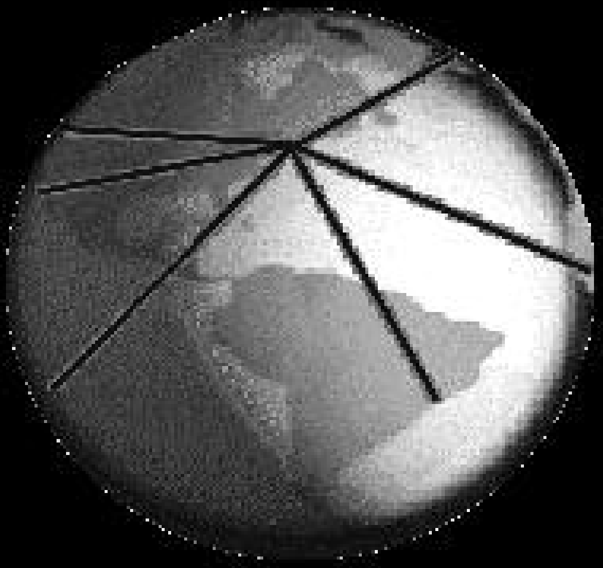
HIPAA: Security Challenges

Agenda

- Critical Issues - Landscape & “*The threat*”
- Requirements
- Technologies
- End-to-end Security

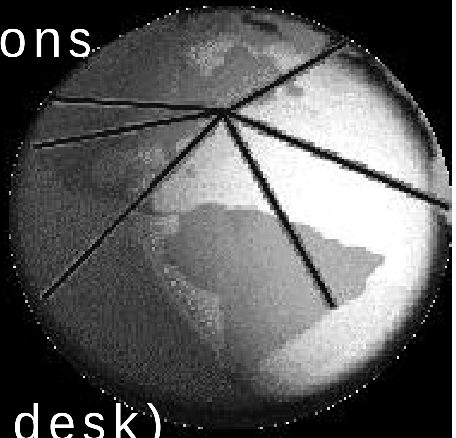
The Internet Changes Everything

- Low cost communications
  - More users = more security
- Standards based
  - HTML, HTTP, JAVA, CORBA, IIOP
- High availability worldwide
  - ANY Data, ANY browser, ANY time...



The Internet Changes Everything... How?

- Security
  - Use of unsecured uncontrolled networks
  - Too many Users have too many passwords
  - Adding & Deleting Users in Multiple Locations



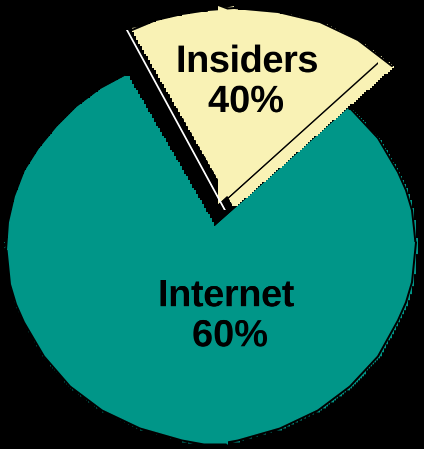
- Administration
  - Distributed User Account Information
  - Password Maintenance (50% calls to help desk)
  - Increases with move to extranets & Internet

Security and Privacy - The Threat

Who's the bad guy? Competitors, foreign governments, network hackers, disgruntled ex-employees, news and media, curious patients, unauthorized employees, etc?

How do I protect my information from the bad guys, without making employees and authorized users less productive?

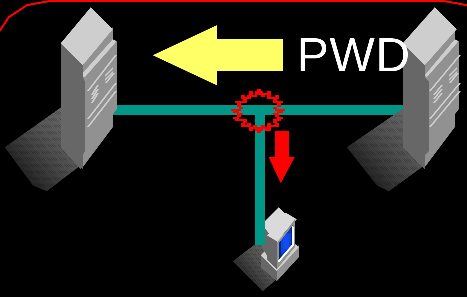
How can I administer security consistently, reliably, and cost effectively across all of my distributed information resources ?



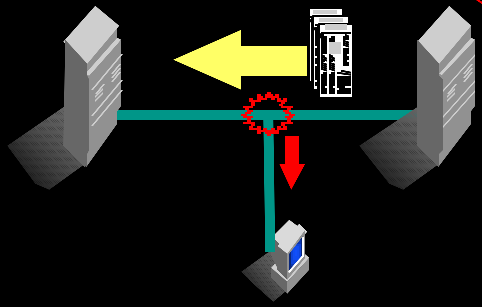
Studies show 40% breeches are by authorized users, but account for 80% of losses.

Source: 2000 Computer Security Institute and FBI Survey

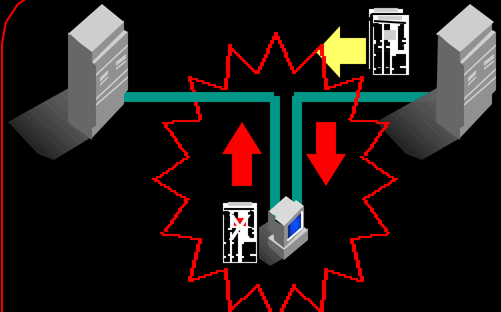
Common Security Breaches



PASSWORD SNOOPING



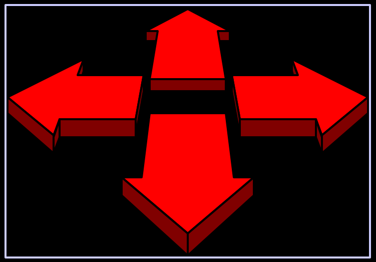
DATASTREAM SNOOPING



DATASTREAM MODIFICATION

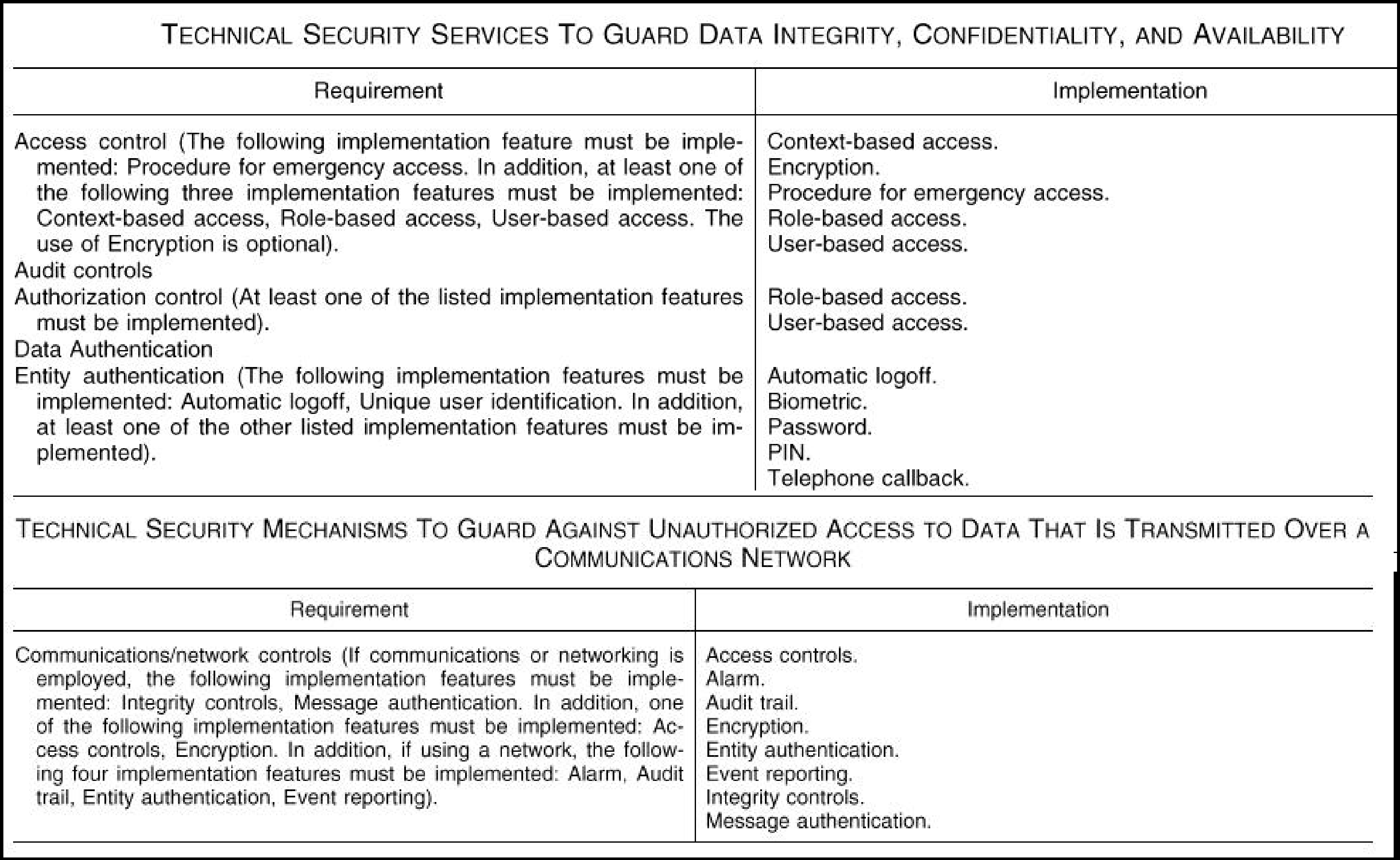
ESTABLISHING USERS & AUTHORIZATIONS

USERS HAVE TOO MANY PASSWORDS



DISTRIBUTED SECURITY ADMINISTRATION

Health Insurance Portability and Accountability Act (HIPAA)



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 implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional).	Context-based access. Encryption. Procedure for emergency access. Role-based access. User-based access.
Audit controls	
Authorization control (At least one of the listed implementation features must be implemented).	Role-based access. User-based access.
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.

TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK

Requirement	Implementation
Communications/network controls (If communications or networking is employed, the following implementation features must be implemented: Integrity controls, Message authentication. In addition, one of the following implementation features must be implemented: Access controls, Encryption. In addition, if using a network, the following four implementation features must be implemented: Alarm, Audit trail, Entity authentication, Event reporting).	Access controls. Alarm. Audit trail. Encryption. Entity authentication. Event reporting. Integrity controls. Message authentication.

HIPAA Issues: Technical and Physical Security

- Know your users - Strong user identification and authentication
- Protect data on the move - Privacy & integrity of communications
- Protect data at rest - Access control
- Provide effective Audit mechanisms - Proactive and historical

Enterprise Security Issues

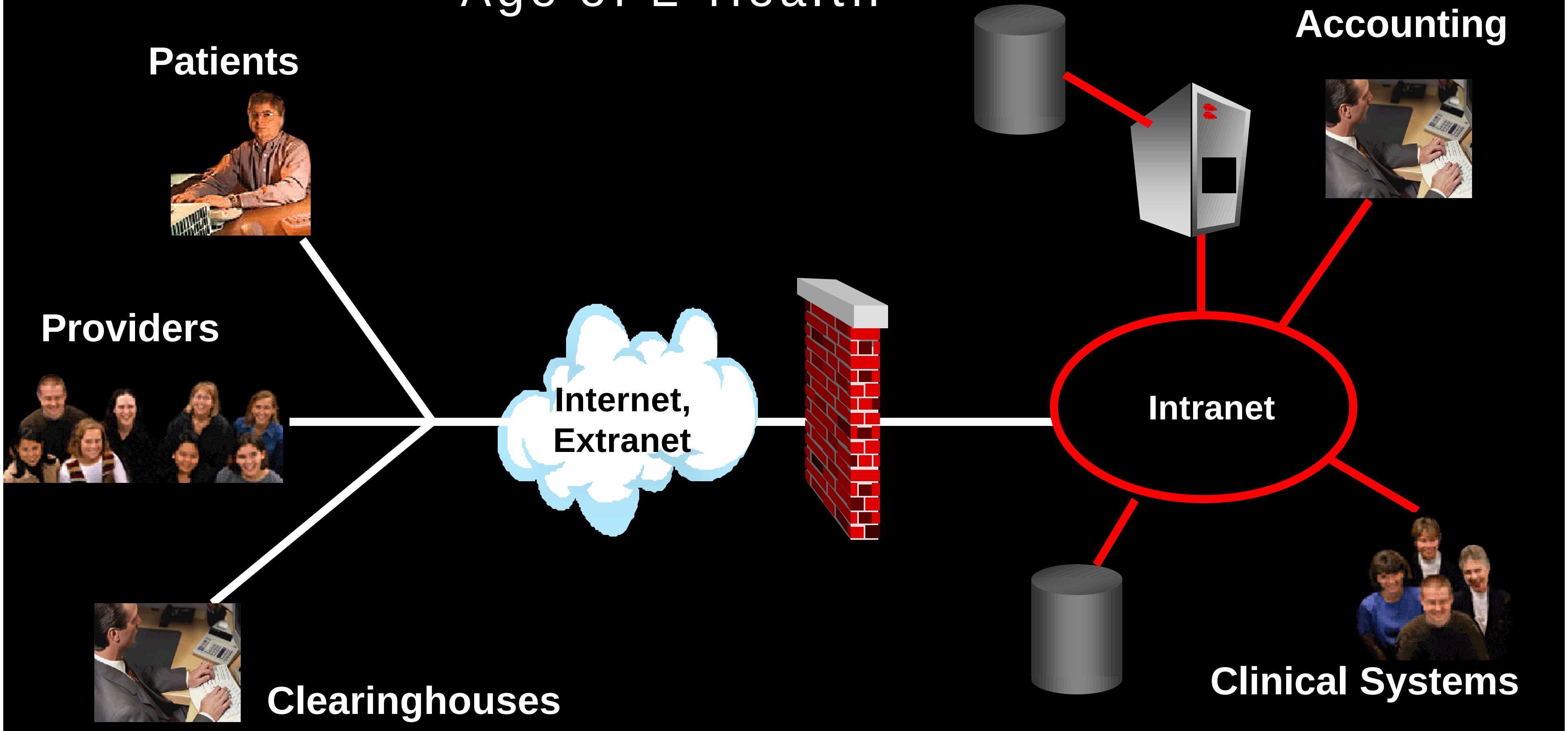
- Strong user authentication → *Smartcards, biometrics, - PKI (X.509v3 Certificates)*
- Privacy & Integrity of communications → *Encryption (RC4, DES, MD5, etc.)*
- Access control → *Mandatory Access Control Policies-Fine-Grained AC*
- User Account Management → *LDAP Directory Integration*
- Assurance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

Technologies

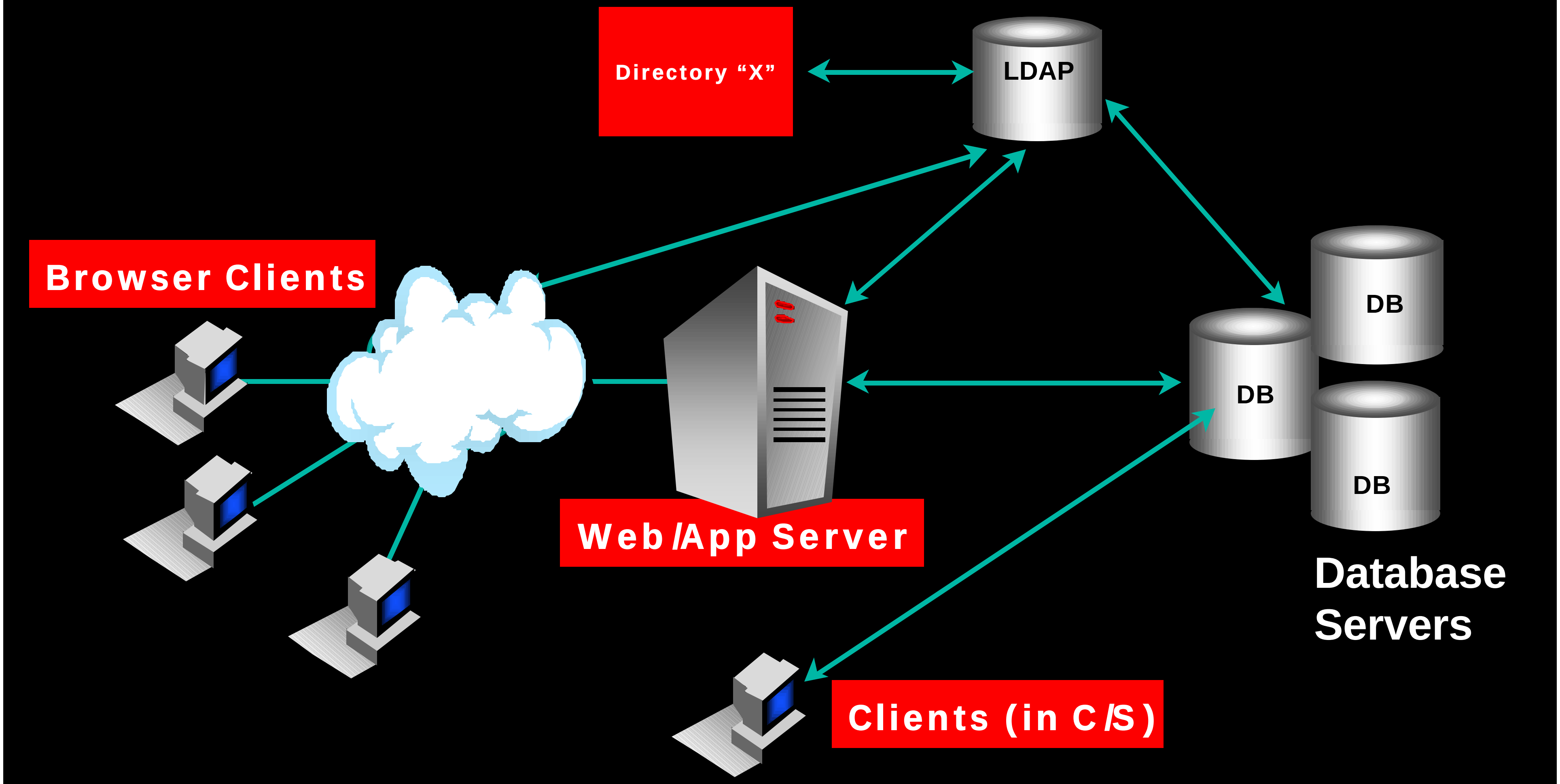
- Strong Authentication Mechanisms & PKI
- Encryption
- Mandatory Access Control
- User Management/Directory Services - LDAP
- Audit Controls

New Era Of Responsibilities

Age of E-Health



Security Architecture



Directory “X”

LDAP

Browser Clients

Web /App Server

DB

DB

DB

Database Servers

Clients (in C /S)

Identification and Authentication

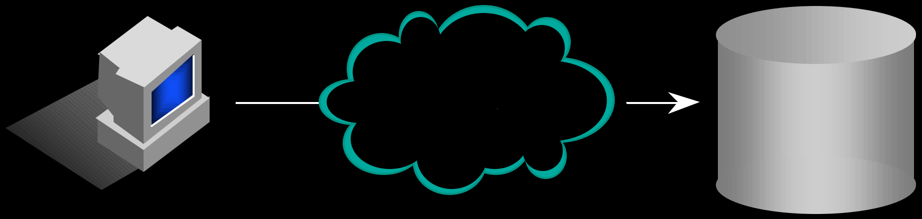
Know your Users

Security Challenges of the Internet

Who is accessing your data?

- Who can access your data?
  - There are over 40 million Internet hosts today
  - You need to know who is accessing your network
- The solution:
  - Strong Authentication of users

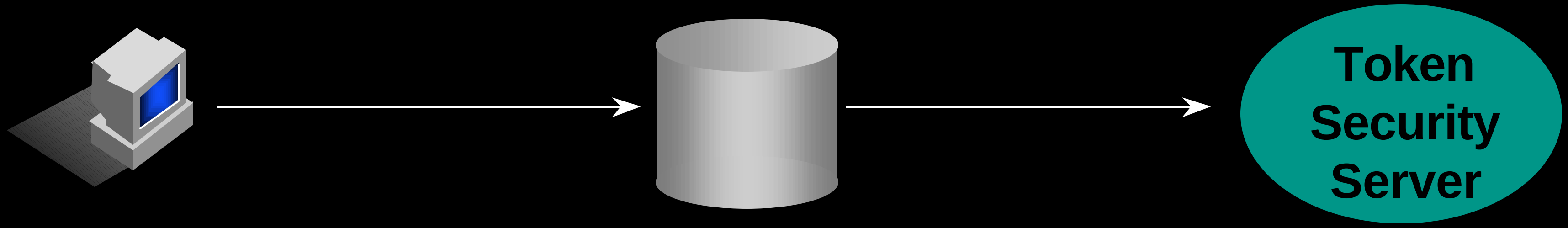
Integration with Biometric Devices



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.

Public Key Infrastructure Support

- X.509V3 Certificates for Authentication
- Secure Sockets Layer (SSLv3) for Network Integrity & Confidentiality
- Lightweight Directory Access Protocol (LDAP v3) for centralized user management and credential storage
- Leading PKI Vendors
  - Verisign, Oracle,Entrust, Netscape, Novell, Microsoft, GTE, ...

Privacy and Integrity

Protect Data “on-the-move”

Security Challenges of the Internet

Keeping Your Data Private

- How can I ensure data communications are private?
  - 100% of non-secured Internet communications can be read by an experienced user
- The solution:
  - Encryption and data integrity insure privacy

Two approaches to Secure Communication

Hardware

- Faster
- Physical device
- May not be available externally

Software

- Available on all Machines
- Easy to upgrade
- Less performant
- Less secure ?

Secure Sockets Layer (SSL)

Standards compliance reduces complexity

- SSL is a industry-standard protocol for using Public Key Infrastructure (PKI) to secure Internet connections
- SSL provides security by:
  - Encrypting all traffic (including Triple DES)
  - Checking the integrity of data
  - Authenticating clients and servers
  - Supporting single sign-on

Secure Socket Layer (SSL)

SSL provides :

VeriSign™

www.verisign.com

- Authentication
  (checks that the user and server are both who they claim to be)
- Secure data transmission (encryption)
- Data integrity

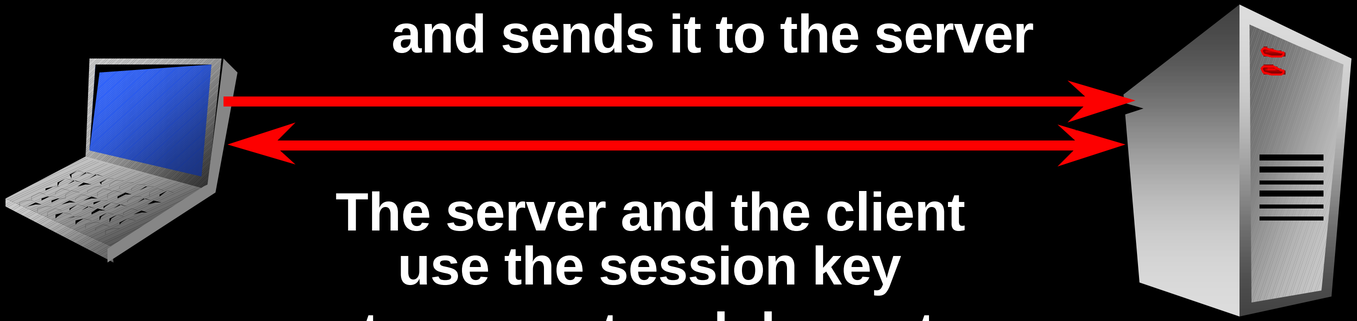
Encryption

The communication is encrypted!

The client uses the selected cypher

to create a session key

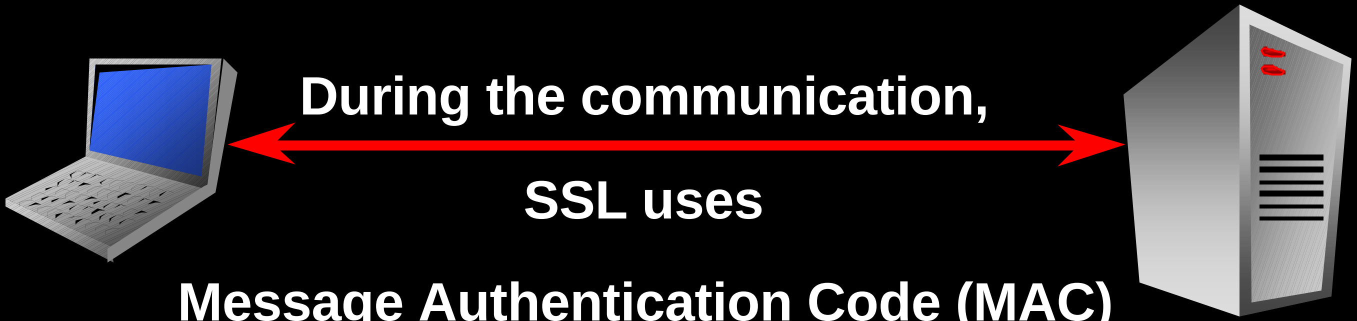
and sends it to the server



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.

Access Control

Protect Data at-rest

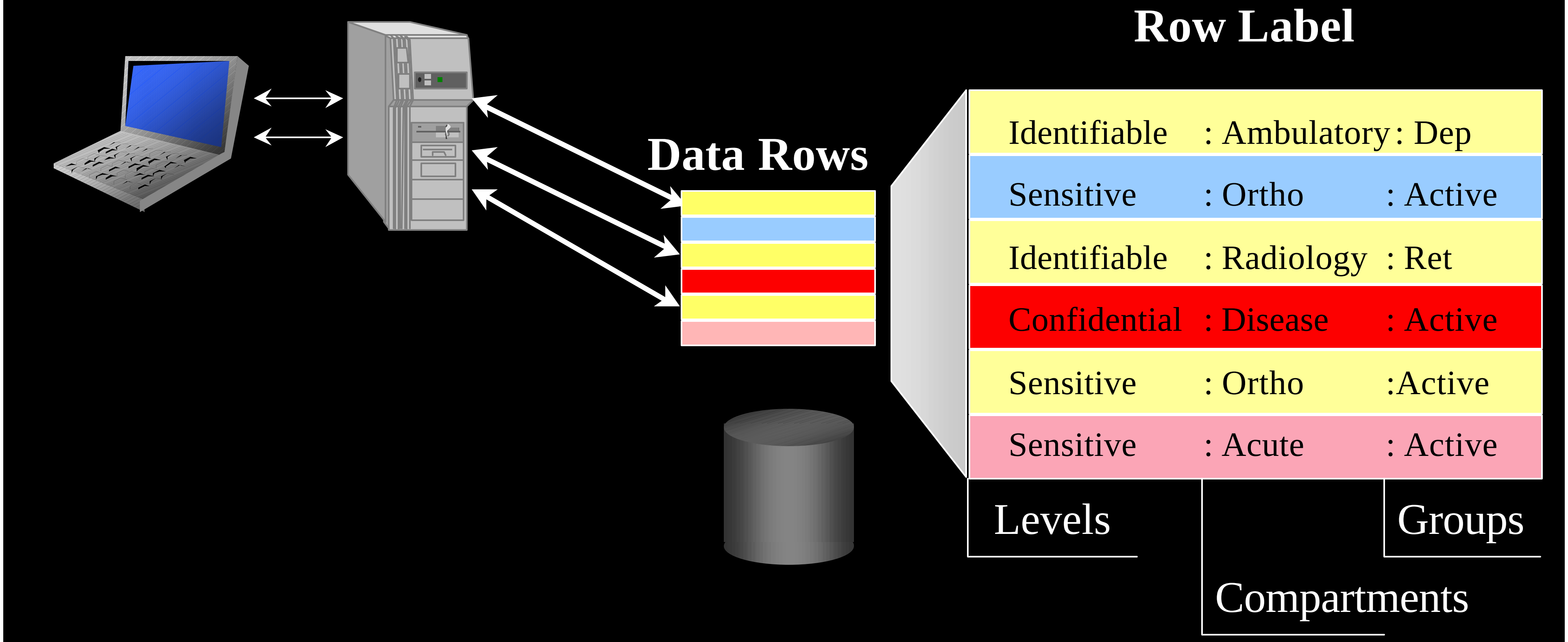
Access Control: Enforcement Mechanisms

- 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 Controls - MLS:
Label-based Access

User	Label
Dr. Murphy	Sensitive : Ortho,Acute : Active



Row Label

Identifiable	: Ambulatory	: Dep
Sensitive	: Ortho	: Active
Identifiable	: Radiology	: Ret
Confidential	: Disease	: Active
Sensitive	: Ortho	:Active
Sensitive	: Acute	: Active
Levels	Compartments	Groups

Server Based Access Control
Data Labels

Benefits

- Enables Flexible, Policy-based Access Control
- Tools for easy policy creation / management
- Supports New and Legacy Applications
- Proven for high security environments

User Management

The Way Things are Today

- Information is managed in the applications or in proprietary directories
- Same information is represented many different ways
- High cost of ownership associated with maintenance
- Inability to leverage this information with Internet ready applications quickly and easily

ORACLE

Security Challenges of the Internet

How To Manage Security Costs?

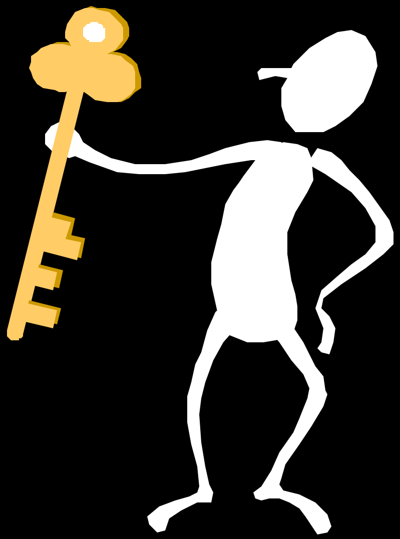
- How can I reduce costs and manage complexity for users?
  - Average corporate user has 14 passwords
    - Users “cheat” by writing down or using easy-to-remember (and break) passwords
  - High cost of management of security if not managed efficiently/centrally
- The solution:
  - Single sign-on reduces number of passwords for lower cost and complexity

Single Sign-On

Reduce Costs and Complexity

- Single sign-on to ease use and administration
  - Users log in only once and need only one password
  - Simplifies administration
  - Dramatically decreases costs
  - Increases security, by centralizing login process

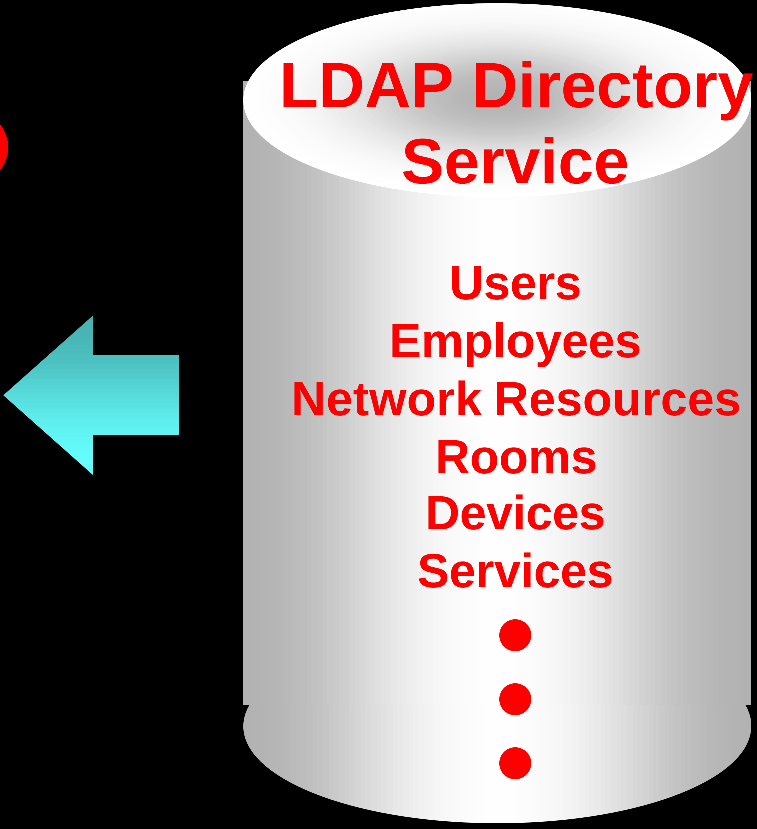
LDAP: The Emerging Solution



- Directory service standard based on the ISO X.500 specification
- Lightweight, browser-friendly client implementation
- Protocol standard defined and maintained by the IETF
- Need for interoperability is driving rapid adoption

Entries are Identified by Distinguished Names

dn:uid=ddavis, ou= Orthopedics, o=Mercy, c=us
uid:ddavis
password:secret
emailAddress: ddavis@Mercyhospital.com
mailhost:pop1.mercyhealth.com
homeTelephoneNumber:210-555-1212
employeeNumber:13974
●
●
●



Evaluated Technology

Use what works.

Your Applications: *Security Built In?*

COMMON
EAL4
CRITERIA

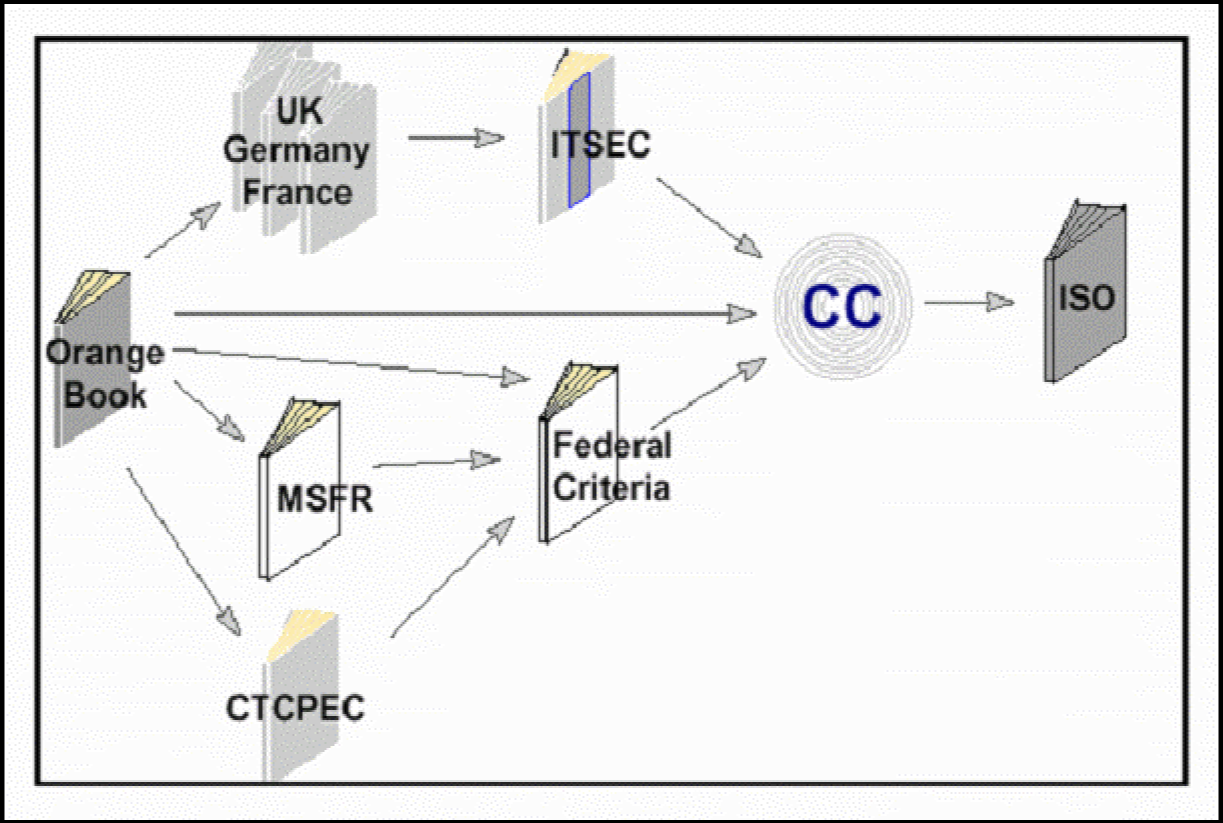
NCSC
C2
EVALUATED

ITSEC
E3
EVALUATED

NCSC
B1
EVALUATED

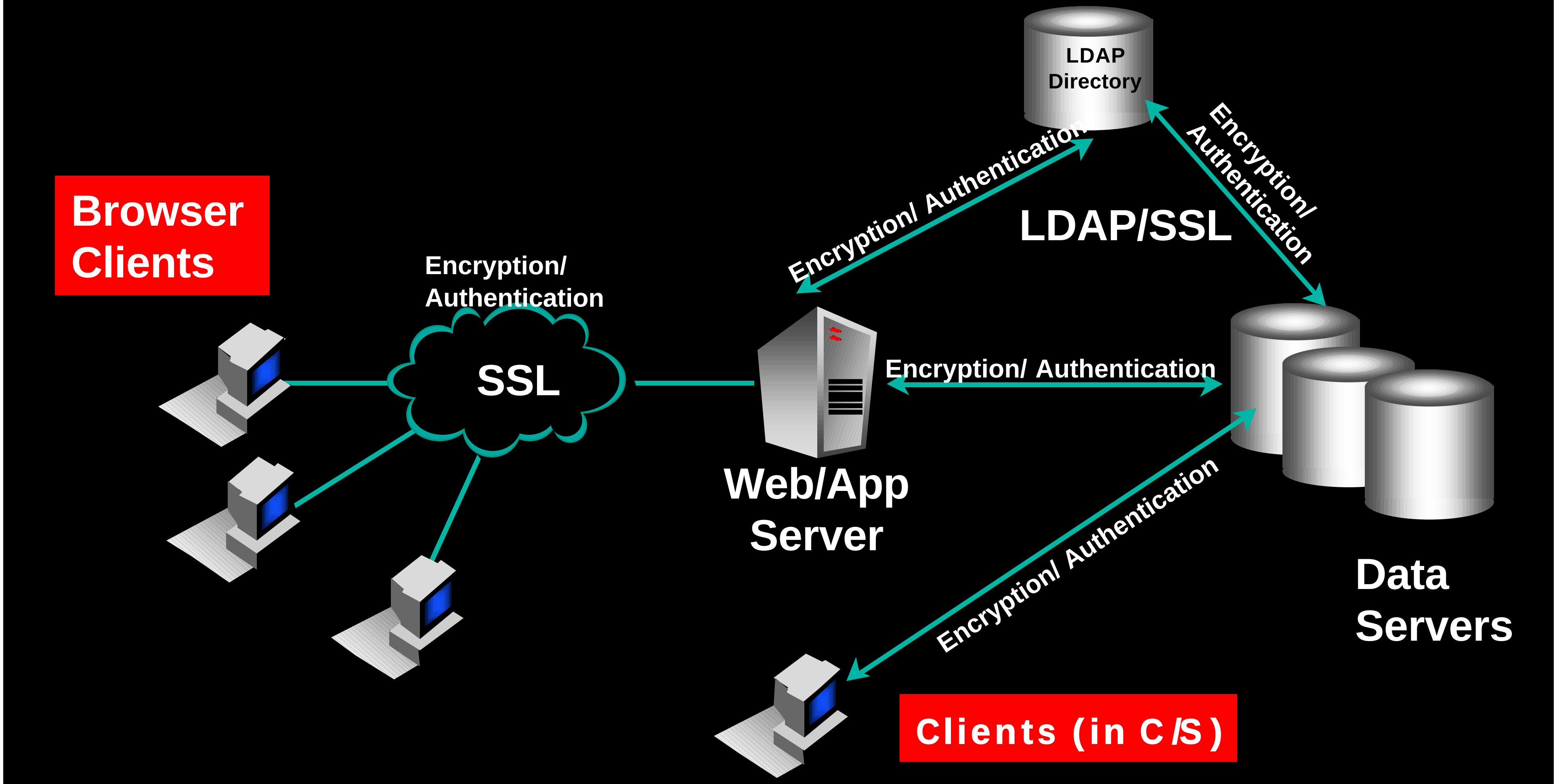
- C2/E3/EAL4 evaluated
  - US TCSEC (Orange Book) C2
  - European ITSEC E3 certified
  - Common Criteria replaced TCSEC/ITSEC
- Comprehensive Security Functionality
- Rigorous Design and Testing

Why Common Criteria ?



ISO Standard 15408 - Common Criteria
for Information Technology Security Evaluation

End-to-end Security Architecture



Browser Clients

Encryption/ Authentication

SSL

Web/App Server

Encryption/ Authentication

LDAP Directory

LDAP/SSL

Encryption/ Authentication

Encryption/ Authentication

Data Servers

Encryption/ Authentication

Clients (in C/S)

Responsibilities - Summary

Customer
Auditor
Vendor

- Industry can and must build more secure product through
  - better engineering
  - product assessments and formal evaluations
  - heightened incident response
- Customers must be more demanding, and more discriminating
- Auditors must review all security policies for secure configurations

ORACLE®

SOFTWARE POWERS THE INTERNET