Oracle 11g and Governance

How can Oracle 11g new features help with your compliance needs

With increasing regulatory compliance throughout our business environment how can we use Oracle 11g to support regulatory requirements while improving the safety, security and minimize the impact on the business

Introductions:

- *Dan Morgan*
- *Oracle Ace Director*
- University of Washington
  - Author UW Oracle curricula
  - Primary program instructor (1999 – present)
- PSOUG Education Chair
- UKOUG Member
- Presenter: OOW, US, UK, Canada, & Japan
- Database professional since 1969
  - IBM Mainframes: Fortran IV and COBOL
    - 10+ years and no I don't want to talk about it
- Oracle RDBMS since version 6
- More than 20 years of hands-on consulting

Introductions:

- Victoria Whitlock
- 22 years of IT experience
  - 7 years at Oracle
- Author
- Recognized SME
  - Compliance: Strategic & Tactical
  - Business Integration
  - Consultant
  - Data Base Administrator
  - Corporate Educator
  - Project Management

What is Governance ?

- The process of decision-making and the process by which decisions are implemented (or not implemented)
- Governance can be used in many contexts such as corporate governance, local governance or IT governance

What is Compliance ?

- Noun
  - Compliance - acting according to certain accepted standards; "their financial statements are in conformity with generally accepted accounting practices"
- Noncompliance - the failure to obey
- Often used with FUD: Fear Uncertainty and Doubt
- A word that gets tossed around without understanding
- Used interchangeably with Governance

What are the regulatory requirements you might face ?

- *PCI – payment card industry standards – credit card information and security*
- *SOX – Sarbanes Oxley – a requirement for transparency of financial information Increasingly part of non public companies*

What are the regulatory requirements you might face ?

- *HIPAA - Health Insurance Portability and Accountability Act of 1996*
  1) electronic transactions and code sets
  2) security
  3) unique identifiers
  4) privacy

What are the regulatory requirements you might face ?

- GBLA Gramm-Leach-Bliley Act *regulates financial institutions and provides for:*
  1) limited privacy protections against the sale of private financial information
  2) codifies protection against “pre-texting” to obtain personal financial information through false pretenses
  3) allow consumers the right to opt out from limited “nonpublic personal information”

What are the regulatory requirements you might face ?

- FCRA Fair Credit Reporting Act 1971
  Accuracy and fairness of credit reporting
  1) safeguard integrity and accuracy of collected and disseminated data
  2) including internet access and use
  3) safe disposal of information derived from credit reports

More Regulations

- The Fair and Accurate Credit Transaction Act of 2003 (FACTA) *added new sections to the Federal Fair Credit Reporting Act*
  - credit and debit card receipts may not include more than the last five digits of the card number
  - card's expiration date be printed on the cardholder's receipt
  - allows consumers who request a copy of their file to also request that the first 5 digits of their Social Security number (or similar identification number) not be included in the file
  - procedures for proper document disposal
  - requires notification to the consumer if credit score was used to determine viability for credit

International Regulations -Canada

- Based on ten privacy principles developed by the Canadian Standards Association
- Privacy Commissioner of Canada and the Federal Court oversee review issues
- Personal Information Protection and Electronic Documents Act (PIPEDA) 2004
  - law that protects personal information in the hands of private sector organizations
  - provides guidelines for the collection, use and disclosure of that information in the course of commercial activity
  - applies to both traditional, paper-based business as well as on-line commercial activities
- Applies to all personal information (not employee personal information) in any interprovincial and international transborder data flow

European Union

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- Law for privacy and electronic communications
- More harmonized information provisions between member states
- International negotiations and access restrictions to Personal Data by employers outside the EU
- Have issues with the United States use of privacy
- International issues are tricky and complex

Data in the US considered UNSAFE

- Brussels, 17 August 2007
- ARTICLE 29 DATA PROTECTION WORKING PARTY

- *Following the conclusion of the new long-term PNR agreement between the EU and the US, the Art. 29 Data Protection Working Party has issued today an opinion analysing the privacy impact of the transfer of passenger data to the US on fundamental rights and freedoms and in particular the passengers' rights to data protection. The opinion concludes that the safeguards of the new agreement are markedly lower than those of the previous deal and serious questions and shortcomings remain unaddressed. The level of data protection of the new agreement must be considered unsatisfactory*

- Accepted data protection standards such as those enshrined in Convention 108 of the Council of Europe or the EU Data Protection Directive are not fully respected

Things to Know

- Compliance is: ***Good Engineering Practices*** applied consistently throughout the business
- It is here to stay
- Buying a tool does not make you compliant
- Types of Compliance
  - Government Compliance
  - Industry Standards Organizations
  - Corporate Standards
  - International Standards
  - Accounting Standards
  - Industry Specific Compliance

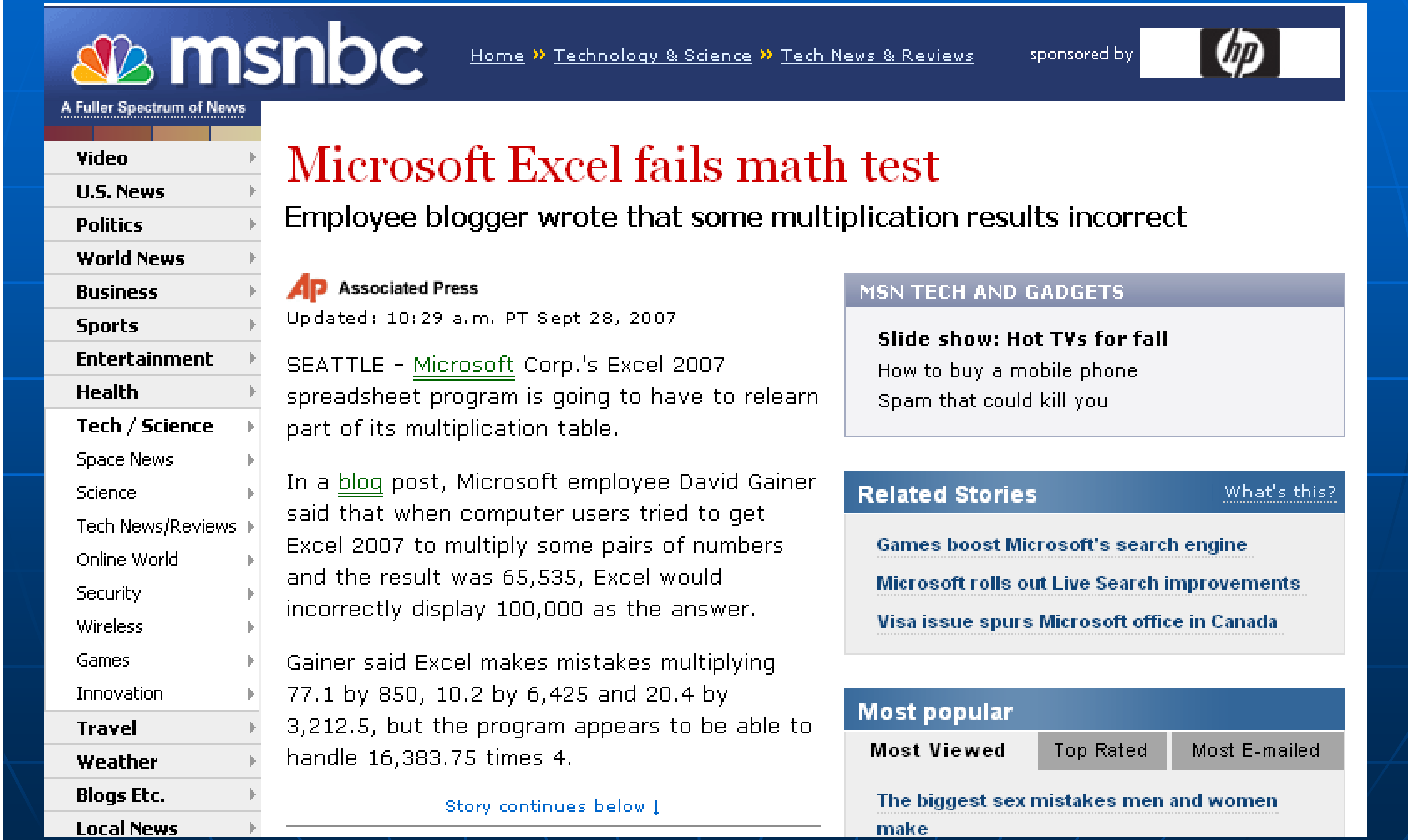
Common IT Issues

- Documentation of systems and process
- User accounts, roles, privileges, access controls
- Identity management
  - Access Revocation
  - Aged or stale passwords, password complexity
  - policy enforcement
- Auditing – FGA, Flashback Archive, Audit Vault
  - Two-factor Authentication
- Requires 128-bit SSL encryption and effective management of crypto key transmission and storage
- Develop and maintain secure systems and applications
- Unvalidated Input
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management

Common IT Issues

- Documentation of systems and process
- **User accounts, roles, privileges, access controls**
- **Identity management**
  - Access Revocation
  - **Aged or stale passwords, password complexity**
  - **policy enforcement**
- **Auditing**
  - Two-factor Authentication
- **Requires 128-bit SSL encryption and effective management of crypto key transmission and storage**
- **Develop and maintain secure systems and applications**
- **Unvalidated Input**
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- **Injection Flaws**
- **Improper Error Handling**
- **Insecure Storage**
- Denial of Service
- **Insecure Configuration Management**

Uncommon IT Issues to



Microsoft Excel fails math test

Employee blogger wrote that some multiplication results incorrect

Associated Press
Updated: 10:29 a.m. PT Sept 28, 2007

SEATTLE - Microsoft Corp.'s Excel 2007 spreadsheet program is going to have to relearn part of its multiplication table.

In a blog post, Microsoft employee David Gainer said that when computer users tried to get Excel 2007 to multiply some pairs of numbers and the result was 65,535, Excel would incorrectly display 100,000 as the answer.

Gainer said Excel makes mistakes multiplying 77.1 by 850, 10.2 by 6,425 and 20.4 by 3,212.5, but the program appears to be able to handle 16,383.75 times 4.

Story continues below ↓

MSN TECH AND GADGETS

Slide show: Hot TVs for fall
How to buy a mobile phone
Spam that could kill you

Related Stories What's this?

- Games boost Microsoft's search engine
- Microsoft rolls out Live Search improvements
- Visa issue spurs Microsoft office in Canada

Most popular

Most Viewed | Top Rated | Most E-mailed

The biggest sex mistakes men and women make

Common Business Issues

- Incident Response
- Awareness and protection against the latest threats
- Data Retention
- Electronic Discovery
- Meta Data Management
- Protecting Intellectual Property
- Policy and Procedures
- Integration of business, finance and IT
- Multiple compliance requirements
- Conflicting requirements
- Legal issues
- Identity management
- Access Revocation
- Aged or stale passwords, password complexity
- Policy enforcement
- Auditing
- Improper Error Handling
- Denial of Service

Common Business Issues

- Incident Response
- Awareness and protection against the latest threats
- **Data Retention**
- Electronic Discovery
- **Meta Data Management**
- Protecting Intellectual Property
- **Policy and Procedures**
- Integration of business, finance and IT
- Multiple compliance requirements
- Conflicting requirements
- Legal issues
- **Identity management**
- Access Revocation
- **Aged or stale passwords, password complexity**
- Policy enforcement
- **Auditing**
- **Improper Error Handling**
- Denial of Service

Our Issues are the Same

- Document systems and processes
- User accounts, roles, privileges, access controls
- Identity management
- Access Revocation.
- Aged or stale passwords, password complexity
- Policy enforcement
- Auditing
- Two-factor Authentication
- Develop and maintain secure systems and applications
- Unvalidated Input
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- Injection Flaws
- Improper Error Handling
- Insecure Storage
- Denial of Service
- Insecure Configuration Management

- Incident Response
- Awareness and protection against the latest threats
- Data Retention
- Electronic Discovery
- Meta Data Management
- Protecting Intellectual Property
- Policy and Procedures
- Integration of business, finance and IT
- Multiple compliance requirements
- Conflicting requirements
- Legal issues
- Identity management
- Access Revocation
- Aged or stale passwords, password complexity
- Policy enforcement
- Auditing
- Improper Error Handling

Our Issues are the Same

- **Document systems and processes**
- **User accounts, roles, privileges, access controls**
- **Identity management**
- Access Revocation.
- **Aged or stale passwords, password complexity**
- Policy enforcement
- **Auditing**
- **Two-factor Authentication**
- **Develop and maintain secure systems and applications**
- **Unvalidated Input**
- Cross Site Scripting (XSS) Flaws
- Buffer Overflows
- **Injection Flaws**
- **Improper Error Handling**
- **Insecure Storage**
- Denial of Service
- Insecure Configuration Management

- **Incident Response**
- Awareness and protection against the latest threats
- **Data Retention**
- Electronic Discovery
- **Meta Data Management**
- **Protecting Intellectual Property**
- Policy and Procedures
- Integration of business, finance and IT
- Multiple compliance requirements
- Conflicting requirements
- Legal issues
- **Identity management**
- Access Revocation
- **Aged or stale passwords, password complexity**
- **Policy enforcement**
- **Auditing**
- **Improper Error Handling**

Who is responsible?

- Ultimately it is the Board of Directors for public companies
  - However that is a cop out answer
- CEO, CIO, IT Managers, all employees
- Every person in the company
- Corporate Culture

Regulatory Requirements and Frameworks

- CoBit – standards based IT framework
- There is a large overlap among regulatory requirements 85% is what Forester group estimated in 2006
  - A single change or improvement can satisfy many requirements
  - Coordinate your efforts between business and IT

Things to think about

- Business and IT need to take advantage of the tools that can make complying with regulatory requirements and need to:
  - Provide value to the business
  - Lower the total cost of ownership
  - Increase IT system reliability
  - Secure personal data

The basic requirements

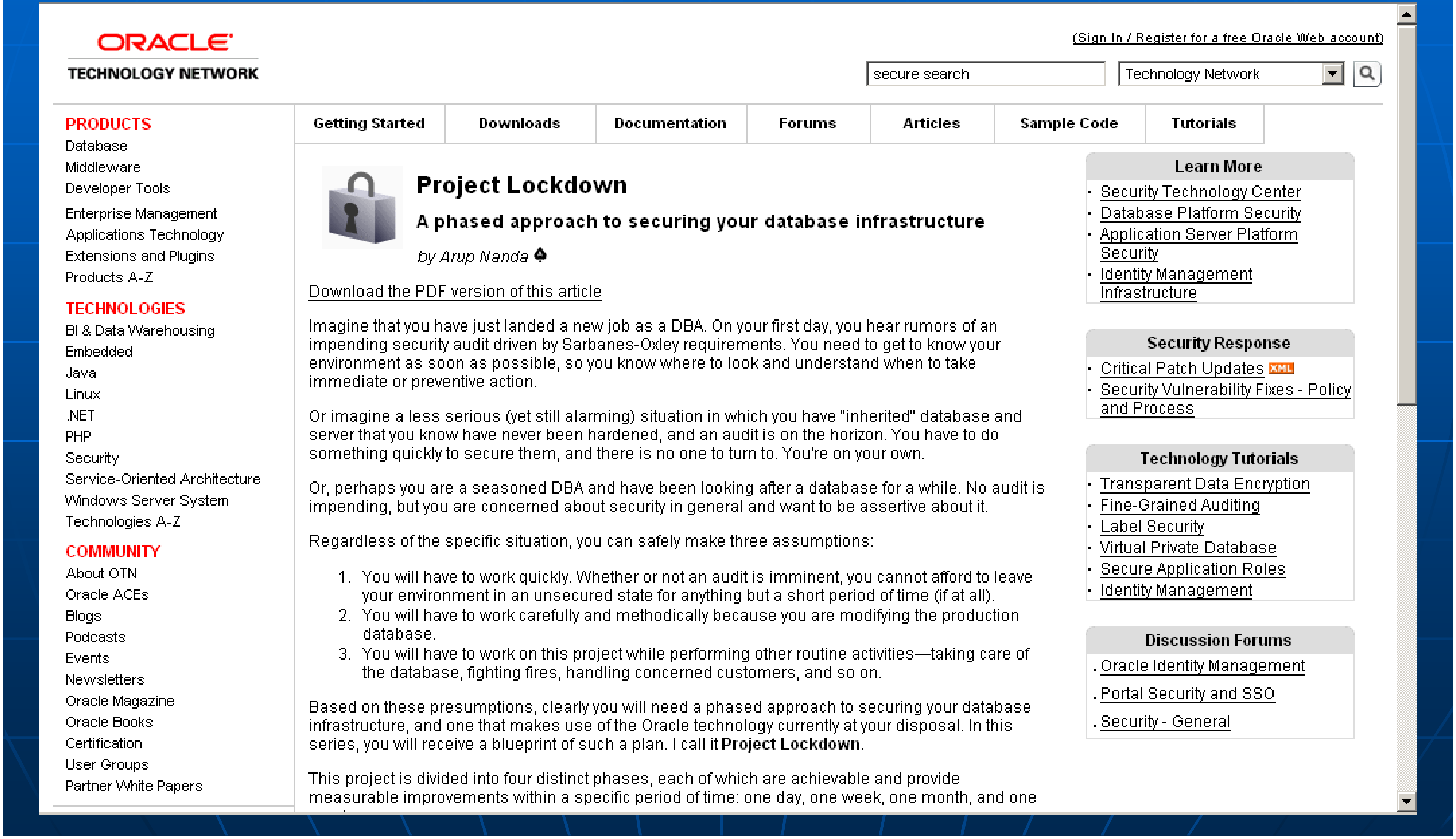
- Provisioning access to all systems that have sensitive information
- Protecting data outside the secure perimeter
- How do I prevent unauthorized access/modification to my data?
- How do I monitor my configuration?
- How do I track changes?
- How to I provision and terminate users ?
- How can I prove it ?

Things you can do in 9i+

- Follow Oracle best practices guidelines: Project Lockdown
- Secure your data center infrastructure
- Encryption network traffic and use Valid Node Checking
- Do NOT use Oracle's default roles
- Do NOT leave CREATE privileges in production schemas
- Do NOT use SYSDBA unless absolutely required
  - Use SYSOPER for startup and shutdown
- Create specific users to manage database auditing and access control
- Implement Audit Vault
- Implement Consumer Groups & Resource Management
- Implement Cryptography with the OBFUSCATION TOOLKIT
- Implement DDL Event Triggers with System Events
- Implement Product User Profiles
- Implement System Event Triggers with System Events
- Use Profiles: Password Complexity, Expiration, Lockout

Project Lockdown

www.oracle.com/technology/pub/articles/project_lockdown/index.html



Project Lockdown

A phased approach to securing your database infrastructure

by Arup Nanda ♠

Download the PDF version of this article

Imagine that you have just landed a new job as a DBA. On your first day, you hear rumors of an impending security audit driven by Sarbanes-Oxley requirements. You need to get to know your environment as soon as possible, so you know where to look and understand when to take immediate or preventive action.

Or imagine a less serious (yet still alarming) situation in which you have "inherited" database and server that you know have never been hardened, and an audit is on the horizon. You have to do something quickly to secure them, and there is no one to turn to. You're on your own.

Or, perhaps you are a seasoned DBA and have been looking after a database for a while. No audit is impending, but you are concerned about security in general and want to be assertive about it.

Regardless of the specific situation, you can safely make three assumptions:

1. You will have to work quickly. Whether or not an audit is imminent, you cannot afford to leave your environment in an unsecured state for anything but a short period of time (if at all).
2. You will have to work carefully and methodically because you are modifying the production database.
3. You will have to work on this project while performing other routine activities—taking care of the database, fighting fires, handling concerned customers, and so on.

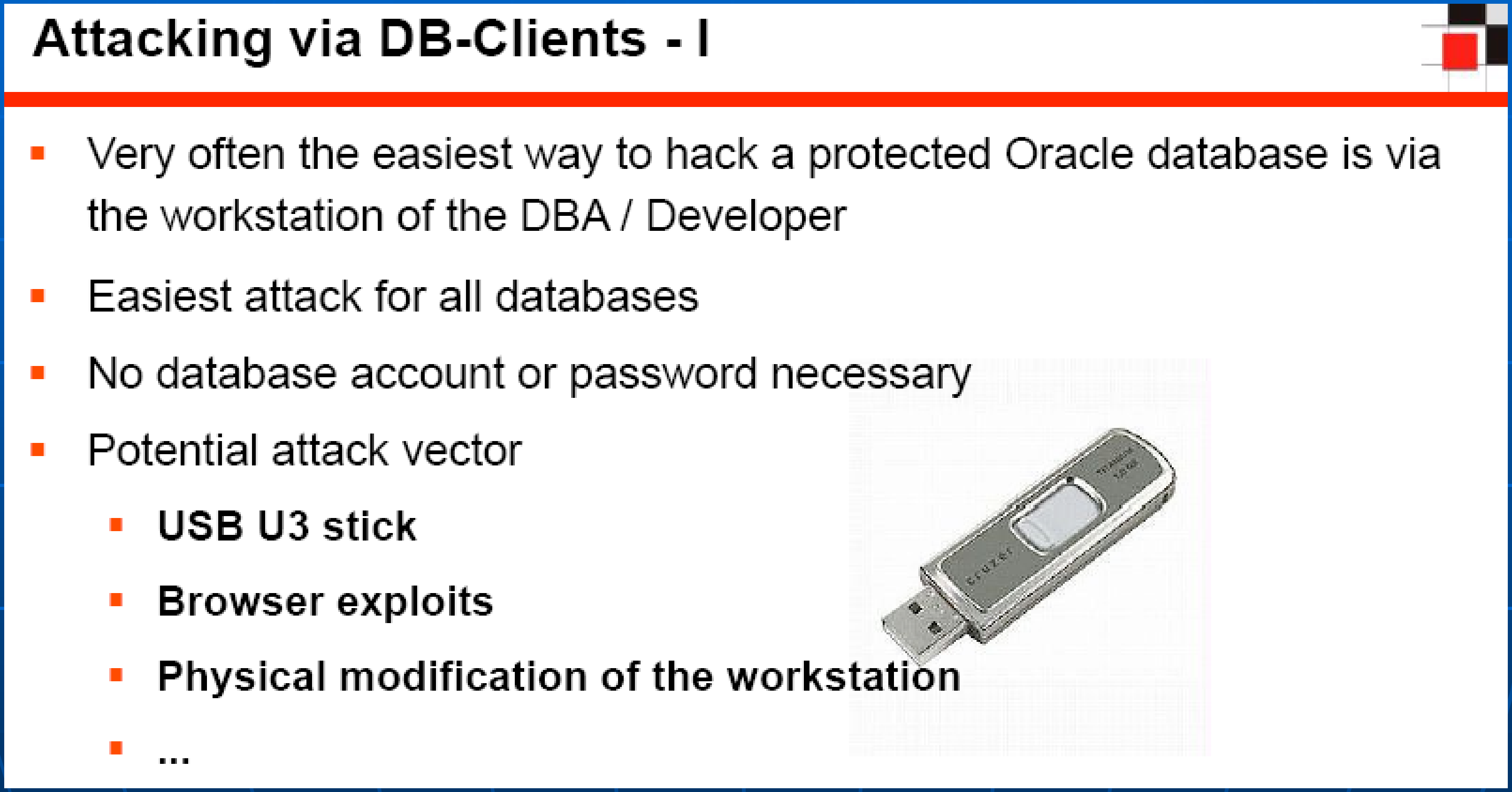
Based on these presumptions, clearly you will need a phased approach to securing your database infrastructure, and one that makes use of the Oracle technology currently at your disposal. In this series, you will receive a blueprint of such a plan. I call it **Project Lockdown**.

This project is divided into four distinct phases, each of which are achievable and provide measurable improvements within a specific period of time: one day, one week, one month, and one

Keep Patching Current

- CPU January 2006
  - Privilege escalation via Alter Session
- CPU October 2006
  - Update tables via inline views
- CPU July 2007
  - Update tables via inline views
  - Privileges escalation via DBMS_SQL

Emerging Threats



Attacking via DB-Clients - I

- Very often the easiest way to hack a protected Oracle database is via the workstation of the DBA / Developer
- Easiest attack for all databases
- No database account or password necessary
- Potential attack vector
  - **USB U3 stick**
  - **Browser exploits**
  - **Physical modification of the workstation**
  - **...**

Source: Alexander Kornbrust: Red Database Security, GmbH

Things you can do in 10g

- Audit Vault
- Cryptography (DBMS_CRYPTO and WALLETS)
- Database Vault
- Feature Usage Reporting
- Fine Grained Auditing (FGA)
  - do not use default user accounts or SYS
- OEM Grid Control Monitoring
- Secure Backup
- Transparent Data Encryption (table level)

Things you can do in 11g

- Flashback Archive
  - ORA_ROWSCN Pseudocolumn
- Network Access Control List (ACL)
  - UTL_HTTP
  - UTL_INADDR
  - UTL_MAIL
  - UTL_SMTP
  - UTL_TCP
- New PL/SQL Warnings
  - PLW-06009
- SecureFiles
- Tablespace Encryption

Other things you can do

- Multi-factor authorization
- Strong protections for personally identifiable information (PII)
- Integrated with Fusion Middleware Identity Management
- Use new external password store when possible for batch jobs
- Enterprise Manager Configuration Scanning
  - Basic configuration scanning in 10g R1
  - Even better in 10g R2
- Audit sys operations
- Don't use PII data in foreign and primary keys
- Record tables and views containing PII data
- SYSDBA Strong Authentication
- Fine-Grained Access Control on Network Call-outs from the Database
- Parameters for Enhanced Security of Database Communication
- Encrypted Dump File Sets
- OLAP Security Enhancements
- Automatic Health Monitoring
- New Capabilities for Medical Data
- Database Cloning Enhancements
- Storage / Audit Report and Metric Enhancement
- Automatic Health Monitoring
- New Capabilities for Medical Data
- Storage / Audit Report and Metric Enhancement

Flashback Archive

```
CREATE FLASHBACK ARCHIVE [DEFAULT] <flashback_archive_name>
TABLESPACE <tablespace_name>
[QUOTA <integer_value <M | G | T | P>]
RETENTION <retention_value> <YEAR | MONTH | DAY>;
```

```
Connected to:
Oracle Database 11g Enterprise Edition Release 11.1.0.6.0 - Beta
With the Partitioning, Oracle Label Security, OLAP, Data Mining,
Oracle Database Vault and Real Application Testing options

SQL> SELECT name, value
  2  FROM gv$parameter
  3  WHERE name LIKE '%retention%';

NAME                           VALUE
------------------------------ ------------------------------
db_flashback_retention_target  1440
undo_retention                 900
```

Network Access Control

DBMS_NETWORK_ACL_ADMIN

Built-in package in 11g provides security for network related PL/SQL packages UTL_TCP, UTL_HTTP, UTL_SMTP, UTL_MAIL, and UTL_INADDR.

ADD_PRIVILEGE	Adds a privilege to grant or deny the network access to the user in an access control list (ACL)
ASSIGN_ACL	Assigns an access control list to a network host, and optionally specific to a TCP port range
CHECK_PRIVILEGE	Check if a privilege is granted to or denied from the user in an access control list
CREATE_ACL	Creates an access control list with an initial privilege setting
DELETE_PRIVILEGE	Creates an access control list with an initial privilege setting
DROP_ACL	Drops an access control list
UNASSIGN_ACL	Unassigns the access control list of a network host

PLW-06009

Procedure 'string' OTHERS handler does not end in RAISE or RAISE_APPLICATION_ERROR

The OTHERS handler can exit without executing some form of RAISE or or a call to the standard procedure RAISE_APPLICATION_ERROR.

```
CREATE OR REPLACE PROCEDURE
plw06009 IS
 CURSOR c IS
 SELECT table_name
 FROM all_tables;
BEGIN
  OPEN c;
  CLOSE c;
EXCEPTION
  WHEN OTHERS THEN
    NULL;
END plw06009;
/
```

SecureFiles

```
SQL> SELECT name, value
  2  FROM gv$parameter
  3  WHERE name LIKE '%secure%';

NAME                              VALUE
--------------------------------- ---------
db_securefile                     PERMITTED
optimizer_secure_view_merging     TRUE
```

```
CREATE TABLE sec_tab2 (
rid  NUMBER(5),
bcol BLOB)
LOB (bcol)
STORE AS SECUREFILE bcol2 (
TABLESPACE securefiletbs
RETENTION MIN 3600 COMPRESS ENCRYPT CACHE READS)
TABLESPACE uwdata;
```

Tablespace Encryption

```
CREATE TABLESPACE securespace
DATAFILE 'c:\temp\secure02.dbf' SIZE 25M
ENCRYPTION USING 'AES256'
DEFAULT STORAGE(ENCRYPT);
```

```
SQL> SELECT ta.table_name, ts.tablespace_name, ts.encrypted
  2  FROM user_tables ta, user_tablespaces ts
  3  WHERE ta.tablespace_name = ts.tablespace_name
  4  ORDER BY 2, 1;

TABLE_NAME                     TABLESPACE_NAME                ENC
------------------------------ ------------------------------ ---
T1                             SECURESPACE                    YES
T2                             SECURESPACE2                   YES
AIRPLANES                      UWDATA                         NO
SERVERS                        UWDATA                         NO
SERV_INST                      UWDATA                         NO
```

Oracle's Best Error Message

ORA-28365: wallet is not open

Cause: The security module wallet has not been opened.

Action: Open the wallet.

Q&A