Holistic Database Security

Robert P. Lockard
Oraclewizard, Inc.
Glen Burnie, MD
USA
rob@oraclewizard.com

Robert Lockard

- US Navy 1978 – 1982
- George Mason University Math, Physics 1983 - 1987
- The American University Computer Science 1987 - 1992
- Canon USA, IDMS and Oracle Programmer 1986 – 1994
- Oracle Consulting 1994 – 1996
- Oraclewizard 1996 – Present
  - Financial Intelligence Systems (FinCIN, FDIC)
  - Defence Cyber Crimes

That feeling we get when we have a Security Incident

Incidents Identity Theft and Credit Card Fraud

IRS Data Breach 2015

103,000 tax payer records

Confirmed loss of $39 Million false tax returns

Anthem 2015

80 Million customer records

Home Depot 2014

56M Credit and Debit card numbers

Target Corporation

40M Credit and Debit card numbers

Incidents

Computer Intrusion

- In reports to FinCEN, computer intrusion is the primary method to collect victim identifiers including financial account info (39.5%).
- **TREND Steeply DOWN**
- The drop in reported computer intrusions may be related to the effectiveness of countermeasures and more sophisticated less detectible intrusion.
- So are we stopping the script kiddies and not detecting the more sophisticated hackers?

Takeover of Existing Account(s) and Direct Theft of Funds

- Thieves used account access information derived from
  - computer intrusion (viruses including esp. key loggers)
  - Phishing, spear phishing, and whaling
  - physical theft from victim's home, vehicle, mail, or trash.
- Accessed account through online banking or investment services, or by phone, fax, or mail.
- Often changed account or contact info including
  - Address, email address, account credentials, phone number.
- Liquidated securities holdings.
- Sent proceeds by ACH or check to thief-controlled account or had check sent to new address; or used requested duplicate or cloned debit card tied to account to drain funds.

Database Breaches

- About 0.5% of sample referenced database breaches that exposed personal identifiers.
- An identity thief apparently hacked into a state's sex offender registry to retrieve the personal identifiers of the registrants. The thief then used the identifiers to set up unauthorized investment accounts. The filer discovered the likely source of the identifiers by searching victim names on the Internet.
- A filer's former employee sold several dozen sets of account holder identifiers to identity thieves.
- A contract employee of a firm exposed thousands of customer accounts by accessing the company's customer database from a public computer.

More Novel Scenarios

- Public Computer Infection
- Thieves stayed at four and five star hotels.
- Infected public computers with key loggers.
- Gathered personal and financial account information from wealthy.
- Drained accounts.

Set up of New Unauthorized Account(s) Using Victim Identifiers

- Thieves who lacked account credentials, but had sufficient victim identifiers often set up new unauthorized accounts in victim names.
- Mainly funded from existing demand accounts using ACH, fraudulent or counterfeit checks.
- Typically, immediate attempt to move money out of account by ACH, by checks written on the account or drawn on official disbursement account of investment firm, or by use of debit card issued at account opening; all before funding ACH transfer(s) or check(s) returned unauthorized or counterfeit.

My Experience with Social Engineering

- Call to the help desk for information on transmitting sensitive information.
- Help Desk transferred the call to me.
- Two People, first was a from the business unit. Second person was from the business security division

Agenda

- Risks
- Audit
- Real Application Security
  - Realms
  - Virtual Private Database (VPD)
  - Redaction
- Encryption
  - Network
  - Tablespace
  - Table
- Database Vault
- Database Firewall

What could possibility go wrong?

Risk Assessment

Follow the data
- Identify sensitive data.
- Identify all access paths to the data.
- How do user group access the data?

Where do you build the security?
- Database
- Application
- Network
- All of the above

Risk Mitigation Template

Audit

Standard Audit

Unified Audit - 12C

Fine Grained Auditing

All audits are post event

Unified Audit

Unified Audit – 12C

Check if unified audit is on

Select value from v$option where parameter = 'Unified Auditing';

Enable Unified Auditing

- [oracle@owirdb1 ~]$ cd $ORACLE_HOME/rdbms/lib
- [oracle@owirdb1 lib]$ make -f ins_rdbms.mk uniaud_on ioracle

Unified Audit

Unified Audit Policies - Predefined policies

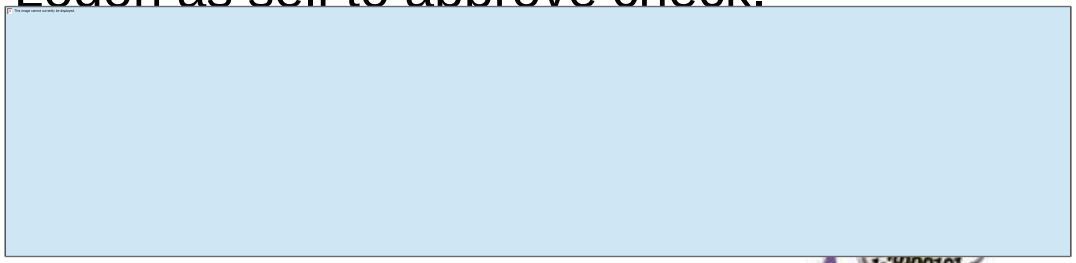
- ORA_LOGON_FAILURES
- ORA_SECURECONFIG
- ORA_DATABASE_PARAMETER
- ORA_ACCOUNT_MGMT
- ORA_CIS_RECOMMENDATIONS
- ORA_RAS_POLICY_MGMT
- ORA_DV_AUDPOL

Fine Grained Audit

Audit Use Case
NATHAN MUELLER - ING

$8.5M Fraud over four years.

- Should have been caught
- Shared logins for convenience
  - Separation of duties
  - Logon as one person to request a check
  - Logon as self to approve check.



Redaction Use Cases

Redaction Use Cases

- Sensitive Information – either by itself or in combination
  - Full name (if not common)
  - Home address
  - Email address (if private from an association/club membership, etc.)
  - National identification number
  - Passport number
  - IP address (in some cases)
  - Vehicle registration plate number
  - Driver's license number
  - Credit card numbers
  - Digital identity
  - Date of birth

Redaction Privileges

- Grant execute on DBMS_REDACT to <user>;
- grant select on Sys.redaction_policies to <user>;
- grant select on Sys.redaction_columns to <user>;
- grant execute on dbms_redact to <user>;

Redaction

- dbms_redact
  - add_policy
  - alter_policy
  - enable_policy
  - disable_policy
  - drop_policy

Redaction Demo

Virtual Private Database

- Use Case
  - Access HR Records by
    - Time
    - IP Address
    - Role

Virtual Private Database Demo

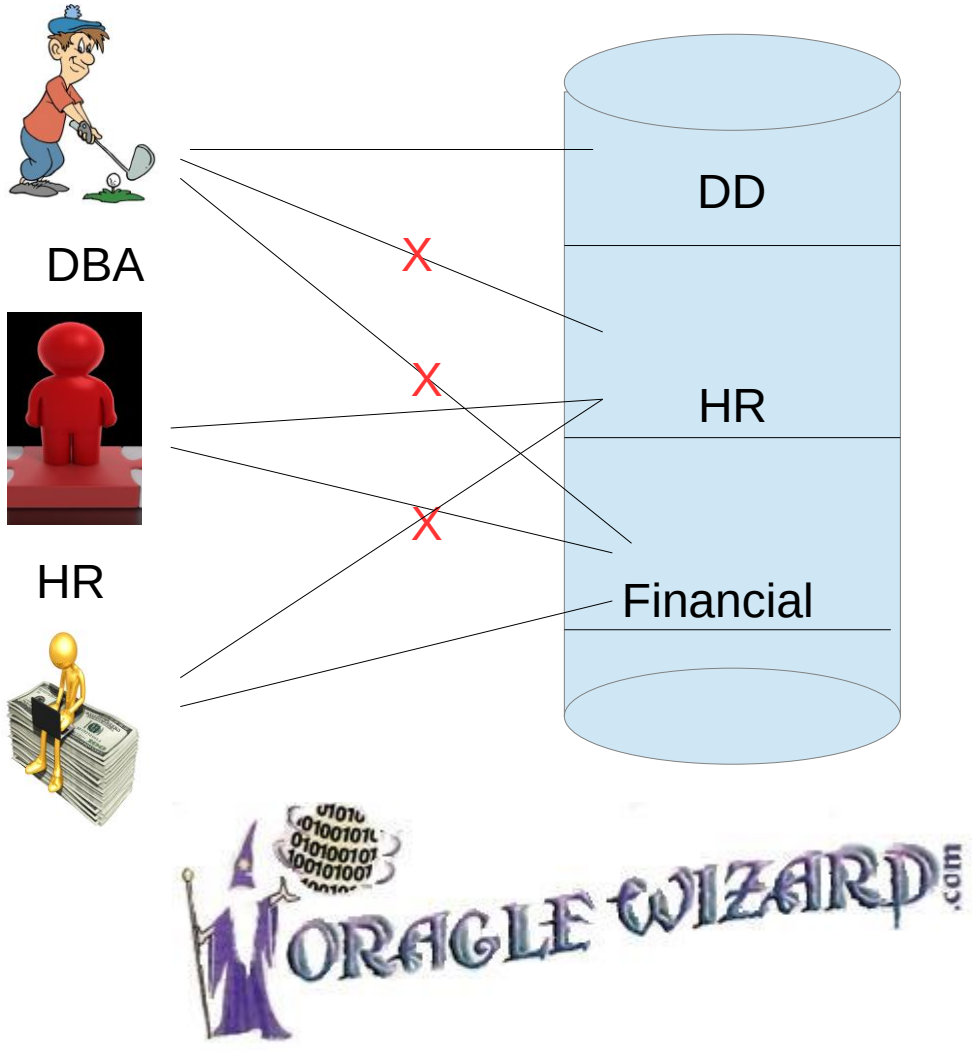
-

Encryption

- Algorithms
- Data at rest
  - Tablespace
  - Table
  - Column
- Data in motion

Database Vault

- Separation of duties



Database Firewall