Effective Database Security

Database Top 10 Threats

NY Oracle Users Group

June 6, 2007

Idan Soen

Imperva Senior Security Engineer

idan@imperva.com

Database Top 10 Threats According to:
Imperva's Application Defense Center (ADC)

- Security Research Team focused on database and web application security issues
  - Discovered over 50 commercial application vulnerabilities
    - 18 published, including Oracle, MS-SQL, and DB2
  - Today's top ten is the result of ADC research and analysis of the state of database security

- Led by Amichai Shulman, Imperva CTO
  - Named to InfoWorld's "Top 25 CTO" list for 2006

Database Top 10 Threats

Agenda

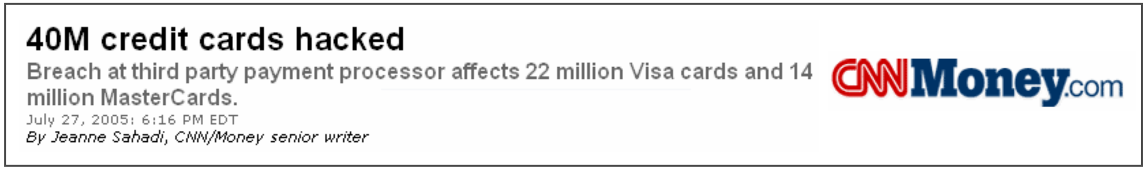
- Database Security Drivers
- Database Top 10
- Database Top 10 Walkthrough
  - Definition
  - Consequences
  - Mitigation Techniques
- Imperva’s Approach to Database Security

Database Security Drivers

Implications of Data Breach

Direct and Indirect Financial Loss

- Brand damage
- Service shut down
- Partner loss
- Customer loss
- Lawsuits
- Company shut down
- Fire sale of assets
- Federal, internal, and external Investigations
- Fines
- Increased regulations



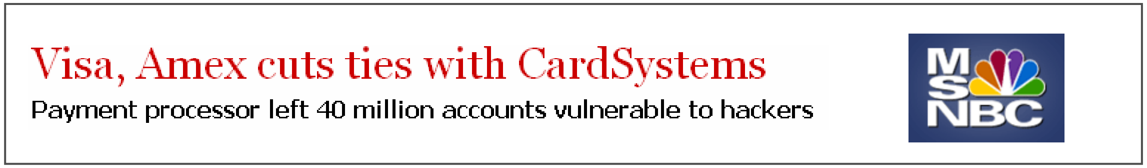
40M credit cards hacked

Breach at third party payment processor affects 22 million Visa cards and 14 million MasterCards.

July 27, 2005: 6:16 PM EDT

By Jeanne Sahadi, CNN/Money senior writer

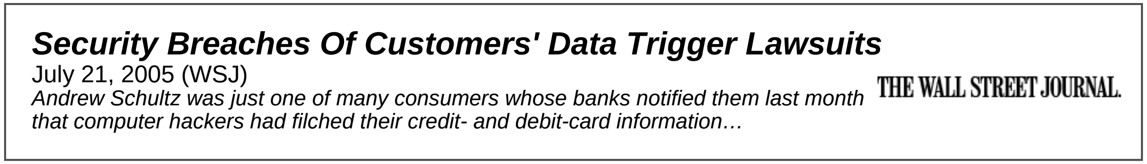
CNNMoney.com



Visa, Amex cuts ties with CardSystems

Payment processor left 40 million accounts vulnerable to hackers

MSNBC

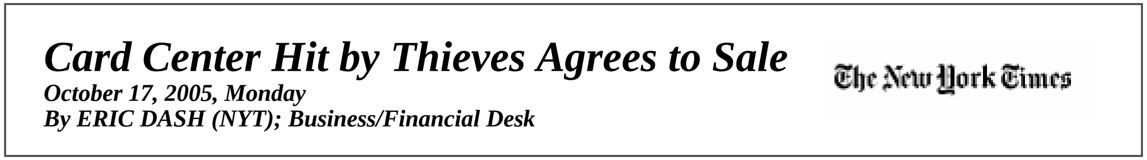


Security Breaches Of Customers' Data Trigger Lawsuits

July 21, 2005 (WSJ)

Andrew Schultz was just one of many consumers whose banks notified them last month that computer hackers had filched their credit- and debit-card information…

THE WALL STREET JOURNAL.

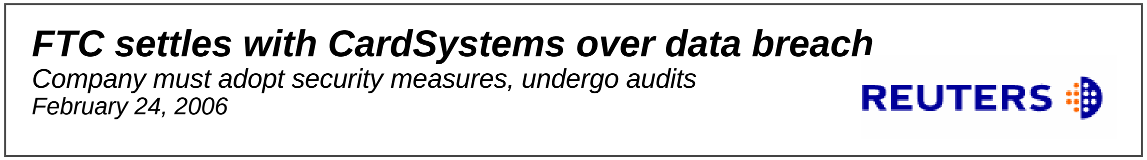


Card Center Hit by Thieves Agrees to Sale

October 17, 2005, Monday

By ERIC DASH (NYT); Business/Financial Desk

The New York Times



FTC settles with CardSystems over data breach

Company must adopt security measures, undergo audits

February 24, 2006

REUTERS

Database Top 10 Drivers

- Effective Database Security
  - Allocate resources and attention to topmost threats
  - Threats apply across all database vendors
- Universal Guidelines for Mitigation
  - Do not re-invent the wheel every time
- Standard for Evaluation
  - Criteria for evaluation of database security solution
  - Criteria for evaluating the security of a database deployment

Database Top 10 Walkthrough

1. Excessive Privilege Abuse
2. Legitimate Privilege Abuse
3. Privilege Elevation
4. Database Platform Vulnerabilities
5. SQL Injection
6. Weak Audit
7. Denial of Service
8. Database Communication Protocol Vulnerabilities
9. Weak Authentication
10. Backup Data Exposure

Database Top 10 Threats
#1 - Excessive Privilege Abuse

- Definition: Users (or applications) granted database access privileges in excess of “business need-to-know”
  - Hard to obtain a true list of required privileges
    - Even harder to keep this list updated
  - Database ACL semantics are too limited
    - Not enough to specify operations allowed for table by user
- Consequence:
  - Any “minor” breach becomes a major incident!
  - See SQL Injection
- Mitigation
  - More granular ACLs: Query ACLs
    - What queries are allowed against the table by this user
  - Automatic and Dynamic ACL profiling

Mitigation

Query Access Control Lists

Query Control List

- ***Select * from orders where order_id = ?***
- ***Select * from users where username = ? And password = ?***

Data Leakage
via Database Access

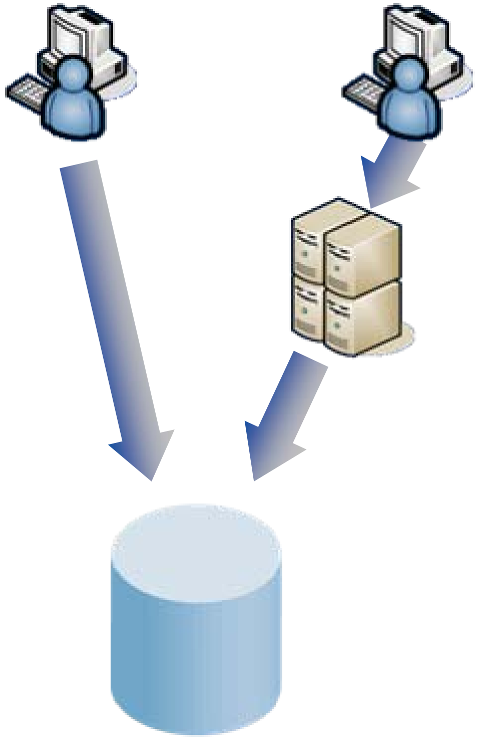
Normal Usage

```
Select * from orders
where order_id = 60
```

Privilege Abuse

```
Select username,
password from
AdminUsers
```

New table



Data Leakage
via Web Application

Normal Usage

```
Select * from users where
username = ‘john’ and
password = ‘smith’
```

SQL Injection

```
Select * from users where
username = ‘john’ and
password = ‘smith’
or 1=1
```

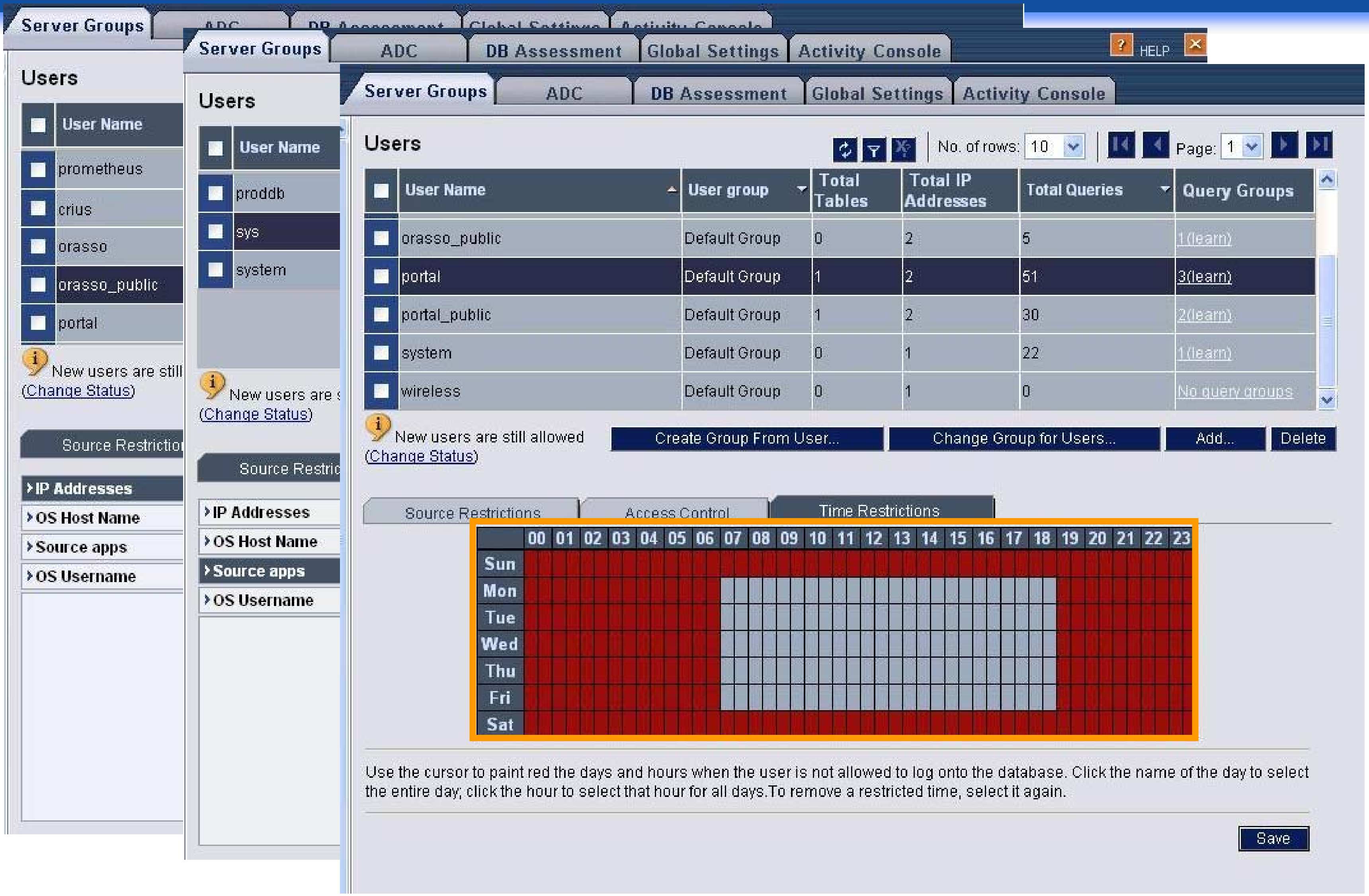
Additional Clause

Database Top 10 Threats
#2 - Legitimate Privilege Abuse

- Definition: Abuse legitimate db privileges for unauthorized purposes
  - Use simple and available desktop tools
  - Retrieve large quantities of data
  - Store sensitive data locally
  - Make unauthorized changes
- Consequence
  - Data theft
  - Data loss
  - Embezzlement
- Mitigation
  - More granular ACL: Context based ACL
  - ACL augmented with the context of query
    - E.g. Client machine, client software, time-of-day

Mitigation

Context based ACL



Server Groups | ADC | DB Assessment | Global Settings | Activity Console

Users

□	User Name
□	prometheus
□	crius
□	orasso
□	orasso_public
□	portal

New users are still
(Change Status)

Source Restriction

- IP Addresses
- OS Host Name
- Source apps
- OS Username

Server Groups | ADC | DB Assessment | Global Settings | Activity Console | HELP

Users

□	User Name
□	proddb
□	sys
□	system

New users are s
(Change Status)

Source Restric

- IP Addresses
- OS Host Name
- Source apps
- OS Username

Server Groups | ADC | DB Assessment | Global Settings | Activity Console

Users

No. of rows: 10 Page: 1

□	User Name	User group	Total Tables	Total IP Addresses	Total Queries	Query Groups
□	orasso_public	Default Group	0	2	5	1 (learn)
□	portal	Default Group	1	2	51	3(learn)
□	portal_public	Default Group	1	2	30	2(learn)
□	system	Default Group	0	1	22	1 (learn)
□	wireless	Default Group	0	1	0	No query groups

New users are still allowed
(Change Status)

Create Group From User... | Change Group for Users... | Add... | Delete

Source Restrictions | Access Control | Time Restrictions

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Mon	🟥	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟥	🟥	🟥	🟥	🟥
Tue	🟥	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟥	🟥	🟥	🟥	🟥
Wed	🟥	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟥	🟥	🟥	🟥	🟥
Thu	🟥	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟥	🟥	🟥	🟥	🟥
Fri	🟥	🟥	🟥	🟥	🟥	🟥	🟥	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	🟥	🟥	🟥	🟥	🟥
Sat	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

Use the cursor to paint red the days and hours when the user is not allowed to log onto the database. Click the name of the day to select the entire day; click the hour to select that hour for all days.To remove a restricted time, select it again.

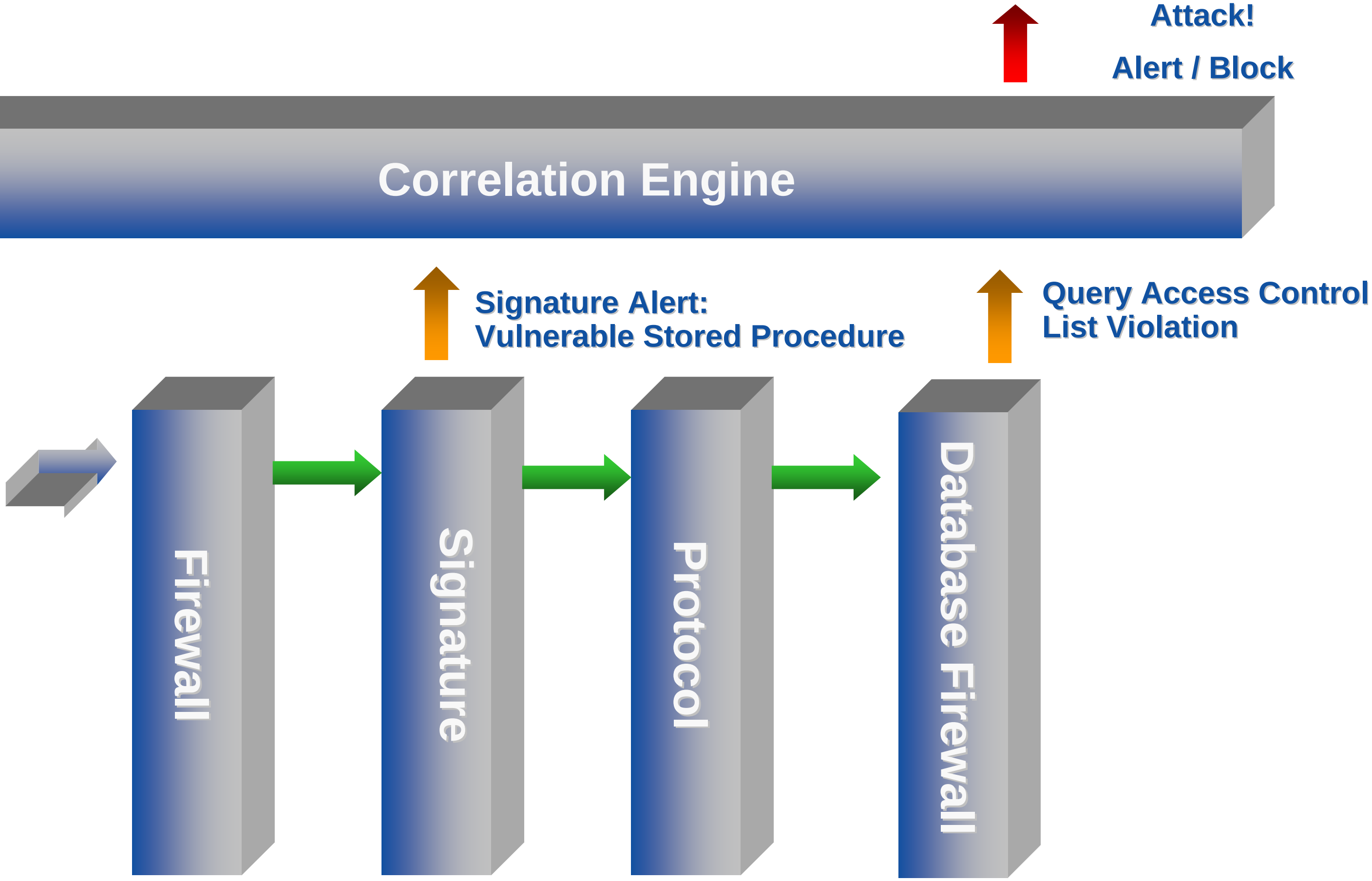
Save

Database Top 10 Threats
#3 - Privilege Elevation

- Definition: Low privileged user exploit database vulnerabilities to gain administrative privileges.
  - Susceptible objects
    - Stored procedures
    - SQL Statements
    - Built-in functions
  - Types of vulnerabilities
    - Buffer Overflow
    - SQL Injection
    - Semantic glitches
- Consequence
  - Any “minor” breach becomes a major incident
  - Built-in access control becomes ineffective
- Mitigation
  - More granular ACL: Query level ACLs
  - Traditional IPS: Patterns for susceptible objects
  - Correlated detection:

Mitigation

Correlation Detection



Attack!

Alert / Block

Correlation Engine

Signature Alert:
Vulnerable Stored Procedure

Query Access Control
List Violation

Database Top 10 Threats

#4 - Database Platform Vulnerabilities

- Definition: Vulnerabilities in underlying operating systems and services installed on a database server
  - OS - Windows 2000, UNIX, etc.
  - Additional Services – eg. SNMP, NETBios, DCOM, DNS, etc.
  - Example: Blaster worm on Windows machines running MS SQL Server
- Consequence
  - Server is compromised
  - Direct access to database files
  - Local access through admin roles
  - Install backdoors
- Mitigation
  - Network ACLs: Simple FW to allow access only to required services
  - Network IPS: Traditional detection of known vulnerabilities

Database Top 10 Threats
#5 - SQL Injection

- Definition: Attacker inserts an unauthorized SQL **statement** through an SQL **data** channel:
  - Data Channel - e.g., Parameter of stored procedures or Web form
  - Most common attack type on web connected databases
- Consequence
  - Access to unauthorized data
  - Unauthorized data manipulation
  - Denial of Service
  - Privilege elevation
- Mitigation
  - More granular ACL: Query ACLs
  - Automatic and dynamic generation of ACLs
  - Correlation with Web front end

Database Top 10 Threats
#6 - Weak Audit

- Definition: Audit policies that rely on built-in database mechanisms suffer a number of weaknesses

  - Usually due to:
    - Performance degradation and DBA attention span
    - Knowing what matters in the mountain of audit data
    - Vulnerability to privilege elevation as well as other database attacks
    - Limited granularity
    - Proprietary

  - No end-to-end identity tracking
    - In 3 tier environments
    - Application server uses a pooled connection policy to access database
    - Built in mechanism only records account name and have no information with respect to the actual end user.

Database Top 10 Threats
#6 - Weak Audit

- Consequence
  - Regulatory problems
  - Data is not there when you need it
- Mitigation
  - Independent auditing device
  - See Imperva Webinar on “Database Auditing”
  - See Imperva white paper “Risky Business – The Self Auditing DB”
  - See Imperva Webinar on “Top Audit Issues”
  - See Imperva white paper “What Auditors Want – Database Auditing”

Database Top 10 Threats
#7 - Denial of Service

- Definition: Attacks that affect the availability of information from the database to users
  - A general type of attack, many technique exists:
    - Specific vulnerabilities: SQL injection, platform vulnerabilities, database vulnerabilities
    - Resource oriented attacks: Exhaustion of specific resources such as bandwidth, CPU and database connections
- Consequence
  - Critical for modern day organizations
  - Paralyzing the entire operation of an organization or part of it

Database Top 10 Threats

#7 - Denial of Service

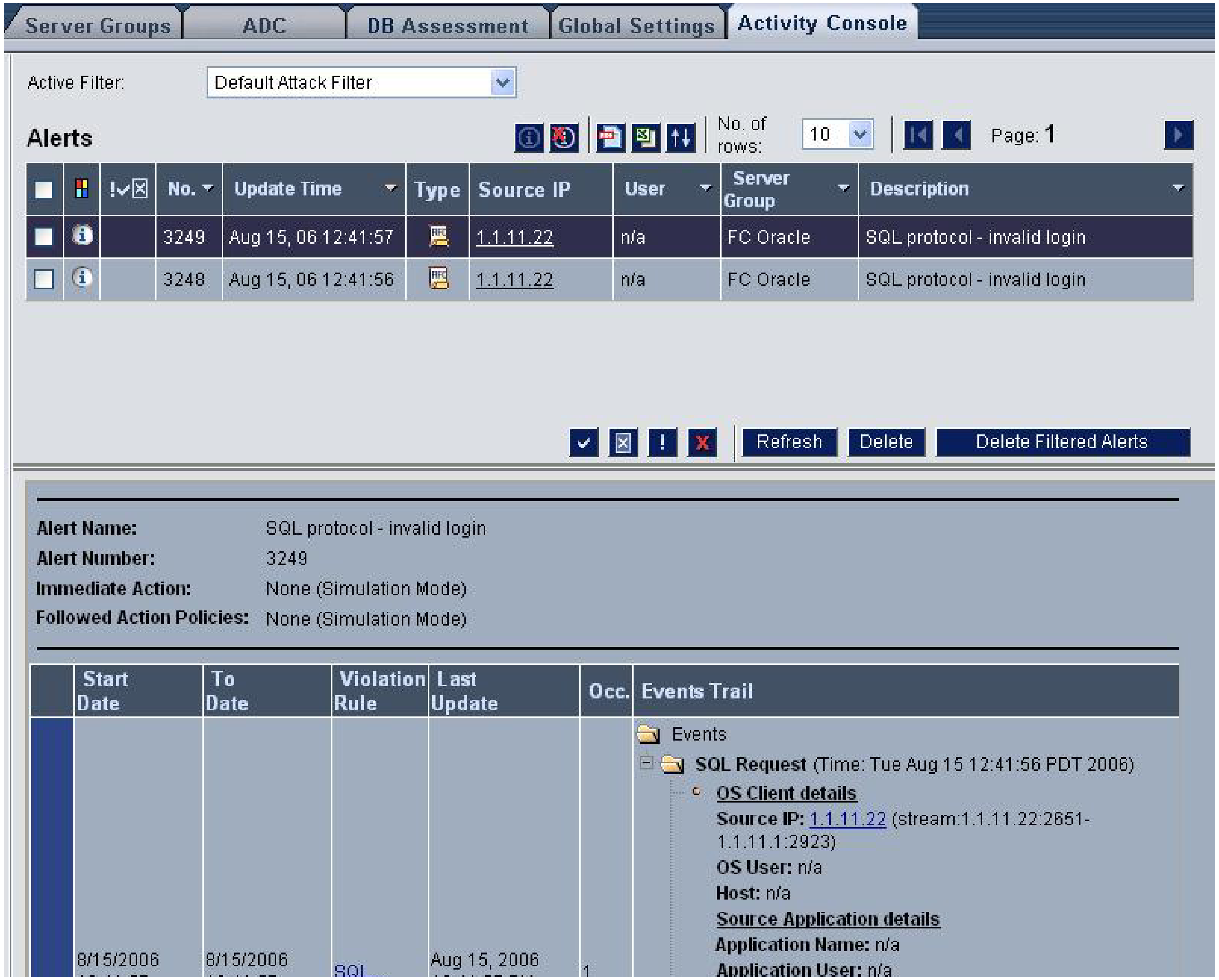
- Mitigation
  - Specific mechanisms for specific vulnerabilities
  - Resource control mechanisms
    - Timing responses
    - Sizing responses
    - Connection control
  - Problem detection
    - Timing latency in system
      - If there is a dramatic increase in latency then DoS detected and addressed

Database Top 10 Threats
#8 - Database Communication Protocol Vulnerabilities

- Definition: Tampering with db related network protocol messages
  - Each vendor relies on proprietary network protocol to communicate data and commands
  - Such complex (and mostly obscure) protocols are prone to security vulnerabilities
- Consequence
  - Unauthorized data access and manipulation
  - Denial of Service
- Mitigation
  - Protocol validation engine (addresses even unknown vulnerabilities)
    - Only let through normal client generated messages
    - Throw out requests that use hidden qualities or features of the protocols
  - Reactive protocol validation (addresses known vulnerabilities)
    - Checks for specific known attacks

Database Top 10 Threats

#8 - Database Communication Protocol Vulnerabilities



Active Filter: Default Attack Filter

Alerts

No. of rows: 10

Page: 1

□		!✓☒	No.	Update Time	Type	Source IP	User	Server Group	Description
□	ℹ		3249	Aug 15, 06 12:41:57		1.1.11.22	n/a	FC Oracle	SQL protocol - invalid login
□	ℹ		3248	Aug 15, 06 12:41:56		1.1.11.22	n/a	FC Oracle	SQL protocol - invalid login

Alert Name: SQL protocol - invalid login

Alert Number: 3249

Immediate Action: None (Simulation Mode)

Followed Action Policies: None (Simulation Mode)

	Start Date	To Date	Violation Rule	Last Update	Occ.	Events Trail
	8/15/2006	8/15/2006	SQL	Aug 15, 2006	1	Events **SQL Request** (Time: Tue Aug 15 12:41:56 PDT 2006) **OS Client details** **Source IP:** 1.1.11.22 (stream:1.1.11.22:2651-1.1.11.1:2923) **OS User:** n/a **Host:** n/a **Source Application details** **Application Name:** n/a **Application User:** n/a

Database Top 10 Threats
#9 - Weak Authentication

- Definition: Weak account names and/or passwords
  - Account name often adhere to some organizational standard (e.g. John.Smith, Jane.Doe, JSmith, J.Doe)
  - Bad (or rather predictable) choice of passwords by users
- Consequence
  - Credential theft
  - Brute force attacks are feasible
- Mitigation
  - Use two factor authentication
  - Enforce strong password policy

Database Top 10 Threats
#9 - Weak Authentication (cont.)

- Mitigation (cont.)
  - Detect identify related attacks
    - Brute force
    - Unauthorized use of credentials
  - Actively assess authentication mechanism
    - Make sure users choose strong passwords

Database Top 10 Threats
#10 - Backup Data Exposure

- Definition: Unencrypted data on Back-up Tapes and Disk
  - Many recent incidents where backup media is lost or stolen
- Consequence
  - Exposure of huge amounts of sensitive information
- Mitigation
  - End-to-end encryption:
    - Problematic: Application dependent, complex key management, persistent exposure if user’s key is lost
  - Disk encryption: data have to be encrypted again for backup
  - Database encryption: Performance degradation
    - Indexing encrypted information
  - A better solution is yet to be found

Question & Answer

Thank You

Imperva, Inc.

950 Tower Lane, Suite 1550
Foster City, CA 94404
Sales: (866) 926-4678

www.imperva.com