WHITE PAPER

Scanning Databases for Credit Card Data

A DbScanLabs White Paper

Published March 2013

DBScanLabs, Pty Ltd

Suite 392, 585 Little Collins Street Melbourne 3000, Victoria Australia

info@dbscanlabs.com

http://www.dbscanlabs.com

EXECUTIVE SUMMARY

With the arrival of PCI DSS compliance there has been a lot of focus on locating and securing all data pertaining to credit cards. The PCI Council has published a very detailed list of compliance requirements in this regard (https://www.pcisecuritystandards.org)

It is vital that all organisations, irrespective of whether they want to be PCI compliant or not, locate and secure Credit Card information. Failure to do so could result in serious breaches and loss of business and reputation.

As part of normal day to day business operations, Credit card data can end up on file systems and in databases in the clear. In most cases the administrators and end users are unaware of the total volumes and exact locations of this data. For example in one case, call centre operators were entering clear text credit card data in a comments field as part of an operational procedure. Over time, this resulted in more than 100,000 cards being stored in a database in the clear. The designers of the system, the Database Administrators in charge of the database and the application support team were all unaware of this. As part of a PCI Audit requirement they all stipulated that the system did not store Credit Card data. It came as huge surprise to all, when a scan of the database revealed 100,000+ credit cards stored in the clear.

Is credit card data stored in the clear on your databases and file systems?

If the answer is No, how can you be 100% sure that this is correct?

If the answer is Yes, do you know exactly where and how much?

The bottom line is, all businesses need to check whether credit card data is being stored in the clear, in file systems and databases. Once such data has been located then it's a matter of either removing it, or if it is required for business processes, securing it.

A key point to note is that relying on system designers, system/database administrators and/or end users to provide information about where credit card data could exist in the clear, is fraught with danger.

The only full proof method to locate such data is to SCAN the file systems and databases.

A number of very efficient file system scanners exist. As such scanning large file systems for clear card data is not a problem. Scanning operational databases for clear card data is however a totally different proposition. To achieve this you require a smart database scanning tool.

ABOUT THIS WHITE PAPER

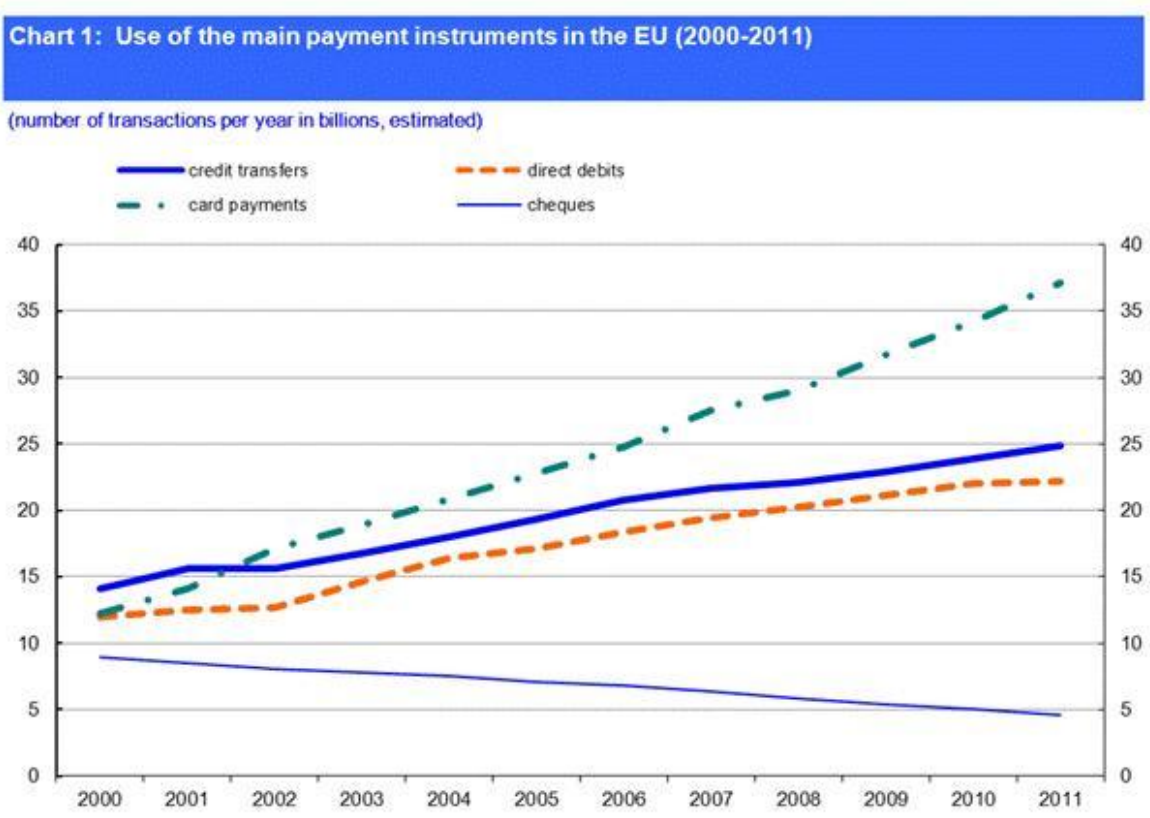
The purpose of this white paper is twofold:

- To outline the need to regularly scan databases for clear card data
- Highlight the different features and core functionality that a database scanner should have

The Oracle Database Scanner from DB Scan Labs is used to demonstrate some of the features.

USAGE AND STORAGE OF CREDIT CARDS IS ON THE RISE

According to "2012-2017 Retail Point of Sale Forecast from Javelin" cash payments do not prevail anymore at points of sale. As of June 2012, debit card payments currently hold the largest share (31%), followed by credit cards (29%).[1] As can be seen from the diagram below the use of credit and debit cards is on the rise. The forecasts are that this will continue worldwide for the next 5 years at least. Credit card Point-of-Sale purchases are expected to grow from 29% to 33% by 2017.[2]



Source: ECB [3] (http://www.ecb.int/press/pr/date/2012/html/pr120910.en.html)

The only way to obtain information about what clear card data is stored in your systems is to SCAN REGULARLY.

As part of standard transaction processing, it is not unusual to store credit card data either temporarily or permanently on the file system or in a database.

Credit card data is stored

- To support the transaction process
- For audit and historical purposes
- To uniquely identify clients

Storage methods can be broadly classified as

- Truncated/Masked (only store the first 6 and last 4 digits of the card)
- Hashed (convert card number to a long hash value using non reversible algorithm)
- Encrypted (encrypt the card number using software or hardware based encryption)
- Store in the clear

Systems that weren't designed with Security and PCI Compliance in mind often store credit cards in the clear, as it provides a simple way of:

- Uniquely identifying a client and/or transaction.
- reconciling a disputed transaction

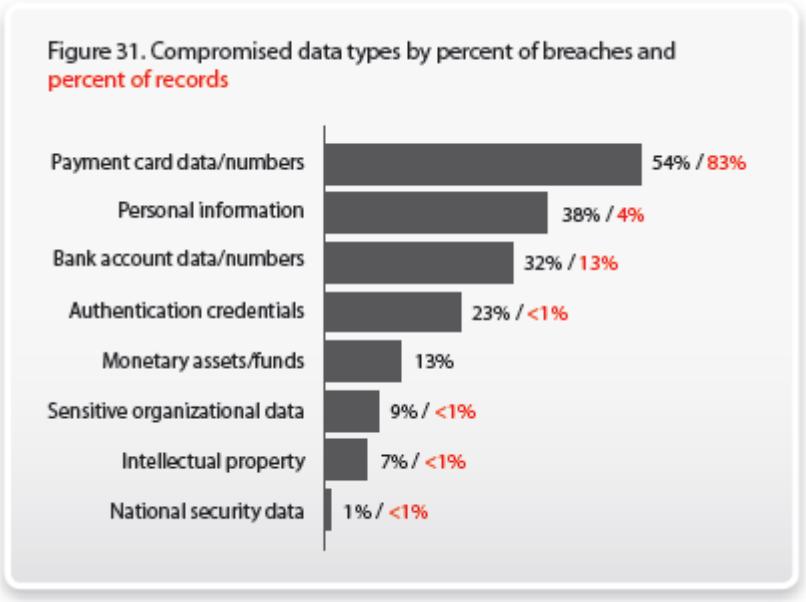
Truncated/Masked cards are not suitable for this as they are not unique.

Hashed cards provide a unique identifier, while Encrypted cards do provide the ability to decrypt the card back to its original value.

However, as hashing and encryption/decryption operations are relatively complex, some systems just resort to storing card data in the clear.

SOLUTIONS THAT WON'T SOLVE THE PROBLEM

The problem is as follows: If your system stores card data in the clear on either the files system or the database, then you are vulnerable (see the diagram below).



Source: Verizon 2010 Data Breach Investigation Report [4]

There is a number of ways that this sensitive data can be obtained by unauthorised users. One of the most common leaks is the database backups being restored elsewhere and sensitive data extracted.

The key issue is working out what clear card data is stored where.

The methods available for working this out are as follows:

- Carry out a data audit by looking at all the system design documents and talking to the designers of the system(s)
- Look at the file/table structures and try to determine where clear card data could be stored
- Construct and maintain an asset register by interviewing all the key skill groups

Unfortunately, none of these methods will provide conclusive and up to date information.

The only way to locate clear card data on the file systems and databases is to perform FULL scans REGULARLY.

It is not uncommon for large corporations to spend millions of dollars on the following :

- constructing an asset register of all systems that store card data
- building a secure area to store this sensitive data
- storing the sensitive data encrypted and/or hashed

However, we have come across a few examples where

- PCI compliance was obtained based on the contents of the asset register constructed
- It was subsequently discovered that databases outside of this secure area, contained credit card data in the clear.

They were obviously missed during the initial construction of the asset register, either due to incomplete information or the offending databases were brought in house after the asset register was created.

SCANNING DATABASES CAN BE COMPLEX

Scanning files systems is relatively easy. In general such scans use little processing power and rarely cause any performance impact.

Scanning databases on the other hand is much more complex task.
Some key factors to consider with database scanning are:

Performance Impact	Can the scanning be done in a non-intrusive manner with minimal impact to applications and end users?
Scan Efficiency	A generic scanner that works for all databases is not ideal. Specific scanners for specific database types are far more efficient.
Scan Completenes	Are all the data types supported and will all the occurrences of clear card data be found?
Scheduling flexibility	Can scans be scheduled to run during non-peak windows, can scans be paused and resumed?
DB platform awareness	The scanning tool should make full use of the key database features. For example for Oracle databases, it should be aware of parallelisation options, partitioning etc.
Database size	Ability to work with large databases – i.e. databases of size 10TB and larger

(The Oracle database scanner from DBScanLabs caters for all of the above)

Can your database scanner scan with minimal impact to performance?

Can it scan multi-terabyte databases?

SOME SCENARIOS

Db Scan Labs have come across the following scenarios at client sites :

SCENARIO 1

A Company conducts a detailed in house audit of all its databases but not all Card Data is picked up. This was primarily due to the lack of in house expertise with regard to certain databases. Legacy systems, where the original SME's are no longer with the company and/or recently acquired systems, with little subject matter expertise, were the main contributors.

SCENARIO 2

A Company attains PCI DSS compliance. However, it then acquires another company and a collection of new databases are brought in house. The fact that they contain clear card data goes undetected for an entire year.

SCENARIO 3

A company detects a database with clear card data and implements a successful program to encrypt and secure this data. However, the fact that this data had been previously copied over to a non-production database, which has then subsequently been cloned many times, goes undetected for 6 months.

Carry out scheduled scans of your databases.

SCENARIO 4

A similar variant of the above is that a downstream warehouse database has received feeds containing clear card data. Even though the source system was listed as a PCI Asset and all the data subsequently hashed, the fact that the downstream warehouse had 4 years of clear card, data went undetected for 8 months.

Treat it like scanning for viruses.

SCENARIO 5

A company goes through a rigorous process to secure its card data. However, a new code drop inadvertently stores some clear card data in a temporary table. This goes undetected during testing and is only picked up 3 weeks later in production entirely by accident.

So how can an organisation ensure that ALL its databases have no clear card data?

The answer is to scan ALL databases and to scan them regularly.

The standard objections to this are:

- It’s too hard and involves too much work
- It will impact production databases and hence is not feasible.

Given the new generation of flexible, efficient database scanners, these objections are no longer relevant.

BEST PRACTICE FOR SCANNING

It is best if databases deemed to be at risk are scanned regularly. Database scanning for credit card data should be viewed in a similar way to "virus scanning".

Some possible scanning schedules are as follows :

Small (< 200GB) OLTP type transactional database

- Full scan of the database every week.
- Incremental/sample scans every day

Medium (<1TB) Data warehouse

- Full scan every month
- Incremental/sample scans every week

Large (>1TB) Data Warehouse

- Full scan every quarter
- Incremental/sample scans every month

Most important – pick an effective database scanning tool, that is fast, efficient, low impact and flexible.

Pick an effective and efficient database scanning tool

ABOUT DB SCAN LABS

DBScanLabs is an Australian software company headquartered in Melbourne, Victoria.

We specialize in creating database scanning products designed to assist companies with PCI Compliance audits. We aspire to deliver benefits for merchants and PCI QSAs who use our products to achieve the following functions:

1. Identify unprotected Payment Card Data across the company databases.

2. Produce comprehensive and accurate report to use in PCI audit.

3. Reduce the risk of Payment Card Data theft.

We focus on solving the problem of identifying security weaknesses in storage and handling of Payment Card Data in databases. This is achieved by providing the industry with rapid ability to identify unprotected data and mitigate that risk.

For more information, please visit http://www.dbscanlabs.com

---

[1] Javelin's "2012-2017 Retail Point of Sale Forecast"

[2] http://www.business2community.com/infographics/2012-us-credit-card-usage-statistics-0335200#2zQHQqiVAzOF7Lkz.99

[3] European Central Bank, http://www.ecb.int/press/pr/date/2012/html/pr120910.en.html

[4] Verizon, 2010 Data Breach Investigation Report, http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf