Credit Card Data Security

by Kartik Subbaraman, Lead Consultant in the Enterprise Solutions Group at Infosys Technologies Limited

Abstract:

Credit Cards have become ubiquitous as a payment mechanism in today's world. However, dealing with credit cards also leads to a host of security challenges in maintaining and securing card holder data. Oracle provides many security features in I-Payments (R11i)/ Payments (R12) module for securing card holder information. Typically implementation teams associate credit card security in Oracle as encryption of card holder data in the database. However, there are other critical components of data security which merit equal attention. This paper highlights these components and outlines a four step approach which will be helpful to the program management teams to ensure that customer credit card data is safeguarded in a reliable manner.

Introduction

From the early 1920's when credit cards were first introduced in the United Sates for selling fuel to automobile owners, credit cards today have come a long way. In 2009, Credit cards and charge cards were used to make close to 2 billion purchases in the UK totaling up to £139.0 billion in value.

As technology has proceeded in providing convenience of use for consumers and corporations, most organisations have been struggling to catch up to the ever increasing threats of data security. Innovative hackers have been able to find loopholes in several vulnerable areas across widely inter-connected networks and use it to their advantage, leading not only to sizable revenue losses to the organisation but also to customer dissatisfaction and loss of trust, both of which are very difficult to regain.

As per recent estimates, losses on cards due to fraud in 2009 totaled £440 million in the UK alone.

Oracle Functionality

Credit Card transactions in Oracle can originate from Oracle Order Management, Receivables, i-receivables or i-store modules. The business user/customer keys in the credit card number and relevant details for authorization and settlement. Oracle I-payments (R11i) and Oracle Payments (R12) essentially acts as an integrator with a payment processor for sending/ receiving information. The payment processor further integrates with the credit card issuing bank to validate, authorise and settle transactions. In this data flow, security vulnerabilities can occur in the form of:

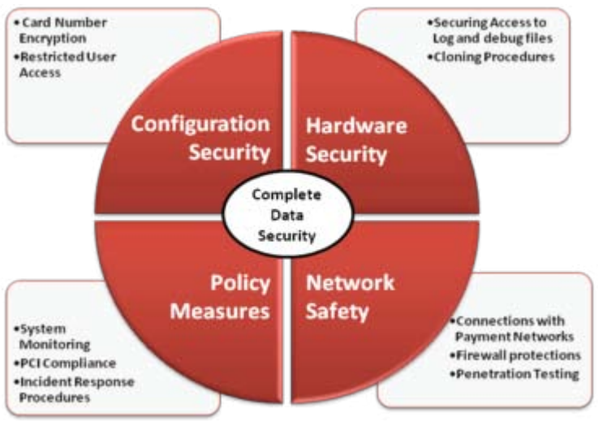
1) Storage of Card Numbers: Where inadequate procedures have been adopted to encrypt card numbers or to secure access to databases/files where card numbers are stored.

2) Inadequate Usage Restrictions: Where proper policies have not been put in place to restrict only the authorised users to have access to card holder information.

3) Unsecured Areas in the Network: Where all aspects of network security have not been adequately examined and protected on a continuing basis.

Approach

With a view of minimising the security risks in the areas highlighted above and to enable organisations to form a holistic view of their data security paradigm, the various facets of data security and their mitigation procedures have been classified into a FOUR step methodology depicted in the diagram below:



Security Methodology

1) Configuration Security

Configuration security implies "Set Up" functions which are needed for ensuring a minimum level of data safety within the Oracle Applications framework. Data encryption and securing user access are the two areas of Configuration security.

a. Data Encryption
Credit Card Numbers have to be masked in the front end and encrypted in the database. Standard Oracle offers the security key and the wallet functionality to store and maintain encryption keys used for encrypting credit card numbers. Generally it is advisable to change the security keys once a year, so as to prevent chances of fraud. The access to change security keys should be restricted to one or two members of the internal IT security team only.

Certain payment processors also offer "Token Number" functionality. In this credit card numbers are not stored in organisation's Oracle Applications system, but are sent to the payment processors who send back Token Number associated with the credit card number. This token number gets stored and referenced in Oracle for all future transactions. Organisation can make use of this service based on volumes and enterprise procedures.

b. Restricted User Access
Standard Oracle offers a form function to view unencrypted credit card data. Ideally only select internal IT security team members should have access to the responsibility (which has this function attached). For other users who want to have access to unencrypted customer credit card number a proper framework must be put in place to ensure that any such requests have a valid business reason and are well documented.

2) Hardware Security

Hardware security covers securing access vulnerabilities in the files and folder structures in the Oracle Database system. This can be achieved by:

a. Securing Access to Logs/Files
Debug logs and settlement/ acknowledgement files are two areas which could potentially have an impact on data security. In certain cases, when debug is enabled for order management/receivables/ payment applications, unencrypted credit card numbers could be stored in the debug log files. Access to the folders containing such log files should be restricted. Any log files that needs to be provided to any IT support personnel must be cleansed of all such credit card numbers.

In a processor based model (FDC North etc.) settlement files are sent to the payment processors and acknowledgement files received from them. These files could contain unencrypted credit card numbers. The directories in which these files are stored should be secured and these files must be password protected and archived in a regular manner.

b. Cloning Procedures
One area that data security is often overlooked is security of a cloned instance. Instances are cloned for a variety of needs and made available to employees, contractors and support personnel for their daily activities. The cloned instance contains the same data as that of a production instance. It is extremely critical that a full sanity check be done of the cloned instance. This would involve updating all tables with Dummy credit card numbers and removing any logs/ files (mentioned above) that could potentially have credit card numbers. Typically access control on a cloned instance is far more lenient than a production instance and hence the risk of data pilferage from a cloned instance is higher.

3) Network Safety

Appropriate firewalls should be in place restricting access to the Oracle Applications database server and all internal application servers. External communications can be handled by using a proxy server in the DMZ (de-militarized zone) that limits connections to only approved sites.

Credit card authorisation and settlement requests communicate with an external payment system. This is outside of the organisations network. It is important to ensure that all such communication is secured by following an HTTPS or SFTP protocol.

If there are instances where organisation data is being accessed by external parties like customers/suppliers (i-receivables/i-store/i-supplier) it is advisable to get a PEN (Penetration) Testing done by a qualified professional on a regular basis. This will ensure that any vulnerable points in the network are identified and corrected.

4) Policy Measures

Procedures must be put in place for Continuous Monitoring and Tracking access to networks and cardholder data. Audit trails, tracking on invalid logon attempts, Use of identification and authentication mechanisms are some of the ways in which tracking can be done.

The Payment Card Industry (PCI) has released a broad list of PCI Compliance procedures, which must be adopted by organisations dealing with payment cards. It is advisable to conduct a periodic audit to ensure that the organisation is in compliance with the relevant compliance procedures. Oracle releases critical Security Patch Updates on a regular basis. Organisations must prioritize these patches and devote the necessary resources to test and apply the patches in the required timeframe.

In reality, in spite of the best efforts of organisations security breaches do occur. Hence it is important to have Well Documented Mitigation Procedures covering all aspects of the business in case such an event occurs. This will help an organisation to respond quickly and effectively to any such challenges in a calm and organised manner.

Conclusion

Reliable organisation security is a system and a continuous process. As the old adage goes "A chain is only as strong as its weakest link", organisations today have to concentrate on giving a complete systemic thought to their data security requirements. A comprehensive use of the features provided by Oracle along with regular due diligence and monitoring procedures will go a long way in preventing data theft and safeguarding an organisation's image in today's challenging environment.

References:

1) UK Card Association Press Releases

2) Oracle I-payments/Payments User guide.

ABOUT THE AUTHOR

■ Kartik Subbaraman (kartik_subbaraman@infosys.com) is a Lead Consultant in the Enterprise Solutions Group at Infosys Technologies Limited. He has overall 8 years of experience post his MBA, which includes 7 years of experience in the Oracle Applications space. In this span, he has worked and successfully delivered multiple end to end Oracle Implementations for Retail, Manufacturing and Hi-Tech vertical clients. He has worked on multiple Oracle i-payment implementations for various clients.