
Encryption Overview



Using Encryption to address the biggest security threats
facing organizations today!

By Craig Moir

April 2011

Version 1

Encryption Overview

CONTENTS

What security problems do we face today?

Insider Threats

Meeting Regulatory Compliance Requirements

Separation of Duties (SoD)

Principle of Least Privilege

Data Theft

Personally Identifiable Information (PII)

Identity Theft

Components on Enforcing Security

The MyDBA Solution

References



Encryption Overview

What Security problems do we face today?

The most pressing security problems facing organizations today are :

- **Protecting sensitive data against insider threats;**
- **Meeting regulatory compliance requirements; and**
- **Enforcing Separation of Duties.**

Encryption Overview

Insider Threats

Although external exploits by criminals breaking into systems get big headlines, industry specialists estimate that **80% to 90% of the damage to information systems is done by insiders**, which typically gets hushed up.

Encryption Overview

Meeting Regulatory Compliance Requirements

- **King III - King Report on Governance for South Africa 2009**
- **Sarbanes–Oxley Act of 2002**
- **Other Laws:**
 - ✓ Health Information Portability and Accountability Act (HIPAA)
 - ✓ UK Data Protection Act
 - ✓ Family Educational Rights and Privacy Act (FERPA)
 - ✓ California Breach Law
 - ✓ Federal Information Security Management Act (FISMA)
 - ✓ European Union Data Protection Directive

Encryption Overview

Separation of Duties (SoD)

Definitions:

- The main objective is to prevent a single person from defrauding the organization.
- A security principle that says no one person should be able to effect a breach of security.
- *This principle prevents any part of the computer system from being under the control of a single person.*

Encryption Overview

Principle of Least Privilege

Definitions:

- **The principle of least privilege requires that a user be given no more privilege than necessary to perform a job.**
- **A process, user or a program must be able to access only such information and resources that are necessary for its legitimate purpose.**

Encryption Overview

Data Theft

- **Employees have access to and are entrusted with highly sensitive and confidential information.**
- **80%-90% of all data theft is perpetrated by office workers.**
- **Modern methods and terminology for data theft**
 - ✓ Thumbsucking – Downloading and theft of sensitive data via USB flash drive.
 - ✓ Pod Slurping - – Downloading and theft of sensitive data via iPOD.
 - ✓ Bluesnarfing – Access and theft via BlueTooth connectivity.
 - ✓ Sneakernet - Theft via magnetic tape, floppy disks, compact discs, USB flash drives, or external hard drives.

Encryption Overview

Personally Identifiable Information (PII)

- Refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
- Legislation in most countries require PII to be *encrypted*.
- **PII examples**
 - ✓ *Full name (if not common),*
 - ✓ *Identification number*
 - ✓ *Vehicle registration number*
 - ✓ *Face, fingerprints, or handwriting*
 - ✓ *Credit card numbers*
 - ✓ *Digital identity*
 - ✓ *Birthday and Birthplace*
 - ✓ *Genetic information*

Encryption Overview

Identity Theft

- **Sources such as the non-profit Identity Theft Resource Centre sub-divide identity theft into five categories:**
 - ✓ Business/commercial identity theft (using another's business name to obtain credit)
 - ✓ Criminal identity theft (posing as another person when apprehended for a crime)
 - ✓ Financial identity theft (using another's identity to obtain credit, goods and services)
 - ✓ Identity cloning (using another's information to assume his or her identity in daily life)
 - ✓ Medical identity theft (using another's identity to obtain medical care or drugs)
- **The Federal Trade Commission in the US estimates that 9 million Americans are victims of Identity Theft every year.**

Encryption Overview

Components for Enforcing Security

- Authentication
- Authorization
- Access control
- Auditing
- **Encryption**
- **Abuse of privilege**
- **Data or service theft**

Encryption Overview

The MyDBA Solution

- MyDBA has developed an encryption plugin module for use in the Microsoft **.NET Framework**.
- Implemented via the **.NET Data Adaptor**.
- Resides on the Application tier in the form of a service.
- Allows encryption at table level or **column level**.
- Easily **encrypt PII** and meet worldwide regulatory compliance requirements.
- Prevents abuse of privilege i.e. DBA cannot see sensitive data.
- Mitigates **all** data theft scenarios.

Encryption Overview

MyDBA Consulting Services

For more information on MyDBA's **Encryption** and database **Security** services please contact us on:



info@mydba.co.za



0861 911 DBA



+27 11 808 6451



<http://www.mydba.co.za/>

Disclaimer: This document is provided for information purposes only. While MyDBA has taken care to ensure that the content on this document is accurate, the information is provided "as is" and is not warranted to be error-free. Your use of and reliance on the information is entirely at your own risk. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the prior written permission of MyDBA.



Encryption Overview

References

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html>

http://en.wikipedia.org/wiki/Data_theft

http://en.wikipedia.org/wiki/Data_spill

http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml

http://en.wikipedia.org/wiki/Identity_theft

<http://www.informit.com/articles/article.aspx?p=1220308>

<https://www.infosecisland.com/blogview/10771-Top-Ten-Breaches-By-Infamous-Insiders.html>

<http://technet.microsoft.com/en-us/library/bb510663.aspx>