

The Power of Effective Database Encryption

By Frank Yip

Technical Manager / **InfiniSec Asia Limited**

Copyright 2005 InfiniSec Asia Ltd.

www.infinisec.com

Agenda

- 📄 ***Is your database secure?***
- 📄 ***The effective way to protect database***
- 📄 ***Benefits of database encryption***
- 📄 ***Different protection approaches comparison***
- 📄 ***Steps to effective database encryption***

Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

Impact of Database Attack

- Database becomes the storage of valuable information of an organization
 - Customers privacy data
 - Business transaction
 - Formula, competitive information
 - And more.....

When database stores large amount of digital asset, it is easily becomes the target of attack



- ✘ Financial Loss
- ✘ Loss of Credibility
- ✘ Loss Competitive Edge

Challenges always exist

In today's enterprise environment

- The database systems are distributed
 - How to deploy database security across the enterprise?
 - How to enforce unified data security policy across the enterprise?
- The data inside database is shared by multiple parties such as partners, contractors, company internal users
 - How to make data securely shared among them?

Database is never secure without encryption

“On 25 February 2005, Bank of America disclosed that in late December 2004 it lost computer backup tapes containing information from **1.2 million** federally issued credit cards.”

---Gartner Research

“美滙豐停 **18萬** Master卡

滙豐銀行美國分行發現有零售商洩漏大批信用卡資料，觸發歷來最大規模的信用卡集體停辦事件之一.....”

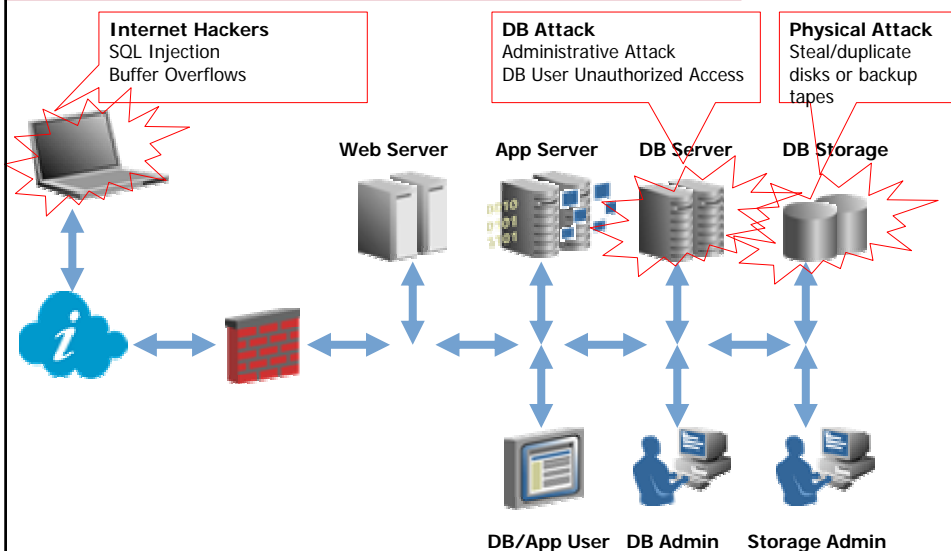
---經濟日報

“美銀職員盜客資料

美國四間銀行有 **七十萬** 名客戶的財務紀錄被銀行職員盜取，然後賣給收集個人資料的公司。.....”

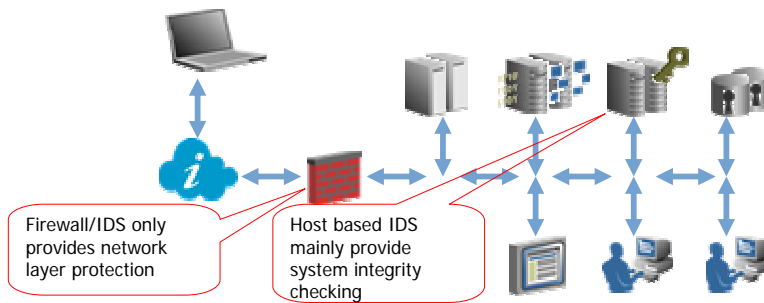
---蘋果日報

Source of Threats



What can be done to protect DB?

- ❏ Can firewalls, IDS or strong authentication help?
 - ⊖ Yes, but they are not enough
- ❏ The best way to secure data at rest is **encryption**
 - ⊖ It is the most effective defense to protect data
 - ⊖ It complements other security solutions



Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

Security Guideline / Regulation

- ❏ **Government Security Regulation**
 - ▶ **HK GOV**
 - ⊖ Data must be classified into different categories, e.g
 - Top secret, secret, confidential, sensitive, or public
 - ⊖ Confidential data must be encrypted when they are in transmission and storage
 - ⊖ Encryption strength
 - Encryption key must be at least 128 bits
 - ⊖ Enforce Separation of Duties
 - ⊖ Audit log must be performed for shared data access
 - ▶ **USA – Sarbanes-Oxley Act (SOX)**
 - ▶ **JAPAN - Privacy Law**
- ❏ **Other Regulation/Guideline**
 - ▶ **Hong Kong Monetary Authority**
 - ⊖ Technology & Risk Management Guideline also has the data security requirement
 - ⊖ Expect all banking and finance institute shall follow
 - ▶ **VISA CISP**
 - ⊖ Expect all VISA merchants shall enforce data protection to protect customer privacy information
 - ▶ **HIPPA, GLBA**

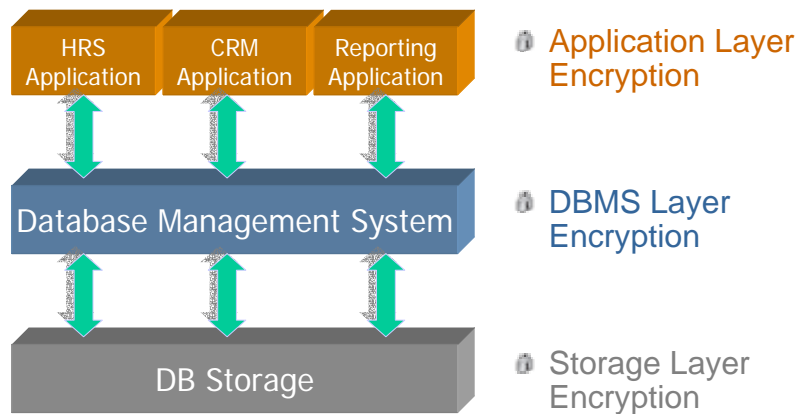
Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

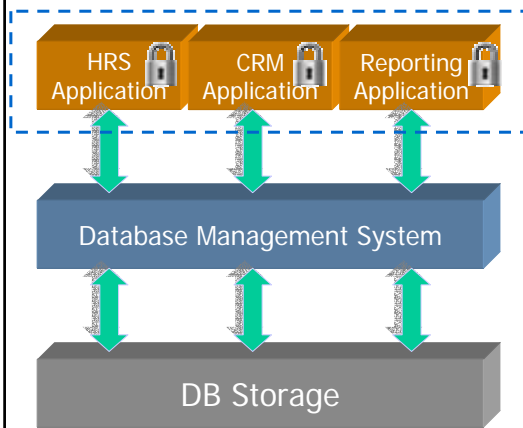
Benefits of DB Encryption

- ✔ Secure company's most valuable data
 - 🔒 Enhance the database security protection
 - 🔒 Reduce the database security risk
 - 🔒 Ensure normal business operation
 - 🔒 Maintain company's competitive edge
- ✔ Secure database outsourcing
- ✔ Fulfill the requirements of various governance regulation
 - 🔒 Most straightforward and effective approach to fulfill the requirements
 - 🔒 Guarantee customer's confidence to use the company's services

Which is the best solution for Database Encryption



Application Level Encryption



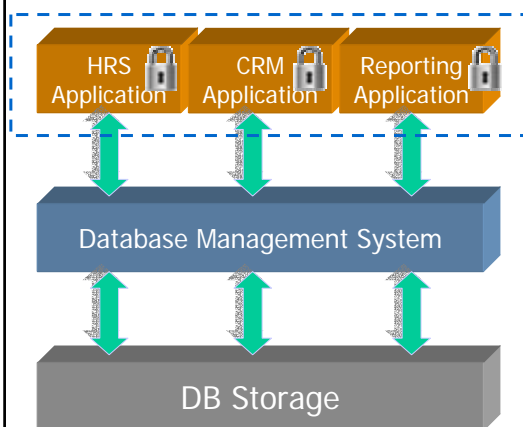
Technical Approach

- Develop the application so that it has built-in encryption/decryption capabilities
- Need to develop/buy crypto API
- Need to develop a secure key management
- Data is encrypted or decrypted at application side

Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

Application Level Encryption



Pros

- End to End data protection
- Data is in encrypted format at link level
- Data is in encrypted format at storage level
- Only authorized user can decrypt the data through application

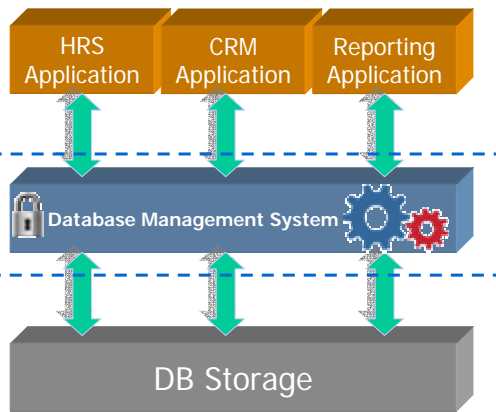
Cons

- Need large development efforts
- Must reprogram all the applications if they need to access the shared encrypted data
- Must have the source code of application
- Huge on-going maintenance cost
- Difficult to enforce enterprise security policy enterprise widely

Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

DBMS Level Encryption

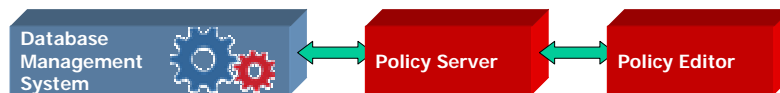


Technical approach

- ❶ Add an extra layer inside database
- ❷ Implement transparent encryption through views, triggers and packages
- ❸ Provide encryption management and key management functions
- ❹ Provide enhanced the database access control at DBMS level

DBMS Level Encryption

Separate Data Security Management



Enforcement point

- ❶ Provide real time encryption/decryption
- ❷ Enforce the encrypted data access control policy
- ❸ Log the data access activities

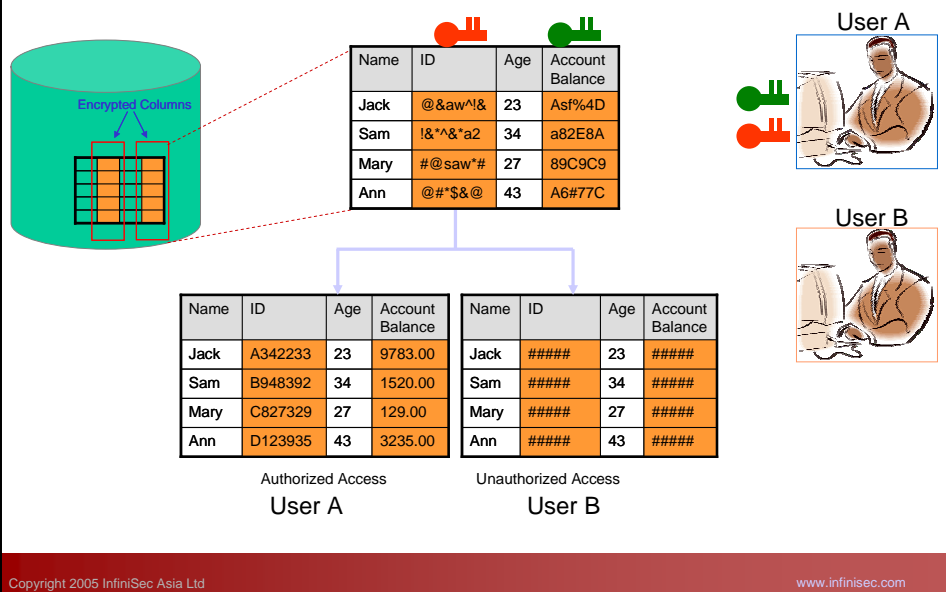
Policy Server

- ❶ Centralized policy management
- ❷ Synchronize policy to target DB servers

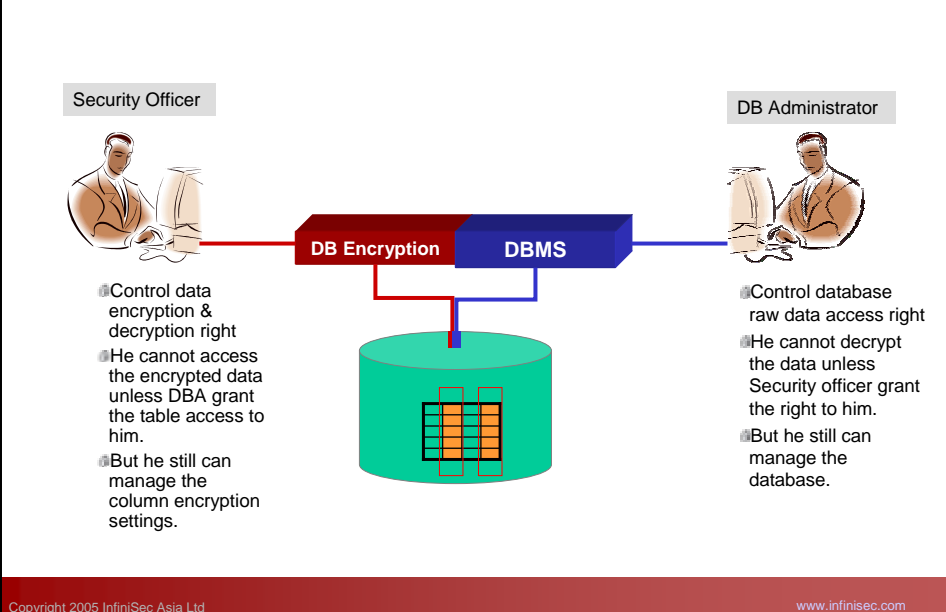
Policy Editor

- ❶ Define encryption keys
- ❷ Define column encryption
- ❸ Define access control for encrypted data

DBMS Level Encryption



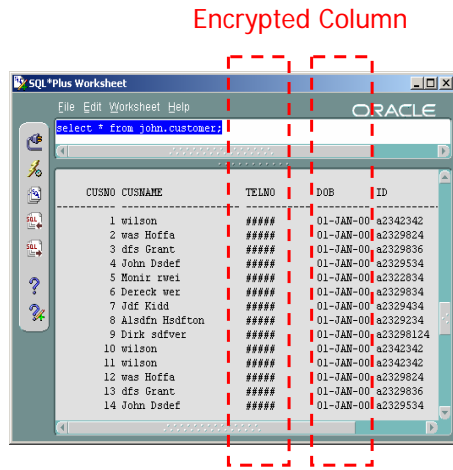
Enforce Separation of Duties



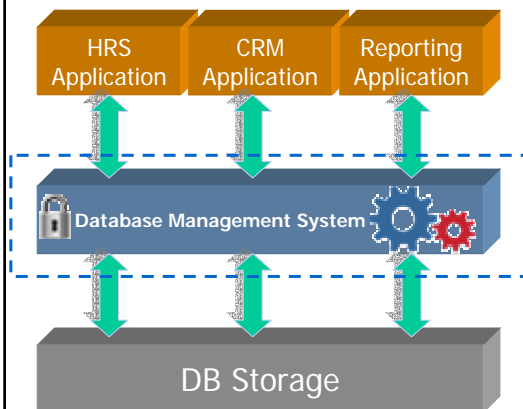
DBMS Level Encryption

General functions

- ❶ Columns level selectively encryption
- ❷ Shared/Unique encryption key for each columns
- ❸ Provide granular encryption access control base on
 - User, IP, Time, Type of Operation, and target encrypted data
- ❹ Prevent DB administrative attack
- ❺ Provide audit on the encrypted data access
- ❻ Provide database migration utility



DBMS Level Encryption



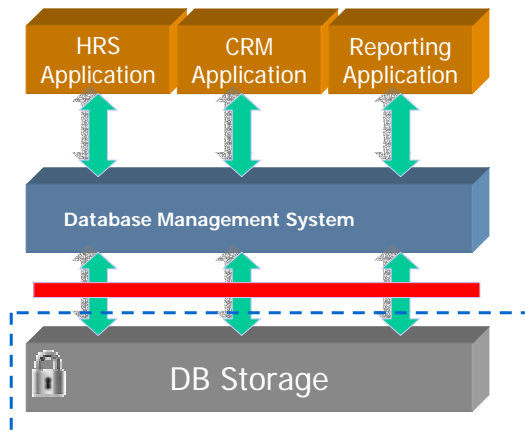
Pros

- ✔ Transparent to application
- ✔ Real time encryption
- ✔ Short deployment time
- ✔ Less maintenance cost
- ✔ Can enforce data security policy enterprise widely
- ✔ Flexible deployment
- ✔ Enforce separation of duties
- ✔ Data is encrypted in disk and backup media

Cons

- ✘ Data is in plaintext on the link between DB and Application
- ✘ Cause performance overhead to DB

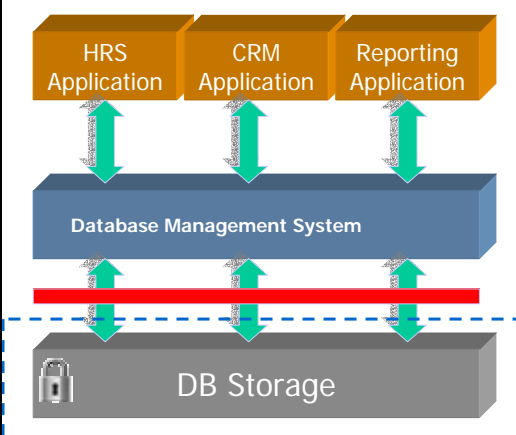
Storage Level Encryption



Technical Approach

- Add an encryption filter between DB server operating system and the DB storage system
- Whole hard disk or partition encryption
- Real time encryption at disk I/O level
- Support SAN, NAS, Fiber Channel protocol

Storage Level Encryption



Pros

- ✔ Reduce the risk of physical attack
- ✔ Relatively simple to implement
- ✔ Short deployment time
- ✔ Easy to maintain
- ✔ Transparent to DBMS and Application

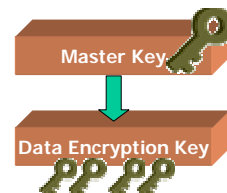
Cons

- ✘ Cannot prevent DB level attack such as SQL injection, DBA attack
- ✘ Cannot log DB level data access activities
- ✘ Data is in plaintext on the link between DBMS and Application

Key Management Issue

Key protection in database encryption

- ❗ No plain key should be stored in disk
- ❗ Keys should be automatically generated
- ❗ Data encryption keys should be renewable



Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

Steps to Effective Database Encryption

- ❗ Define company security policy for data protection
 - ❗ Classify the data into different security level
- ❗ Identify the right solutions
 - ❗ Security
 - DBA attack prevention
 - Granular access control
 - Data must be encrypted in disk and backup
 - ❗ Maintenance and Management
 - Centralized policy management
 - Easy to back and restore
 - Does the management require in-depth DB knowledge?
 - ❗ Integration with current environment
 - Application transparency
 - High availability
- ❗ Proper implementation to minimize the performance impact
 - ❗ Selectively encryption
 - ❗ Do not encrypt the index column



Copyright 2005 InfiniSec Asia Ltd

www.infinisec.com

Summary

- ❏ External and internet threats to database
- ❏ Limitation of perimeter defense
- ❏ Database encryption is a best way to secure the data at rest
 - ❖ Application level encryption
 - ❖ DBMS level encryption
 - ❖ Storage level encryption
- ❏ Several important criteria when selecting the approach
- ❏ Deploy with thorough planning can minimize the performance impact

Questions



Thank You !

Copyright 2005 InfiniSec Asia Ltd.

www.infinisec.com