Securing Data at Rest Using Empress Database - the Ultimate Line of Defense

Empress Software Inc.

Agenda

➢ About Data Encryption

➢ Empress Database Encryption Solution

➢ Live Example

➢ Summary

Securing Data At Rest …

Securing data at rest *means:*

➢ Protecting data in persistent storage but excludes any data that traverses the network or that which resides in temporary memory

Why Should We Encrypt Data?

Regulatory Requirements

- ➢ Health Insurance Portability and Accountability Act (HIPAA)
- ➢ Gramm-Leach-Blilely Act (GLBA)
- ➢ Sarbanes-Oxley Act (SOX)
- ➢ Visa Cardholder Information Security Program (VISP)
- ➢ European EU Data Protection Directive
- ➢ Japan's PIP Act

What Are the Threats?

➢ Hard Disk with a Database Might Be Stolen

➢ Machine/Embedded System with a Database Might Be Stolen

➢ Device with a Database is Mobile and Might Be Lost

➢ Backup Media with a Database Might Be Lost/Stolen

➢ Unauthorized User Viewing File System with a Database Data

➢ Hard Disk with a Database Might Be Improperly Recycled

➢ …

Data Encryption Options

- **Application-Level Encryption**
  - Custom code; data cannot be sorted, compared and analyzed

- **Database-Level Encryption**
  - Too complex to use

- **File-Level Encryption**
  - No fine grain control

Application

Database

File System
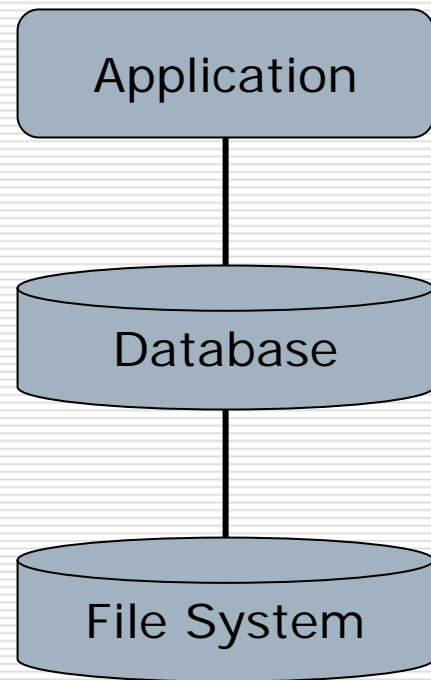
Data Encryption Methodology Types

➢ **Data-in-Motion Encryption**

      Protects data over the networks

➢ **Data-at-Rest Encryption**

      Stores encrypted data inside the database
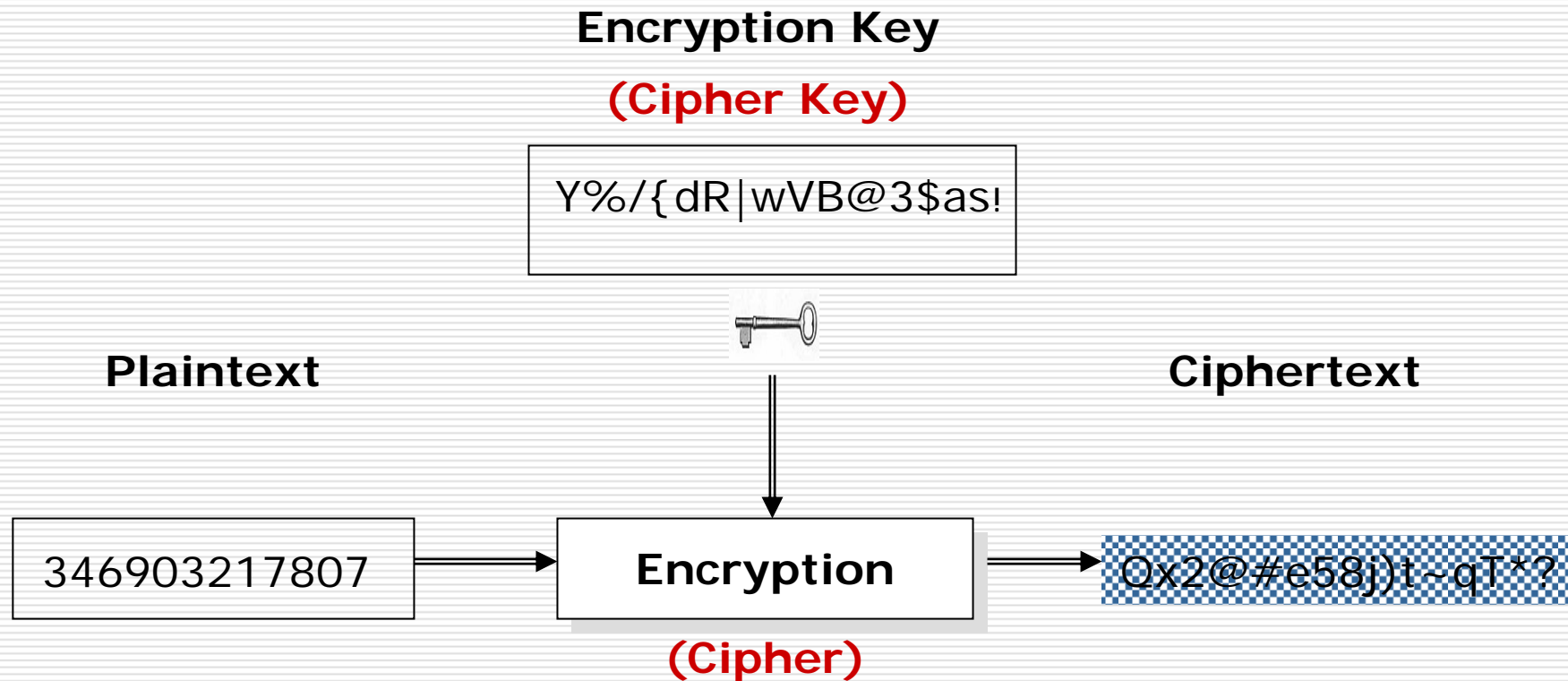
Solution Using Empress Database

- ➢ Secures all database data (includes protection of all logs and backup files)
- ➢ Efficient security solution (low performance overhead)
- ➢ No need for application code changes
- ➢ No need for adding external provisions (e.g. stored procedures, triggers, views, etc.)
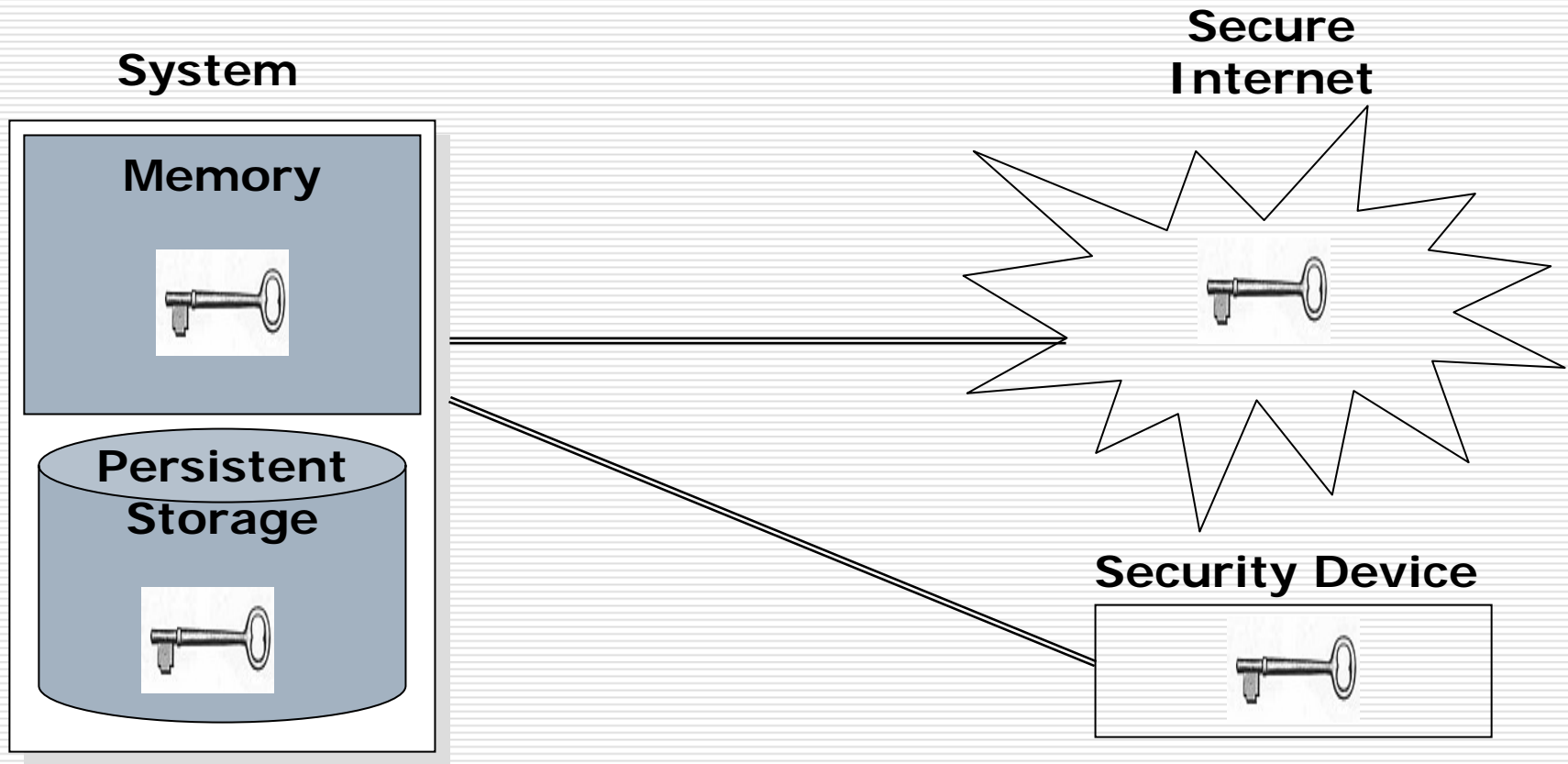
Data Encryption

Encryption Key

(Cipher Key)

Y%/{dR|wVB@3$as!

Plaintext

346903217807

Encryption

(Cipher)

Ciphertext

Ox2@#e58j)t~qT*?

Data Decryption

Decryption Key

Y%/{dR|wVB@3$as!

Ciphertext

Original Plaintext

Ox2@#e58j)t~qT*? → **Decryption** → 346903217807

Key Management

Encryption Key Can Be Stored in Different Places

Granularity of Encrypted Data

➢ Database

➢ Table

➢ Column

SQL Commands with Encryption

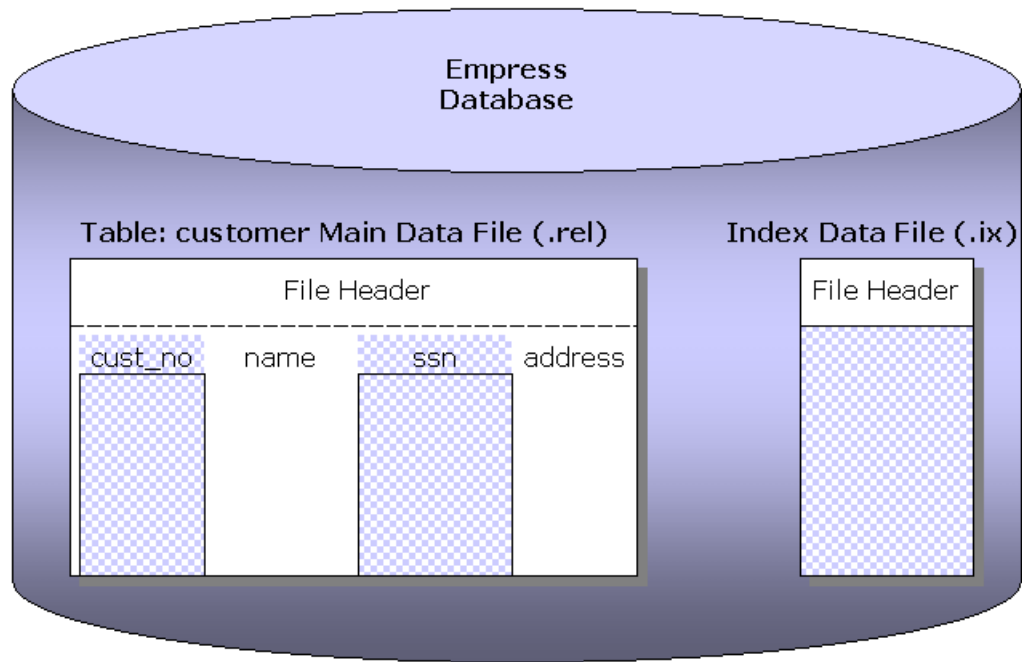➢ Encryption is done at column level

CREATE TABLE customer (
    cust_no INTEGER NOT NULL ENCRYPTED,
    name CHAR(20),
    ssn CHAR(9) ENCRYPTED,
    address TEXT);

CREATE UNIQUE INDEX customer_index ON
    customer(cust_no);

Empress Database Encryption
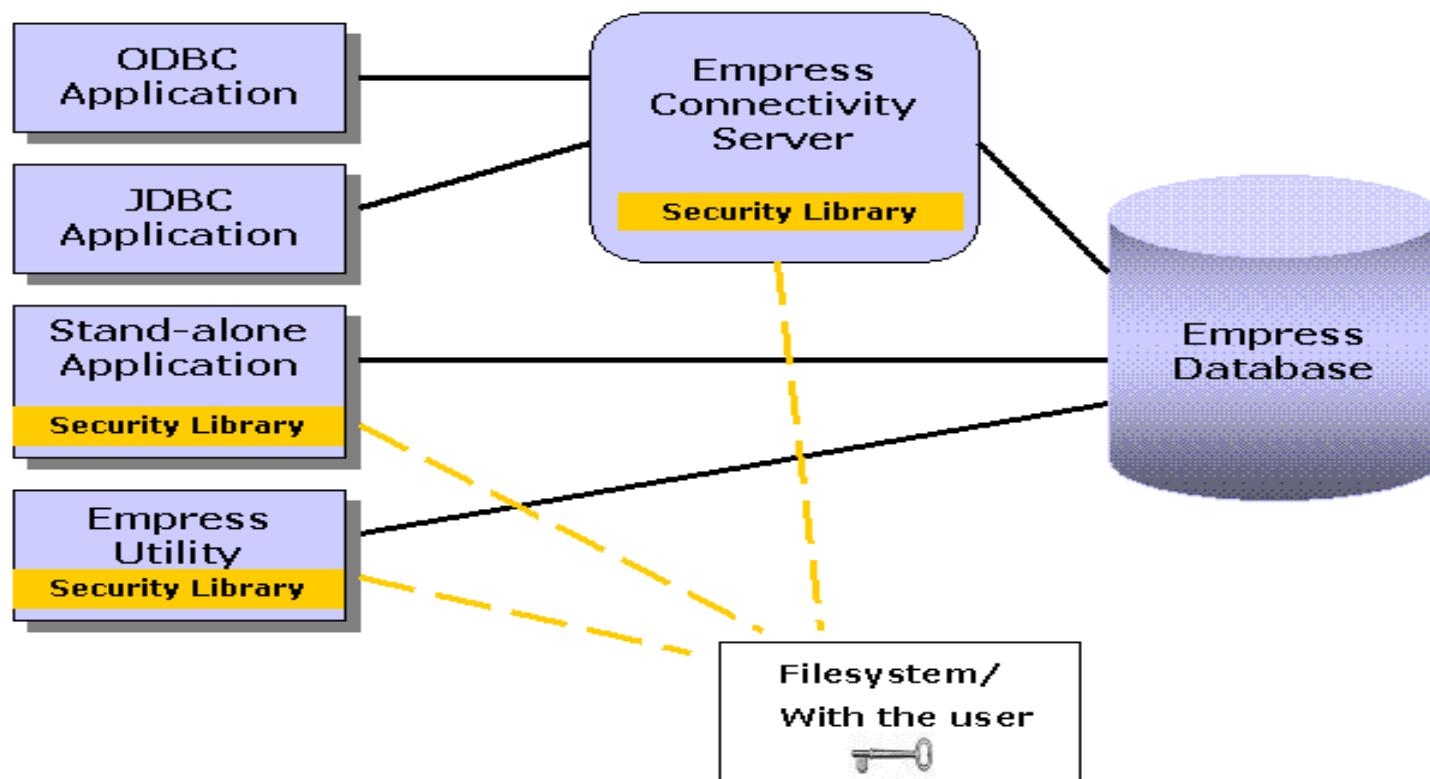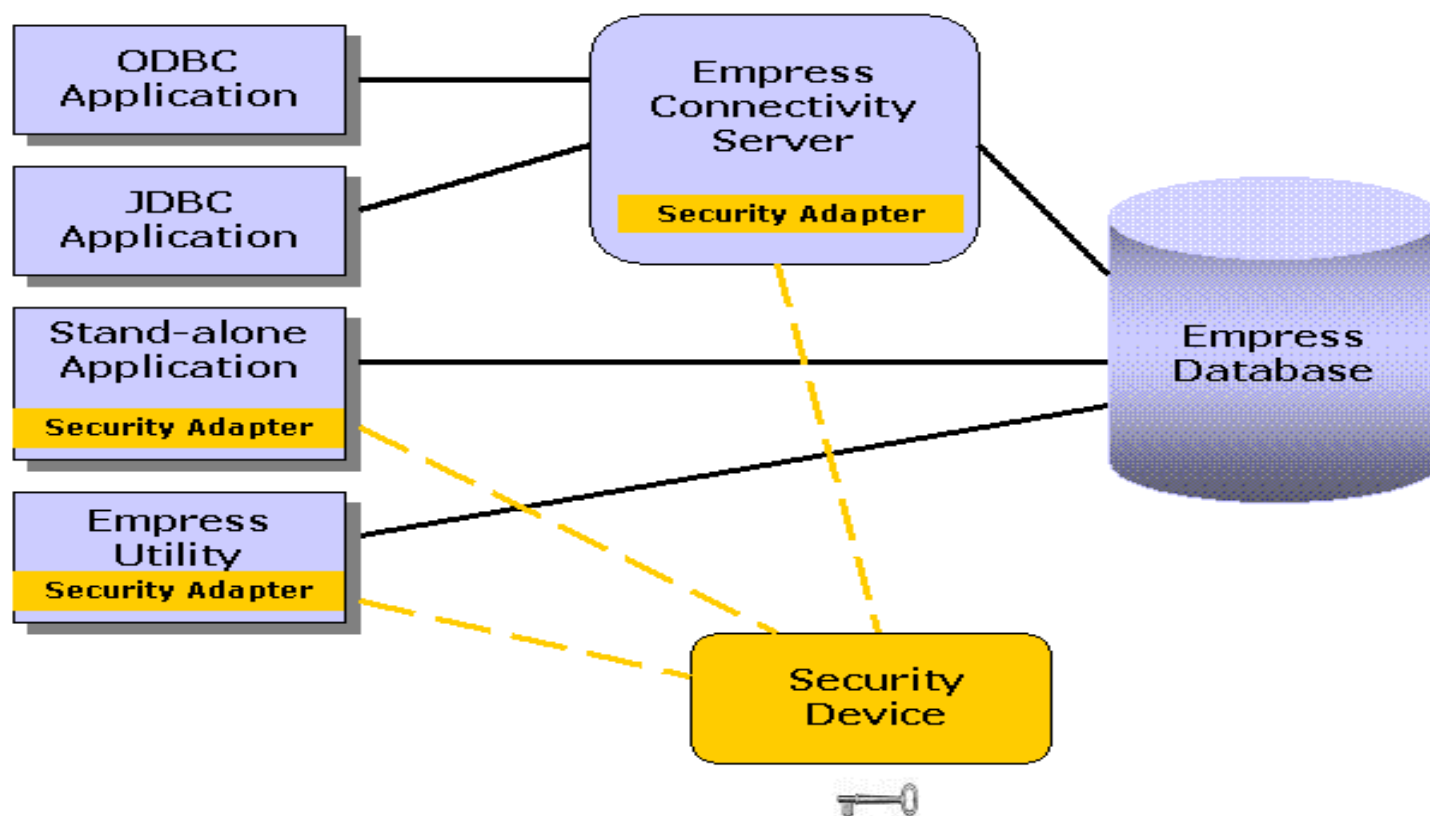
Argument for Empress Solution

➢ Applications are unaffected by the encryption

➢ Implement database encryption solution without changes in legacy applications

Database Encryption (SW Solution)

Database Encryption (HW Solution)

Empress Solution Characteristics

➢ There will be NO data from encrypted columns stored on the disk in plaintext

➢ Encryption on any column data type is allowed

➢ Ability to create indexes on the encrypted columns of any Empress data type

Empress Solution Characteristics

➢ cryptographic algorithms supported by GNU gcrypt library, Ingrian or user defined

➢ Good cipher choice: AES256

➢ All data in encrypted columns will be encrypted with same cipher and one cipher key

How Does It Work?

➢ An Example in Linux

➢ Show difference between two tables, one using and one not using encryption

➢ Show indexing

Argument for Empress Solution

➢ Low Performance Overhead

Database Encryption

The Forrester Wave™: Database Encryption Solutions

"Need for database-level encryption has grown significantly," but it is:

➢ Too Complex To Use

➢ Extra Effort Needed for Application Management

➢ Having an Impact on Application Response Time

➢ Extra Effort Needed for Key Management

Database Encryption

Empress Database Encryption Solution

➢ Simple To Use

➢ No Extra Effort Needed for Application Management

➢ No Significant Impact on Application Response Time

➢ Some Extra Effort Needed for Key Management

➢ Transparent Solution for Different Platforms

Contact Information

Empress Software Inc.

Phone: 301-220-1919
Toll Free: 1-866-626-8888
info@empress.com
www.empress.com