DbEncrypt

database encryption solution

For Microsoft SQL Server

APPLICATION SECURITY, INC.

www.AppSecInc.com

Agenda

- **There is a problem…**
  - Main Problem
  - Existing Solution Shortcomings
  - More Granular Industry Problems
- **There is a solution…**
  - ASI's DbEncrypt
  - Who Benefits? How? Why?
  - Key Technology Differentiation
- **There is a way… and a plan…**
  - What's included?
  - Our Organization, Current Position and Future Plans

APPLICATION SECURITY, INC.

www.AppSecInc.com

Main Problem

- The prevention of unwanted users or personnel from viewing data (“data-at-rest”)
  - Outside Intrusions
  - Internal Personnel
  - Administrative Personnel
    - Database Administrators
    - System Administrators
    - General Administrators

Existing Data Security Solutions

- Security and Data Protection Solutions
  - Existing security solutions do not address this "main problem"
    - Vulnerability Assessment, IDS, Firewalls, Single Sign-On
  - Backup Solutions
    - Provides protection for "off-line" data
- Existing Encryption Solutions
  - Existing Data Encryption ("data-in-transit")
    - SSL, PKI, etc.

Database Security in General

- Non-existent controls and mechanisms
  - Nothing preventing unwanted personnel or even the DBA from seeing data
- Traditional Database Security Concepts Do Not Apply in Today's World
  - Access Control and Permissions

Granular Industry Problems

- **Service Provider** & **E-Business** in General (ASPs, ISPs, MSPs, and Internal / External Systems)
  - Providing the data security guarantee
  - Overcoming customer and partner fears
  - Establishing accountability for data security

Granular Industry Problems

- Regulatory Requirements
  - VISA CISP
    - Requirement #3: Encrypt Stored Data
      - Minimum account information to be encrypted is the Visa account number and expiration date
  - Gramm-Leach-Bliley Act
    - Interagency Guidelines (Manage & Control Risks)
      - Encryption of electronic customer information in transit or in storage
    - TITLE V – PRIVACY
      - Subtitle A – SEC. 501 PROTECTION OF NONPUBLIC PERSONAL INFORMATION

DbEncrypt™ is the Answer

- **Main Problem**:
  - The prevention of unwanted users or personnel from viewing data ("data-at-rest")
- **Answer**:
  - A flexible infrastructure designed to encrypt column and row-level data stored in the tables of a database.

APPLICATION SECURITY, INC.

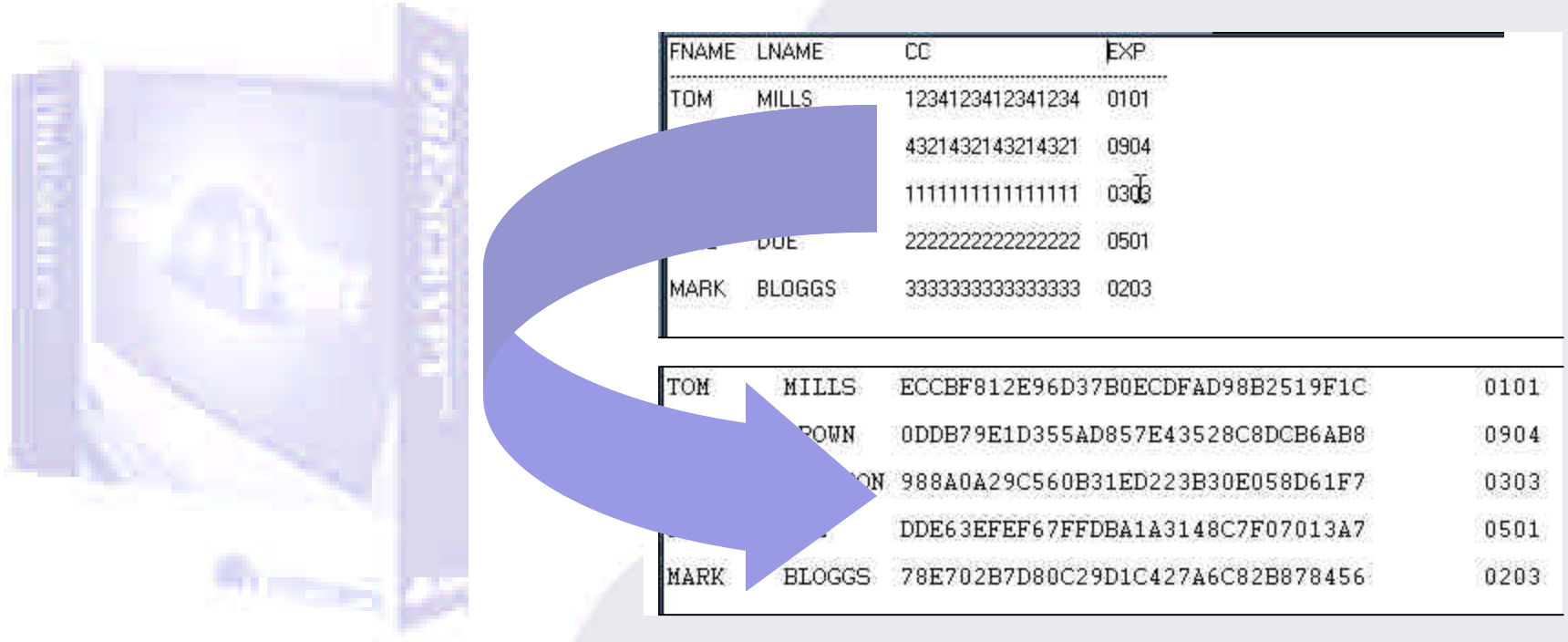
www.AppSecInc.com

DbEncrypt™ Key Features

- Database Column and Row-Level Encryption
- Access to world-class security resources that facilitate effective data protection
- Controls and mechanisms providing authentication, encryption, and data integrity

DbEncrypt™ Key Features

- Database Column and Row-Level Encryption



FNAME	LNAME	CC	EXP
TOM	MILLS	1234123412341234	0101
		4321432143214321	0904
		1111111111111111	0303
	DOE	2222222222222222	0501
MARK	BLOGGS	3333333333333333	0203

TOM	MILLS	ECCBF812E96D37B0ECDFAD98B2519F1C	0101
	BROWN	0DDB79E1D355AD857E43528C8DCB6AB8	0904
	JONES	988A0A29C560B31ED223B30E058D61F7	0303
	DOE	DDE63EFEF67FFDBA1A3148C7F07013A7	0501
MARK	BLOGGS	78E702B7D80C29D1C427A6C82B878456	0203

APPLICATION SECURITY, INC.

www.AppSecInc.com

DbEncrypt™ Key Features

- Access to world-class security resources that facilitate effective data protection
- Encryption Algorithms - complete list at:

  http://www.appsecinc.com/products/dbencrypt/mssql/algorithms.html

  – 25 of the strongest and most widely analyzed algorithms
    - AES
    - RSA
    - DES
    - RC4
    - MD5
    - SHA-1
    - Blowfish
    - Twofish

DbEncrypt™ Key Features

- Controls and mechanisms providing authentication, encryption, and data integrity

Flexible for All User Levels

- DbEncrypt™ can be utilized as a:
  - **Turnkey solution** to automatically and transparently encrypt data in columns and rows

OR

  - As a **low-level API** providing cryptographic algorithms for SQL developers

APPLICATION SECURITY, INC.

www.AppSecInc.com

Turnkey Transparent Solution…

- **Who benefits?:**

  Database Administrators (DBAs) and Developers that **do not want to bother with the details** – transparent encryption functionality

- **How do they benefit?:**

  Point-and-click on columns and tables to…

  - Encrypt Data
  - Create triggers and views to transparently encrypt/decrypt data
  - Manage the encryption keys

APPLICATION SECURITY, INC.

www.AppSecInc.com

Low-Level API…

- **Who benefits?:**

  Database Administrators and Developers that wish to **build their own encryption systems** utilizing the API features

- **How do they benefit?:**
  - SQL Programmers to use encryption as they see fit
  - Provides developers with the ability to write proprietary encryption systems while still harnessing the power and capabilities of DbEncrypt™

Availability and Price

- Evaluation Copies Available for Download:
  - http://www.appsecinc.com/downloads/
- Price:
  - $9995 per instance with volume discounts
  - Additional 20% for Maintenance, Upgrades, and Technical Support (**MASTER Subscription Program**)
- Updates are easily downloadable from:
  - http://www.appsecinc.com/downloads/

Who is Application Security, Inc.

- Unique Position and Background
  - SHATTER focuses research on producing the following security solutions for database, groupware, web, and ERP applications:
    - Database Encryption
    - Penetration Testing/Vulnerability Assessment
    - Intrusion Detection

APPLICATION SECURITY, INC.

www.AppSecInc.com

Application Security, Inc. Family Suite

- **Database Encryption**
  - DbEncrypt for Oracle
  - DbEncrypt for Microsoft SQL Server
- **Application Pen Test / Vulnerability Assessment**
  - AppDetective for Oracle
  - AppDetective for Microsoft SQL Server
  - AppDetective for Sybase
  - AppDetective for Lotus Notes/Domino
  - Versions coming soon for Oracle Application Server, IBM DB2, MySQL, and Exchange
- **Intrusion Detection (Coming Soon)**
  - AppRadar

APPLICATION SECURITY, INC.

www.AppSecInc.com

Wrapping Up…

- **The problem…**
  - Main Problem
  - Existing Solution Shortcomings
  - More Granular Industry Problems
- **The solution…**
  - ASI's DbEncrypt
  - Who Benefits? How? Why?
  - Key Technology Differentiation
- **The way… and the plan…**
  - What's included?
  - Our Organization, Current Position and Future Plans

APPLICATION SECURITY, INC.

www.AppSecInc.com