Encryption
Key Management
Simplified

Sensitive Data and Key Management for DBAs

Jonathan Intner

13 December, 2011

NYOUG, New Yorker Hotel

VORMETRIC

Agenda

- Introduction
- Audience
- Sensitive Data
  - What makes data sensitive?
  - Where might sensitive data exist in-and-around an Oracle database?
- Key Management
  - What is Key Management?
  - Why should DBAs care?
- Who is Vormetric and what do we do?

VORMETRIC

Introduction

- Presenter:
  - Jonathan Intner,
    - DBA by trade
    - Solution Architect working for Vormetric
- Contributors:
  - A number of people within Vormetric helped me with this presentation, but the following deserve particular mention:
    - Sol Cates
    - Tony Hadfield
    - Todd Thiemann

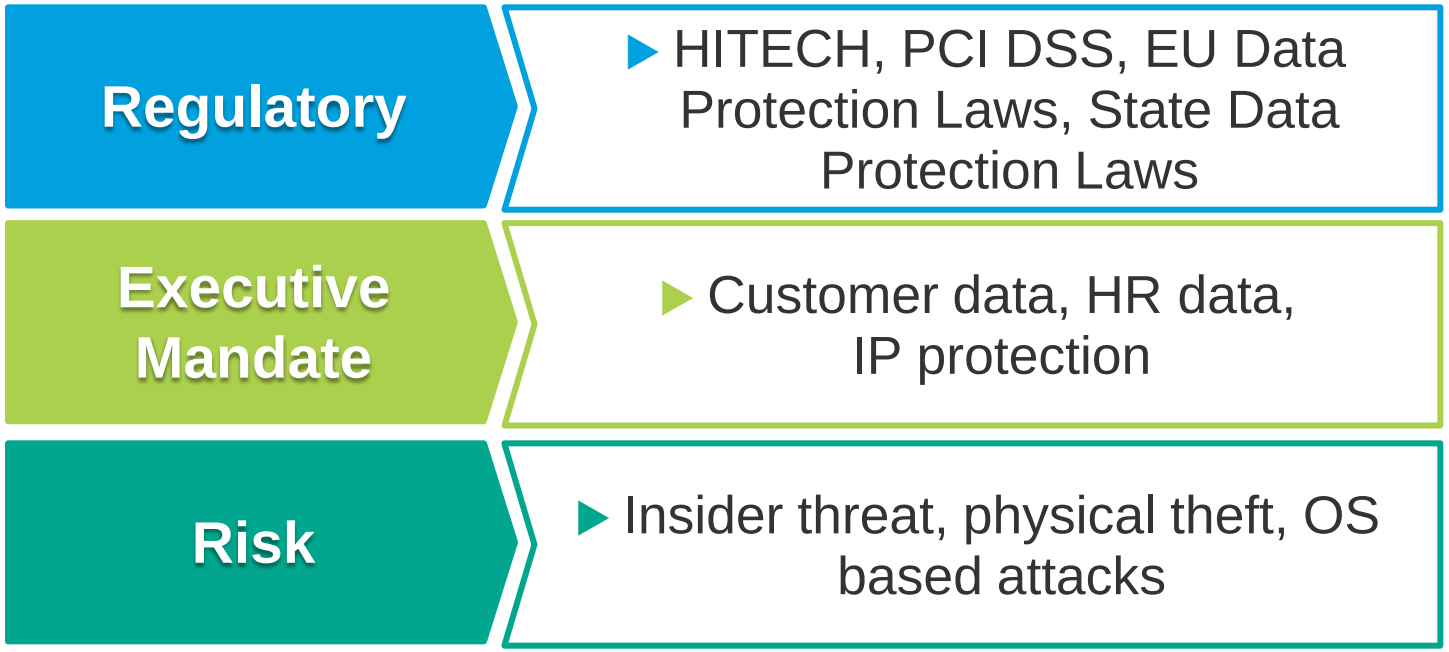
VORMETRIC

Audience

- Trade?
  - DBAs
  - SAs
  - Developers
  - Other
- Currently securing data?
  - Encryption
  - Access controls
- Why are you here?
  - Audit finding?
  - Don’t want to see your company listed in the Privacy Rights Clearinghouse Chronology of Data Breaches?

VORMETRIC

What makes data sensitive



VORMETRIC

Types of Sensitive Data

- Personally Identifiable Information (PII)
  - Sensitive PII is highly regulated by government data breach notification laws
  - Non-sensitive might still be significant
    - For example, the Sony breach
- Protected Health Information (PHI)
- Intellectual Property (IP)

VORMETRIC

Data Breach

- Loss of sensitive PII or PHI
- Government regulations
  - EU
  - US
    - Today: state-by-state
    - Federal regulation is under discussion
    - Massachusetts has one of the most stringent regulations in the US
- URLs:
  - http://www.privacyrights.org/data-breach
  - http://datalossdb.org/
  - http://www.ncsl.org/default.aspx?tabid=13489

VORMETRIC

PCI & PCI DSS

- Payment Card Industry, Data Security Standard
- Provides a nifty framework that can be used in addition to the somewhat vaguer government regulations
- Mandated by the credit card industry if your company stores, transmits or processes credit card data

VORMETRIC

Key PCI terms

- **PAN or Primary Account Number** – Credit Card Number
- **Merchant** – any company that accepts credit card payments. Can be online or brick and mortar.
- **Service Provider** – any company that stores, processes, or transmits cardholder data on behalf of another company. Processors, Gateways, DSEs are all Service Providers.
- **Acquiring Bank** – owns the merchant account and is responsible for their merchants' compliance.
- **QSA** – Qualified Security Assessor: determines if a company has complied with PCI
- **Levels 1, 2, 3, 4** – categorization made by the card associations based on the transaction volume of the company. Service providers and merchants have different thresholds.

VORMETRIC

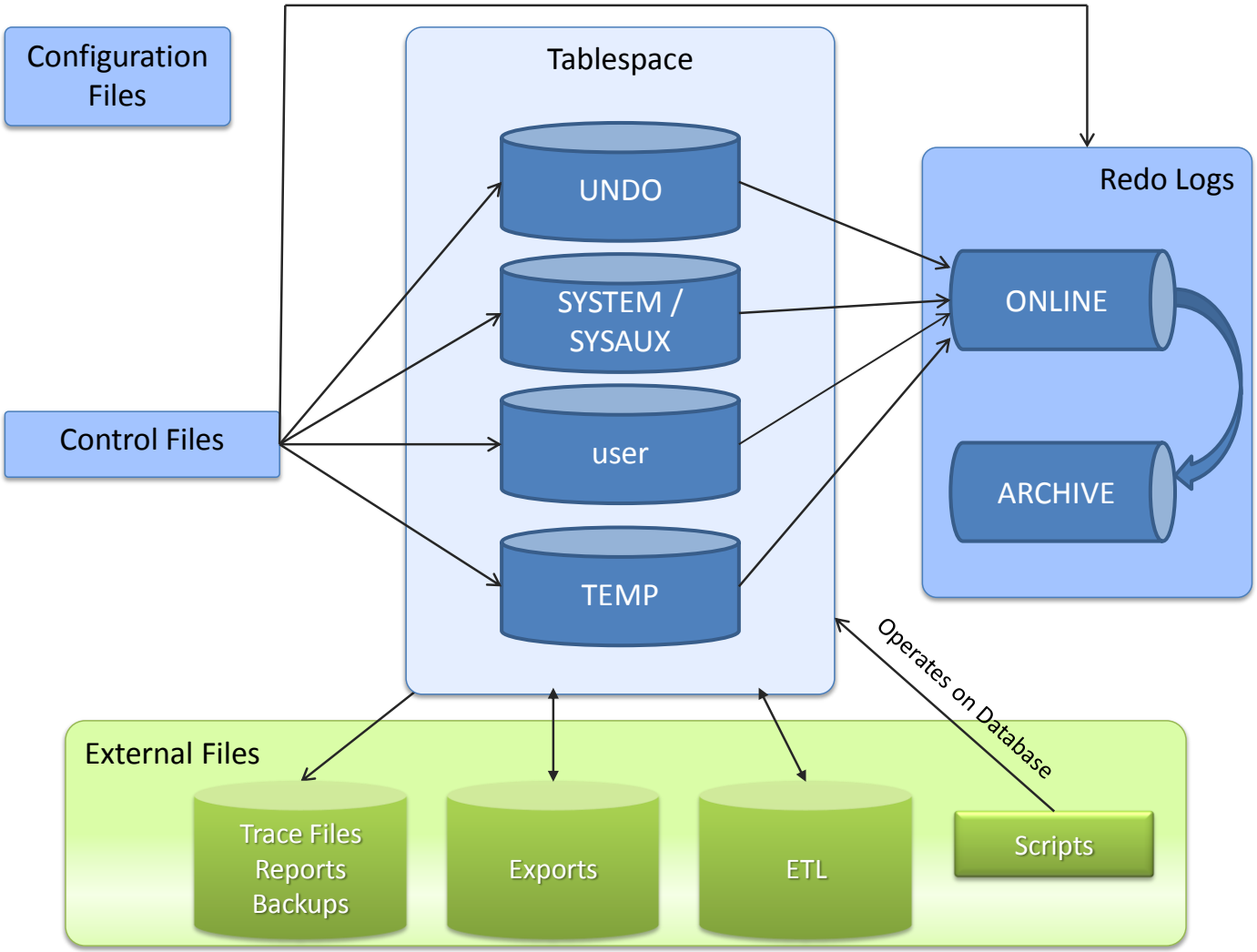
Quick “taste” of PCI DSS Requirements

- Available at the following URL: https://www.pcisecuritystandards.org/security_standards/documents.php
- Req’t 2, Do not use vendor-supplied defaults for system passwords and other security parameters
- Req’t 3, Protect stored cardholder data
  - > Keep those CRUD diagrams up-to-date
  - > Encrypt data!! And properly manage the keys associated with the encrypted data
- Maintain a Vulnerability Management Program
  - > CPUs or PSUs are a must
- Implement Strong Access Control Measures
- And so on

Questions

Why protect data

Files in-and-around an Oracle Database



VORMETRIC

Tablespaces

- "User"
  - Aka "Application" tablespaces
  - Some will contain sensitive data, others not
- "Internal"
  - SYSTEM / SYSAUX / PERFSTAT
    - Unlikely to contain sensitive data, unless tools like AWR or PERFSTAT is being used to capture bind variables
  - UNDO
  - TEMP
    - It is arguable, that UNDO and TEMP will only contain sensitive data
      - Under specific circumstances
      - And, in any case, their containing this data will be transient

VORMETRIC

Redo Logs

- Online
- Archive
- Back to the diagram
- Config files

VORMETRIC

Other files

- ETL
  - Extraction, Transformation and Load
- Exports
  - Conventional
  - Datapump
- Reports
- Scripts
- Error-reporting
  - Trace files
  - Alert logs
- Back to the Diagram

Key Management

VORMETRIC

- Key types:
  - Asymmetric
  - Symmetric
- Asymmetric key algorithms:
  - Original: Diffie-Hellman
  - Current: RSA
    - Ron Rivest, Adi Shamir and Leonard Adleman, not the company!
- Symmetric key algorithms
  - 3DES
  - AES
    - 128-bit
    - 256-bit
    - ARIA

VORMETRIC

What is Key Management?

- Where are they stored?
- How are they accessed/made available?
- What availability requirements exist?
- Who manages the keys?
- What regulations are involved with key management?
  - HITECH
  - PCI-DSS #3.6
  - And so on
- What kinds of keys can be managed, using which interfaces?

VORMETRIC

Active vs. Passive Key Management

- Active
  - Primary requirements
    - Encryption system must support a standards-based interface
    - Key manager must support interface
  - Primary benefits
    - Centralized key generation
    - Automated backup
    - Policy based key management
    - Audit of key management process
- Passive
  - Primary requirements
    - Integrated key manager must store keys in separate files or have ability to parse keys into separate elements
    - Integrated key manager must have backup capability
  - Primary benefits
    - Centralized backup and ability to restore
    - Central point to manage key states
    - Secure key store
    - Audit of key restoration

Gartner on Key Management

- Organizations need to consider access control when deploying encryption —typical encryption deployments provide the decryption mechanisms to anyone who is granted access to the data. Without removing illegitimate access grants, "guest" and other default accounts can be privy to sensitive information beyond their true entitlements.
- Furthermore, encryption deployments need to have centralized key management. Without key management, organizations will not have auditing capabilities and will lack the ability recover data where a key has been lost or a password has been forgotten.
- Lastly, key management without key backup will inevitably result in inadvertent digital data shredding. The act of encrypting data with a good encryption solution involves rendering data in a form that is virtually impossible to simply resolve back to its original form. Most modern cryptographic algorithms are design to require thousands of years of all the currently available computing cycles. If a key is lost, organizations must categorically assume the data is lost.

“Data Encryption for Compliance and Information Governance” Eric Ouellet, Gartner (June 2011)

VORMETRIC

The Enterprise Key Management Pain

- **Complexity & Messy Management**
  - > Widespread encryption adoption due to regulatory & risk drivers, but multiple encryption solutions increases risk of loss of keys and can lead to poor key management
  - > Varied models of key management
- **Poor Security:** Weak key management can damage the utility of encrypting data
  - > No centralized management, weak security for stored keys, inadequate separation of duties model
- **Ensuring Availability**: Mission critical data now encrypted
  - > Access to the key must be robust, highly available and rapidly restorable

VORMETRIC

Major Requirements Key Management

- **Availability**:
  - Can **never** lose a key
- **Security**:
  - Keys cannot be compromised
- **Manageability**:
  - Must centrally manage key expiration and key activity
- **Governance**:
  - Must meet regulatory and compliance requirements

VORMETRIC

Key Management Challenge: Interfaces

- Many encryption vendors do not support standards-based key management interfaces
- Many key management interfaces to consider
  - PKCS#11 – Oracle 11gR2 TDE
  - EKM/MSCAPI – Microsoft SQL Server 2008 TDE
  - 1619 draft – Some tape backup vendors (EOL)
  - KMIP – Recently finalized by OASIS, evolving as the standard

Broad key management today requires both active key management and key vaulting

Questions?

Key Management

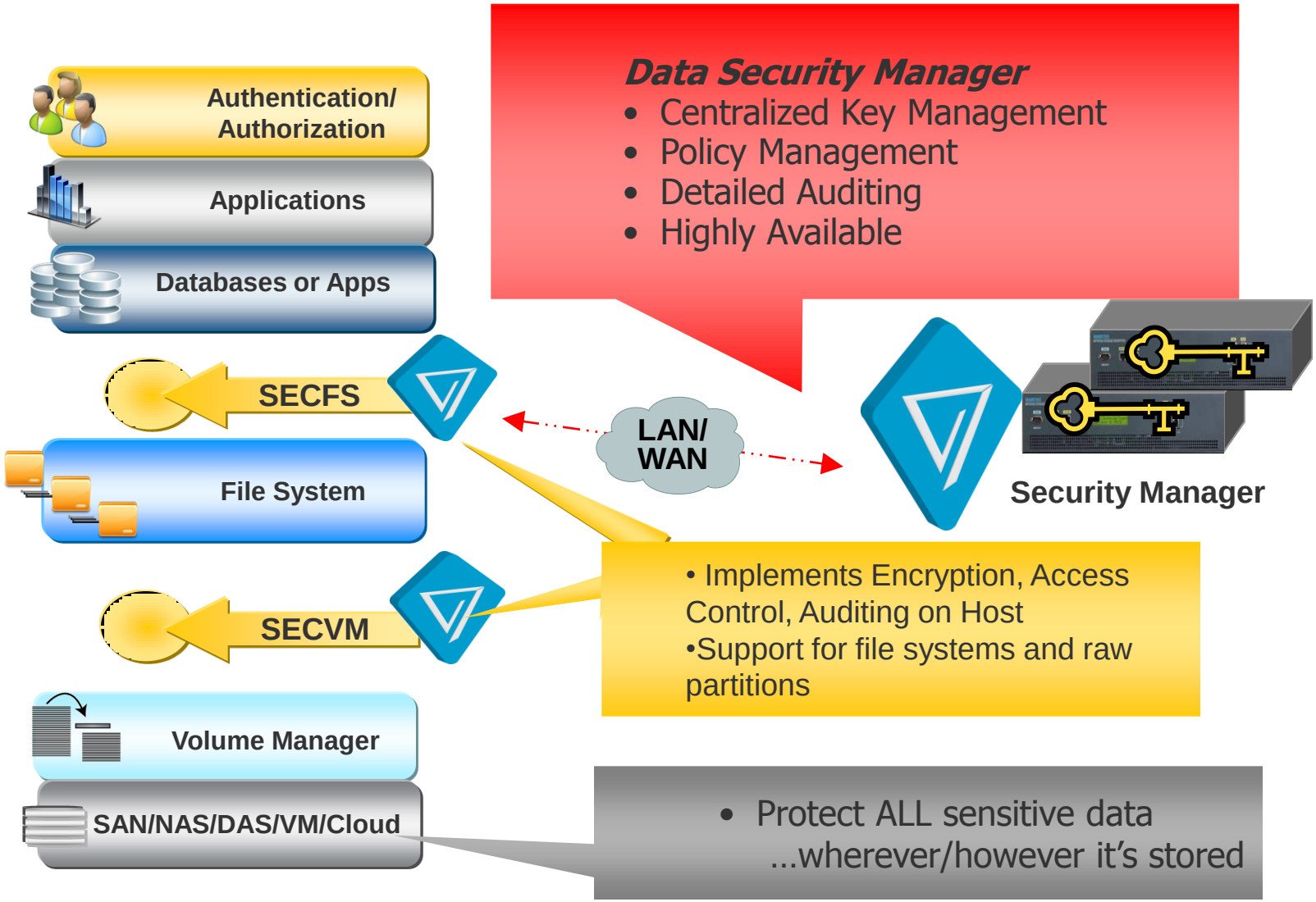
VORMETRIC

URLs

- Vormetric:
  - http://www.vormetric.com
- Data breach tracking sites:
  - Privacy Rights Clearinghouse Chronology of Data Breaches, http://www.privacyrights.org/data-breach
  - Open Security Foundation Data Loss database, http://datalossdb.org/
- List of US State Data Breach Notification Laws:
  - http://www.ncsl.org/default.aspx?tabid=13489
- Payment Card Interface/Data Security Standard:
  - https://www.pcisecuritystandards.org/security_standards/documents.php
- Oracle's Database 11*g*: Interactive Quick Reference
  - Google the above or
  - http://blogs.oracle.com/databaseinsider/entry/now_available_-_oracle_databas

Vormetric Marketing

Vormetric Data Security Architecture



VORMETRIC

Introducing Vormetric Key Management

- Management of Oracle TDE Master Encryption Keys (MEK)
  - Secure storage and centralized management of Master Encryption Key
  - Avoids cost of Hardware Security Module(HSM) per database server
  - Overcomes Oracle TDE key management pain, enabling broader deployments
- Management of SQL Server 2008 TDE Database Encryption Keys (DEK)
  - Avoids cost of HSM (the Data Security Manager **is** the HSM)
  - Overcomes SQL Server key management pain, enabling broader deployments
- Key Vault
  - Repository for third party keys of any strength, both symmetric and asymmetric
  - Expiration tracking

Backup

PCI Levels

- Merchant Levels
  - Level 1 - >6 M transactions of any one brand
  - Level 2 - 150,000 – 6M
  - Level 3 - 20,000-150,000
  - Level 4 - <20,000

- Service Provider Levels (Visa)
  - Level 1 – All endpoints (connect into VisaNet)
  - Level 2 – > 1 M transactions
  - Level 3 – <1M transactions

- Service Provider Levels (Master Card)
  - Level 1 – All Third Party Providers (registered) and Data Storage Entities (DSE) storing on behalf of Level 1 & 2 merchants
  - Level 2 – All DSEs storing on behalf of Level 3 merchants
  - Level 3 – All others not defined

Standards Background: PKCS#11, MSCAPI & KMIP

- PKCS#11
  - One of the family of standards called Public-Key Cryptography Standards (PKCS) published by RSA Laboratories that defines a platform-independent API to cryptographic tokens such as Hardware Security modules (HSMs). PKCS#11 defines the most commonly used cryptographic object types and all the functions needed to use, create/generate, modify, and delete objects.
- Extensible Key Management and Microsoft Cryptographic API (MSCAPI)
  - SQL Server provides data encryption capabilities and Extensible Key Management (EKM) using MSCAPI, an application programming interface included with Microsoft Windows that provides services to secure Windows-based applications using cryptography.

Standards Background: PKCS#11, MSCAPI & KMIP (continued)

- KMIP
  - The Key Management Interoperability Protocol (KMIP) is intended to establish a single, comprehensive protocol for the communication between enterprise key management systems and encryption systems. By using a consolidated protocol, organizations will be able to simplify key management and reduce operational costs. The KMIP standards efforts are governed by OASIS (Organization for the Advancement of Structured Information Standards).