

MySQL Security: Best Practices

Sastry Vedantam
sastry.vedantam@oracle.com

ORACLE



Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

43%

of companies have experienced a data breach in the past year.

Source: Ponemon Institute, 2014

Mega Breaches

Note DBIR 2015 should be coming out soon I think – so we can pull 2014 numbers maybe



552 Million identities exposed in 2013. 493% increase over previous year

77%

Web sites with vulnerabilities. 1-in-8 of all websites had a critical vulnerability.



Breaches that exposed more than 10 million records in 2013.



Total Breaches increased 62% in 2013

Source: Internet Security Threat Report 2014, Symantec



Database Vulnerabilities

- Poor Configurations
 - Set controls and change default setting
- Over Privileged Accounts
 - Privilege Policies
- Weak Access Control
 - Dedicated Administrative Accounts
- Weak Authentication
 - Strong Password Enforcement
- Weak Auditing
 - Compliance & Audit Policies
- Lack of Encryption
 - Data, Back, & Network Encryption
- Proper Credential or Key Management
 - Use `mysql_config_editor` , Key Vaults
- Unsecured Backups
 - Encrypted Backups
- No Monitoring
 - Security Monitoring, Users, Objects
- Poorly Coded Applications
 - Database Firewall

Database Attacks

- SQL Injection
 - Prevention: DB Firewall, White List, Input Validation
- Buffer Overflow
 - Prevention: Frequently apply Database Software updates, DB Firewall, White List, Input Validation
- Brute Force Attack
 - Prevention: lock out accounts after a defined number of incorrect attempts.
- Network Eavesdropping
 - Prevention: Require SSL/TLS for all Connections and Transport
- Malware
 - Prevention: Tight Access Controls, Limited Network IP access, Change default settings

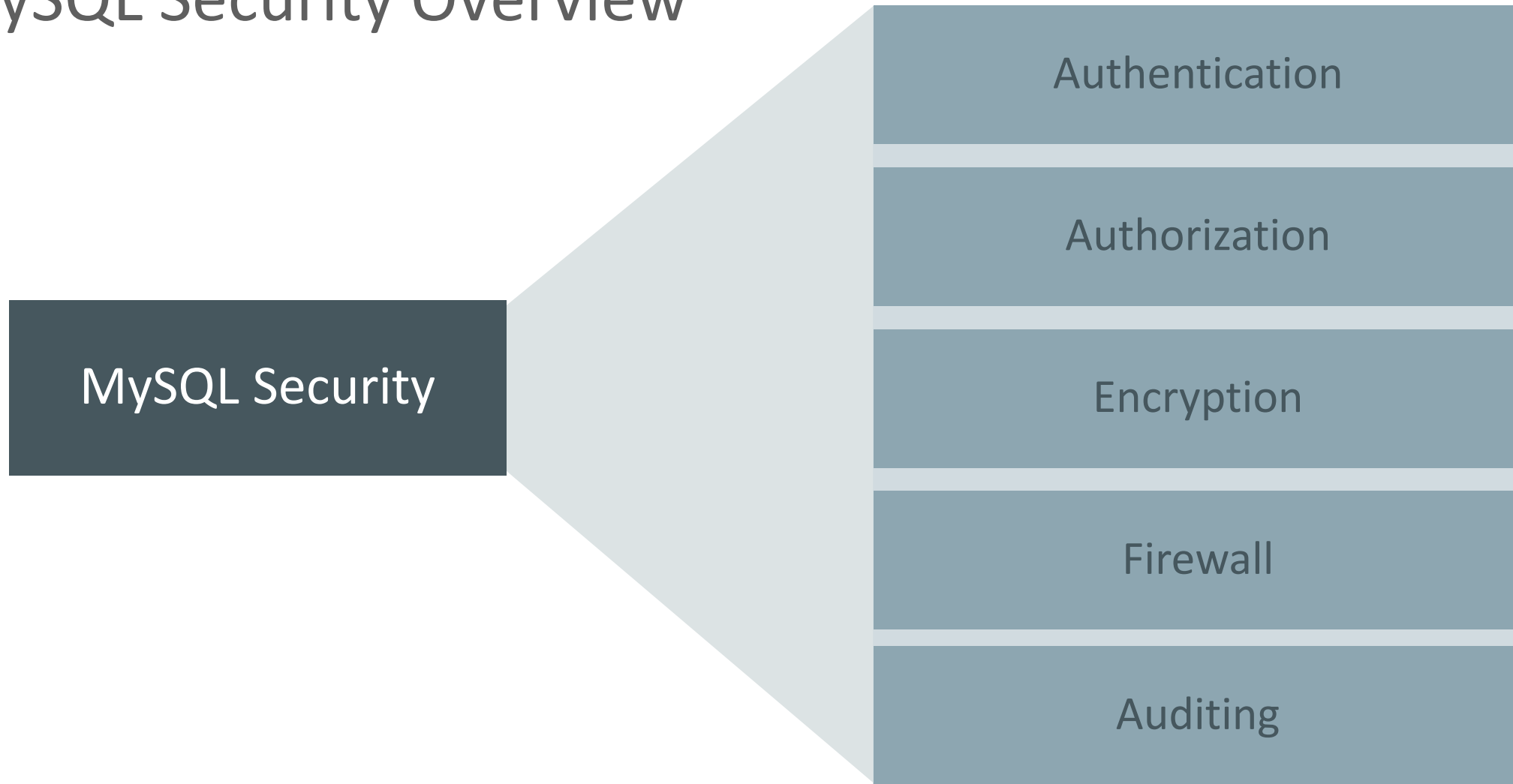
Regulatory Compliance

- Regulations
 - PCI – DSS: Payment Card Data
 - HIPAA: Privacy of Health Data
 - Sarbanes Oxley: Accuracy of Financial Data
 - EU Data Protection Directive: Protection of Personal Data
 - Data Protection Act (UK): Protection of Personal Data
- Requirements
 - Continuous Monitoring (Users, Schema, Backups, etc)
 - Data Protection (Encryption, Privilege Management, etc.)
 - Data Retention (Backups, User Activity, etc.)
 - Data Auditing (User activity, etc.)

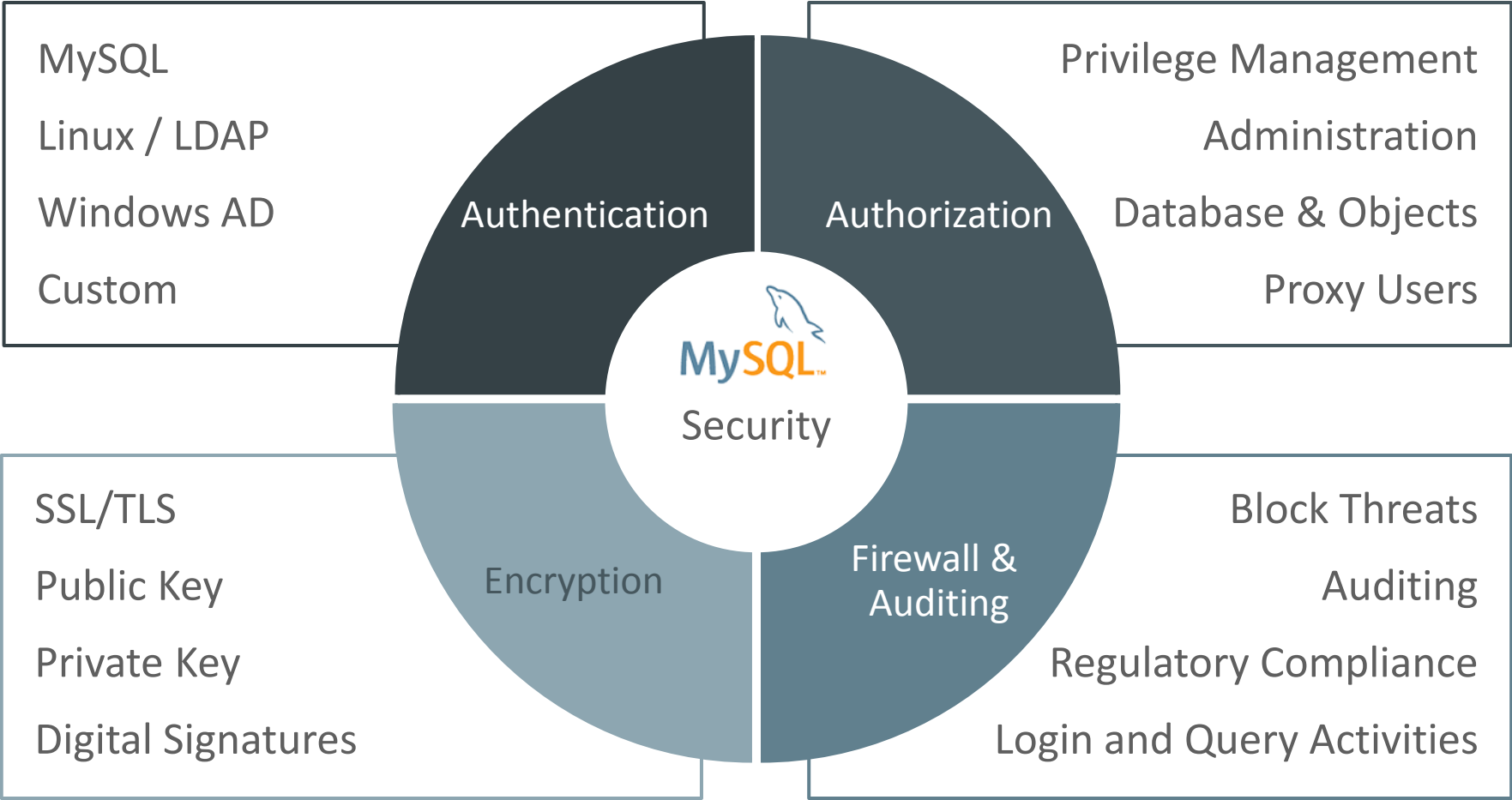


Data Protection Act 1998

MySQL Security Overview

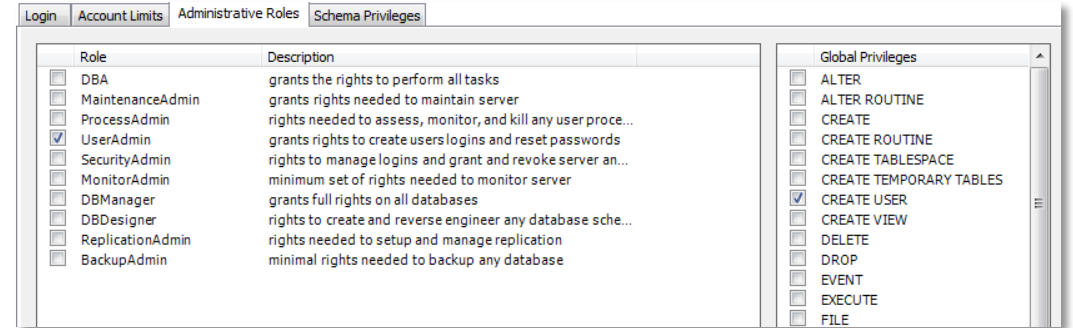


MySQL Security Overview



MySQL Authorization

- Administrative Privileges
- Database Privileges
- Session Limits and Object Privileges
- Fine grained controls over user privileges
 - Creating, altering and deleting databases
 - Creating, altering and deleting tables
 - Execute INSERT, SELECT, UPDATE, DELETE queries
 - Create, execute, or delete stored procedures and with what rights
 - Create or delete indexes



Security Privilege Management in MySQL Workbench

MySQL Privilege Management Grant Tables

user

- User Accounts
- Global Privileges

db

- Database Level Privileges
- Database, Tables, Objects
- User and host

tables_priv

- Table level privileges
- Table and columns

columns_priv

- Specific columns

procs_priv

- Stored Procedures
- Functions
- Single function privilege

proxies_priv

- Proxy Users
- Proxy Privileges

MySQL Authentication

- Built in Authentication
 - user table stores users and encrypted passwords
- X.509
 - Server authenticates client certificates
- MySQL Native, SHA 256 Password plugin
 - Native uses SHA1 or plugin with SHA-256 hashing and per user salting for user account passwords.
- MySQL Enterprise Authentication
 - Microsoft Active Directory
 - Linux PAMs (Pluggable Authentication Modules)
 - Support LDAP and more
- Custom Authentication

MySQL Password Policies

- Accounts without Passwords
 - Assign passwords to all accounts to prevent unauthorized use
- Password Validation Plugin
 - Enforce Strong Passwords
- Password Expiration/Rotation
 - Require users to reset their password
- Account lockout (in v. 5.7)

MySQL Encryption

- SSL/TLS Encryption
 - Between MySQL clients and Server
 - Replication: Between Master & Slave
- Data Encryption
 - AES Encrypt/Decrypt
- MySQL Enterprise Encryption
 - Asymmetric Encrypt/Decrypt
 - Generate Public Key and Private Keys
 - Derive Session Keys
 - Digital Signatures
- MySQL Enterprise Backup
 - AES Encrypt/Decrypt

Database Firewall

- SQL Injection: #1 Web Application Vulnerability
 - 77% of Web Sites had vulnerabilities
 - 1 in 8 critical vulnerabilities
- MySQL Enterprise Firewall
 - Monitor database statements in real-time
 - Automatic White List “rules” generation for any application
 - Out of policy database transactions detected and blocked

Database Auditing

- Auditing for Security & Compliance
 - FIPS, HIPAA, PCI-DSS, SOX, DISA STIG, ...
- MySQL built-in logging infrastructure:
 - general log, error log
- MySQL Enterprise Audit
 - Granularity made for auditing
 - Can be modified live
 - Contains additional details
 - Compatible with Oracle Audit Vault.

MySQL Database Hardening

Installation

- Mysql_secure_installation
- Keep MySQL up to date
 - MySQL Installer for Windows
 - Yum/Apt Repository

Configuration

- Firewall
- Auditing and Logging
- Limit Network Access
- Monitor changes

User Management

- Remove Extra Accounts
- Grant Minimal Privileges
- Audit users and privileges

Passwords

- Strong Password Policy
- Hashing, Expiration
- Password Validation Plugin

Encryption

- SSL/TLS for Secure Connections
- Data Encryption (AES, RSA)

Backups

- Monitor Backups
- Encrypt Backups

MySQL Enterprise Edition

- MySQL Enterprise **Authentication**
 - External Authentication Modules
 - Microsoft AD, Linux PAMs
- MySQL Enterprise **Encryption**
 - Public/Private Key Cryptography
 - Asymmetric Encryption
 - Digital Signatures, Data Validation
- MySQL Enterprise **Firewall**
 - Query Monitoring, White List Matching,
- MySQL Enterprise **Audit**
 - User Activity Auditing, Regulatory Compliance
- MySQL Enterprise **Monitor**
 - Changes in Database Configurations, Users Permissions, Database Schema, Passwords
- MySQL Enterprise **Backup**
 - Securing Backups, AES 256 encryption

MySQL Enterprise Monitor

- Enforce MySQL Security Best Practices
 - Identifies Vulnerabilities
 - Assesses current setup against security hardening policies
- Monitoring & Alerting
 - User Monitoring
 - Password Monitoring
 - Schema Change Monitoring
 - Backup Monitoring
 - Configuration Management
 - Configuration Tuning Advice
- Centralized User Management

Item	Info	Coverage	Schedule	Event Handling	Parameters
Account Has An Overly Broad Host Specifier	?	100% (103/103)	5m	0 2 0	0
Account Has Global Privileges	?	100% (103/103)	5m	0 2 0	0
Account Has Old Insecure Password Hash	?	100% (103/103)	6h	0 2 0	0
Account Has Strong MySQL Privileges	?	100% (103/103)	5m	0 2 0	0
Account Requires Unavailable Authentication Plugins	?	100% (103/103)	6h	1 3 0	0
Insecure Password Authentication Option Is Enabled	?	100% (103/103)	6h	0 2 0	0
Insecure Password Generation Option Is Enabled	?	100% (103/103)	6h	0 2 0	0
LOCAL Option Of LOAD DATA Statement Is Enabled	?	100% (103/103)	5m	0 2 0	0
Non-Authorized User Has DB, Table, Or Index Privileges On All Databases	?				
Non-Authorized User Has GRANT Privileges On All Databases	?				
Non-Authorized User Has Server Admin Privileges	?				
Policy-Based Password Validation Does Not Perform Dictionary Checks	?				
Policy-Based Password Validation Is Weak	?				
Policy-Based Password Validation Not Enabled	?				
Privilege Alterations Detected: Privileges Granted	?				
Privilege Alterations Detected: Privileges Revoked	?				
Privilege Alterations Have Been Detected	?				
Root Account Can Login Remotely	?	100% (103/103)	5m	0 2 0	0
Root Account Without Password	?	100% (103/103)	5m	1 3 0	0
SHA-256 Password Authentication Not Enabled	?	100% (103/103)	6h	0 2 0	0
Server Contains Default "test" Database	?	100% (103/103)	5m	0 3 0	0
Some User Accounts Without A Password	?	100% (103/103)	5m	0 2 0	0

Problem Description
When users create weak passwords (e.g. 'password' or 'abcd') it compromises the security of the server, making it easier for unauthorized people to guess the password and gain access to the server. Starting with MySQL Server 5.6, MySQL offers the 'validate_password' plugin that can be used to test passwords and improve security. With this plugin you can implement and enforce a policy for password strength (e.g. passwords must be at least 8 characters long, have both lowercase and uppercase letters, and contain at least one special nonalphanumeric character).

Links and Further Reading
[MySQL Manual: The Password Validation Plugin](#)
[MySQL Manual: Keeping Passwords Secure](#)
[Blog: New 5.6 password verification plugin \(and impacts to PASSWORD\(\) function\)](#)
[Blog: Implementing a password policy in MySQL](#)

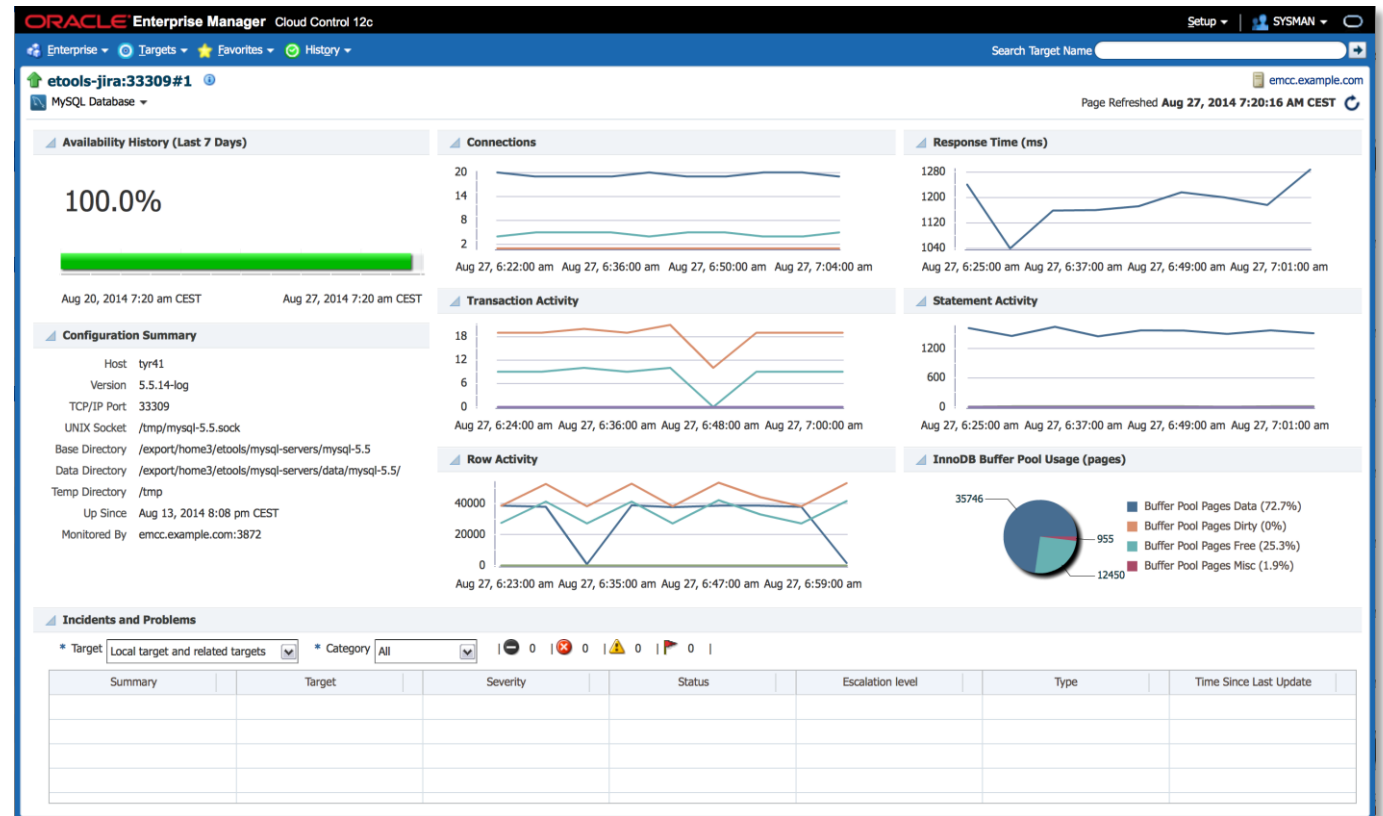
Expression
%status% == "ACTIVE" && %validate_password_policy% == THRESHOLD

"I definitely recommend the MySQL Enterprise Monitor to DBAs who don't have a ton of MySQL experience. It makes monitoring MySQL security, performance and availability very easy to understand and to act on."

Sandi Barr
Sr. Software Engineer
Schneider Electric

































Oracle Enterprise Manager for MySQL

- Availability monitoring
- Performance monitoring
- Configuration monitoring
- All available metrics collected
 - Allowing for custom threshold based incident reports
- MySQL auto-detection



MySQL Enterprise Firewall

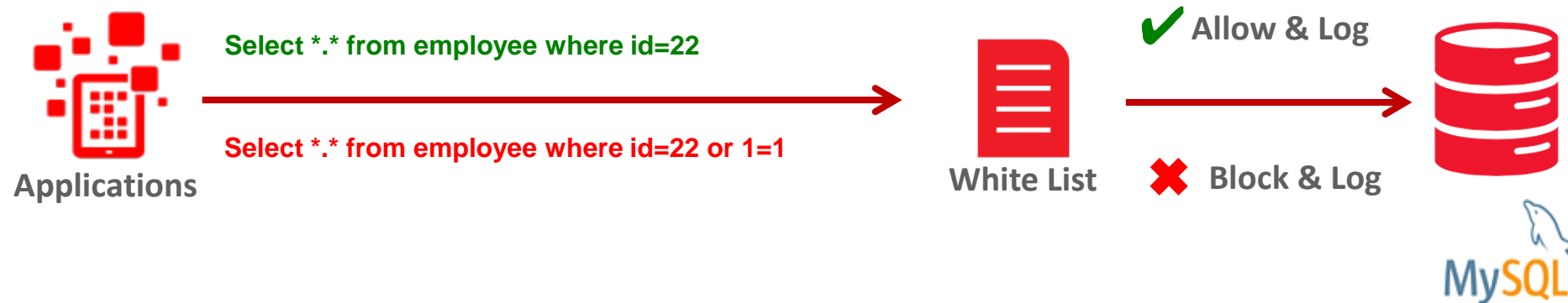
- Real Time Protection
 - Queries analyzed and matched against White List
- Blocks SQL Injection Attacks
 - Positive Security Model
- Block Suspicious Traffic
 - Out of Policy Transactions detected & blocked
- Learns White List
 - Automated creation of approved list of SQL command patterns on a per user basis
- Transparent
 - No changes to application required

Enterprise Firewall		Configured: 8 of 8
<input type="checkbox"/> Item		Info
<input type="checkbox"/>   	Account Has Overly Permissive White List	
<input type="checkbox"/>   	Account Sending Excessive Percentage of Blocked Queries	
<input type="checkbox"/>   	Account Without Firewall Protection	
<input type="checkbox"/>   	Excessive Number of Queries Blocked By Firewall	
<input type="checkbox"/>   	Firewall Max Query Size Too Small	
<input type="checkbox"/>   	Firewall Not Enabled	
<input type="checkbox"/>   	Firewall Not Installed	
<input type="checkbox"/>   	Firewall Trace Has Been Enabled	

MySQL Enterprise Firewall monitoring

MySQL Enterprise Firewall

- SQL Injection Protection with Positive Security Model



- Out of policy database transactions detected and blocked
- Logging & Analysis

Integrates MySQL with existing security infrastructures

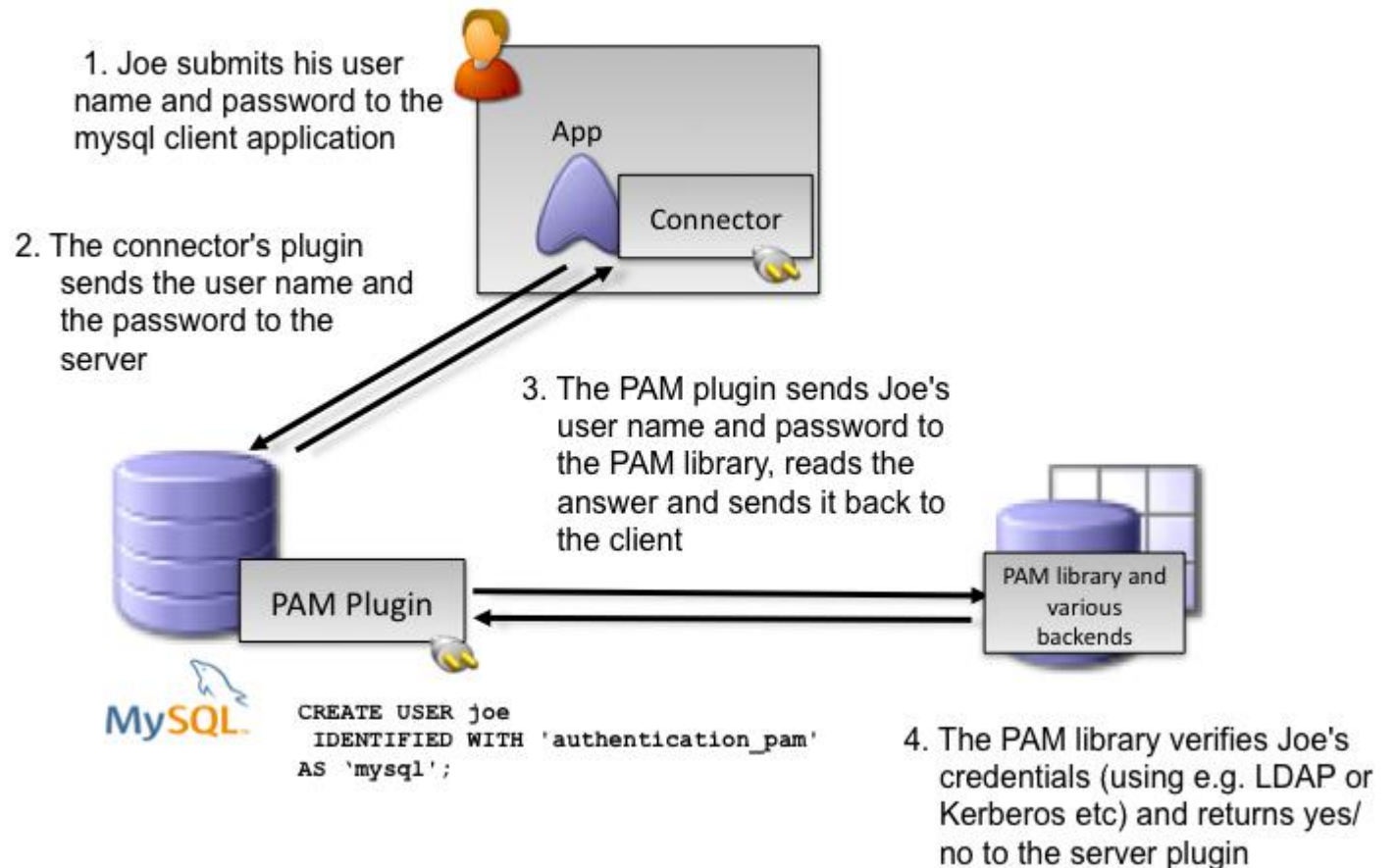
MySQL Enterprise **Authentication**

- Integrate with Centralized Authentication Infrastructure
 - Centralized Account Management
 - Password Policy Management
 - Groups & Roles
- PAM (Pluggable Authentication Modules)
 - Standard interface (Unix, LDAP, Kerberos, others)
 - Windows
 - Access native Windows service - Use to Authenticate users using Windows Active Directory or to a native host



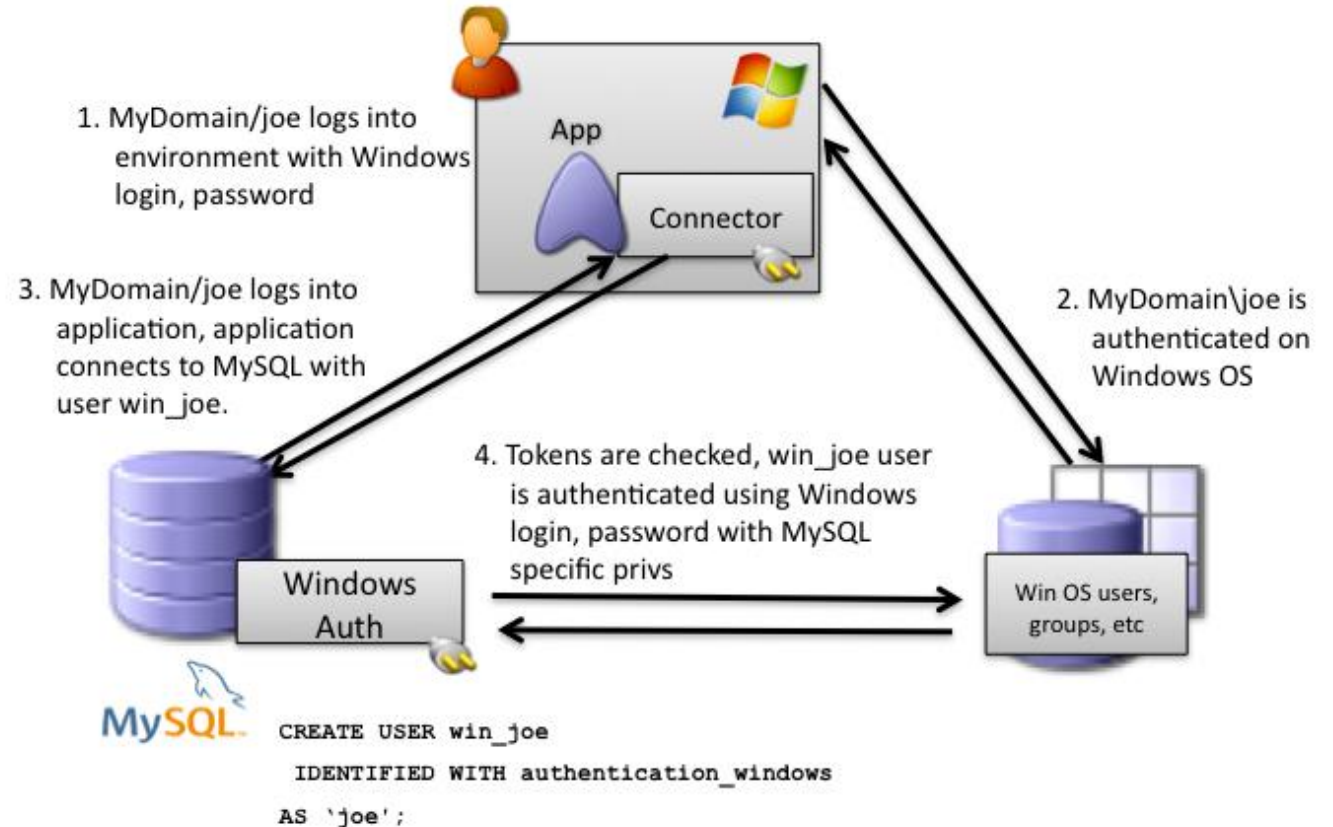
MySQL Enterprise Authentication: PAM

- Standard Interface
 - LDAP
 - Unix/Linux
- Proxy Users



MySQL Enterprise Authentication: **Windows**

- Windows Active Directory
- Windows Native Services

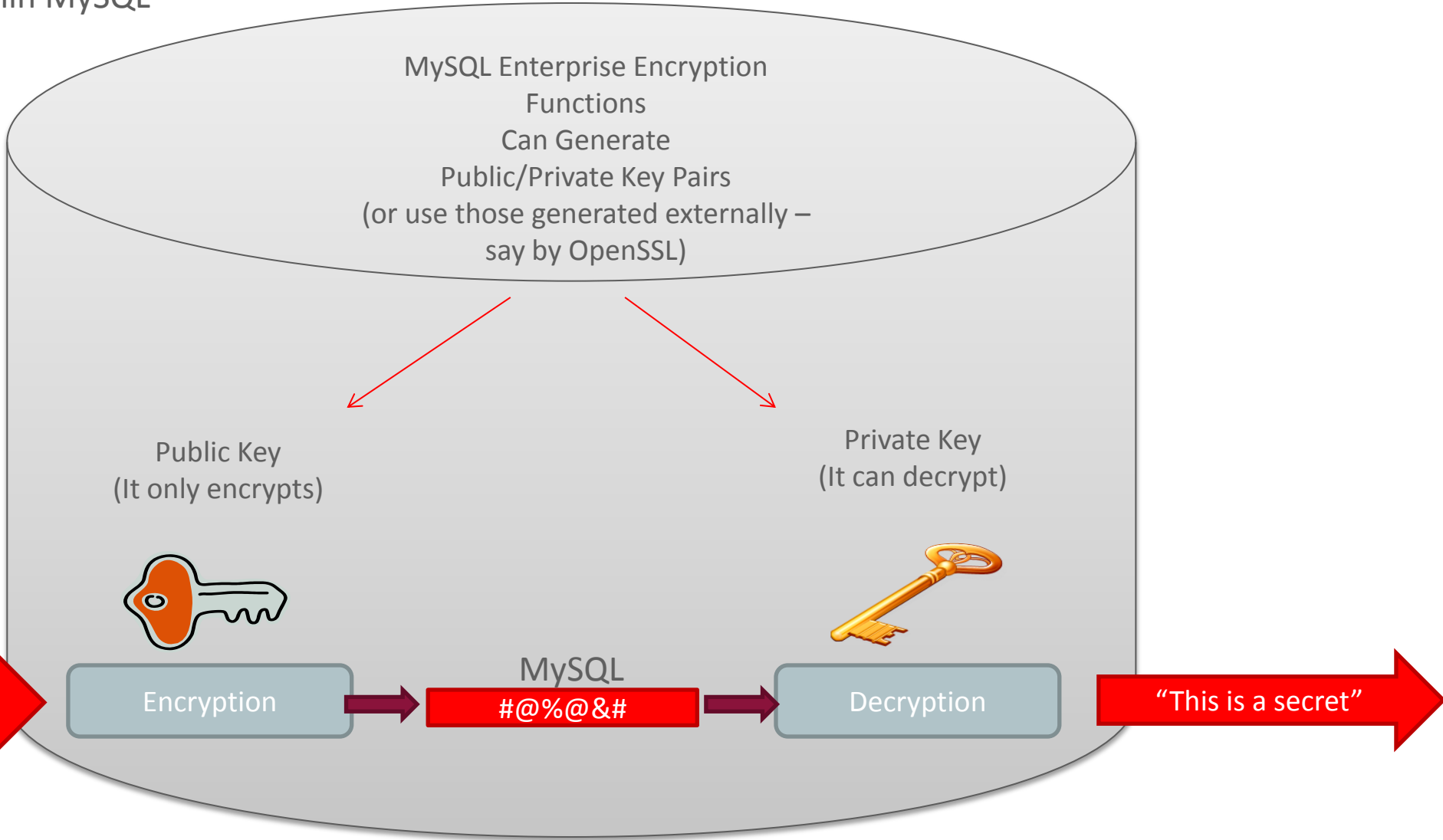


MySQL Enterprise Encryption

- MySQL encryption functions
 - Symmetric encryption AES256 (All Editions)
 - Public-key / asymmetric cryptography – RSA
- Key management functions
 - Generate public and private keys
 - Key exchange methods: DH
- Sign and verify data functions
 - Cryptographic hashing for digital signing, verification, & validation – RSA, DSA



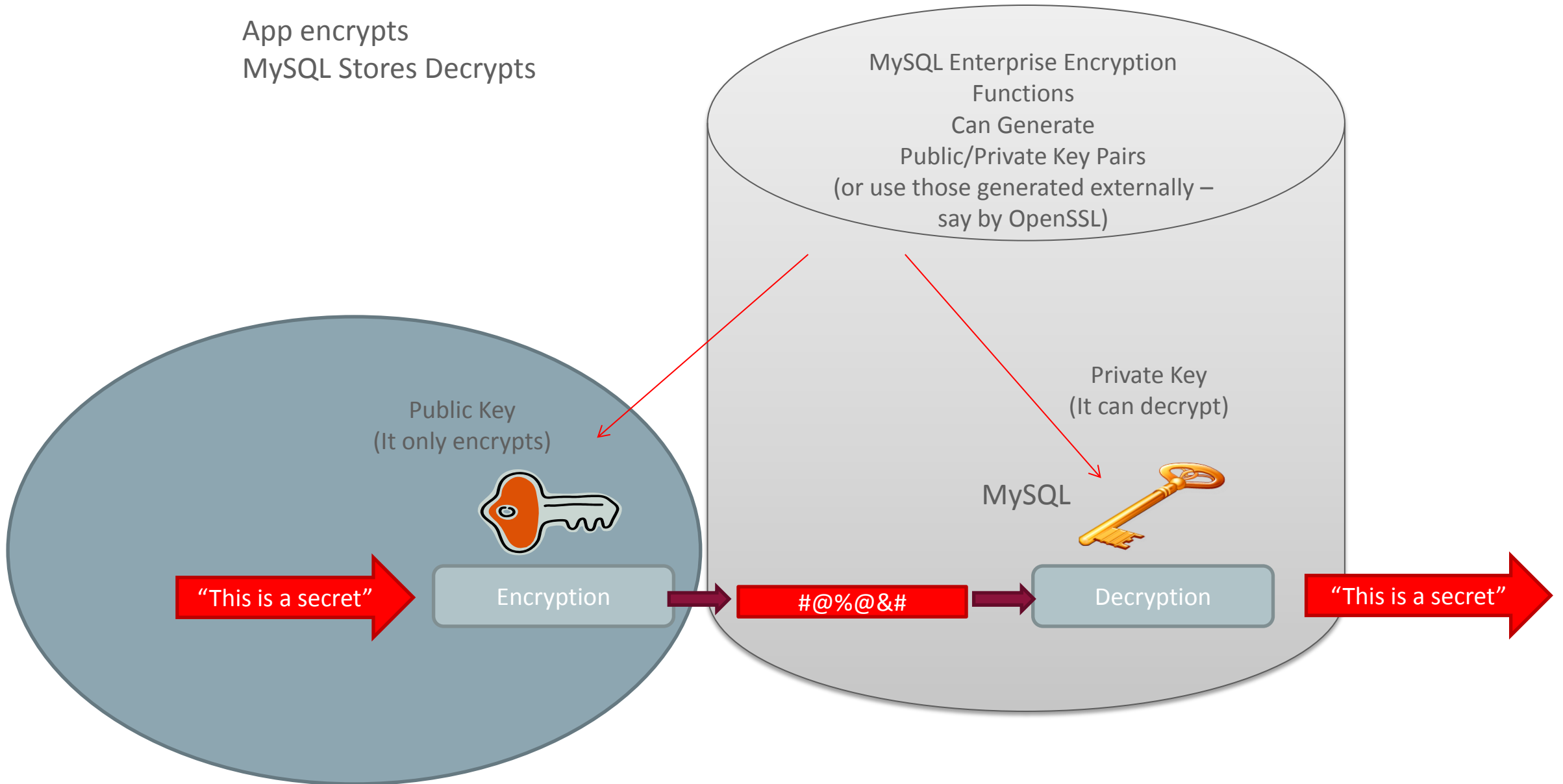
All within MySQL



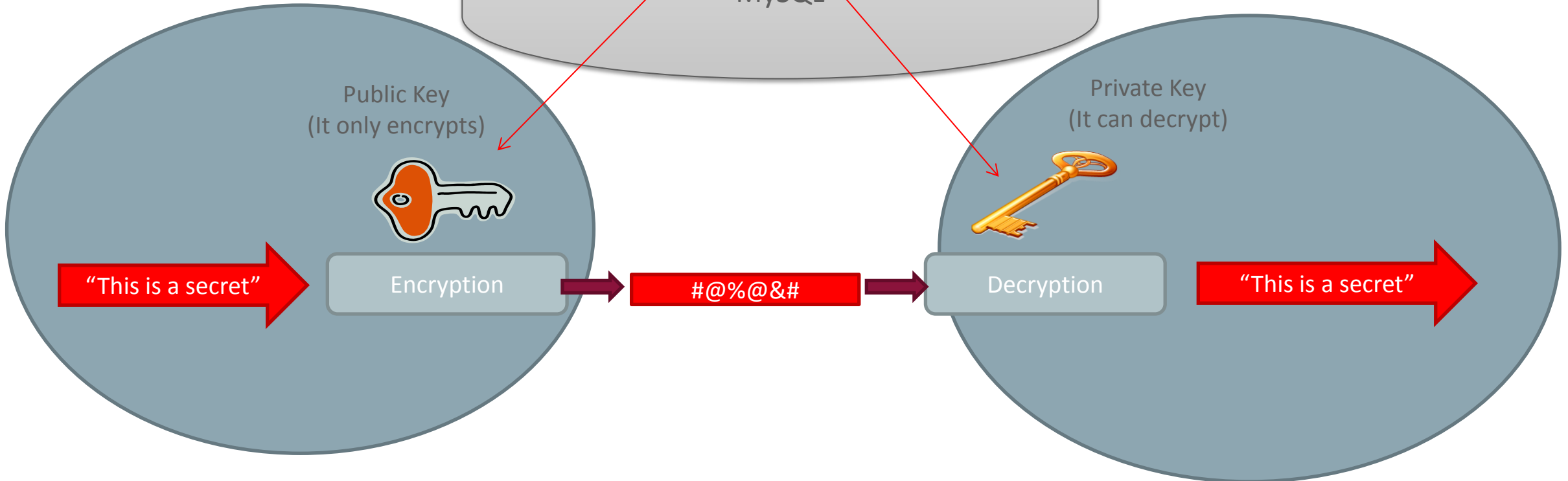
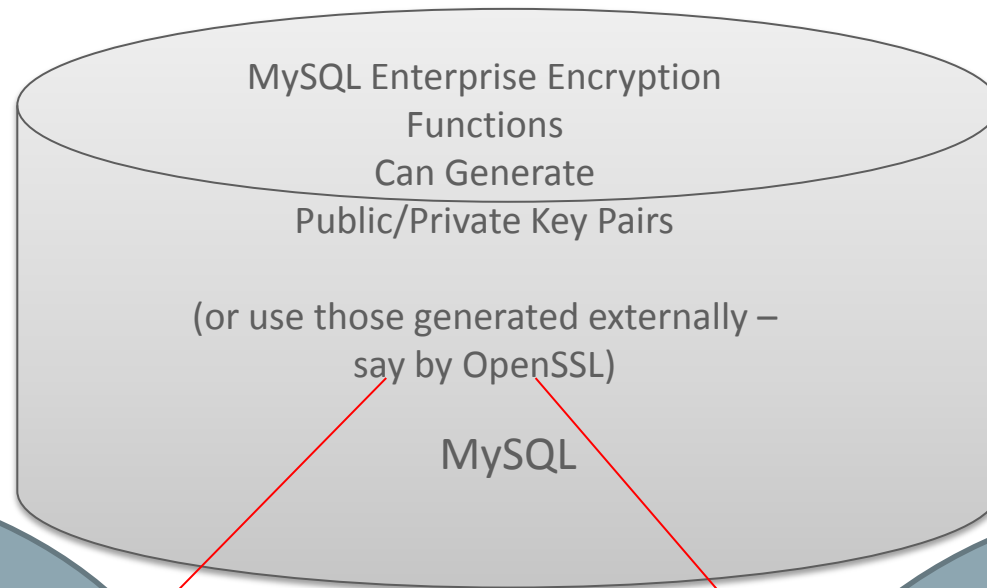
Could be
From Client App
Within MySQL (function call)



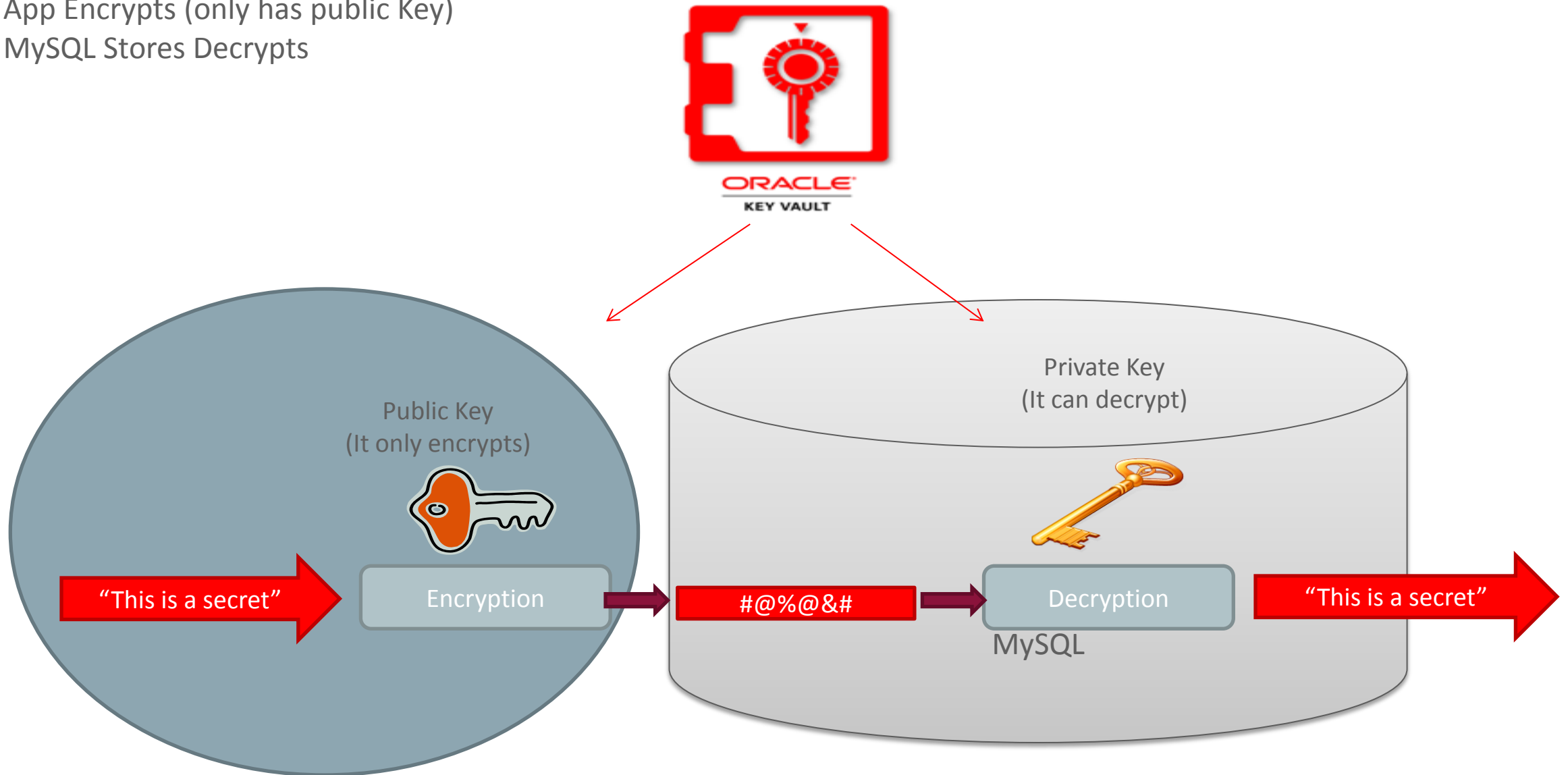
App encrypts
MySQL Stores Decrypts



App encrypts
MySQL Stores
App Decrypts



Oracle (or other) Key Vault Generates Keys
App Encrypts (only has public Key)
MySQL Stores Decrypts



MySQL Enterprise **Audit**

- Out-of-the-box logging of connections, logins, and query
- User defined policies for filtering, and log rotation
- Dynamically enabled, disabled: no server restart
- XML-based audit stream per Oracle Audit Vault spec

Adds regulatory compliance to
MySQL applications
(HIPAA, Sarbanes-Oxley, PCI, etc.)

MySQL Enterprise Audit

```
mysql> INSTALL PLUGIN audit_log SONAME 'audit_log.so';
```

```
mysql> SHOW VARIABLES LIKE 'audit_log%';
```



audit_log_buffer_size	1048576
audit_log_connection_policy	ALL
audit_log_current_session	OFF
audit_log_exclude_accounts	
audit_log_file	audit.log
audit_log_flush	OFF
audit_log_format	NEW
audit_log_include_accounts	
audit_log_policy	ALL
audit_log_rotate_on_size	0
audit_log_statement_policy	ALL
audit_log_strategy	ASYNCHRONOUS

1. DBA enables Audit plugin

```
shell> mysql -h joeshost -u joe -p  
Enter password: *****
```



```
mysql> SELECT * FROM joes_table;
```

FIRST_NAME	LAST_NAME
Joe	User

2. User Joe connects and runs a query



3. Joe's connection & query logged

```
<?xml version="1.0" encoding="UTF-8"?>  
<AUDIT>  
  <AUDIT_RECORD  
    TIMESTAMP="2012-08-02T14:52:12"  
    NAME="Audit"  
    SERVER_ID="1"  
    VERSION="1"  
    STARTUP_OPTIONS="--port=3306"  
    OS_VERSION="i686-Linux"  
    MYSQL_VERSION="5.5.28-debug-log"/>  
  <AUDIT_RECORD  
    TIMESTAMP="2012-08-02T14:52:41"  
    NAME="Connect"  
    CONNECTION_ID="1"  
    STATUS="0"  
    USER="joe"  
    PRIV_USER="root"  
    OS_LOGIN=""  
    PROXY_USER=""  
    HOST="SERVER1"  
    IP="127.0.0.1"  
    DB="joes_db"/>  
  <AUDIT_RECORD  
    TIMESTAMP="2012-08-02T14:53:45"  
    NAME="Query"  
    CONNECTION_ID="1"  
    STATUS="0"  
    SQLTEXT="SELECT * FROM joes_table;"/>  
</AUDIT>
```


MySQL Enterprise Backup

- Online Backup for InnoDB (scriptable interface)
- Full, Incremental, Partial Backups (with compression)
- Strong Encryption (AES 256)
- Point in Time, Full, Partial Recovery options
- Metadata on status, progress, history
- Scales – High Performance/Unlimited Database Size
- Windows, Linux, Unix
- Certified with Oracle Secure Backup, NetBackup, Tivoli, others

Oracle Audit Vault and Database Firewall

- Oracle DB Firewall
 - Oracle, MySQL, SQL Server, IBM DB2, Sybase
 - Activity Monitoring & Logging
 - White List, Black List, Exception List
- Audit Vault
 - Built-in Compliance Reports
 - External storage for audit archive

ORACLE®

Database
Firewall



MySQL Central @ OpenWorld

October 25 – 29, San Francisco

- Keynote
- Conferences Sessions
- Birds-of-a-feather sessions
- Tutorials
- Hands-on Labs
- Demos
- Receptions
- OpenWorld Extensive Content



Thank You

