MySQL Enterprise Security

Mike Frank
Product Management Director
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.
Program Agenda

1. Security Challenges
2. MySQL Security Solutions
3. The Details
4. New in MySQL 8
89% of Organizations Experienced Data Breaches, According to New Ponemon Report

Source: *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data*, conducted by Ponemon Institute

66% of the largest businesses in the UK have suffered a cyberattack or data breach within the past twelve months

Source: *UK government’s Cyber Security Breaches Survey 2016*

25% experience a repeated breach at least one a month

Source: *UK government’s Cyber Security Breaches Survey 2016*
Mega Breaches

429 Million identities exposed in 2015.

75%
Web sites with vulnerabilities. 15% of all websites had a critical vulnerability.

In 2015, a record of nine mega-breaches were reported.

9
One worlds largest 191M.
(Mega-breach = more than 10 million records.)

Mobile Vulnerabilities on the rise – up 214%

Infection by SQL Injection still strong.

Malware attacks on databases

Source: Internet Security Threat Report 2016, Symantec
Complexity grows
Risk Grows

Risk Multipliers
- High Availability
- Database Consolidation
- Legacy Applications
- Outsourcing
- Cloud

Cloud/OS/DB Admin  Test/Dev  Hackers  AppUser  HelpDesk

Applications  DB  OS  Backup  Network
Regulatory Compliance

• Regulations
  – PCI – DSS: Payment Card Data
  – HIPAA: Privacy of Health Data
  – Sarbanes Oxley, GLBA, The USA Patriot Act:
    Financial Data, NPI "personally identifiable financial information"
  – FERPA – Student Data
  – EU General Data Protection Directive: Protection of Personal Data (GDPR)
  – 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.)
Principles of Securing Databases

- **Assess**
  - Locate Risks and Vulnerabilities, Ensure that necessary security controls are

- **Prevent**
  - Using Cryptography, User Controls, Access Controls, etc

- **Detect**
  - Still a possibility of a breach – so Audit, Monitor, Alert

- **Recover**
  - Ensure service is not interrupted as a result of a security incident
  - Even through the outage of a primary database
  - Forensics – post mortem – fix vulnerability
MySQL Security Overview

MySQL Security

- Authentication
- Authorization
- Encryption
- Firewall
- Auditing
- Monitoring
- Availability
MySQL Enterprise Edition

- MySQL Enterprise **TDE**
  - Data-at-Rest Encryption
  - Key Management/Security

- MySQL Enterprise **Authentication**
  - External Authentication Modules
    - Microsoft AD, Linux PAMs

- MySQL Enterprise **Encryption**
  - Public/Private Key Cryptography
  - Asymmetric Encryption
  - Digital Signatures, Data Validation
  - User Activity Auditing, Regulatory Compliance

- MySQL Enterprise **Firewall**
  - Block SQL Injection Attacks
  - Intrusion Detection

- 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 **Thread pool**
  - Attack Hardening
MySQL Security Architecture

- Workbench
  - Model
  - Data
  - Audit Data
  - User Management

- Enterprise Monitor
  - Identifies Vulnerabilities
  - Security hardening policies
  - Monitoring & Alerting
  - User Monitoring
  - Password Monitoring
  - Schema Change Monitoring
  - Backup Monitoring

- Enterprise Authentication
  - SSO - LDAP, AD, PAM

- Access Controls

- Firewall

- Thread Pool
  - Attack minimization

- Network Encryption
- Strong Authentication

- Enterprise Audit
  - Powerful Rules Engine

- Audit Vault

- Data Encryption
  - TDE
  - Encryption
  - PKI

- Key Vault

- Enterprise Backup
  - Encrypted

- HA
  - InnoDB Cluster

- Assess
- Prevent
- Detect
- Recover

- Enterprise Authentication
- Network Encryption
- Strong Authentication
- Access Controls
- Firewall
- Thread Pool
- Audit Vault
- Data Encryption
- Key Vault
- Enterprise Backup
- HA
- InnoDB Cluster

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.
What is Transparent Data Encryption?

• Data at Rest Encryption
  – Tables spaces, Disks, Storage, OS File system

• Transparent to applications and users
  – No application code, schema or data type changes

• Transparent to DBAs
  – Keys are hidden from DBAs, no configuration changes

• Requires Key Management
  – Protection, rotation, storage, recovery
Biggest Challenge: Encryption Key Management

Management
- Proliferation of encryption wallets and keys
- Authorized sharing of keys
- Key availability, retention, and recovery
- Custody of keys and key storage files

Regulations
- Physical separation of keys from encrypted data
- Periodic key rotations
- Monitoring and auditing of keys
- Long-term retention of keys and encrypted data
MySQL Enterprise TDE: Goals

• Data at Rest Encryption
  – Tablespace Encryption

• Key Protection
  – Most Important and Difficult

• Strong Encryption
  – AES 256

• Simple to Manage
  – One master key for whole MySQL instance

• High Performance & Low Overhead
  • Simple Key Rotation without massive decrypt/encryption costs

• High Quality Infrastructure
  • Expand and support more security capabilities - encryption, keys, certs, ...
MySQL Transparent Data Encryption

Encrypted Database Files

Tablespace Key

Master Key

Accesses Files Directly

Information Access Blocked By Encryption

Malicious OS User / Hacker
Using MySQL Transparent Data Encryption is EASY

Plugin Infrastructure
- New plugin type: keyring
- Ability to load plugin before InnoDB initialization: --early-plugin-load

SQL
- New option in CREATE TABLE ENCRYPTION="Y"
- New SQL: ALTER INSTANCE ROTATE INNODB MASTER KEY

Keyring plugin
- Used to retrieve keys from Key Stores
- Over Standardized KMIP protocol

InnoDB
- Support for encrypted tables
- IMPORT/EXPORT of encrypted tables
- Support for master key rotation
Example Commands

• Installation
  – Set configuration for MySQL to talk to Oracle Key Vault
  – Connect to MySQL
    • `install plugin okv_kmip_keyring_file soname 'okv_kmip_keyring.dll';`

• Encrypt a table
  – `CREATE TABLE `<table>`` ( `ID` int(11) NOT NULL AUTO_INCREMENT, `Name` char(35) NOT NULL DEFAULT '', `...` ENGINES=InnoDB ... ENCRYPTION="Y"

• Rotate Master Key
  – `ALTER INSTANCE ROTATE INNODB MASTER KEY;`
PCI DSS

PCI DSS v3.0
November 2013

3.5 Store cryptographic keys in a secure form (3.5.2), in the fewest possible locations (3.5.3) and with access restricted to the fewest possible custodians (3.5.1)

3.6 Verify that key-management procedures are implemented for periodic key changes (3.6.4)

And more!
Key Vaults and Key Stores: General Purpose

- Databases
- Servers
- Middleware

- Administration Console, Alerts, Reports
- Secure Backups

- Wallets
- Keystores
- = Certificates
- = Password/phrases
- = Credential Files/Other
Oracle Key Vault

- Turnkey solution based on hardened stack
- Includes Oracle Database and security options
- Open x86-64 hardware to choose from
- Easy to install, configure, deploy, and patch
- Separation of duties for administrative users
- Full auditing, preconfigured reports, and alerts
MySQL Enterprise TDE: KMIP Compliant

• DBA never knows the Master Key
• Only a Key Vault Admin(s) have Master Key access
• Keys are protected and secure
• Enables customers to meet regulatory requirements
MySQL Enterprise Firewall

• Real Time Protection
  – Queries analyzed and matched against White List

• Blocks SQL Injection Attacks
  – Block Out of Policy Transactions

• Intrusion Detection
  – Detect and Alert on Out of Policy Transactions

• Learns White List
  – Automated creation of approved list of SQL command patterns on a per user basis

• Transparent
  – No changes to application required
MySQL Enterprise Authentication

• Integrate with Centralized Authentication Infrastructure
  – Centralized Account Management
  – Password Policy Management
  – Groups & Roles

Supports
  – Linux PAM (Pluggable Authentication Modules)
  – Windows Active Directory
  – LDAP

Integrates MySQL with existing security infrastructures
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
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
- New Features Coming Soon

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

- **Enterprise Authentication**
  - SSO - LDAP, AD, PAM

- **Workbench**
  - Model
  - Data
  - Audit Data
  - User Management

- **Enterprise Monitor**
  - Identifies Vulnerabilities
  - Security hardening policies
  - Monitoring & Alerting
  - User Monitoring
  - Password Monitoring
  - Schema Change Monitoring
  - Backup Monitoring

- **Enterprise Audit**
  - Powerful Rules Engine

- **Access Controls**

- **Firewall**
  - Thread Pool
  - Attack minimization

- **Network Encryption**
  - Strong Authentication

- **Enterprise Backup**
  - Encrypted

- **Audit Vault**

- **Key Vault**
  - Data Encryption
    - TDE
    - Encryption
    - PKI
  - HA
    - Innodb Cluster

- **Assess**
- **Prevent**
- **Detect**
- **Recover**

**Users**

**Firewall**

**Network Encryption**

**Strong Authentication**

**Access Controls**

**Thread Pool**
- Attack minimization

**Audit Vault**

**Strong Authentication**

**Enterprise Backup**

**HA**
- Innodb Cluster

**Data Encryption**
- TDE
- Encryption
- PKI
New Security Features in MySQL 8.0
New! MySQL Roles

Improving MySQL Access Controls
• Introduced in the 8.0.0 DMR
• Easier to manage user and applications rights
• As standards compliant as practically possible
• Multiple default roles
• Can export the role graph in GraphML
Role Examples

```sql
CREATE ROLE `r1`, `admin-db1`, `admin-db2`, `admin-db1t1`, `admin-db2t1`, `app-updater`;

CREATE USER `app-middleware-db1`@localhost, `app-middleware-db2`@localhost, `app`@localhost;

GRANT `admin-db1`, `app-updater` TO `app-middleware-db1`@localhost;
GRANT `r1` TO `app-middleware-db1`@localhost WITH ADMIN OPTION;
GRANT `admin-db2t1` TO `admin-db1`;
GRANT `admin-db1t1` TO `admin-db1` WITH ADMIN OPTION;
GRANT `admin-db1t1` TO `admin-db2`, `app`@localhost;
GRANT `admin-db2` TO `app-middleware-db2`@localhost;
```
New! Atomic ACL Statements

• Long standing MySQL issue!
  – For Replication, HA, Backups, etc.

• Possible now - ACL tables reside in 8.0 InnoDB Data Dictionary

• Not just a table operation: memory caches need update too

• Applies to statements performing multiple logical operations, e.g.
  – CREATE USER u1, u2
  – GRANT SELECT ON *.* TO u1, u2

• Uses a custom MDL lock to block ACL related activity
  – While altering the ACL caches and tables
New! Dynamic Privileges

Provides finer grained administrative level access controls

• Too often super is required for tasks when less privilege is really needed
  – Support concept of “least privilege”

• Needed to allow adding administrative access controls
  – Now can come with new components
  – Examples
    • Replication
    • HA
    • Backup

• Give us your ideas
Why Dynamic Global Privileges?

• How to add a new global privilege (the 5.7 version)
  – Add a column in mysql.user
  – Extend the parser
  – Amend ACL cache code: reading, caching, writing, upgrade, ...
  – Add checks for the new privilege

• Not possible from a plugin!

• Abuse of existing privileges (SUPER)!

• The SUPER-potent SUPER!
Dynamic Privileges at Work

• SUPER privilege split into a set of dynamic privileges, e.g.
  – SYSTEM_VARIABLES_ADMIN
  – ROLE_ADMIN
  – CONNECTION_ADMIN, etc.

• Each plugin can now register and use their own unique privileges

• All existing MySQL plugins currently using SUPER are updated to add specific privileges, e.g.
  – FIREWALL_ADMIN
  – AUDIT_ADMIN
  – VERSION_TOKEN_ADMIN

Feature Request from DBAs
Security Direction

Continuing to focus a great deal on security

New things are in the works

Especially in these areas

• TDE / Encryption
• Audit
• Firewall
• Authentication

Customer feedback and requirements drive our priorities

Tell us what you want, need, etc.

Tell us problem uses cases to solve
Enterprise Security Architecture

- **Enterprise Authentication**
  - SSO - LDAP, AD, PAM

- **Enterprise Monitor**
  - Identifies Vulnerabilities
  - Security hardening policies
  - Monitoring & Alerting
  - User Monitoring
  - Password Monitoring
  - Schema Change Monitoring
  - Backup Monitoring

- **Workbench**
  - Model
  - Data
  - Audit Data
  - User Management

- **Access Controls**

- **Firewall**
  - Thread Pool
  - Attack minimization

- **Enterprise Audit**
  - Powerful Rules Engine

- **Enterprise Backup**
  - Encrypted

- **Data Encryption**
  - TDE
  - Encryption
  - PKI

- **Key Vault**

- **Audit Vault**

- **Network Encryption**
- **Strong Authentication**

- **Firewall**

- **Enterprise Authentication**
- **Network Encryption**

- **Access Controls**

- **Enterprise Monitor**
- **Audit Vault**

- **Enterprise Audit**
  - Powerful Rules Engine

- **Enterprise Backup**
  - Encrypted

- **HA**
  - InnoDB Cluster

- **Assess**
- **Prevent**
- **Detect**
- **Recover**
Safe Harbor Statement

The preceding 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.