Hackers Move Away, We are Always Encrypted

Reinaldo, Kibel, Database Strategist, Dell Technologies
Moderated By: Anil Desai
Technical Assistance

If you require assistance during the session, type your inquiry into the question pane on the right side.

Maximize your screen with the zoom button on the top of the presentation window.

Please fill in the short evaluation following the session. It will appear in your web browser.
Empower users with new insights through familiar tools while balancing the need for IT to monitor and manage user created content. Deliver access to all data types across structured and unstructured sources.

Redgate Software makes ingeniously simple software used by 650,000 IT professionals who work with SQL Server, .NET, and Oracle. More than 100,000 companies use Redgate products, including 91% of the Fortune 100. Redgate’s philosophy is to design highly usable, reliable tools which elegantly solve the problems that developers and DBAs face every day.
Join PASS

PASS is a not-for-profit organization which offers year-round learning opportunities to data professionals.

MEMBERSHIP IS FREE, JOIN TODAY

www.pass.org
Reinaldo Kibel

BIOGRAPHY POINT ONE
Data Strategist at Dell Technologies
over 18 years of experience in Microsoft SQL Server technology

BIOGRAPHY POINT TWO
Work in one of the largest MS SQL installation in the world at Dell Technologies

BIOGRAPHY POINT THREE
Worked at Microsoft amongst other companies
Participate TAP for Office 2016, SharePoint 2016

url
@sqlmii
https://www.linkedin.com/in/reinaldo-kibel-59477a1/
Hackers Move Away, We are Always Encrypted

Reinaldo, Kibel, Database Strategist, Dell Technologies
Hackers move away, we are
Always Encrypted

Reinaldo Kibel, Database Strategist, Dell Technologies

Credits to:
Ruy Pimentel, Database Engineer, Dell Technologies
Jakub Szymaszek, Senior Program Manager SQL Server team
Reinaldo Kibel

BIOGRAPHY POINT ONE
Data Strategist at Dell Technologies
over 18 years of experience in Microsoft SQL Server technology

BIOGRAPHY POINT TWO
Work in one of the largest MS SQL installation in the world at Dell Technologies

BIOGRAPHY POINT THREE
Worked at Microsoft amongst other companies
Participate TAP for Office 2016, SharePoint 2016
Encryption and cyber security has a major stake in our companies

- Verizon is pushing for a $1 billion discount off its pending $4.8 billion agreement to buy Yahoo, several sources told The Post exclusively.
- The request comes on the heels of the web giant getting bludgeoned by bad news in the past few days.
- Yahoo revealed two weeks ago that it had been hacked in 2014 and that usernames and passwords for 500 million accounts were swiped.
- Then, earlier this week, it was learned that Yahoo had been ordered by a secret Foreign Intelligence Surveillance Court to scan emails for terrorist signatures
Gartner – key technologies

Key Technologies Will Deliver Change

Q. In your opinion, which three of these technologies have the most potential to change your organization over the next five years?

- **81%** Advanced Analytics
- **48%** Internet of Things
- **43%** Digital Security
- **40%** Business Algorithms

Machine Learning: 22%
Virtual Customer Assistants: 19%
Augmented Reality: 13%
Blockchain: 10%
Autonomous Vehicles: 7%
Smart Robots: 6%

Percentage of respondents to select each technology in top three
If you are thinking about a career change in 2016, then you might want to have a look at the burgeoning cybersecurity market which is expected to grow from $75 billion in 2015 to $170 billion by 2020

More than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past 5 years
SQL Server 2016: Everything built-in

Industry leader in Mission Critical OLTP
Most secure database
Highest performing data warehouse
End-to-end mobile BI on any device
In-database Advanced Analytics

In-memory across all workloads

Consistent experience from on-premises to cloud

The above graphics were published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Microsoft. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner’s research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

National Institute of Standards and Technology Comprehensive Vulnerability Database update 10/2015

TPC-H 10TB non-clustered results as of 04/06/15, 5/04/15, 4/15/14 and 11/25/13, respectively. http://www.tpc.org/tpch/results/tpch_perf_results.asp?resulttype=noncluster
Most secure database

Layers of protection

Monitor activity

- Advanced Threat Analytics
- SQL Server auditing

Control access

- Windows Authentication
- Row-level security
- Dynamic data masking

Protect data

- Always Encrypted
- Transparent data encryption

Least vulnerable 6 years in a row & most utilized

* National Institute of Standards and Technology Comprehensive Vulnerability Database update 10/2015
SQL Server 2016 – security enhancements

Transparent Data Encryption
TDE

Encrypt data files
Encrypting data at rest
Database encryption key (DEK), symmetric key secured using certificate stored in master database
or an asymmetric key protected by an EKM module
before they are written to disk and decrypted when read into memory

Easy-Medium to Implement

*Weak security

Dynamic Data Masking
DDM

anonymize sensitive data
real-time obfuscation of data to prevent unauthorized access
Controls how the data appears in the output of database queries
No changes to dB operations
No changes to application code

Easy to implement

*ok security

Always Encrypted

protect sensitive data
separation between those who own (and can view it) and those who manage the data
encryption transparent to applications
client application. The driver encrypts the data in sensitive columns before passing the data to the Database Engine

Complex to implement

*Best security
Challenge - Implementation of SA password rotation

Dell security auditors required that ‘sa’ account password be rotated as during installation of SQL Server, DBA knows the sa password. And ‘hackers to be’ can find that information on the installation files.

Automatic rotate the password
Password request to be logged
Always Encrypted
Always Encrypted

column master key (CMK) is a key encrypting key that is always in client’s control and is stored in an external key store, not on SQL Server

works by transparently encrypting the data in the application

ensures sensitive data is never seen in plaintext in a SQL Server instance

Always Encrypted uses the AEAD_AES_256_CBC_HMAC_SHA_256 algorithm to encrypt data in the database

SQL Server will only handle the encrypted data and not plaintext values

If SQL Server is compromised all an attacker can get is cyphertext of sensitive data
Protect your data at rest and in motion without impacting database performance

Always Encrypted

Apps

Trusted

SELECT Name FROM Swimmers WHERE SSN=@SSN

@SSN='753-92-9954'

Result Set

753-92-9954

Client side

Enhanced ADO.NET Library

SQL Server

SELECT Name FROM Swimmers WHERE SSN=@SSN

@SSN=0x7ff654ae6d

Result Set

<table>
<thead>
<tr>
<th>Name</th>
<th>SSN</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ryan Lochte</td>
<td>0x7ff654ae6d</td>
<td>USA</td>
</tr>
<tr>
<td>Michael Phelps</td>
<td>1x7fg655se2e</td>
<td>USA</td>
</tr>
<tr>
<td>Ryan Lochte</td>
<td>0x7ff654ae6d</td>
<td>USA</td>
</tr>
<tr>
<td>Chad Le Clos</td>
<td>0y8fj754ea2c</td>
<td>RSA</td>
</tr>
</tbody>
</table>

NEW*
Definitions - Keys

Column Master Key - CMK

Encrypts and protect a CEK
key-protecting key that encrypts one or more column encryption keys
stored in a key store that is external the database and is accessible to a client application
must be deployed on each client machine that needs access to the unencrypted data
Not stored in the DB

Column Encryption Key - CEK

protect data on a column by encrypting the column
Encrypted values of column encryption keys are stored in the database in system catalog views
Not Stored in the DB
Column Master Key storage

Windows Certificate Store

Azure Key Vault

Hardware Security Module
**SSMS - CREATE COLUMN MASTER KEY**

- USE [24HOP_Security]
- CREATE COLUMN MASTER KEY [24HOP_MasterKey]
  - WITH
    - KEY_STORE_PROVIDER_NAME = N'MSSQL_CERTIFICATE_STORE',
    - KEY_PATH = N'LocalMachine/My/2F7BD30F157AC7F6B004A968AE31CE748C73793A'
  - GO
### Column Encryption Types

**Deterministic**

Encryption uses a method which always generates the same encrypted value for any given plain text value. Using deterministic encryption allows grouping, filtering by equality, and joining tables based on encrypted values, but can also allow unauthorized users to guess information about encrypted values by examining patterns in the encrypted column. This weakness is increased when there is a small set of possible encrypted values, such as True/False. Deterministic encryption must use a column collation with a binary2 sort order for character columns.

**Randomized**

Uses a method that encrypts data in a less predictable manner. Randomized encryption is more secure, but prevents equality searches, grouping, indexing, and joining on encrypted columns.

Choose randomized for data that will just be returned, and deterministic for data that will be searched.
Tools for Managing Always Encrypted Keys

**SQL Server Management Studio (SSMS)**

provides dialogs and wizards that combine tasks involving key store access and database access, so SSMS does not support role separation, but it makes configuring your keys easy. For more information about managing keys using SSMS, see:

- Provisioning Column Master Keys
- Provisioning Column Encryption Keys
- Rotating Column Master Keys
- Rotating Column Encryption Keys

**SQL Server PowerShell**

includes cmdlets for managing Always Encrypted keys with and without role separation. For more information, see:

- Configure Always Encrypted Keys using PowerShell
- Rotate Always Encrypted Keys using PowerShell
Certificates – CMK – Local Computer
Certificate - Thumbprint

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>Always Encrypted Certificate</td>
</tr>
<tr>
<td>Public key</td>
<td>RSA (2048 Bits)</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>RSA (2048 Bits)</td>
</tr>
<tr>
<td>Subject Key Identifier</td>
<td>99 25 38 d7 35 8e 1c 86 65 77 3a</td>
</tr>
<tr>
<td>Key Usage</td>
<td>Key Exportment (20)</td>
</tr>
<tr>
<td>Thumbprint algorithm</td>
<td>sha1</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>2f 7b d3 0f 15 7a c7 f6 b0 04 a9 68 ae 31 ce 74 8c 73 79 3a</td>
</tr>
<tr>
<td>Friendly name</td>
<td>249op_pass</td>
</tr>
</tbody>
</table>

- 2f 7b d3 0f 15 7a c7 f6 b0 04 a9 68 ae 31 ce 74 8c 73 79 3a
Error when trying to access table without CEK
## RDBMS Security Features by Edition

<table>
<thead>
<tr>
<th>Feature</th>
<th>Enterprise</th>
<th>Standard</th>
<th>Web</th>
<th>Express</th>
<th>Express with Advanced Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Row-level security (RLS)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes 1</td>
<td>Yes 1</td>
<td>Yes 1</td>
</tr>
<tr>
<td>Always Encrypted</td>
<td>Yes</td>
<td>Yes 1</td>
<td>Yes 1</td>
<td>Yes 1</td>
<td>Yes 1</td>
</tr>
<tr>
<td>Dynamic data masking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes 1</td>
<td>Yes 1</td>
<td>Yes 1</td>
</tr>
<tr>
<td>Basic auditing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Fine grained auditing</td>
<td>Yes</td>
<td>Yes 1</td>
<td>Yes 1</td>
<td>Yes 1</td>
<td>Yes 1</td>
</tr>
<tr>
<td>Transparent database encryption (TDE)</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Extensible key management</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>User-defined roles</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Contained databases</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption for backups</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

1 NEW to SQL Server 2016 SP1
SSMS 17 new features

INSERTs against encrypted columns with Parameterization in SSMS 17 succeeds

“Hot out of the press”- Updates on Always Encrypted

• There are three updates (all in tooling):
  1) Parameterization for Always Encrypted in SSMS:
  2) Online encryption in PowerShell:
     Search for “online approach” in https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/configure-column-encryption-using-powershell or run get-help Set-SqlColumnEncryption -full. Please, see the download instructions for info on how to install SqlServer PowerShell module (it has been removed from the SSMS installation in SSMS 17).
Take aways:
Overview of Key Management for Always Encrypted
Coming up next!

Passive Security for Hostile Environments

Bob Pusateri
THANK YOU FOR ATTENDING