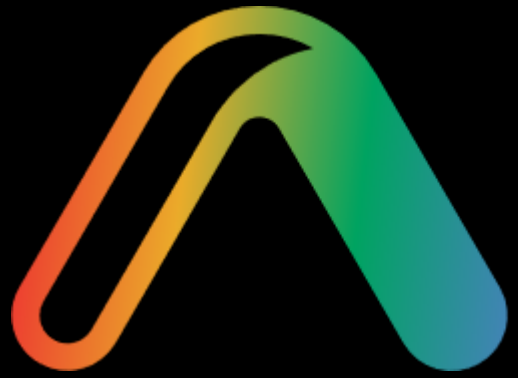


PASS
Data Community
SUMMIT 2021

Presents…

# A Lunar Cat production...

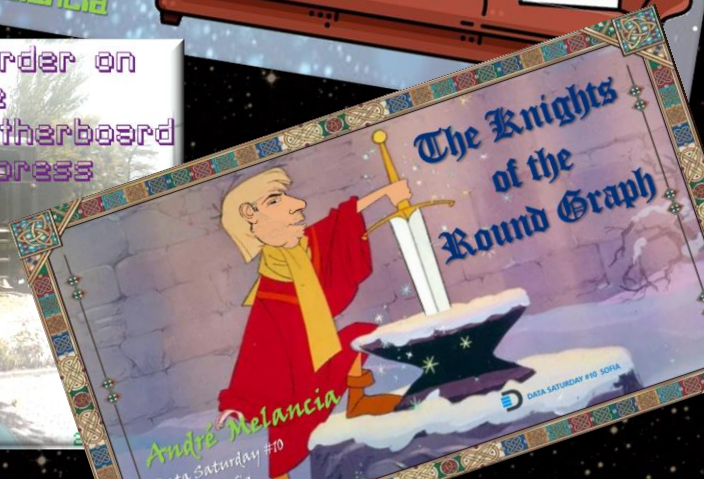
# From the producer of...

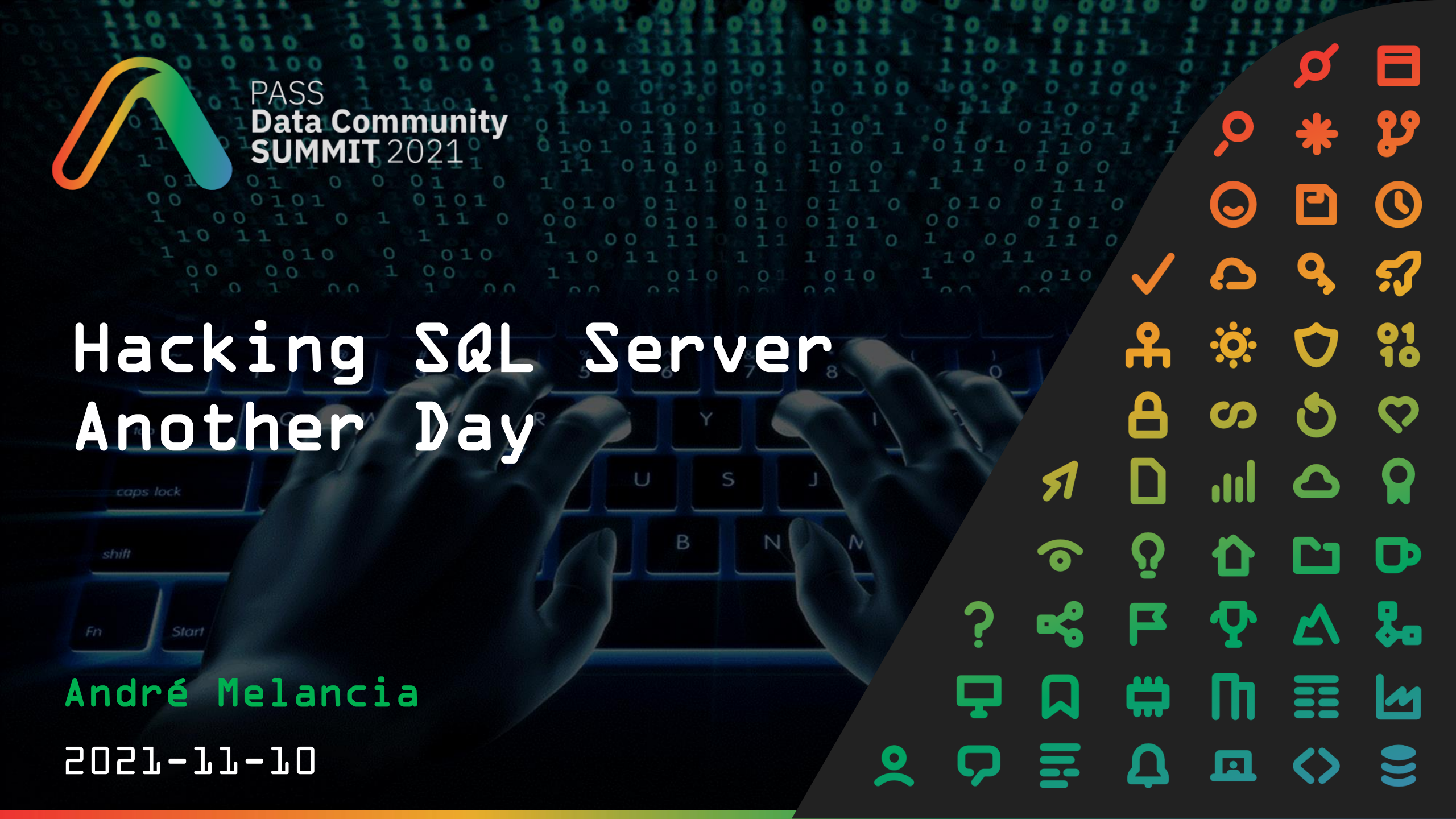








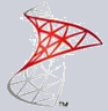






# Hacking SQL Server Another Day

André Melancia

2021-11-10

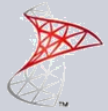


# Disclaimer

This is a SECURITY session!

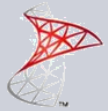
All Microsoft software is perfect (huh…), but…

… configuration is done by humans



# Welcome to the SQL world

- SQL Server
  - Up to 2014, and then 2016/2017/2019/2022
  - A lot of editions!
- Azure
  - VM with SQL Server
  - SQL Managed Instance
  - SQL Database
  - Synapse SQL Dedicated (formerly SQL DW) / Serverless
- Non-Microsoft databases
- Code stuff

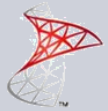


# SQL Server 2016 SP1 licence to use

| Feature | RTM | | | | SP1 | | | |
|---|---|---|---|---|---|---|---|---|
| | Standard | Web | Express | Local DB | Standard | Web | Express | Local DB |
| Row-level security | Yes | No | No | No | Yes | Yes | Yes | Yes |
| Dynamic Data Masking | Yes | No | No | No | Yes | Yes | Yes | Yes |
| Change data capture* | No | No | No | No | Yes | Yes | No* | No* |
| Database snapshot | No | No | No | No | Yes | Yes | Yes | Yes |
| Columnstore | No | No | No | No | Yes | Yes | Yes | Yes |
| Partitioning | No | No | No | No | Yes | Yes | Yes | Yes |
| Compression | No | No | No | No | Yes | Yes | Yes | Yes |
| In Memory OLTP | No | No | No | No | Yes | Yes | Yes | No** |
| Always Encrypted | No | No | No | No | Yes | Yes | Yes | Yes |
| PolyBase | No | No | No | No | Yes | Yes | Yes | No |
| Fine grained auditing | No | No | No | No | Yes | Yes | Yes | Yes |
| Multiple filestream containers | No | No | No | No | Yes | Yes | Yes | No** |

* Requires SQL Server agent which is not part of SQL Server Express Editions

** Requires creating filestream file groups which is not possible in Local DB due to insufficient permissions.

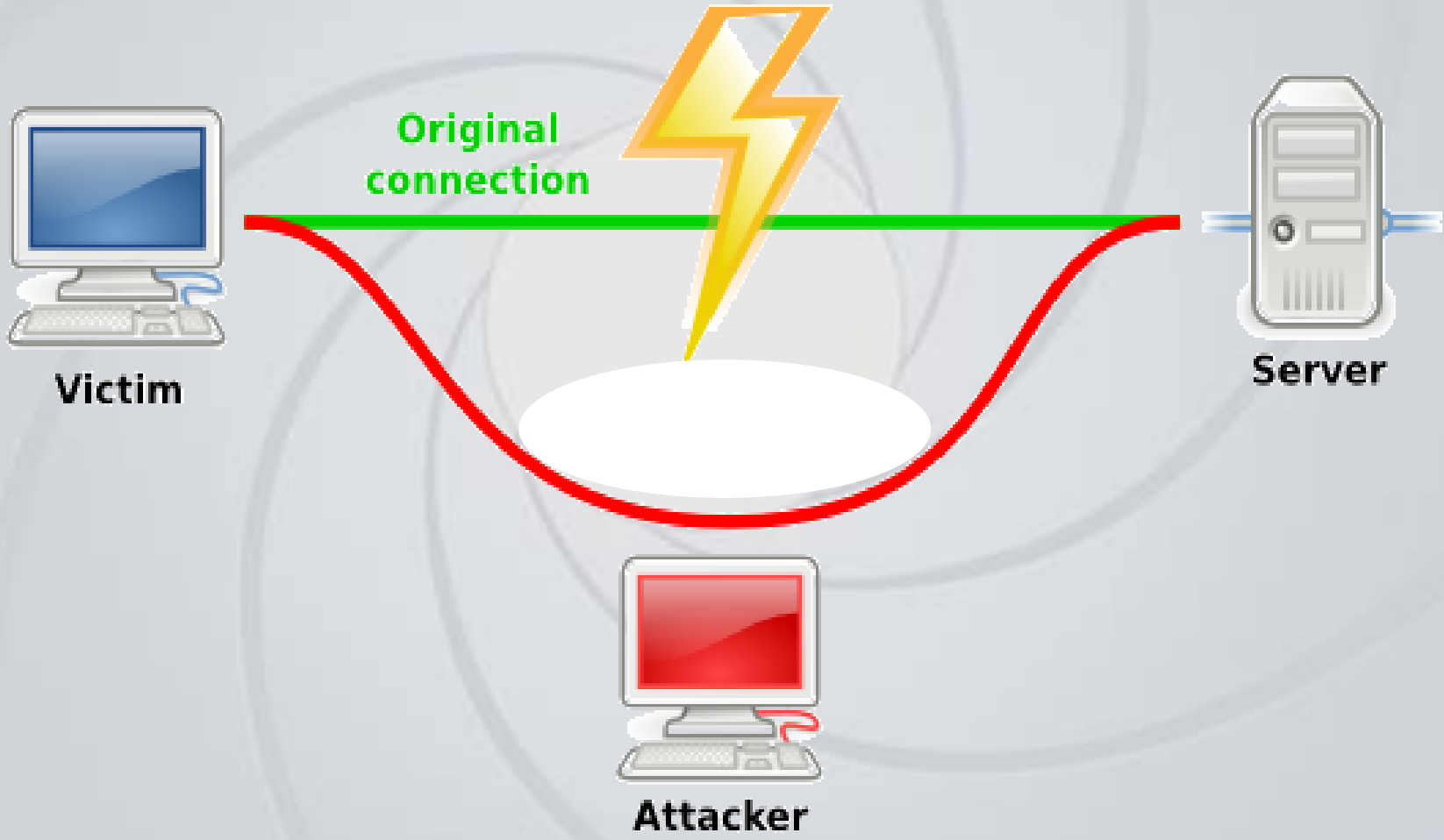


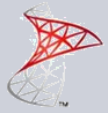
# Requirements for demos

- To run the demos in this session you'll need:
  - SQL Server 2016/2017/2019 (for RLS and OOM)
  - SQL Server 2012+ (for the rest)
  - Visual Studio 2015/2017/2019/2022 (for some demos)
  - Azure Subscription (for some stuff)
    - Try Azure.COM/FREE...


Your next mission, 00-NULL, is to...

# ~~Man-In-The-Middle~~ Person-In-The-Middle



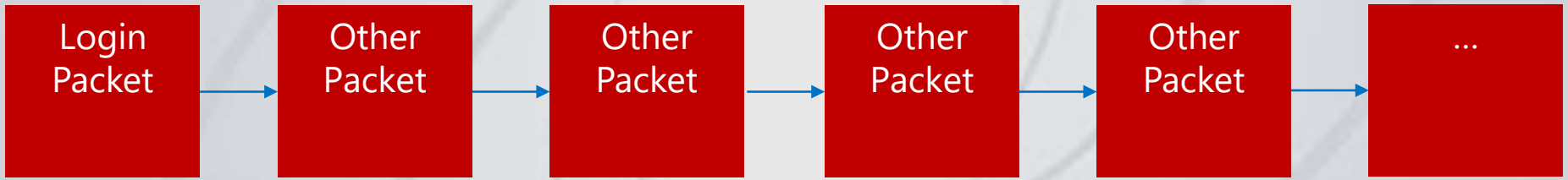


# Man-In-The-Middle

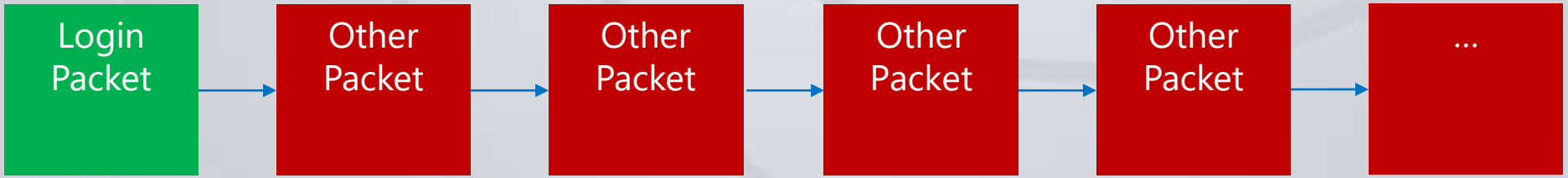
- SQL Server uses TDS (Tabular Data Stream)
  - https://en.wikipedia.org/wiki/Tabular_Data_Stream
  - https://msdn.microsoft.com/en-us/library/dd304523.aspx
- TDS was originally created by Sybase in the 1980s
- Default port: TCP 1433 (default instance)
  - Is it a good idea to change it?
  - Changing to a higher value protects from port scan attacks?
  - Is this a problem in Azure?
  - NO!

# Man-In-The-Middle

- Up to SQL Server 2000, the login/password packet was NOT encrypted.
- Plain text login, weak hash password



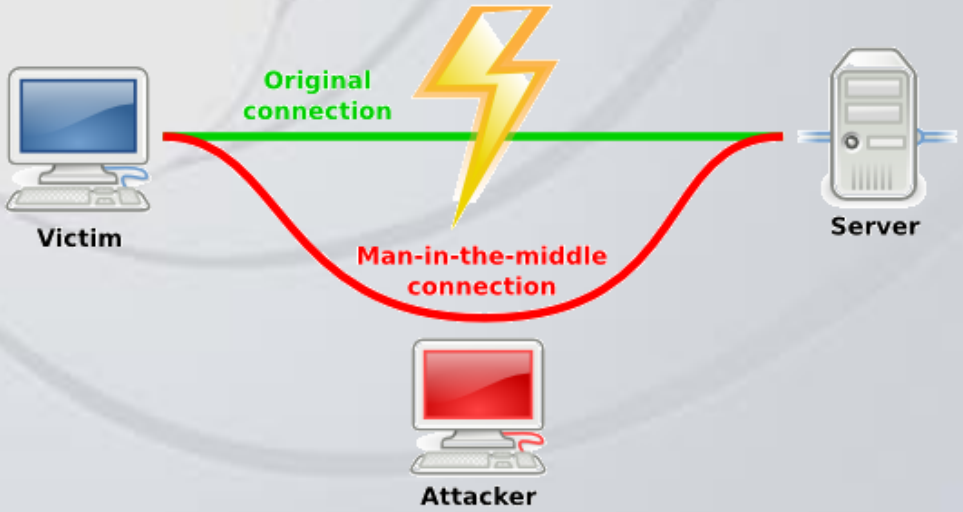

- SQL Server 2005 solves this, but the other packets are unencrypted by default!



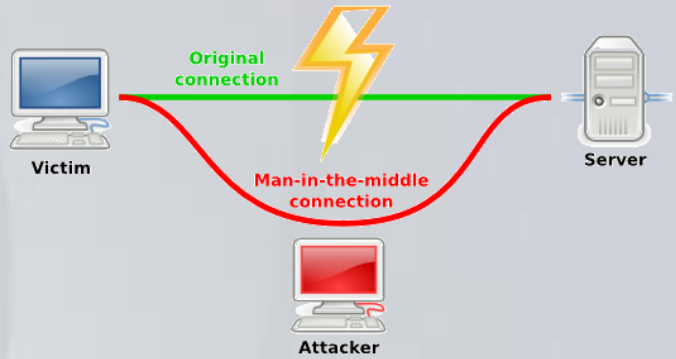
# Man-In-The-Middle

MITM, the hard way:

- Physical network tampering
- Configure/crack the router/switch
- ARP Spoofing
- DNS Poisoning
- Etc.



# Man-In-The-Middle




MITM, the easy way:

- Change the "hosts" file
  - %windir%\System32\Drivers\Etc\Hosts
- Change SQL Server "alias"
  - SQL Server Configuration Manager
  - %windir%\System32\CliConfg.EXE
  - Registry:
    - HKLM\Software\Microsoft\MSSQLServer\Client\ConnectTo (32bit)
    - HKLM\Software\WOW6432Node\Microsoft\MSSQLServer\Client\ConnectTo (64bit)

# Man-In-The-Middle

## ONLY TRY THIS AT HOME!

# Bits in the middle

*WirelessNet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Start Stop Restart Options Open Save Close Reload Find Packet... Previous Packet Next Packet Go to Packet... First Packet Last Packet Auto Scroll in Live Capture

1433 || tcp.port==1434 || tcp.srcport==1434 || tcp.port==1433 || tcp.srcport==1433 || tds || tcp.port==63341 || tcp.srcport==63341 Expression... + MSSQL MSSQL+

| No. | Time | Source | DestPort | Destination | SourcePort | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|
| 11 | 2.… | 192.168.52.74 | 63341 | 52.178.162.183 | 27559 | TCP | 1384 | [TCP segment of a reassembled PDU] |
| 12 | 2.… | 192.168.52.74 | 63341 | 52.178.162.183 | 27559 | TDS | 214 | SQL batch |
| 13 | 2.… | 52.178.162.183 | 27559 | 192.168.52.74 | 63341 | TCP | 56 | 63341 → 27559 [ACK] Seq=89 Ack=1857 Win=514 Len=0 |
| 14 | 2.… | 52.178.162.183 | 27559 | 192.168.52.74 | 63341 | TCP | 1384 | [TCP segment of a reassembled PDU] |
| 15 | 2.… | 52.178.162.183 | 27559 | 192.168.52.74 | 63341 | TCP | 1384 | [TCP segment of a reassembled PDU] |
| 16 | 2.… | 192.168.52.74 | 63341 | 52.178.162.183 | 27559 | TCP | 54 | 27559 → 63341 [ACK] Seq=1857 Ack=2749 Win=259 Len=0 |
| 17 | 2.… | 52.178.162.183 | 27559 | 192.168.52.74 | 63341 | TDS | 298 | Response |
| 18 | 2.… | 192.168.52.74 | 63341 | 52.178.162.183 | 27559 | TCP | 54 | 27559 → 63341 [ACK] Seq=1857 Ack=2993 Win=258 Len=0 |
| 19 | 2.… | 192.168.52.74 | 63341 | 52.178.162.183 | 27559 | TDS | 420 | SQL batch |

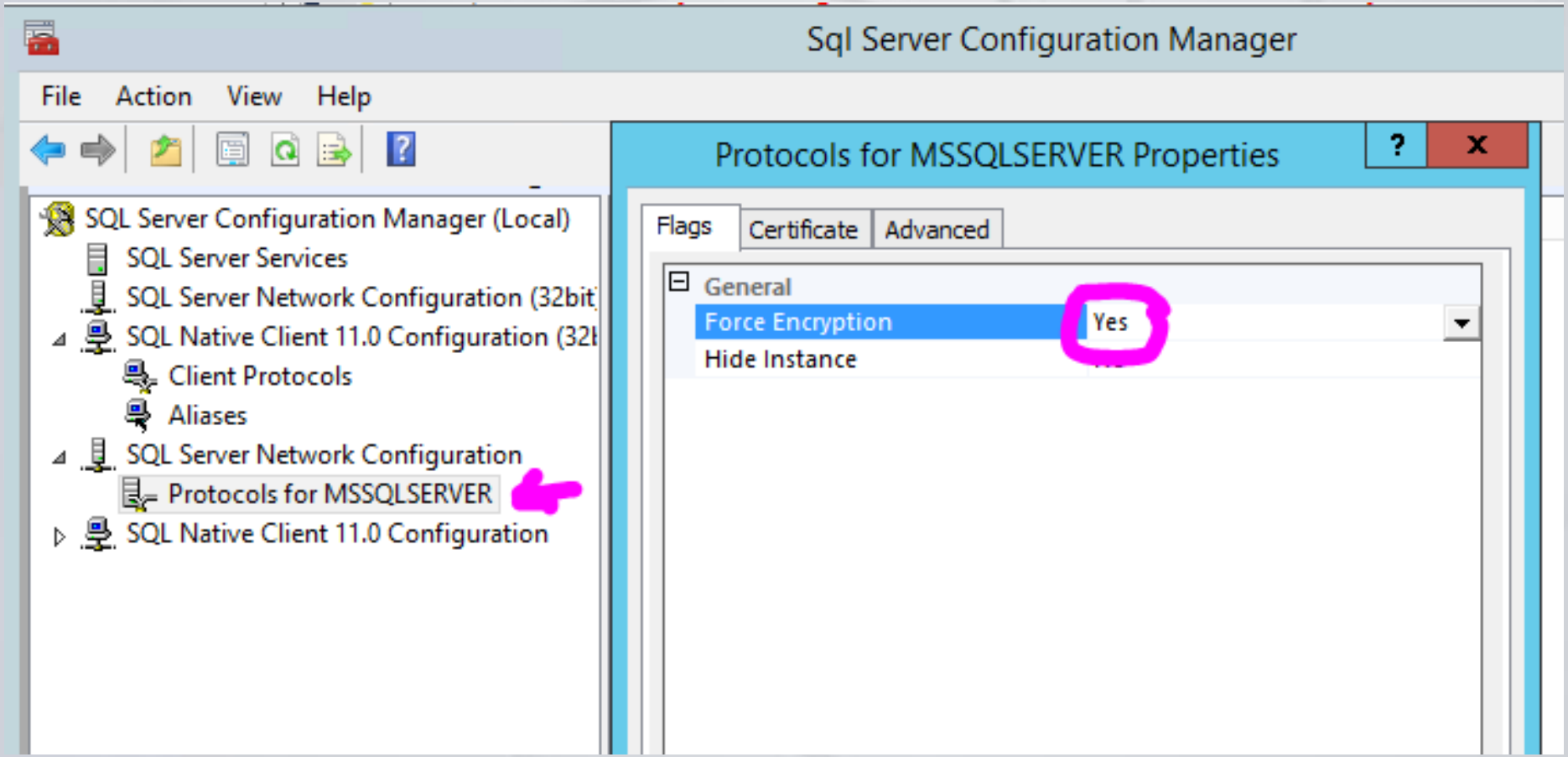
```
> Frame 14: 1384 bytes on wire (11072 bits…
> Ethernet II, Src: IntelCor_21:1f:29 (90:…
> Internet Protocol Version 4, Src: 52.178…
> Transmission Control Protocol, Src Port:…
```

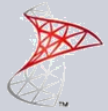
```
0000  1c 65 9d 73 38 07 90 e2  ba 21 1f 29 08 00 45 00   .e.s8... .!.)..E.
0010  05 5a 54 90 40 00 72 06  e2 b1 34 b2 a2 b7 c0 a8   .ZT.@.r. ..4.....
0020  34 4a f7 6d 6b a7 0f 5c  2a ec 43 6f 9c 9f 50 10   4J.mk..\ *.Co..P.
0030  02 02 2d 08 00 00 04 01  0b 58 00 39 01 00 81 07   ..-..... .X.9....
0040  00 00 00 00 00 00 00 08  00 38 06 46 00 69 00 6c   ........ .8.F.i.l
0050  00 6d 00 49 00 44 00 00  00 00 00 08 00 e7 80 00   .m.I.D.. ........
0060  09 04 d0 00 34 09 46 00  69 00 6c 00 6d 00 54 00   ....4.F. i.l.m.T.
0070  69 00 74 00 6c 00 65 00  00 00 00 00 08 00 38 08   i.t.l.e. ......8.
0080  46 00 69 00 6c 00 6d 00  59 00 65 00 61 00 72 00   F.i.l.m. Y.e.a.r.
0090  00 00 00 00 08 00 e7 80  00 09 04 d0 00 34 09 42   ........ .....4.B
00a0  00 6f 00 6e 00 64 00 41  00 63 00 74 00 6f 00 72   .o.n.d.A .c.t.o.r
00b0  00 00 01 00 00 08 00 e7  00 01 09 04 d0 00 34 05   ........ ......4.
00c0  41 00 67 00 65 00 6e 00  74 00 00 00 00 00 20 00   A.g.e.n. t..... .
00d0  a7 0d 00 09 04 d0 00 34  00 00 00 00 00 20 00 3d   .......4 ..... .=
00e0  00 d1 01 00 00 00 0c 00  44 00 72 00 2e 00 20 00   ........ D.r... .
00f0  4e 00 6f 00 aa 07 00 00  18 00 53 00 65 00 61 00   N.o..... ..S.e.a.
0100  6e 00 20 00 43 00 6f 00  6e 00 6e 00 65 00 72 00   n. .C.o. n.n.e.r.
0110  79 00 08 00 53 00 65 00  61 00 6e 00 0d 00 53 6e   y...S.e. a.n...Sn
0120  69 66 66 69 6e 67 20 44  65 6d 6f 4c a6 00 00 eb   iffing D emoL....
0130  7e b9 00 d1 02 00 00 00  2a 00 46 00 72 00 6f 00   ~....... *.F.r.o.
0140  6d 00 20 00 52 00 75 00  73 00 73 00 69 00 61 00   m. .R.u. s.s.i.a.
0150  20 00 77 00 69 00 74 00  68 00 20 00 4c 00 6f 00    .w.i.t. h. .L.o.
0160  76 00 65 00 ab 07 00 00  18 00 53 00 65 00 61 00   v.e..... ..S.e.a.
0170  6e 00 20 00 43 00 6f 00  6e 00 6e 00 65 00 72 00   n. .C.o. n.n.e.r.
0180  79 00 08 00 53 00 65 00  61 00 6e 00 0d 00 53 6e   y...S.e. a.n...Sn
0190  69 66 66 69 6e 67 20 44  65 6d 6f 4c a6 00 00 eb   iffing D emoL....
01a0  7e b9 00 d1 03 00 00 00  14 00 47 00 6f 00 6c 00   ~....... ..G.o.l.
```

Packets: 58 · Displayed: 42 (72.4%) Profile: Default

# Man-In-The-Middle

## Always enable encryption on the SERVER.





# Man-In-The-Middle

## Always enable encryption on the SERVER:

- https://docs.microsoft.com/sql/database-engine/configure-windows/enable-encrypted-connections-to-the-database-engine
  - Enable Encrypted Connections to the Database Engine
- https://docs.microsoft.com/sql/relational-databases/native-client/features/using-encryption-without-validation
  - Using Encryption Without Validation ⚠
- https://docs.microsoft.com/sql/relational-databases/native-client/applications/using-connection-string-keywords-with-sql-server-native-client
  - Using Connection String Keywords with SQL Server Native Client
    - `Encrypt=True`
    - `TrustServerCertificate=False`

# Hacking British plug sockets

# Hacking Indian plug sockets

# Plug sockets happiness level

USA

Denmark


Dude with the unmasking fun...

# Dynamic Data Masking

```
CREATE TABLE Membership
(
  MemberID  int          IDENTITY PRIMARY KEY,
  FirstName varchar(66) MASKED WITH (FUNCTION = 'partial(1,"XXXXXXX",0)')     NULL,
  LastName  varchar(66)                                                   NOT NULL,
  Phone     varchar(66) MASKED WITH (FUNCTION = 'default()')                  NULL,
  Email     varchar(66) MASKED WITH (FUNCTION = 'email()'  )                  NULL
);


Original:
1    Roberto     Tamburello    555.123.4567    RTamburello@contoso.com

Masked:
1    RXXXXXXX    Tamburello    xxxx            RXXX@XXXX.com
```

More info: https://docs.microsoft.com/sql/relational-databases/security/dynamic-data-masking

# Dynamic Data Masking

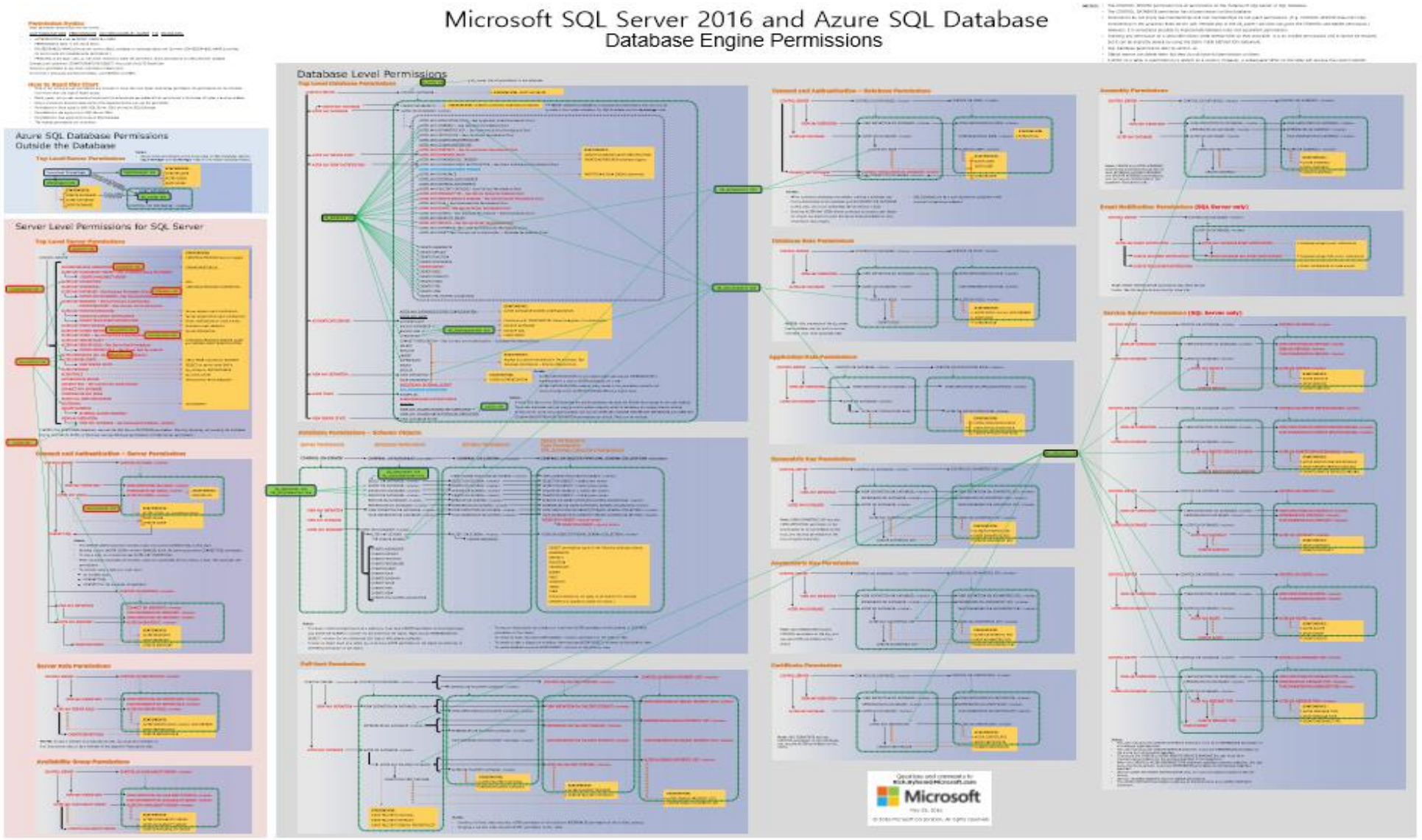
- By Column
- SELECT permission shows masked data
  - To see the data you need UNMASK permission
  - UNMASK used to be DATABASE scope only, now TABLE and COLUMN scope
- Does not prevent UPDATEs to masked columns
- Using SELECT INTO or INSERT INTO doesn't work
  - Output is masked text (trash)
- Hacks?

# Dynamic Data (UN)Masking

ONLY TRY
THIS AT HOME!


007
FACEBOOK.COM/GREGKMK
GREGKMK.DEVIANTART.COM
JB007
Secret agent, secret permissions...

# Permissions poster by Rick Byham

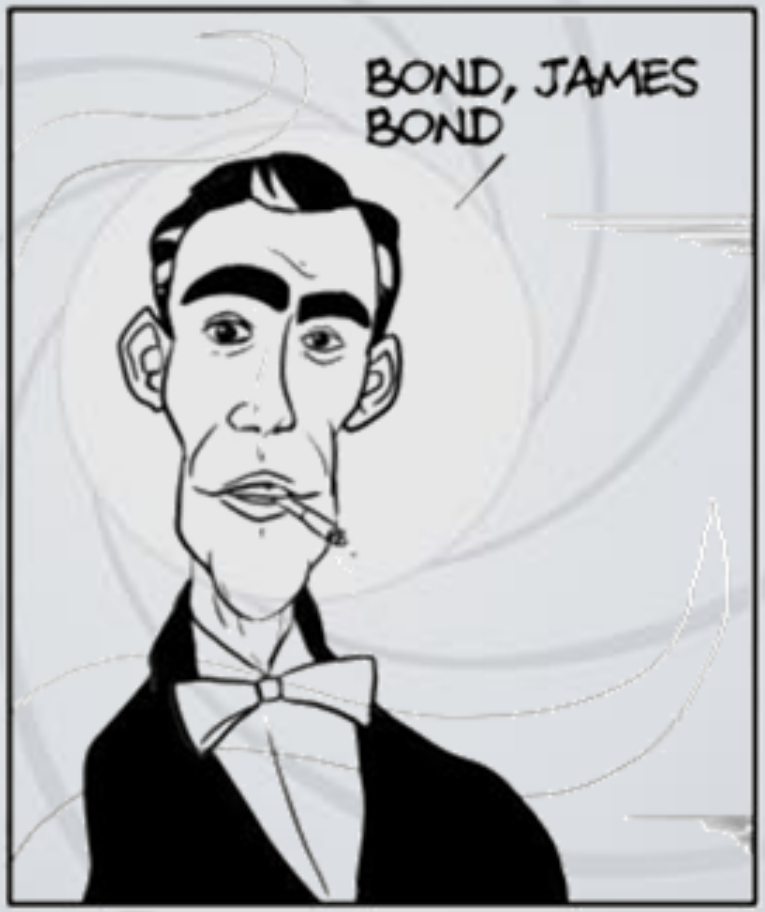


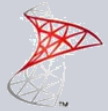

https://github.com/Microsoft/sql-server-samples/tree/master/samples/features/security/permissions-posters


Hotel007
203

# Row Level (In)Security – Demo!

ONLY TRY THIS AT HOME!



# Row Level Security (RLS)

- Function Predicate
  - Defines Business logic/rules/access
  - User defined inline table valued-function (reusable)
- Security Policy
  - Collection of Predicates
  - Predicates added as FILTER or BLOCK

More info: https://docs.microsoft.com/sql/relational-databases/security/row-level-security

# Row Level Security (RLS)

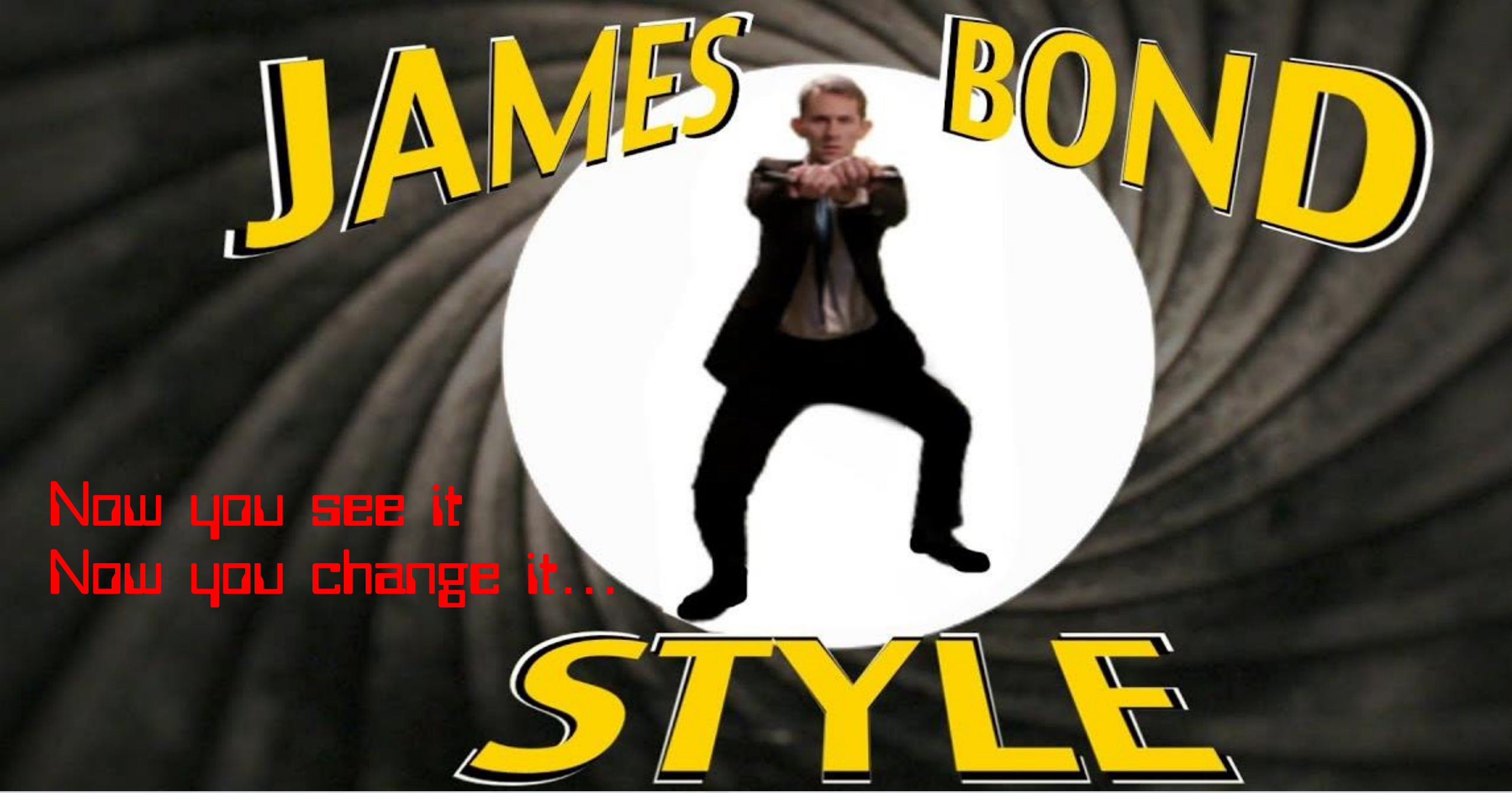
## Other technologies that use RLS

- Power BI
- SQL Server Analysis Services
- Azure Analysis Services
- Non-Microsoft stuff
  - Oracle
  - IBM DB2
  - PostgreSQL
  - MariaDB (but not MySQL)

# Being professional...

Hacking Encrypted
Views and SPs

ONLY TRY
THIS AT HOME!


JAMES BOND
Now you see it
Now you change it...
STYLE

# Transparent Data Encryption (TDE)

- Encrypts the whole Database
- Data is stored encrypted in the storage disks
  - Page level encryption
- Decrypted in RAM on the server (on demand)
  - **Server has the keys!!!**
- Recommended: store the keys and the data in separate storage disks or use a TPM / HSM hardware module
- Transparent to the Apps
  - **Data is decrypted before leaving the server**
- If you have TDE, TEMPDB also gets encrypted!

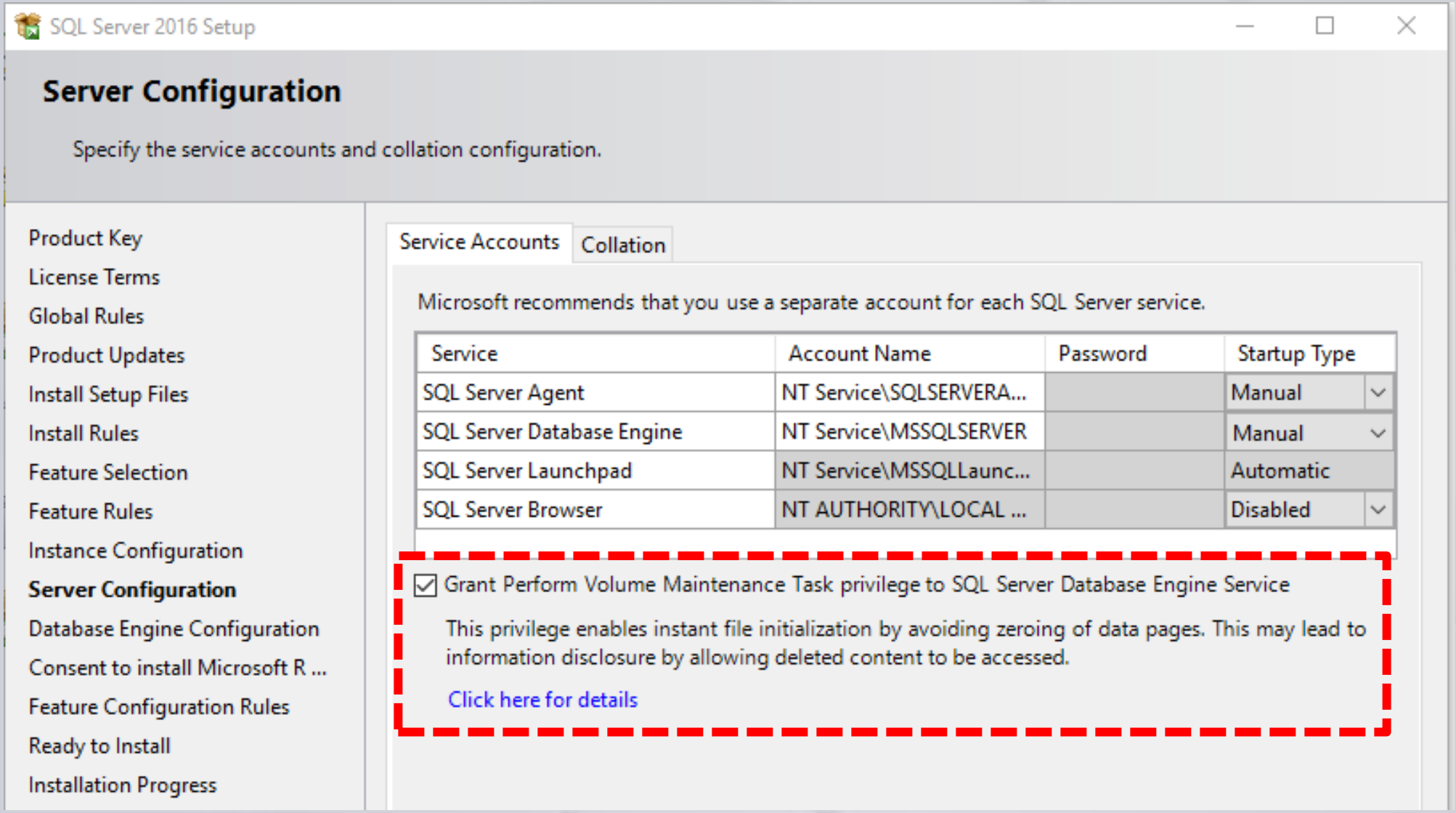
More info: https://docs.microsoft.com/sql/relational-databases/security/encryption/transparent-data-encryption

# Transparent Data Encryption (TDE)

## Hack it?

- Remember… "Server has the keys!!!"
- So… Get the keys from someone's backup…
- Also… Backups and network communication are not encrypted by TDE

# Instant File Initialisation

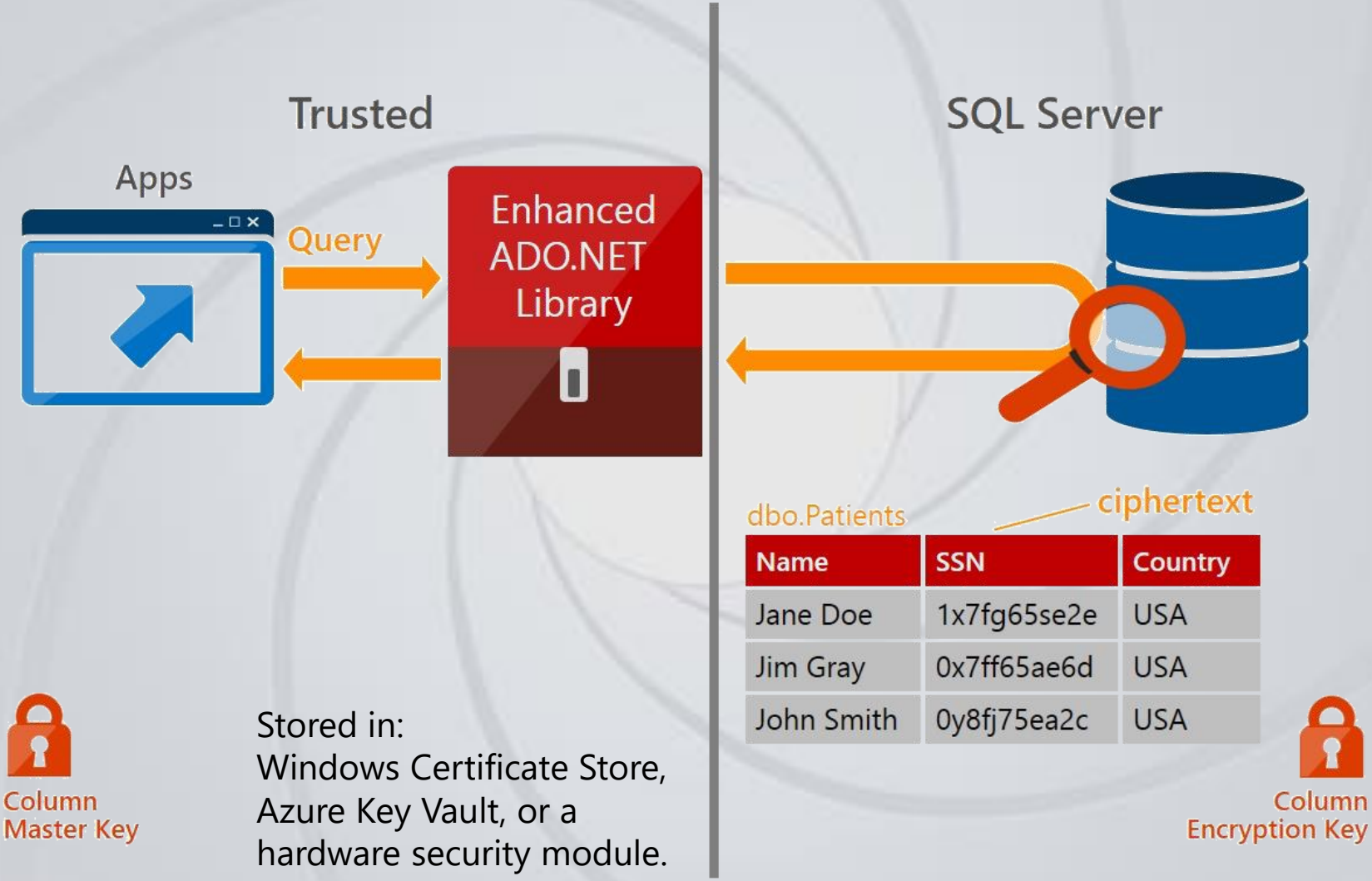


# Instant File Initialisation

## Hack it?

- Just copy the MDF/NDF files you created with IFI...
- ... and all the previous information from the disk is there...

# Always Encrypted




Stored in:
Windows Certificate Store, Azure Key Vault, or a hardware security module.

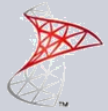
# Always Encrypted

- Everything over the wire is encrypted
- Data is stored encrypted in the database files
- Only the App (client) side has the decryption key
- Encryption is by Column, not Table
- Options:
  - Deterministic (allows equality lookups)
  - Random
- Drivers already available for Linux clients

More info:

http://sqlespresso.com/2017/11/29/how-to-get-started-with-always-encrypted-for-beginners-part-1

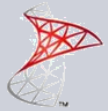
https://docs.microsoft.com/en-gb/archive/blogs/sqlsecurity/getting-started-with-always-encrypted



# Always Encrypted

## Hack it?

| ID | Name | Country | Country [AE-Deterministic] | Country [AE-Random] |
|---|---|---|---|---|
| 1 | Client 1 | PT | 0x28DA20... | 0x334523... |
| 2 | Client 2 | PT | 0x28DA20... | 0x4d3133... |
| 3 | Client 3 | PT | 0x28DA20... | 0x42D320... |
| 4 | Client 4 | PT | 0x28DA20... | 0x24ABD0... |
| 5 | Client 5 | UK | 0x9723AC... | 0xCD3289... |
| 6 | Client 6 | UK | 0x9723AC... | 0x9CD293... |
| 7 | Client 7 | UA | 0x127A2A... | 0xA4387A... |
| 8 | Client 8 | UA | 0x127A2A... | 0x1999BA... |
| 9 | Client 9 | UA | 0x127A2A... | 0x729F2A... |
| 10 | Client 10 | UA | 0x127A2A... | 0x89478A... |
| 11 | Client 11 | RU | 0xF0122E... | 0xFE349A... |
| 12 | Client 12 | PL | 0xEAB53E... | 0xFA100E... |
| 13 | Client 13 | DE | 0x00A3D1... | 0x11AFB1... |



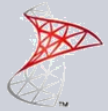
# SQL Injection

- We get the Category parameter in a web page...

```
http://Example.COM/?Cat= FOOD
```

```
SQL = " SELECT *              "
    + " FROM   TableX         "
    + " WHERE  FieldZ = '" + Category + "'; ";
```

- Executing this is NOT SAFE!



# SQL Injection

## Prepared Statement example:

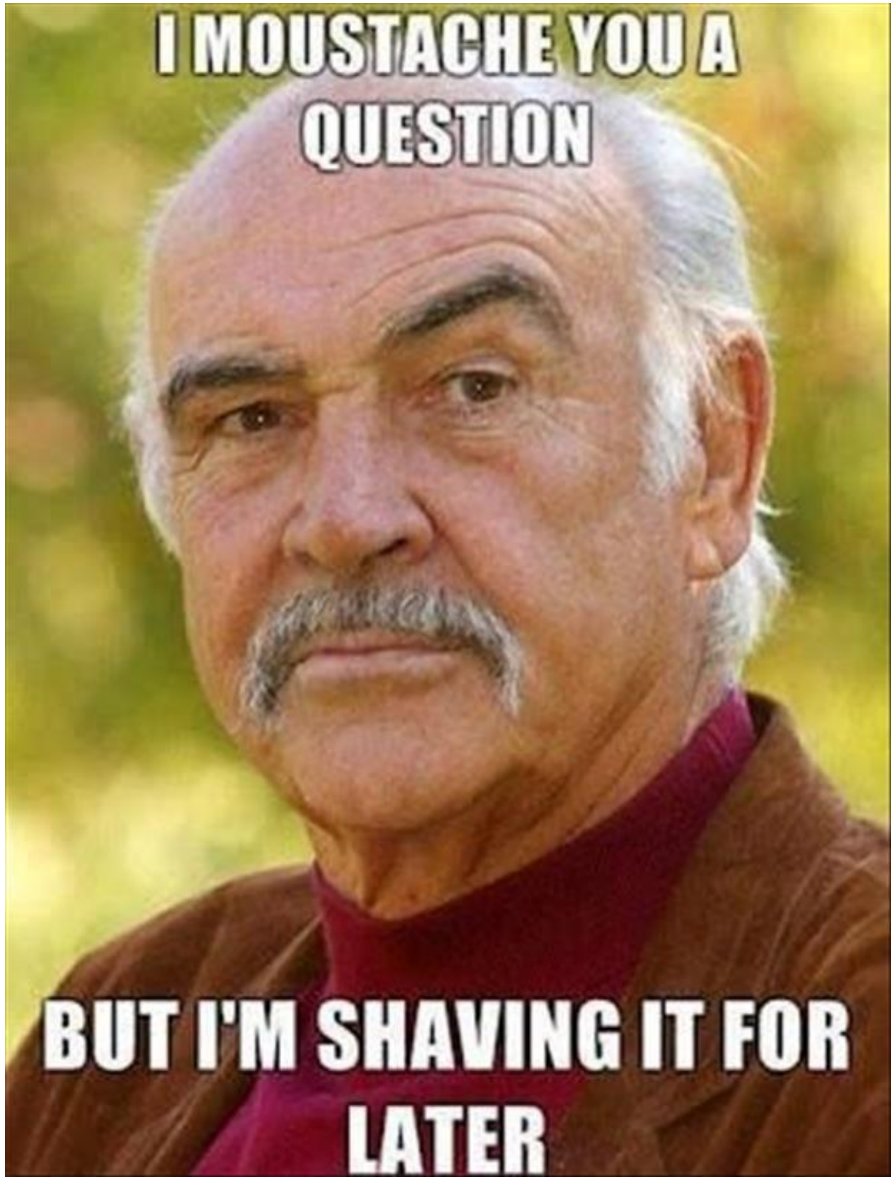
```
SqlConnection connection = new
                           sqlConnection(connectionString))

SqlCommand cmd           = new SqlCommand();
cmd.Connection           = SomeConnection;
cmd.CommandText          = "SP_SalesByCategory";
cmd.CommandType          = CommandType.StoredProcedure;

SqlParameter parameter   = new SqlParameter();
parameter.ParameterName  = "@CategoryName";
parameter.SqlDbType      = SqlDbType.NVarChar;
parameter.Direction      = ParameterDirection.Input;
parameter.Value          = ThatFunnyParameter;
cmd.Parameters.Add (parameter);
```

More info: https://docs.microsoft.com/dotnet/framework/data/adonet/configuring-parameters-and-parameter-data-types

# Even if you can't get the Bond Girl, remember...

- SQL Server 2016, 2017, 2019 and 2022 have a lot of new features...
  - But they're not perfect!
- ALWAYS,
- ALWAYS,
- ALWAYS,
- Install the latest Service Packs, CUs and patches!

# Receive-Questions –Input "Chat"




Sean Connery

1930-2020

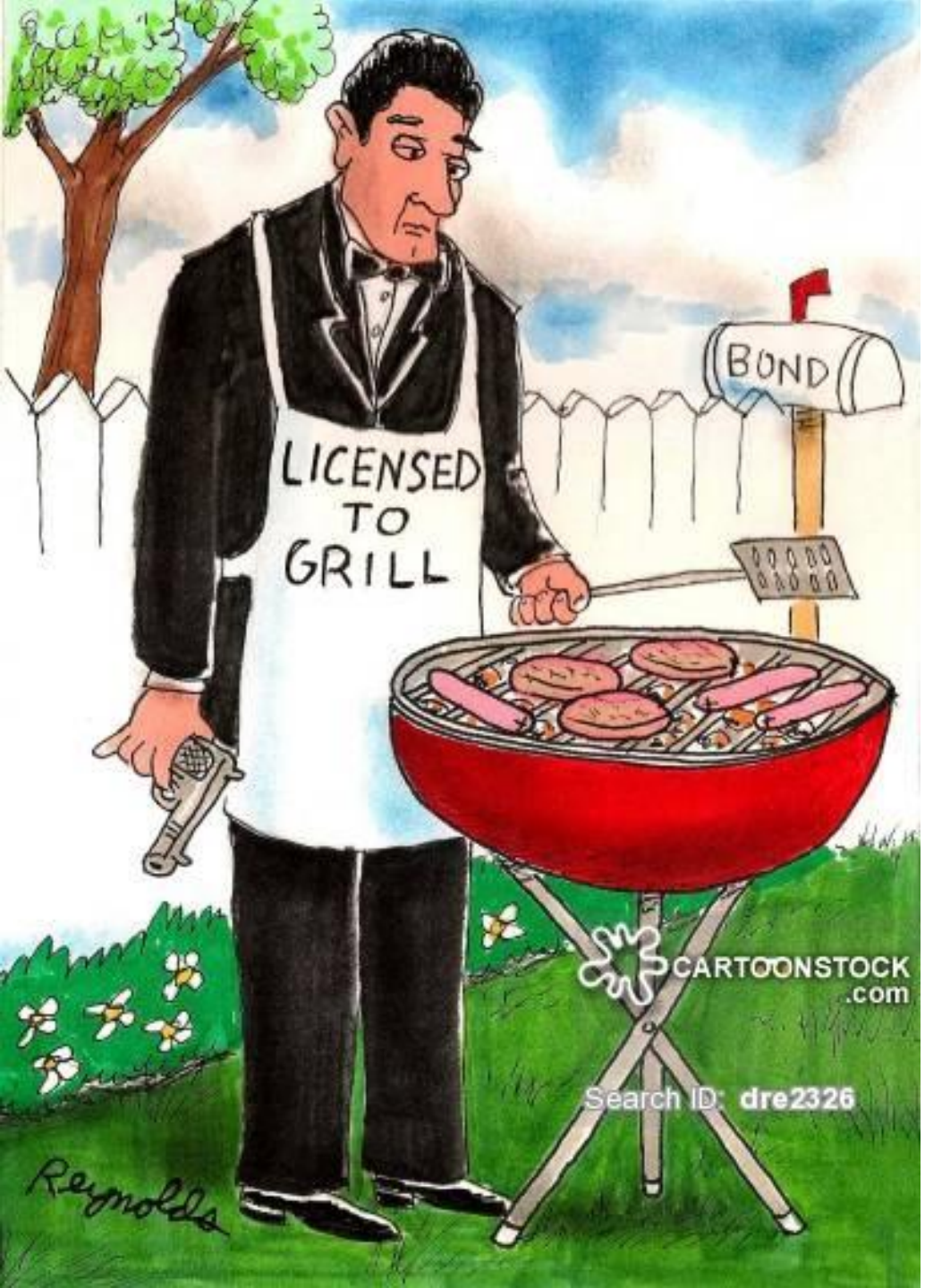
# Session evaluation

Your feedback is important to us

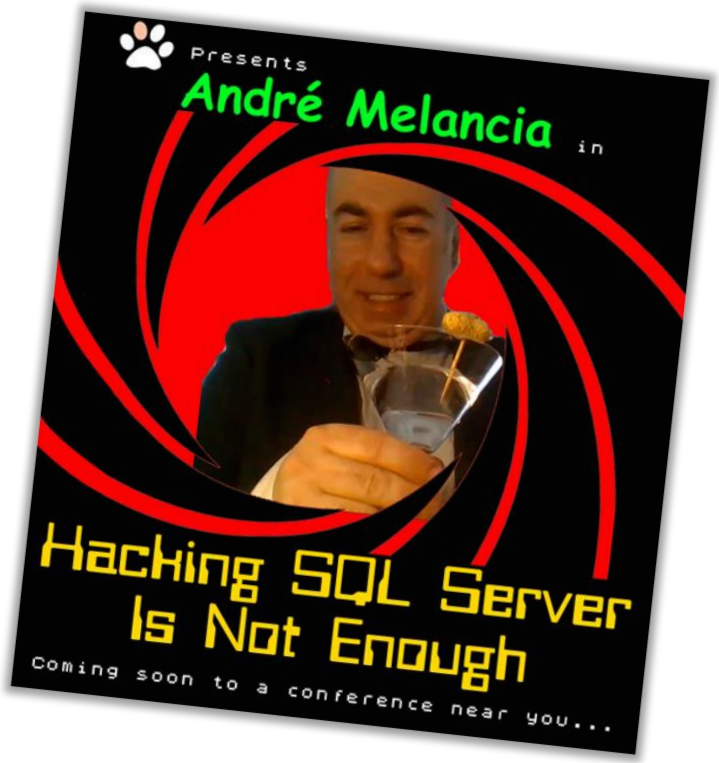
**Evaluate this session at:**

www.PASSDataCommunitySummit.com/evaluation


PASS
**Data Community**
**SUMMIT** 2021




**Thank you!**
**Благодаря!**
**آپکا شکریہ!**
**धन्यवाद !**
**Hvala vam!**
**Danke!**
**ඔයාට ස්තූතියි**
**Obrigado, pá!**
**Ευχαριστώ!**
**¡Muchas gracias!**
**ধন্যবাদ**
**Merci beaucoup!**
**Terima kasih!**
**Grazie mille!**
**Ďakujem!**
**Mulțumesc!**
**Дуже дякую!**
**Labai ačiū!**
**Dziękuję Wam!**
**Mockrát děkuju!**
**Mange tak!**
**Kiitos!**
**Takk fyrir!**
**Dank u wel!**
**Takk!**
**Dank je!**
**Tack så mycket!**
**Köszönöm!**
**Go raibh maith agaibh!**
**Diolch!**




André Melancia
Andy.PT
LunarCat.PT

PASS Data Community SUMMIT 2021