



SOLID
QUALITY
MENTORS



Database Security for Developers

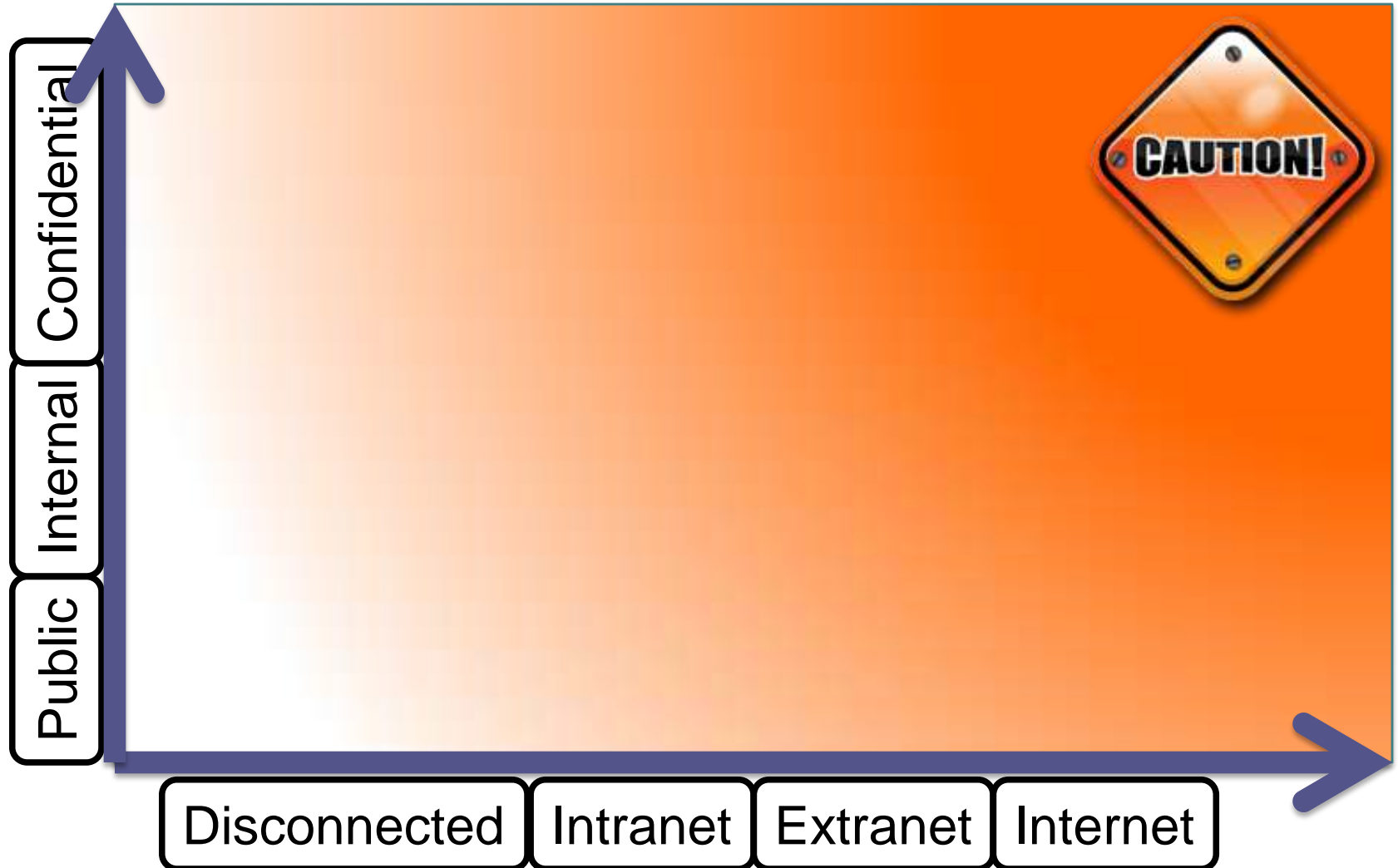
Javier Loria (Javier@SolidQ.com)
Solid Quality Mentors

Agenda

- Security Framework
- SQL Authentication & Authorization
- Signing Data & Data at Rest
- SQL Injection
- SQL Throttling
- Symmetric and Asymmetric Encryption

**SECURITY IS MOSTLY
A SUPERSTITION.
IT DOES NOT EXIST
IN NATURE**

Assets and Environment



Security Properties

Property	Description
Authentication	The identity of users is established (or you're willing to accept anonymous users).
Integrity	Data and system resources are only changed in appropriate ways by appropriate people
Nonrepudiation	Users can't perform an action and later deny performing it.
Confidentiality	Data is only available to the people intended to access it.
Availability	Systems are ready when needed and perform acceptably.
Authorization	Users are explicitly allowed or denied access to resources.

Threats: Stride Model

Authentication

Spoofing Identity

Integrity

Tampering with Data

Non-repudiation

Repudiation

Confidentiality

Information disclosure

Availability

Denial of service

Authorization

Elevation of privilege

Threats and Mitigation (1/2)

Authentication

Spooing Identity

- Appropriate Authentication
- Protect secrets
- Don't store secrets

Integrity

Tampering with Data

- Appropriate Authorization
- Hashes
- Message authentication codes
- Digital signatures
- Tamper-resistant protocols

Non-repudiation

Repudiation

- Digital signatures
- Timestamps
- Audit trails

Threats and Mitigation (2/2)

Confidentiality **I**nformation disclosure

- Authorization
- Privacy-enhanced protocols
- Encryption
- Protect secrets
- Don't store secrets

Availability **D**enial of service

- Authentication
- Authorization
- Filtering
- Throttling
- Quality of service

Authorization **E**levation of privilege

- Run with least privilege

Agenda

- ~~Security Framework~~
- SQL Authentication & Authorization
- Signing Data & Data at Rest
- SQL Injection
- SQL Throttling
- Symmetric and Asymmetric Encryption

↓ Request Network Connection

Connection Established to SQL Server

↓ Login Request

Set Login Credentials

↓ Change to a Database and access authorization

Establish a Database Context

↓ Try to perform an action

Check Permissions for the action

Server Discovery

demo

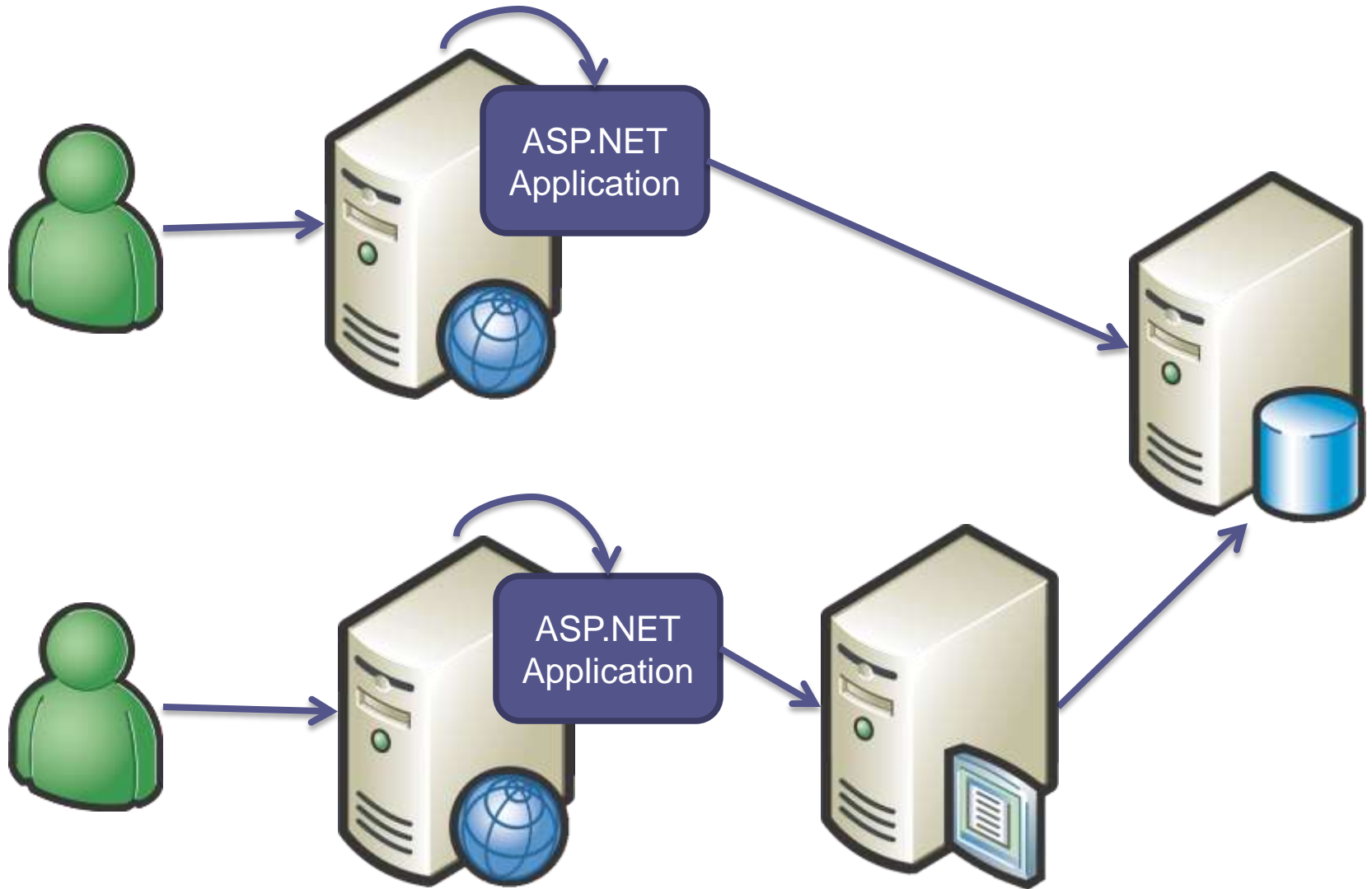
Server Hiding

demo

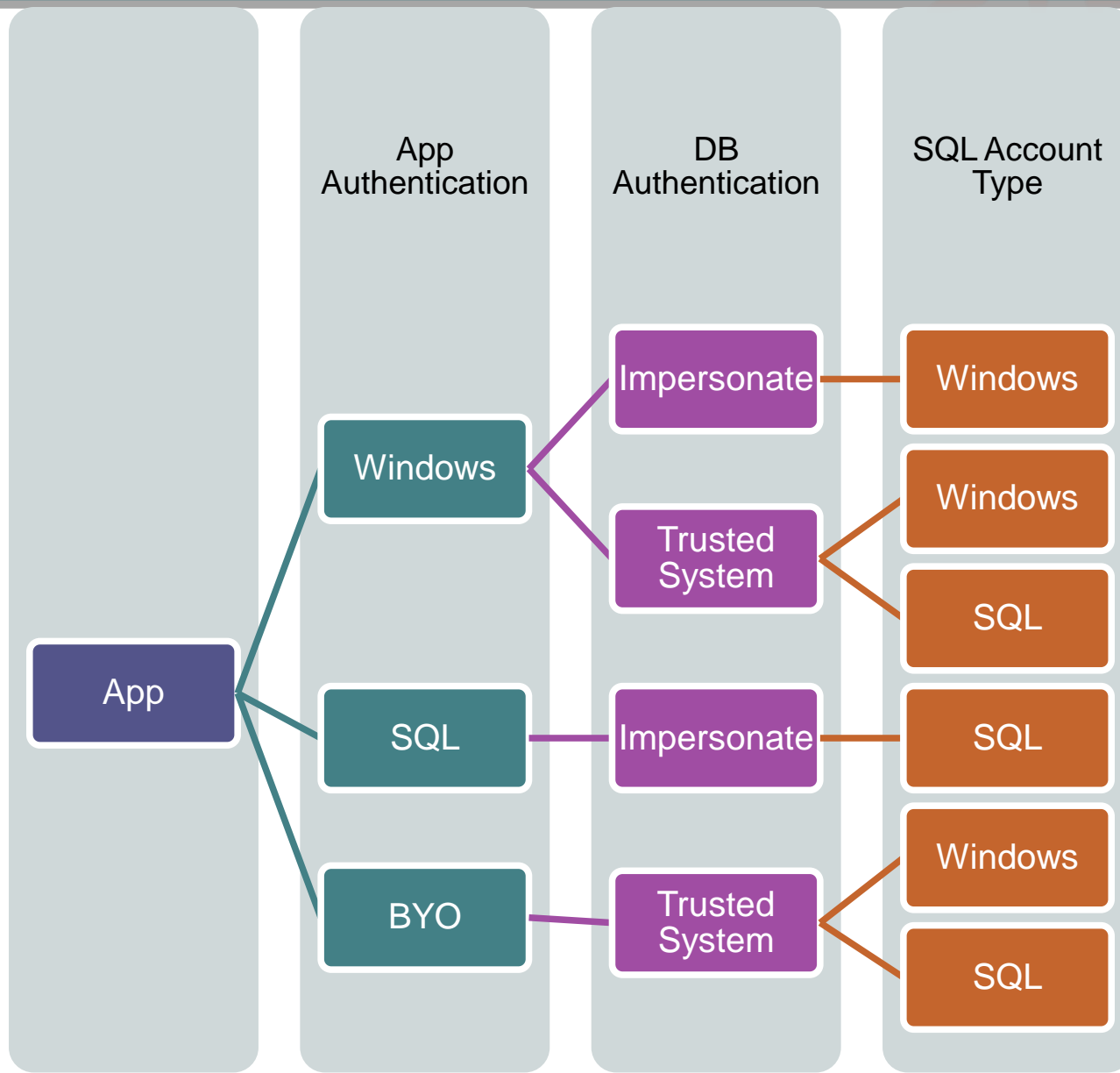
Windows Firewall Configuration

demo

Authentication



Authentication Options



Password Policies

STRIDE

[HOME](#) | [PERSONAL CARDS](#) | [FINANCIAL SERVICES](#) | [TRAVEL](#) | [SMALL BUSINESS](#) | [CORPORATIONS](#) | [MERCHANTS](#)



AMERICAN EXPRESS



[Site Help](#) | [Search](#) | [Contact Us](#)

☐ Online Account Services-User ID / Password

02/06/2010

[DELETE](#)

[REPLY](#)

 [Download](#)  [Print](#)

Response (Gaurav Sharma) 02/06/2010 05:53 AM

Thank you for your email regarding your online password.

I would like to inform you that our website has a 128 bit encryption. With this base, passwords that comprise only of letters and alphabets create an algorithm that is difficult to crack. We discourage the use of special characters because hacking softwares can recognize them very easily.

The length of the password is limited to 8 characters to reduce keyboard contact. Some softwares can decipher a password based on the information of "most common keys pressed".

Therefore, lesser keys punched in a given frame of time lessen the possibility of the password being cracked.

Moreover, American Express is committed to protecting the privacy and security of all of our Cardmembers, both on-line and off-line. We believe that our current security measures, which include our sophisticated monitoring systems to detect unusual or fraudulent card activity, provide strong, ongoing protections for our Cardmembers.

Rest assured, I have forwarded your comments to our webmaster for review. During this review, we may contact you if additional information is required.

[CLOSE MESSAGE CENTER](#)

Your new password **must** comply with the following Federal Desktop Core Configuration (FDCC) requirements:

- The password must have a minimum of 12 characters.
- The password must contain at least one character from at least three of the four following sets of characters:
 - Uppercase Letters (A, B, C, etc.)
 - Lowercase Letters (a, b, c, etc.)
 - Special Characters (~, !, @, #, \$, etc.)
 - Numbers (1, 2, 3, etc.)
- You may not reuse any of your **previous 24** passwords.

It is important to remember that the password you use is **case sensitive**, meaning that the system "knows" the difference between an uppercase "A" and a lowercase "a."

Password Policies

SQL Accounts and Windows Policies

demo

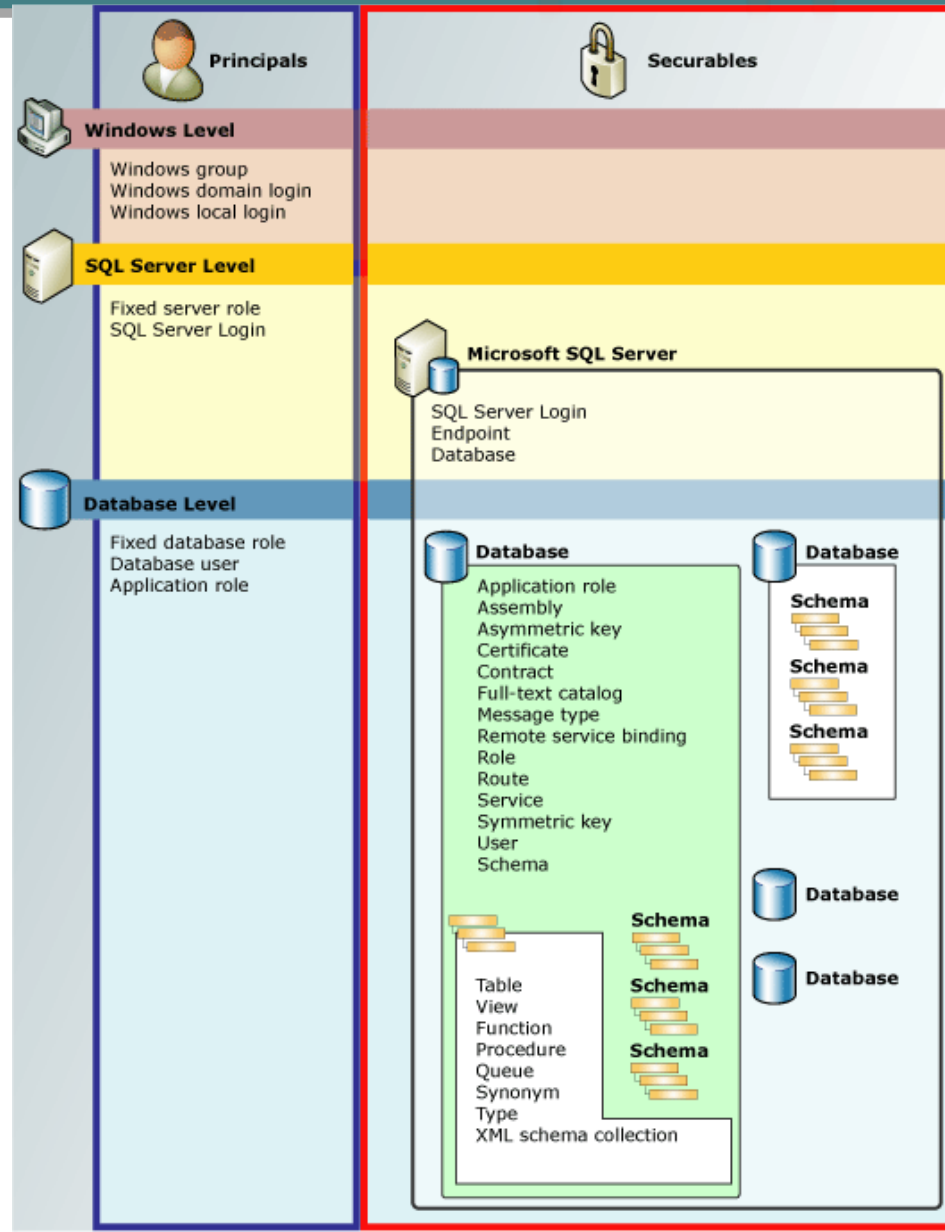
Password Hashing

demo

Permissions



- Types
 - Statement
 - Object
 - Predefined
- DCL Statements
 - Grant
 - Deny
 - Revoke



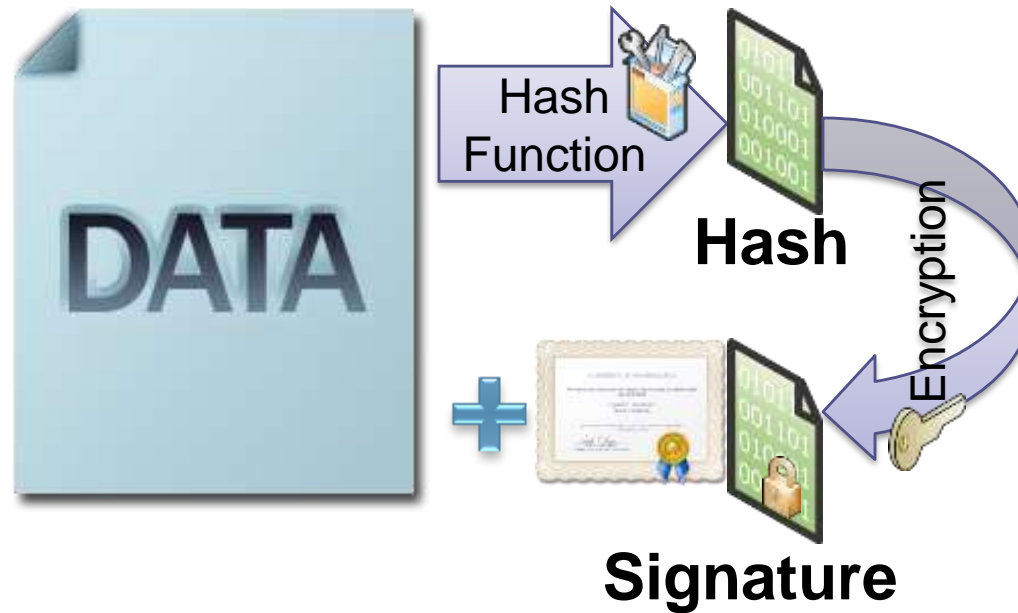
Authorization

demo

Agenda

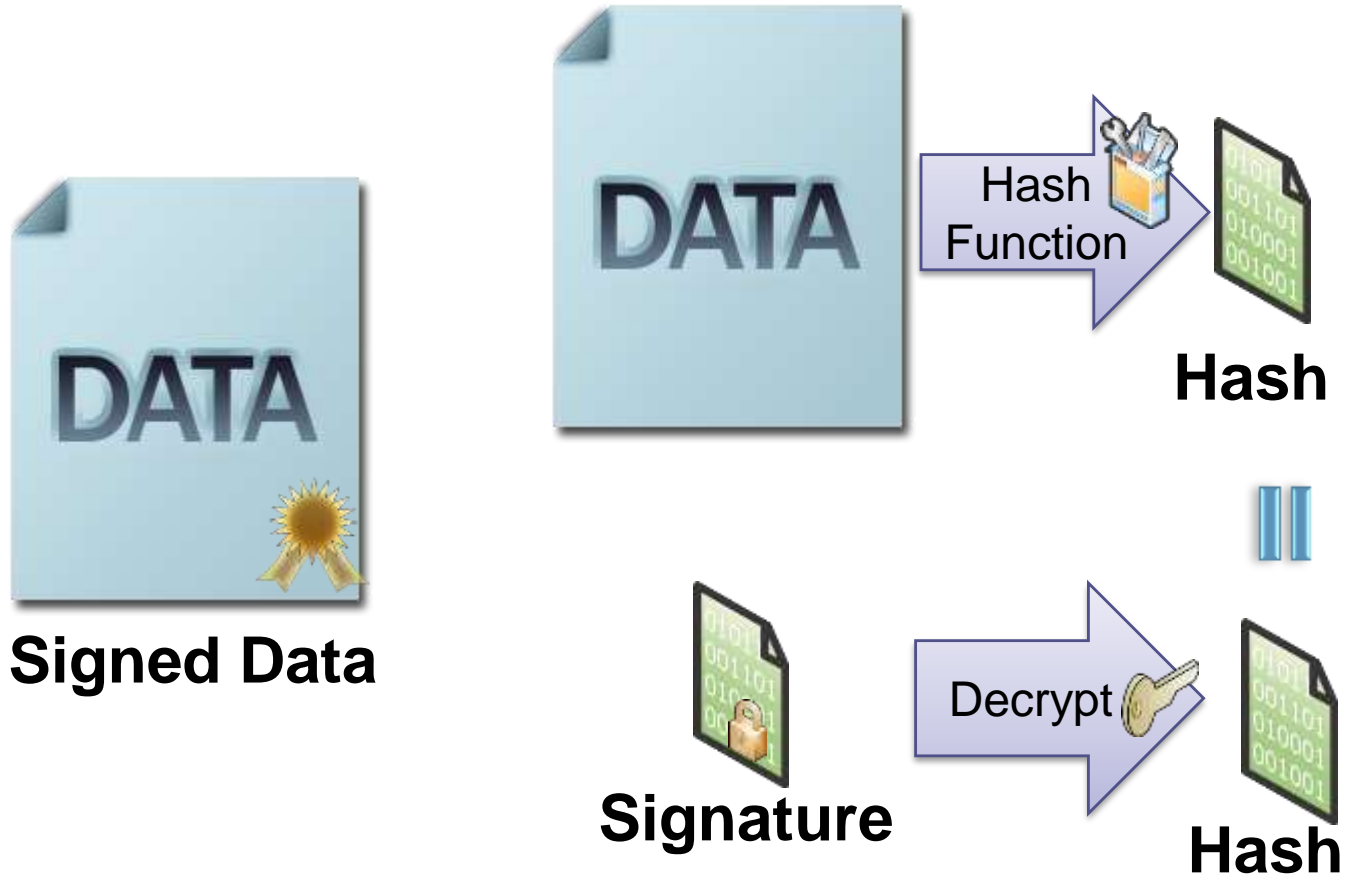
- ~~Security Framework~~
- ~~SQL Authentication & Authorization~~
- Signing Data & Data at Rest
- SQL Injection
- SQL Throttling
- Symmetric and Asymmetric Encryption

Digital Signature: Signing **STRIDE**



Signed Data

DS: Verification



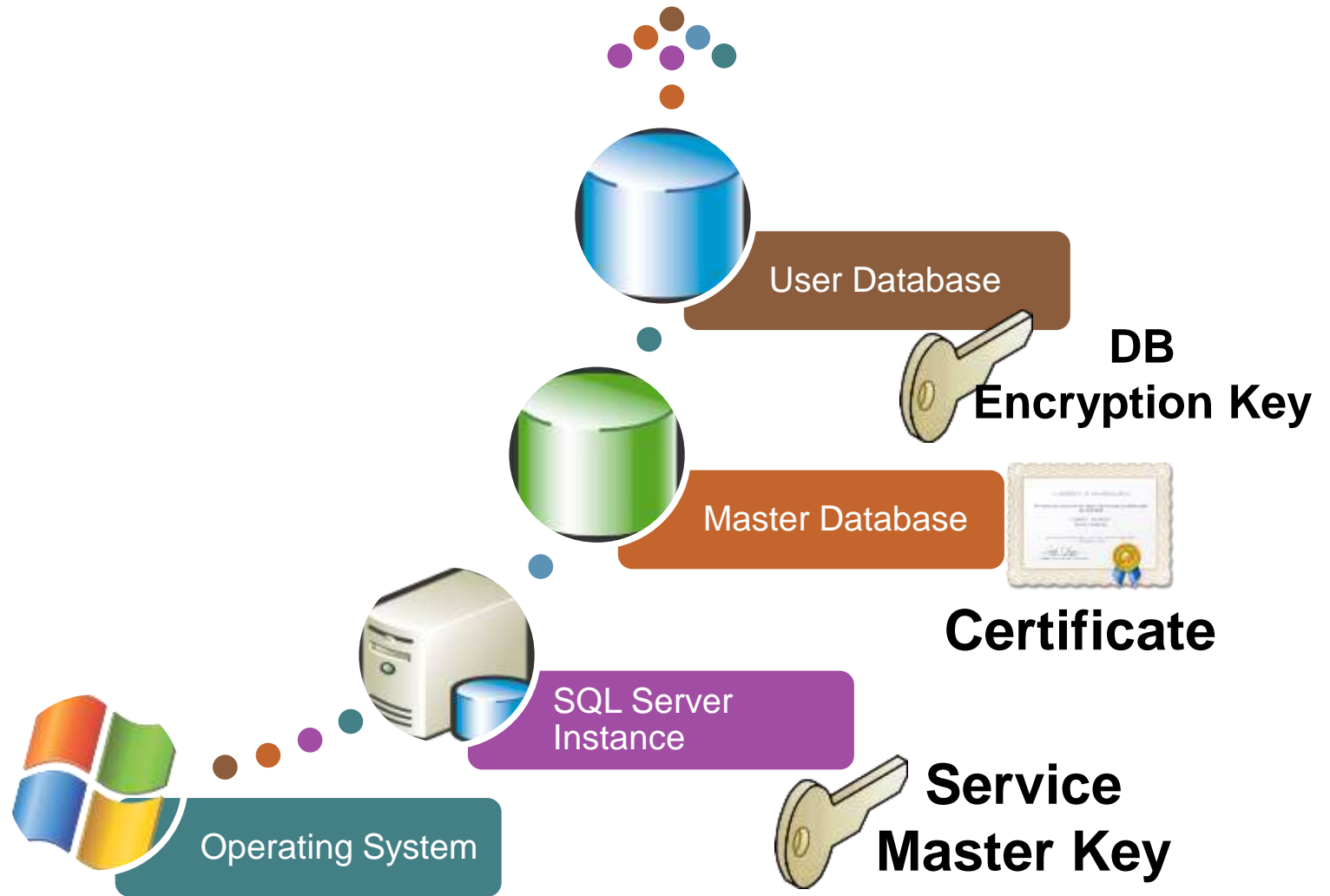
Creating Digital Signatures

demo



**HOW TO PROTECT
DATA AT REST?**

Transparent Data Encryption STRIDE



Certificate

Transparent Data Encryption

demo

Agenda

- ~~Security Framework~~
- ~~SQL Authentication & Authorization~~
- ~~Signing Data & Data at Rest~~
- SQL Injection
- SQL Throttling
- Symmetric and Asymmetric Encryption

SQL Injection

WELL, WE'VE LOST THIS
YEAR'S STUDENT RECORDS.
I HOPE YOU'RE HAPPY.



AND I HOPE
YOU'VE LEARNED
TO SANITIZE YOUR
DATABASE INPUTS.

SQL Injection

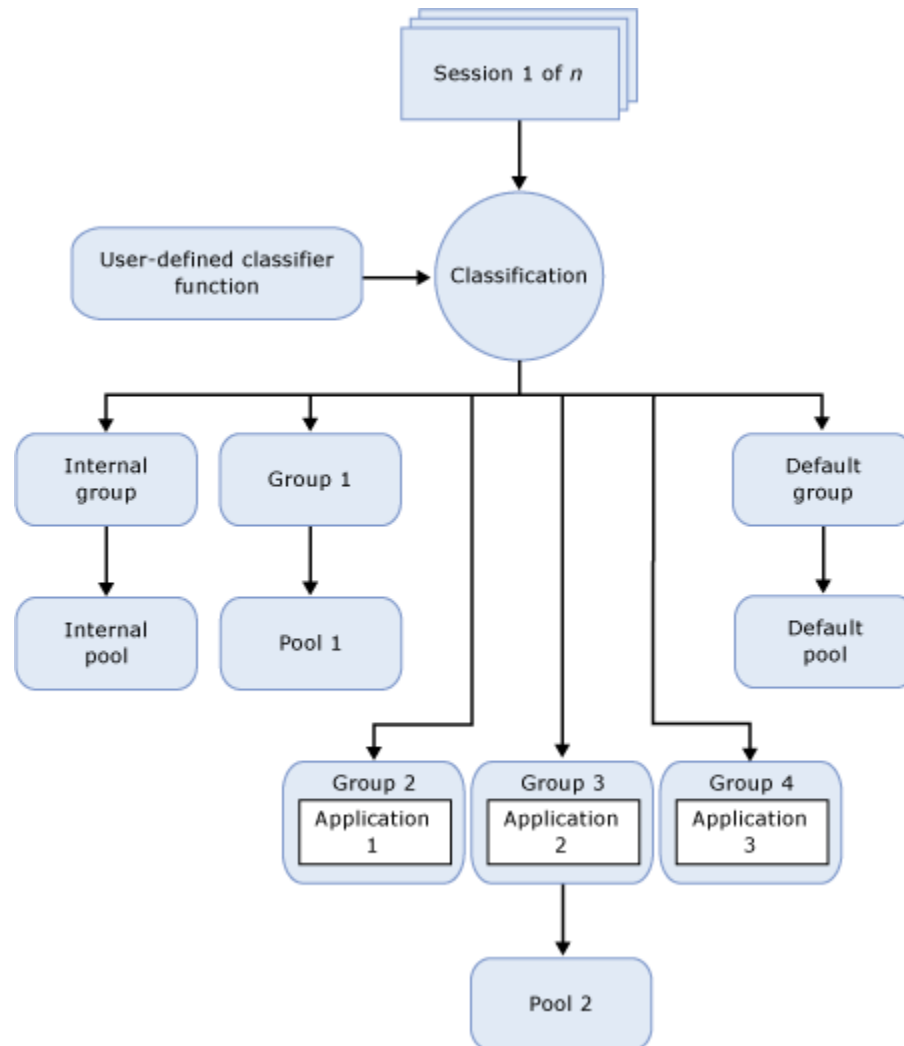
demo

Agenda

- ~~Security Framework~~
- ~~SQL Authentication & Authorization~~
- ~~Signing Data & Data at Rest~~
- ~~SQL Injection~~
- SQL Throttling
- Symmetric and Asymmetric Encryption

Throttling

► Resource Governor



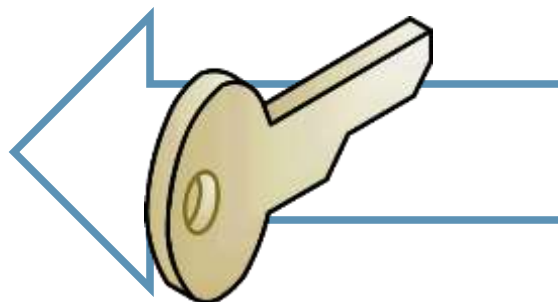
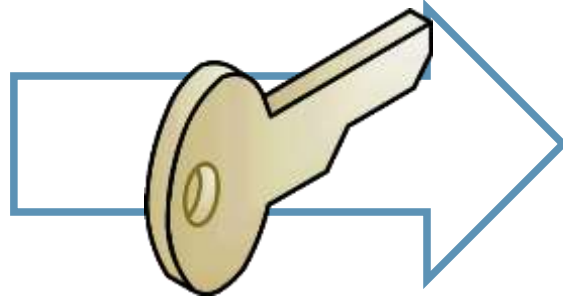
Resource Governor

demo

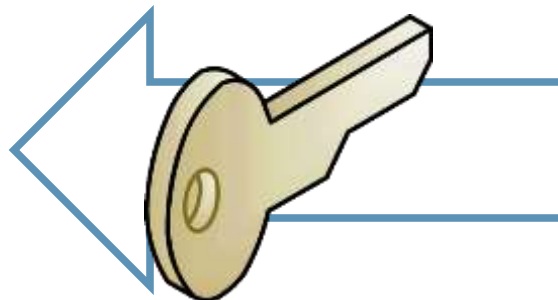
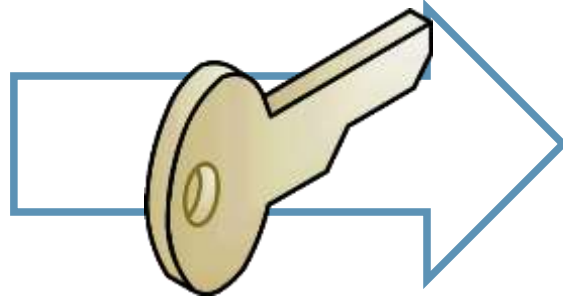
Agenda

- ~~Security Framework~~
- ~~SQL Authentication & Authorization~~
- ~~Signing Data & Data at Rest~~
- ~~SQL Injection~~
- ~~SQL Throttling~~
- Symmetric and Asymmetric Encryption

Symmetric Encryption



Asymmetric Encryption



Asymmetric Encryption

Large Prime Number

359334085968622831041960188598043661065388726959079837



**Key Generation
Algorithm**



Private Key



Public Key

Database Encryption

demo

Agenda

- Security Framework
- SQL Authentication & Authorization
- Signing Data & Data at Rest
- SQL Injection
- SQL Throttling
- Symmetric and Asymmetric Encryption



**Thank
You!!!**

Please remember to fill out evaluations