**Securing application with Access Manager and enabling delegated authorization to third party vendor using OAuth**

### BITS ZG628T: Dissertation

by

Dennis Abraham

2016HT13037

# Dissertation work carried out at

**Infosys Ltd., Mysore**

****

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE**

**PILANI (RAJASTHAN)**

November 2018

**Securing application with Access Manager and enabling delegated authorization to third party vendor using OAuth**

### BITS ZG628T: Dissertation

by

Dennis Abraham

2016HT13037

# Dissertation work carried out at

## Infosys Ltd., Mysore

Submitted in partial fulfillment of M.Tech. Software Systems degree programme

Under the Supervision of

Mahesh Shivananjappa,

Infosys Ltd., Mysore

****

**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE**

**PILANI (RAJASTHAN)**

November 2018

# Introduction

With the emergence of the internet since 1991, the cyber realm has evolved by leaps and bounds. This cyber revolution was complemented by the boom in the software and hardware industry – faster CPU chipsets, efficient instructions, powerful and user-friendly Operating Systems and affordable gadgets for a normal human. In 2018, all fields of business, engineering, medicine, logistics, hospitality, finances are connected to the World Wide Web (WWW) one way or the other. Even emerging countries like India have brought 4G to its average netizens, enabling them to stay connected to others and be tech-savvy.

## Internet Privacy and threats

This huge connected network introduces a new problem – internet privacy. Internet Privacy, also known as Online Privacy, is the right of personal privacy concerning the storing, repurposing, provision to third parties, and displaying information pertaining to oneself via of the Internet. This privacy is always under threat from malicious entities who will misuse the information of the user to get access to their data like phone number, email ID to impersonate and(or) damage the reputation of the victim. There are thousands of cases of identity theft, online money theft, spamming and forgery occurring every year. Some of the infamous ones were the Sony data breach and Madison data breach.

This brings us to a question- how to implement internet security without being intrusive to the user. Internet security has advanced, and it keeps pace with the growth of the internet. Some of the techniques are asymmetric encryption, encoding, security token, One-Time Password (OTP) etc. All these are implemented in today’s internet. For eg., HTTPS encrypts data between the server and the client.

A tool is only as good as the hands that wield it. With increasing security, the malicious predators are also improving. Multiple cases of scammers requesting for user’s bank account information, PAN card number, etc has been surfaced over the years.

## The problem

There are numerous legitimate businesses that manage and aggregate a user’s web accounts and activities. A user could share his personal details to the aggregator and the aggregator in-turn, uses the credentials to login to the web-accounts of user and aggregates it all to its own page.

In Banking and financial sector, the US has many aggregators like Yodlee, Wealthfront etc. These aggregators get user’s spending pattern, account balance and other details from the bank and provide advice on financial well-being. In India we have ICICI’s ‘My Money’ and Aditya Birla’s ‘MyUniverse’ which offer account aggregation.

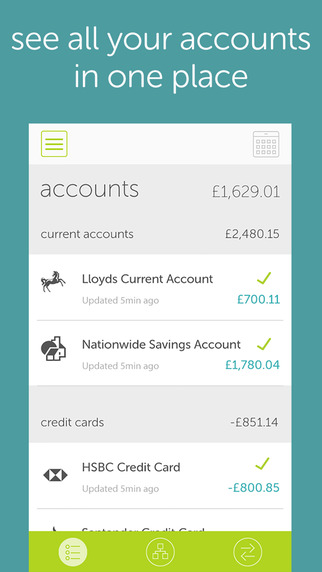


Figure 1 Account aggregator example (OnTrees UK) [http://www.lifehacker.co.uk/2016/01/28/the-11-best-money-management-budgeting-and-personal-finance-apps-for-android-and-ios]

Regardless of the security implemented at the aggregator, storing user credentials at aggregator is quite risky. A solution should be designed to allow aggregators to access limited access to user data without sharing the credentials.

## The Solution

One of the most popular and effective solution is OAuth 2.0 (RFC 6749). This implementation specifies standard to delegate authorization of aggregator’s access to the protected user’s resource, to the user itself. This prevents any sharing of the user’s credentials.

This implementation is used in many platforms like Facebook, Google, Twitter, GitHub, etc. These platforms allow user to login to another web platform like Instagram without creating an account in the client (here, Instagram). The client trusts the authorization server – say Facebook, to authorize the user.

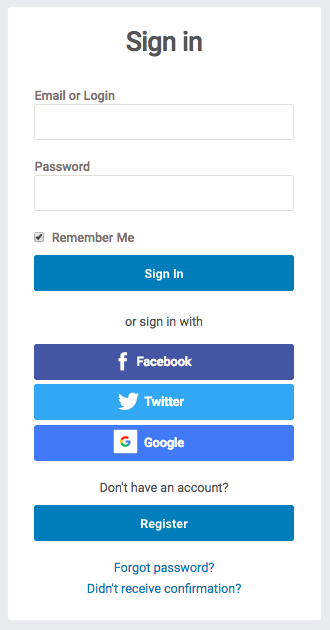


Figure 2 Delegated authentication example [https://helpdesk.bangthetable.com/general-settings/site-settings/enabling-twitter-facebook-and-google-login]

## Need of Access management

Users demand quick and easy access to systems and information whether they’re located in the office, at home or on the road.

Most organizations recognize the need for this access but realize they must balance user demands against difficult security requirements. Cybercriminals know that organizations must support remote users and attempt to exploit enterprise identity systems using social engineering attacks that allow them to **compromise the credentials of legitimate users and gain access to enterprise systems**. In recent years, social engineering has grown into an increasingly common and effective attack vector.

The **demand for secure access poses a serious challenge** to IT professionals. The IT team must simultaneously meet the needs of a diverse landscape of users across numerous, disparate applications. Many scenarios arise daily that require modifications to access permissions. New users are hired and need their access provisioned quickly during their onboarding process. At the same time, current users leave an organization as part of planned retirements or sudden terminations, and they must have their access revoked. Other users change roles within an enterprise because of transfers and promotions and need their access rights updated to reflect their new positions, while removing the permissions they no longer require.

Meeting these demands across a variety of on-premises and cloud applications requires the use of agile and flexible identity and access management solutions. Identity and access management (IAM) products must be able to handle access rights for many different categories of individuals who are using a variety of devices to access different types of data and workloads. Access control systems must be able to integrate with a wide variety of existing and future information systems, allowing users access to the information they need, wherever it is stored.

Identity and access management is the information security discipline that allows users access to appropriate technology resources, at the right time. It incorporates three major concepts: identification, authentication and authorization. Together, these three processes combine to ensure that specified users have the access they need to do their jobs, while unauthorized users are kept away from sensitive resources and information.

# The project

The project contains mainly of two applications – the Online banking app(OLB) and the aggregator vendor.

## Online Banking App (OLB)

This application is a rudimentary banking application for a fictional bank called ‘Royal Bank of Mysore (RBM)’, where the user can credit money to his own account (a cash deposit scenario) and transfer money to other accounts. The application has protection against unauthorized access to the bank resources. User’s session is tracked to provide a smooth user experience.

<Add screenshots>

## Aggregator

This is an application that requests for OLB user account details without soliciting for user’s credentials. Here the OAuth authorization code flow is implemented in which the aggregator must first obtain the consent and eventually an access token for accessing the OLB user account information.

# Technical Design

The project uses multiple technologies and frameworks to provide smooth user experience while providing industry-level protection against unauthorized access of protected resources.

## Business Logic and user Interface

The business logic and the UI has been developed using Spring Boot framework 2.0. Spring Boot is a part of Spring framework, which is an [application framework](https://en.wikipedia.org/wiki/Application_framework) and [inversion of control](https://en.wikipedia.org/wiki/Inversion_of_control) [container](https://en.wikipedia.org/wiki/Servlet_container) for the [Java platform](https://en.wikipedia.org/wiki/Java_platform). The framework's core features can be used by any Java application, but there are extensions for building web applications on top of the [Java EE](https://en.wikipedia.org/wiki/Java_EE) (Enterprise Edition) platform. Spring Boot is a ‘convention over configuration’ for creating standalone Spring based application. The application is exported as an executable java archive (jar) which packs its own Tomcat application server for hosting the web applications and pages.