BUILDING MULTI-FACTOR AUTHENTICATION PROVIDER USING ASP.NET

Adith Prasetya, Anggi Wijaya, Moehammad Radif, Agus Kurniawan

Computer Science Department,
Universitas Indonesia,
Depok, Indonesia, 16424
E-mail: {adith.prasetya, anggi.wijaya, moehammad.radif}@ui.ac.id
agusk@cs.ui.ac.id

ABSTRACT
In this paper, we present an authentication system which can be served as multi-factor authentication provider. This system has supported various authentication methods (ASP Membership, OpenID, and SMS one-time password) in either standard one-factor or multi-factor authentication method. It has been tested with two consumer websites (MOSS 2007 website and ASP .NET MVC website) in either standard XML post or Diffie Hellman protocol. This system was developed as a solution for user's multi-account in multiple websites problem.

Keywords: Diffie Hellman, Multi-factor Authentication, OpenID

1. INTRODUCTION

Authentication is a way to identify or confirm a something's (or someone's) claim to be true and trustworthy (authentic) [1]. In the Internet, authentication is an important part of a website for identifying identity and right of its users. Based on U.S. Federal Financial Institutions Examination Council's, authentication factors whose are used for verifying identity can be differentiated to three categories, such as:

a) Some things user knows (e.g. password or PIN (Personal Identification Number))
b) Some things user has (e.g. ATM (Automatic Teller Machine) card or Smart card)
c) Some things identify the user (e.g. Biometric characteristic, such as eye retina)

A website basically only uses one-factor as its authentication method, valid and registered password (and username). The usage of this one-factor's known as one-factor authentication (OFA). Another known method is multi-factor authentication (MFA). MFA means the usage of more than one authentication factor in one authentication process [1].

MFA basically has better security than OFA, because it uses two or three authentication factor for verifying user's identity. Then the unrighteous third party needs to pass two or three security layer in MFA, comparing to only one in OFA.

MFA indeed has better security than OFA, but it's more uncomfortable for user, and harder to implement for website developer.

Based on second disadvantage of MFA, the owner this project initiates the development of authentication provider as a prototype system, which can be used by other websites as a system to authenticate their users. As the first step, provider has implemented three authentication services, such as ASP Membership, OpenID, and SMS. Its service can be served in two ways; XML post, or Diffie Hellman protocol.

Despite of its potential inconvenience use to user, provider facilitates its user to have one account for multiple consumer websites. This approach prevents user to create many accounts on different website. User simply remembers one account to authenticate his/her identity in multiple websites which have supported provider authentication system.

2. RELATED WORK

Brandon Haynes, Harvard University (May 1, 2009) on his paper titled "A Multi-Factor Authentication Provider For The DotNetNuke® Open-Source Content Management Web Application Framework" wrote that he developed an authentication provider that is designed to extend core DotNetNuke functionality to allow a host to configure enhanced authentication (including, but not limited to, SMS, SMTP, YubiKey, and X.509 certificates) for any number and combination of user roles across any number of websites in a given installation [2].

3. THEORY

3.1. Multi-factor Authentication (MFA)

Based on FFIEC's definition, MFA is authentication method which uses two or more authentication factors. MFA's used for empowering the security of system by additional one or two layer authentication into standard authentication method (OFA).

3.2. ASP .NET MVC

ASP .NET MVC is a framework for developing MVC web based applications developed by Microsoft®. ASP .NET MVC combines the

 ISSN: 1907-5022

effectiveness and regularity of the MVC architecture, the principles of agile software development, and the best components from ASP .NET platform [3].

MVC is a model of software development methodologies that consists of several terms as follows [4]:

a) Model
   Part associated with the data and state management of the application. State data are generally stored in a database application.
b) View
   Part relates to display the user application. All information shown on the view obtained through the model.
c) Controller
   Part used to control user interactivity within applications.

3.3. Microsoft Office SharePoint Server 2007 (MOSS 2007)

Microsoft Office SharePoint Server 2007 (MOSS) is an application web site for the corporate usage created by Microsoft ® Corporation. MOSS is a part of the Microsoft SharePoint platform, and runs on top of Windows SharePoint Services (WSS). MOSS strength lies in the management including organizing information about users in a centralized web-based application, including classifying the data. We can quickly create a SharePoint web site that supports content publishing, content management, records management, or the need for Business Intelligence. You can also conduct effective searches for personnel, documents and data, participate in forms-based business processes, access and analyze large amounts of business data [5].

4. IMPLEMENTATION

4.1 Authentication Factor

Provider has implemented some authentication factors; such as ASP .NET Membership, OpenID, and one-time password (OTP) through SMS.

4.1.1 ASP .NET Membership

This authentication factor is based authentication sub-system which uses ASP .NET 3.5 and SQL Server 2008. The usage of this factor is to guarantee security and provide basic authentication on provider.

4.1.2 OpenID

This authentication factor uses services from OpenID relying party [6] such as MyOpenId (myopenid.com), BlogSpot (blogspot.com), and Wordpress (wordpress.com). The usage of this factor due to many parties that already support the OpenID Standard Authentication; such as Microsoft, MySpace, and PayPal. So, there are a lot more potential users that can use the service from this provider.

4.1.3 Short Message Service (SMS)

This authentication factor uses service from Clickatell® [7] as gateway to send one-time-password (OTP) via SMS (short message). The configuration for this factor requires username and password for a licensed user to be able to use Clickatell® service. There is also a limitation for credit that user can use for each SMS. Other alternative for this factor is that user only need to provide the username.

4.2 Architecture

The development of this provider based on some standard system architecture designs; such as high level architecture, physical design, and class diagram.

4.2.1 High Level Architecture

Authentication system provider architecture is based on three-tier application model as described on Figure 1.

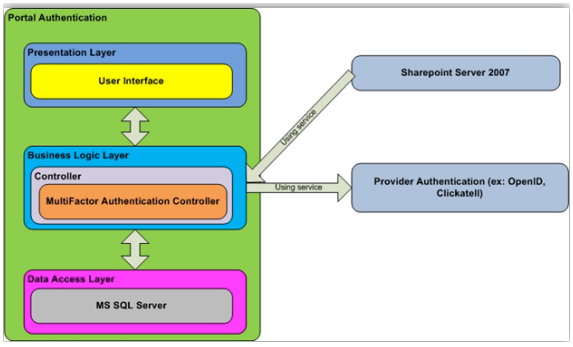


Figure 1: High Level Provider Architecture

Based on figure 1, this provider is parted into three main layers, which are:

a) Presentation Layer (*View on MVC Framework*)
b) Business Logic Layer (*Controller on MVC Framework*)
c) Data Access Layer (*Model on MVC Framework*)

4.2.1.1 Presentation Layer

This layer consists of views that can be used by users to authenticate themselves through the desired method. To improve the user experience of this portal, the implementation of jQuery [8] is necessary, such as login view tab, OpenID plugin login, and option to use a pop up window on consumer site (relying party).

4.2.1.2 Business Logic Layer

Presentation layer consists of controllers that describe the logical flow of authentication that the user performs. The process flow can be viewed on this paper.

4.2.1.3 Data Access Layer

This layer contains the implementation from the access data model to database using MS SQL Server 2008 as the DBMS (Database Management System) using LINQ.

4.2.2 Physical Design

ISSN: 1907-5022

Physically, the design of the providers can be divided into four components as illustrated in Figure 2, as follows:

a) Portal Server
Is a physical description of the provider that developed by authors. Portal server (portal) is the central of communication flow in the provision of authentication services to users.

b) Consumer website
Sites that use portal as their user authentication service provider. In development process, portal uses two consumer websites as an example: site based on MOSS 2007, and ASP MVC.

c) Authentication Provider
Providers used by the portal as an authentication service provider. In this position, the portal serves as consumer website from these providers. For this moment, portal uses OpenID provider (e.g. MyOpenID, MySpace) as OpenID authentication service, and Clickatell for SMS OTP authentication service.

d) Client
Provider's consumer website users that use provider's authentication services.

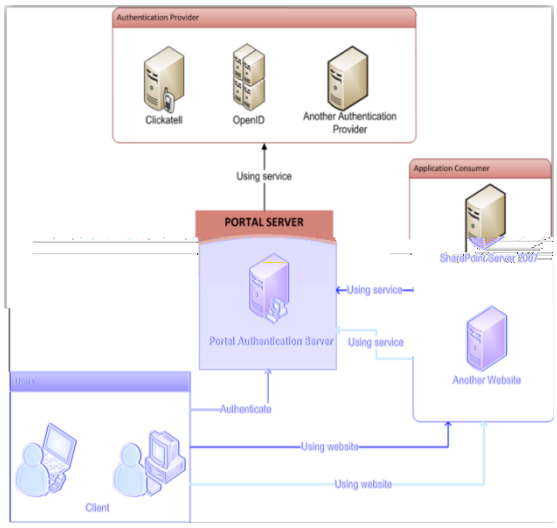


Figure 2: Portal physical architecture model

4.2.3 Class Diagram

Provider development process uses principles of strategy pattern in designing process of class diagram. Strategy pattern is the part of design pattern, a guide in software development. Strategy pattern is the principle whereby the suitable working process algorithm is selected when the application's started [9].

Based on above principle, Figure 3 shows implementation of multi-factor classes that can be defined as following:

a) Authentication
Strategic object which encapsulates supported authentication factor algorithms, such as ASP Membership and OpenID.

b) MultiFactorAuth
Compositor interface which defines generalization of authentication factor algorithm.

c) NormAuth
Subclass of MultiFactorAuth interface which defines authentication factor algorithm through ASP Membership.

d) OpenIDAuth
Subclass of MultiFactorAuth interface which defines authentication factor algorithm through OpenID.

e) SMSAuth
Subclass of MultiFactorAuth interface which defines authentication factor algorithm through SMS OTP.

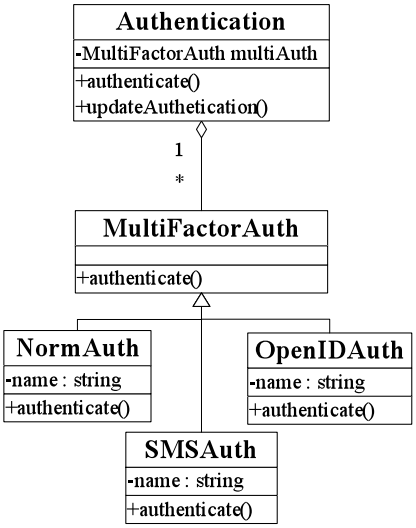
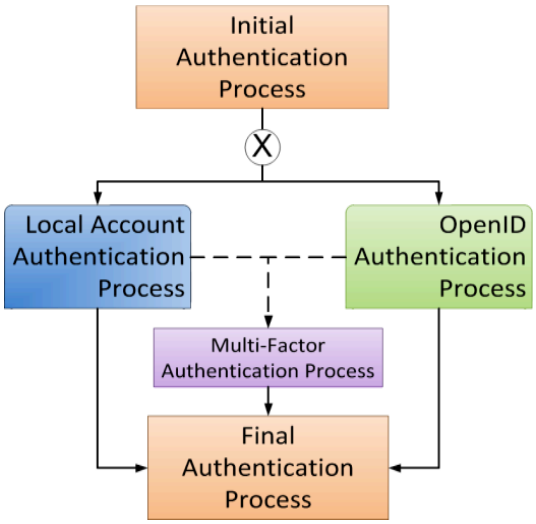


Figure 3: Authentication Provider class diagram

4.3 Provider Authentication Process Flow

Chronology of the authentication process can be illustrated by flow diagram below:



 ISSN: 1907-5022

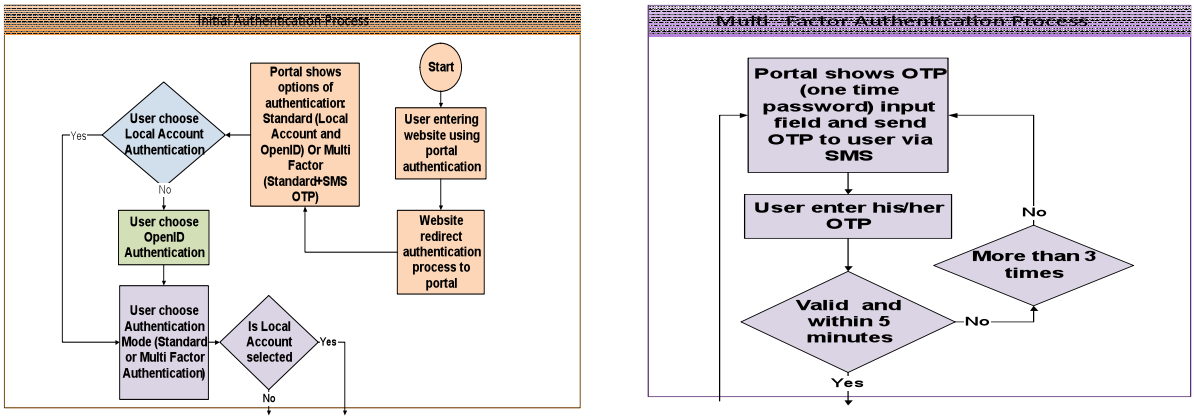


Figure 4: Provider flow diagram

Figure 4 describes flow of authentication process implemented by provider. The first process is user enters portal's consumer website, then when user click login, it directs user to provider to authenticate user's identity.

In provider login page, user can choose to use 'Local Account' for ASP .Net Membership and 'OpenID' for OpenID authentication (steps i-iv). The next process is user can choose whether to use 'Standard' for OFA, and 'Multi-factor' for MFA. The difference in MFA is the usage of SMS OTP as second factor authentication factor (steps 1-4).

i. User chooses an OpenID provider that he wanted to use.
ii. Provider will then direct the user to the login page of chosen OpenID provider.
iii. User does authentication process at chosen OpenID provider.
iv. Authentication process doing successfully, returning to provider.

When user successfully authenticates him/her identity, provider shows confirmation page to confirm user whether to pass user's personal information to previous consumer website. If user confirms 'yes', then provider will send user's

ISSN: 1907-5022

personal information, otherwise provider will send 'no' as the confirmation get parameter.

1. After a successful local authentication process or OpenID account, the provider will make the OTP and send it via SMS to the user.
2. Provider display OTP login page.
3. After receiving a message containing the OTP, the user enters the OTP on the existing field.
4. Provider validates the OTP user. OTP is valid which has not exceeded five minutes, and equal to provider unique OTP for this user.

When user fails to authenticate in first factor authentication phase ('Local Account' and 'OpenID') more than five times, or in second phase of MFA (OTP no longer valid) more than three times, provider will lock user's account for 24 hours.

4.4 Multi-factor Authentication

Provider has implemented MFA as two-factor authentication, such as: ASP Membership – SMS OTP, and OpenID – SMS OTP. Figure 5 shows hierarchical model of provider multi-factor authentication system.

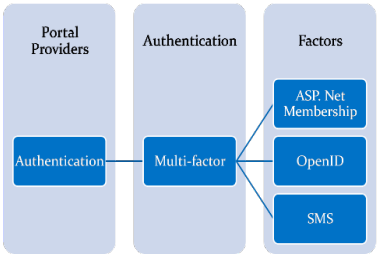


Figure 5: The Provider-Based Hierarchy Associated with the Multi-Factor provider

4.5 SharePoint Consumer Website

Website on this project serves as the Consumer site that has the ability to perform authentication through authentication providers as well as portal authentication with local accounts. Through this capability the user can authenticate without having to create an account in advance, but can do authentication through portal authentication provider website as long as the user has been registered on the portal authentication provider as showed on Figure 6 (comparing to default authentication service on Figure 7). In the making of this website the author using Microsoft Office SharePoint Server 2007 (MOSS) since MOSS has power to organize the management of information about users in a centralized web-based application, including classifying the data. The use of SharePoint in this consumer site is only in the scope of the login authentication because the topic is restricted in Multifactor Authentication [5].

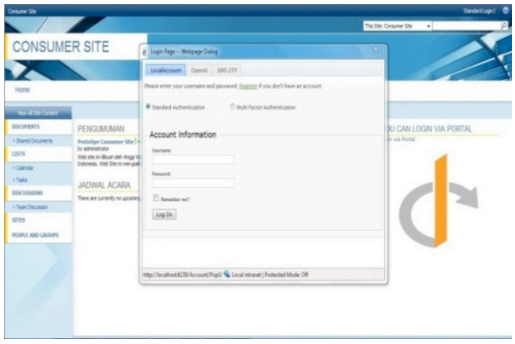


Figure 6: SharePoint authentication through system authentication provider

5. CONCLUSION

The usefulness of the multi-factor authentication is reinforced by this work. We have made a website provider whose function is to receive and send responses if there is some website that want to use the authentication service on our website provider. We also have made a consumer site that used the authentication service from authentication provider. With the ability we have built on our system, user can authenticate to a consumer site they want easily because they do not have to create an account on that consumer site.

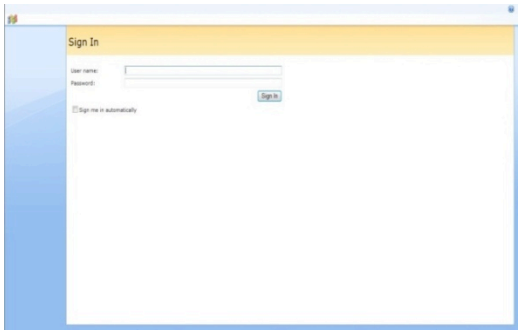


Figure 7: SharePoint authentication through local account

6. FUTURE WORKS

For the future works, the authors are planning to do some of these things (but not limited):

(1) As a reliable multi-factor authentication service provider solution which can be developed further. The usage of strategy pattern principle in development process, expected that provider can implement another standard authentication factor.

(2) Implement the username binding process that has the ability to make user's OpenID account as an alias to user's local account.

(3) Implement another type of authentication factor such as X.509 Client Certificate and YubiKey.

ACKNOWLEDGMENT

We wish to acknowledge Fajar Ramadhany (BataviaSoft) in his idea and support for this project. We also would like to acknowledge Agus

Kurniawan for his recognition, guidance and support since the beginning of this project.

REFERENCES

[1] **U.S. Federal Financial Institutions Examination Council's (FFIEC)**. Authetication in an Internet Banking Environment. [Retrieved: April 2, 2010].

[2] **Haynes, Brandon** (May, 2009). *A Multi-factor Authentication Provider for the DotNetNuke® Open-Source Content Management Web Application Framework*. USA: Harvard.

[3] **Sanderson, Steven** (2008). *ASP.Net MVC Framework Preview*. USA: Apress.

[4] **Conery, Rob., Guthrie, Scoot., Haack, Phil., & Hanselman, Scoot. (2009)**. Professional ASP.Net MVC 1.0. USA: Wiley Publishing, Inc.

[5] **Microsoft**. Microsoft Office SharePoint Server 2007. [Online] [Cited: April, 2010]. http://sharepoint.microsoft.com/product/Pages/default.aspx.

[6] **OpenID**. http://openid.net/ [Online] [Cited: March 2010]

[7] **Clickatell**. http://clickatell.com.

[8] **jQuery**. http://jquery.com.

[9] **Gamma, Eric, et al** (August, 1994). *Design Patterns: Elements of Reusable Object-Oriented Software*. USA: Addison-Wesley Professional.