USER AUTHENTICATION VIA ACTIVE DIRECTORY IN FDBA

Maria Dobreva, Nikolay Pavlov, Asen Rahnev, Angel Golev

Abstract. In this paper we describe authentication mechanism implemented for the Framework for Distributed Business Applications – FDBA. We present the primary functional requirements and describe how they were implemented. This authentication approach interacts with Active Directory Domain Services which is recommended technology for storing identity information within an organization. The key feature is improved security and more efficient user logon process.

Keywords: Authentication, Active Directory, Security, FDBA

1. Introduction

The growing list of authentication options should come as no surprise considering the rapid rate at which applications are moving to the cloud and users are embracing mobile devices. These behavioral and organizational shifts are driving authentication methods in two directions: toward more convenient access to please users and toward more secure access to satisfy IT security teams. The need for user convenience is growing in proportion to the tremendous growth in the number of systems and applications users need. One cannot expect people to remember hundreds of unique passwords and that is why many organizations are betting on single sign-on solution [5]. Many organizations today include computers running both UNIX and Microsoft Windows operating systems in their network environments. Ensuring the security of information located on either type of network infrastructure requires validating every user's identity and specifying which network data each user can access [6]. By establishing the user`s identity a single sign-on

authentication (SSO) can be achieved. SSO is designed to enhance the end user experience during log-ins by making the process quick and simple.

The Framework for Distributed Business Applications – FDBA is a powerful platform for developing state-of-art enterprise resource planning (ERP) and customer relation management (CRM) software products [4]. One of its key features is the variety of ready-to-use components which enable application developers implement various features without writing executable code. Security model in FDBA is a major component which is used in any application, based on FDBA. It is essential to improve our secure model with the security trends.

Our goal is to extend the existing security model of the Framework for Distributed Business Applications (FDBA) [4], more precisely authentication module to support various methods of proving identity. We will implement a new mechanism for login which interacts with the Identity from the Active Directory and provide single-sign on (SSO) authentication solution. SSO simplify authentication and expedites users' access to applications.

2. Requirements

The following user requirements are defined:

- Logon automatically to the system without typing strong passwords
- Logon to the system using a user name and password
- Users to impersonate and log on to the system on behalf of other users

Logon automatically to the system

Users want secure login to the system without typing credentials on every start. Security policies require that passwords meet certain complexity rules: length, mixture of letters, digits and symbols. It is difficult for users to enter complicated passwords to gain access to different system. Very often, users forget their passwords. In order to gain access, they must contact to system administrators who can reset their passwords.

It is a good solution to authenticate users with the same credentials they use to log into their computers. User will not be prompt for credentials, the system will automatically log in.

Windows authentication is a good option because:

- Windows already support basic user account features such as password expiry, password strength, account lockout which are essential for the current security model in FDBA.
- Can provide “invisible” authentication that works without forcing a separate login step.

- User have a single authentication model across different types of applications. This can be used for web services, ASP.NET applications, etc.

Logon to the system using a user name and password

Keep the current authentication model. The system can configure manually which authentication model to use.

Users to impersonate

FDBA supports users to impersonate and log on to the system on behalf of other users. To support this feature both with Windows authentication, system must give chance to user to choose whether to login as yourself or another person – by typing his/her username.

3. Implementation

Authentication process

User authentication module has been extended to maintain logins with an active directory account. When a user attempts to log-in, the authentication module performs the following steps:

- Check whether the application supports user authentication via Active Directory.
- If support then check whether the server provides such a way of authentication.
- User tries to authenticate with the credentials provided by the Windows infrastructure. On success a secure context is established between the client and the WCF service. If the current domain user is associated with application user(s), then the logon process with Windows credentials is successful.
- If support for AD authentication is not available or is available but the logon process is unsuccessful then the standard username and password authentication approach is used.

Server-side implementation

Our implementation uses security mechanism provided by Windows Communication Foundation (WCF). Windows Communication Foundation (WCF) security consists of two primary requirements: transfer security and authorization. In brief, transfer security includes authentication (verifying the identity of both the service and the client), (message encryption), and integrity (digital signing to detect tampering) [2].

The WCF infrastructure is designed to use Windows security mechanisms. If a service that is deployed on an intranet, and whose clients are restricted to members

of the Windows domain, only valid users can log on to the domain. After users are logged on, the Kerberos controller enables each user to establish secure contexts with any other computer or application.

To support both Windows authentication and username/password authentication our service is extended to provide two service endpoints with appropriate set of security settings.

a) Unsecured Endpoint which is used until now and the security and authentication mechanism is provided by a layer below the WCF infrastructure.

```
NetTcpBinding binding = new NetTcpBinding();
binding.Security.Mode = SecurityMode.None;
binding.Security.Transport.ProtectionLevel = ProtectionLevel.None;
binding.Security.Transport.ClientCredentialType =
TcpClientCredentialType.None;
```

b) Endpoint that uses a Windows security:

```
NetTcpBinding binding = new NetTcpBinding();
binding.Security.Mode = SecurityMode.Transport;
binding.Security.Transport.ProtectionLevel =
ProtectionLevel.EncryptAndSign;
binding.Security.Transport.ClientCredentialType =
TcpClientCredentialType.Windows;
```

Each endpoint has its own address. Ports are described in the server configuration file for each application.

```
<add name="TcpPort" value="10001"/>
<add name="TcpPortWindowsAuthentication" value="10011" />
```

Relationship between FDBA application users and Domain user

The security model of FDBA relies that every user account in the system is unique and holds the basic account details with the assigned rights.

To use windows authentication both with the security model of FDBA, somehow the application needs to recognize the application user who is trying to login. To be able to do this a new field is added in Users table – Windows Login Name. The new field is populated with windows account login name in format Domain\Username.

When a domain user is associated with multiple application users, on login he or she must choose the right one to perform login.

When user attempts to login UseWindowsAuthenticationLogin() method checks whether the user can be authenticated via domain account.

- Check if client support windows authentication – this is an option configured in client configuration.
- Get the windows authentication port from the server configuration file. If application supports windows authentication a Windows security service is created.
- Call GetShellUsersByWindowsLoginName(out users)) from a Windows secure service, if security context is established and any of the application users is associated with a domain account, the user can login with the current Windows Identity.

```
var windowsIdentity =
ServiceSecurityContext.Current.WindowsIdentity;
users = application.DataAccess.GetShellUsersByWindowsLogin
                                        Name(windowsIdentity.Name)
```

- Depending on the returned shell users, the user is navigated to adequate login screen.

In case user cannot login using windows authentication the service is redirected to use the Unsecured Endpoint.

User Interface

When the user is successfully validated and authenticated into the system using AD account the following scenarios are available:

- Active Directory account associated with one application user account
  In this case it is unreasonable to require any confirmation through the user interface – the application starts automatically without prompt for user credentials.
- Active Directory account associated with many application user accounts

FDBA supports one AD account to be associated with many application user accounts. In this case the user is navigated to login screen from where the user selects with which identity to perform login. Example of AD account associated with 2 application users.

Figure 1.

- Active Directory account associated with application user(s) and impersonation is available
  FDBA also supports users to impersonate and log on to the system on behalf of other users. User can impersonate if it has General permission. General Permissions in FDBA define access over functionality, which is globally available in the system [1]. In order to support impersonation when such a permission is available, user should choose whether to authenticate as yourself or as another user. To use impersonation only a valid username is required to be passed.

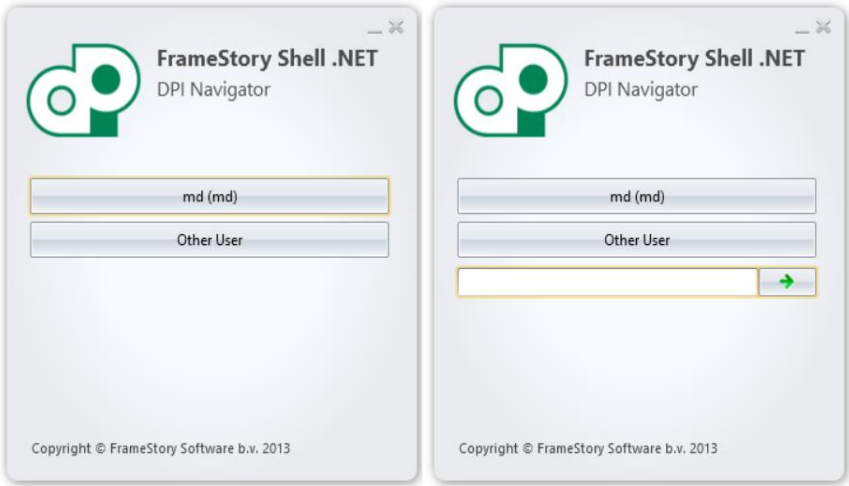

Figure 2.

4. Conclusion

This paper has described the functional requirements architecture and implementation of an alternative method for user authentication via active directory as a standard functionality to the Framework for Distributed Business Applications. This approach provides easier secure user`s access to applications developed by FDBA. In future, we well design and implement user authentication to work with another trusted OAuth Providers like Google or Microsoft.

Acknowledgements

This work is partially supported by the FP17-FMI-008 project of the Scientific Fund of the University of Plovdiv “Paisii Hilendarski”, Bulgaria.

References

[1] Pavlov, N. and M. Dobreva, Security Policies in a Framework for Distributed Business Applications, *MIDOC 2015*, Doctoral Conference in Mathematics and Informatics, MIDOC 2015, October 15-18, 2015, Sofia, ISBN 978-954-07-4186-4, pp. 36-43.

[2] Securing Services https://docs.microsoft.com/en-us/dotnet/framework/wcf/securing-services, retrieved on December 2017

[3] ServiceSecurityContext Class https://msdn.microsoft.com/en-us/library/system.servicemodel.servicesecuritycontext(v=vs.110).aspx retrieved on January 2018.

[4] Pavlov N., *Object-Oriented Framework for Development of Distributed Business Applications*, Ph.D. Thesis, Plovdiv University, Plovdiv, Bulgaria, 2011, (in Bulgarian).

[5] Top 5 Authentication trends in 2017 https://www.rsa.com/en-us/blog/2017-09/top-5-authentication-trends-in-2017, retrieved on December 2017

[6] Overview of Authentication and Authorization Technologies and Solution End States, https://technet.microsoft.com/en-us/library/bb463152.aspx?f=255&MSPPError=-2147217396, retrieved on January 2018

Faculty of Mathematics and Informatics,
Plovdiv University
236 Bulgaria Blvd, Plovdiv 4003, Bulgaria
E-mails: maria.d.dobreva@gmail.com, assen@uni-plovdiv.bg,
nikolayp@uni-plovdiv.bg, angelg@uni-plovdiv.bg

УДОСТОВЕРЯВАНЕ НА ПОТРЕБИТЕЛИ В РАМКА ЗА РАЗПРЕДЕЛЕНИ ОБЕКТНО-ОРИЕНТИРАНИ ПРИЛОЖЕНИЯ С WINDOWS ACTIVE DIRECTORY

Мария Добрева, Николай Павлов, Асен Рахнев, Ангел Голев

Резюме: В тази статия е описан механизъм за удостоверяване, разработен като част от рамката за разпределени бизнес приложения – FDBA. Представени са основните функционални изисквания и тяхната реализация. Този подход за удостоверяване на самоличност взаимодейства с услугите на Active Directory Domain, което е препоръчителна технология за съхраняване на информация на самоличност в рамките на дадена организация. Основната характеристика е подобрената сигурност и по-ефективният процес за вход в системата.

Ключови думи: автентикация, активна директория, сигурност, FDBA