

Re: Login Security for Intranet/Internet application

Source:

<http://www.derkeiler.com/Newsgroups/microsoft.public.dotnet.framework.aspnet.security/2007-04/msg00048.html>

- *From:* "Joe Kaplan" <joseph.e.kaplan@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 18 Apr 2007 11:43:03 -0500
-

You are building what is often called an "extranet" scenario from the identity perspective. There are a bunch of different ways to build these types of things and a lot of the decisions depend on your specific requirements. It is a pretty big topic and probably too broad to fit nicely into a newsgroup post, but here are some high level thoughts:

- You need to decide where the external identities will be stored and how they will be provisioned. For example, if you can provision them in your internal AD in a secure way, then this type of app isn't very different from a standard intranet app. If you need an alternate identity store, then the integration is potentially more complicated.
- Typically, for extranet scenarios you need to provide forms-based login or HTTP Basic authentication with SSL, as you need a logon method that supports plaintext credentials and works over the public internet securely. However, you may also want to support IWA authentication for internal users, which means you may need multiple authentication methods to the application.
- The design of the application itself may drive some of your other decisions. For example, if the application depends on Windows security (uses Windows security tokens for authentication/authorization), then you need a way to get a Windows security context for your external users. This is harder to do with forms-based authentication and complicates things for you. Some app platforms make specific assumptions about how identity is integrated and may complicate your decision (SharePoint V1 and V2 require Windows identities for example).

Microsoft's ADFS (Active Directory Federation Services) provides a nice platform for building these types of apps. ADFS allows you to integrate identities from multiple identity stores and different organizations and build robust ASP.NET apps on top of that with a fair amount of flexibility. It can support all of the points I discussed above. However, it isn't necessarily an easy thing to get up and running. It does give you a strategic platform that you can use to host additional services on top of though, so it may be worth looking at if you think you might do these types of things in the future.

Best of luck!

Joe K.

Re: Login Security for Intranet/Internet application

Joe Kaplan—MS MVP Directory Services Programming
Co—author of "The .NET Developer's Guide to Directory Services Programming"
<http://www.directoryprogramming.net>

"GSwan" <GSwan@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
<news:6597134B-13B2-4C93-B6C3-3FA50D11C202@xxxxxxxxxxxxxxxxxxxx>

Hi All,

I'm really no expert whatsoever when it comes to security in dotnet and have a question about setting up login security to a web application we are building.

The application will be accessible to mainly users within the company but there are also a couple of users that access the system externally and are not on the network.

I'd like to be able to use the active directory as the main means of logging into the system but i also need to ensure users not on the active directory can login too. Once logged in i need specific users to be members of specific roles to allow them access to various features in the application.

Please could someone provide me with ideas on how best to do this. All help is greatly appreciated.

Many thanks in advance,

Grant