

Re: Storing Connection String

Source:

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.adonet/2007-01/msg00082.html>

- *From:* "William \ (Bill) Vaughn" <billvaRemoveThis@xxxxxxxxxxx>
 - *Date:* Wed, 3 Jan 2007 10:41:45 -0800
-

Ah, if the credentials you use for your application can only execute selected (a few, specific) stored procedures (or views), the security is not compromised to that great of an extent. SSPI security is more expensive to manage in that each group (assuming users are members of groups) must also be maintained independently as the users come and go. The same rights must also be assigned to the groups. See Chapter 9 for more information.

--

William (Bill) Vaughn
Author, Mentor, Consultant
Microsoft MVP
INETA Speaker
www.betav.com/blog/billva
www.betav.com

Please reply only to the newsgroup so that others can benefit.
This posting is provided "AS IS" with no warranties, and confers no rights.

Visit www.hitchhikerguides.net to get more information on my latest book:
Hitchhiker's Guide to Visual Studio and SQL Server (7th Edition)
and Hitchhiker's Guide to SQL Server 2005 Compact Edition (EBook)

"Miha Markic [MVP C#]" <miha at rthand com> wrote in message
news:uWdSo6wLHHA.4712@xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Hi John,

"John Stivenson" <JohnStivenson@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in
message news:911A0572-76CC-4C3E-ADAA-85DC0E6215A2@xxxxxxxxxxxxxxxxxxxx

It's a desktop application.

I don't want to use the integrated security because I don't know in which
environment the application will be used.

My idea is to have just one database user whose username and password
would

Re: Storing Connection String

be hard-coded in the application. The connection string would be always the same (except server name, which is stored in config file or registry). The authentication would be application-managed (storing usernames/passwords in the database).

I hope you understand that this is very very weak protection. And a very problematic one. Since you have only one database connection credentials it means that this credentials can do everything (that application can do) to the database. Which means that if an user get hold of connection string he/she can issue sql statements at his/her will to the database – and getting hold of such connection string is not hard. Anyway, in the given context I would encrypt username & password and put them in config file (in case they change). Encryption key might be a certificate stored in windows certificate store. As per database I would use only stored procedures (and maybe views) to and deny access to tables (to maintain integrity and to protect sensitive data if any).

Where in code could I store the connection string in order to be accessible from everywhere (table adapters in several datasets and various command objects)?

In a static property.

Btw, how do I implement separate data tier?

You create a separate assembly which resides on the server and does database operations. Front end communicates with this assembly remotely (using remoting, WCF, web services or whatever) and sends datasets (or any other form of data – but doesn't issue any sql statements) forth and back.

—

Miha Markic [MVP C#, INETA Country Leader for Slovenia]
RightHand .NET consulting & development www.rthand.com
Blog: http://cs.rthand.com/blogs/blog_with_righthand/