

Re: Identity Column

Source:

<http://www.tech-archive.net/Archive/SQL-Server/microsoft.public.sqlserver.programming/2009-06/msg01003.html>

- *From:* "Tony Rogerson" <tonyroger@xxxxxxxx>
 - *Date:* Mon, 15 Jun 2009 16:31:42 +0100
-

You didn't answer my question and again have totally missed the security hole your proposed method has.

So, the end use is using Crystal Reports – where is the magic?

The user will connect using Active Directory (kerberos) from their desktop to the database server or do please explain the magic....

secure tunnels, protocols are just that – encryption of the comms traffic from the client to the database server.

Using stored procedures you permission on the stored proc only; the user can only execute the stored procedure with the parameters defined, there is no select * from [users] to get all the information in your database.

From your answer (lack of understanding of connectivity, how you permission

proc execution) it really does sound like you aren't that much of a Microsoft SQL Server guy afterall; what is it – Oracle? DB2?

Nesting views is not a way forward and I agree just complicates everything.

Sorry Daniel – try again....

"sqlguru" <sqlguru@xxxxxxxx> wrote in message
news:7bea3a7f-eedf-4b33-9eb5-2276ad02bd8f@xx
On Jun 15, 10:18 am, "Tony Rogerson" <tonyroger...@xxxxxxxx> wrote:

lets recap because you have totally missed the point which is the fact that any user can just strike up and connect to your database server – a couple of months ago a very widely effecting virus took advantage of EXACTLY how you recommend people code.

i think you are heading in the right direction by stating "the end user SHOULD NOT be "creating...."

given you have followed best practice and the middle tier doesn't use a single sign on and that each individual user correctly authenticates with

Re: Identity Column

server hardening or lockdowns so they resort to 1980s standards. You're better off powering down your database servers.

Tony, are you aware of FIPS standards? I think not. Your definition of security applies to small business, not enterprises. You cannot use Excel and connect to a database server, ever heard of secure tunnels and other secure protocols? Why would a non-developer (aka end user) have secure tunnel access? Do you actually give out the database password to your end-users, Tony "Randy" Rogerson?

Also, let's say we use stored procedures. What is preventing a developer/dba (there are hybrids right?) from bypassing all the stored procedures? Again, your lack of experience and working with Access constantly is showing.

Usually, most database structure changes require application changes at some point. Sure you can use views on top of views to the nth-degree causing mass confusion in documentation. Well, go work on your access applications, the real developers/dbas are busy.

.