

Re: Protect exe code against being decompiled

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2003-08/0758.html>

From: Chris Jackson (chrisj_at_mvps.org)

Date: 08/06/03

Date: Wed, 6 Aug 2003 12:15:28 -0400

How is this application implemented? You can use the crypto API, but cryptography is not always the solution. I mean, if the user account under which you intend to encrypt your data has the information necessary to encrypt it (the private key) then it has what it needs to unencrypt it to send it, and you are no safer than you are before. So, you now have to figure out how to keep secure. You could have an application where you have an administrative install that encrypts the password. However, then you will have to decrypt it in order to send it over the wire ... decrypted. Still no good.

The point here is this: never, ever design an application that has to send plain text passwords if somebody obtaining these passwords would compromise your infrastructure. Use stronger credentials. Set up a domain, and assign people to roles. Give those roles appropriate permissions. The authentication you pass will be encrypted and unreadable. Don't try to write your own crypto code. Leverage your infrastructure. If the end result is that you have to decrypt and send a plain text password, then you are not secure. If you have users malicious enough to decompile code, then you have users malicious enough to sniff packets.

--

Chris Jackson
Software Engineer
Microsoft MVP - Windows XP
Windows XP Associate Expert

--

"Alexander Wolff" <awolff@concepto.com.uy> wrote in message news:0d6a01c35b69\$9d026760\$a601280a@phx.gbl...

> Hi!

> I would like to know your opinion near the following
> problem:

> I have a SQL Server 2000 application that uses
> a "application role" to activate de user permissions. To do
> this, the Application call a stored procedure named

>

> "set_approle" and a password is specified in the
> parameters list.

> The use of this application role enhances security
> because users can't run anauthorized executables.

> Well but..even so, a malicious user can decompile the
> executable file, obtain the application role password, and

microsoft.public.security: Re: Protect exe code against being decompiled

> this person can do all..
> Somebody knows some tool to encrypt an EXE file of such
> form that the same one is continued being able to execute
> but that simultaneously the EXE cannot be decompiled
> easily?
>
> Also other ideas to protect that a user can obtain the
> password through the code of the EXE are welcomes!
>
> greetings,
> alexander
>