

# .Net Remoting and Stored Usernames and Passwords

---

*Source:*

<http://www.tech-archive.net/Archive/DotNet/microsoft.public.dotnet.framework.remoting/2006-04/msg00040.html>

---

- *From:* [cindy.fisher@xxxxxxxxxxxxxxxxxxxxx](mailto:cindy.fisher@xxxxxxxxxxxxxxxxxxxxx)
  - *Date:* 11 Apr 2006 12:57:19 -0700
- 

Does anyone know if this is a bug or intended behavior by Microsoft?

Apparently, entries in "stored usernames and passwords" (which is enabled by default when you install the OS) overrides the user's security credentials when a .Net Remoting call is made to a machine that has an entry in the list. This a HUGE security breach and a potential nightmare for software developers using .Net Remoting.

I cam across this while I was testing an application I wrote using .Net Remoting 2.0. The remote client kept getting access denied on the remoting call and when I traced it I saw that I was coming into the server as a different user than the one logged onto my client machine. I spent a couple of days trying to figure out how this could be and then I learned about "stored usernames and passwords". It was using security credentials that were stored and the password had expired. This is impersonation without the software intending to impersonate!

Example: A user of your software attempts to perform a task on your application that does Remoting. In the past they have made a remote connection to the machine that hosts the remoting server. The credentials they used to make the remote connection are no longer valid (account was deleted, password changed, etc.) so the task fails because, unlike what is expected, the credentials of the process owner are not passed through to the server but instead the cached credentials that were never considered are used.

This is a serious security violation. Has anyone else come across this. Is Microsoft going to change this behavior?

Cindy