When people ask for security holes as features: Stealing passwords

devblogs.microsoft.com/oldnewthing/20050504-52

May 4, 2005

Raymond Chen

Sometimes people ask for features that are such blatant security holes I don't know what they were thinking.

> Is there a way to get the current user's password? I have a program that does some stuff, then reboots the system, and I want to have the current user's password so I can log that user back in when I'm done, then my program can resume its operation.

(Sometimes they don't bother explaining why they need the user's password; they just ask for it.) Imagine the fantastic security hole if this were possible. Anybody could write a program that steals your password **without even having to trick you into typing it**. They would just call the imaginary `GetPasswordOfCurrentUser` function and bingo! they have your password. For another angle on credential-stealing, read Larry Osterman's discussion of why delegation doesn't work over the network. Even if you didn't want the password itself but merely some sort of "cookie" that could be used to log the user on later, you still have a security hole. Let's call this imaginary function `GetPasswordCookieOfCurrentUser`; it returns a "cookie" that can be used to log the user on instead of using their password.

This is just a thinly-disguised `GetPasswordOfCurrentUser` because that "cookie" is **equivalent to a password**. Log on with the cookie and you are now that person.

Raymond Chen

Follow