Password encryption in Internet Explorer 10

Passcape Software

1 Password encryption in Internet Explorer 10

In connection with the upcoming release of Windows 8 and Internet Explorer 10, we start getting more questions on the safety of storing passwords in the new version of Internet Explorer. So, we have decided to give this matter some attention in our blog.

We have repeatedly expressed our opinion that the password protection in the new version of Internet Explorer will be worse, as the mechanism for storing passwords has changed. Why has the new protection algorithm become more vulnerable? Let's figure it out.

Passwords to websites in Internet Explorer 7-9 were stored in the registry and encrypted with user's DPAPI. But the protection was implemented in a very clever way; the encryption key was comprised of the source URL address. After that the URL of the website was wiped out from the system.

Let's consider an example to make it a bit clearer. For example, you have opened some website, registered with it, entered your password and saved it (or have the Auto Save Passwords setting enabled.) While saving the password, Internet Explorer (7, 8 or 9) encrypts it using DPAPI. For the encryption key it uses the original URL of the web page. Then the encrypted password is written into the registry, and the record on visiting the URL is deleted from the system.

Thus, the registry stores encrypted passwords, but it doesn't have the keys to decrypt them! We can get the encryption key only when we know the URL of the original website, i.e. when the resource is visited again. If a potential intruder steals the encrypted password from the registry, he will be unable to decrypt it (with all other limitations) until he gets the URL of the original website the record belongs to.

Quite smart and cunning, but the algorithm has not been patented by Microsoft, therefore, someone else must have already used it before :) Anyway, it no longer matters, as Internet Explorer 10 uses a different mechanism. All IE 10's passwords are now stored in Windows Vault, protected with the regular DPAPI, and can be easily recovered. At least, easier than in the previous three versions. Windows Vault is a new mechanism for private data storage, which is so lacking in Windows.

Unfortunately, the Vault in Windows 8 features somewhat reduced functionality compared to the previous version used in Windows 7. All private entries of a Vault user can be found in his profile. By default, that's the folder

C:\Users\<USER_NAME>\AppData\Local\Microsoft\Vault\<VAULT_UID>
where **<USER_NAME>** - the user name
<VAULT_UID> - Vault identifier. By default, **4BF4C442-9B8A-41A0-B380-DD4A704DDB28**.

Each IE10 password entry is presented by a file with the .**vcrd** (Vault Credential) extension; the encryption key is stored in the same folder.

The new version of Internet Explorer Password Recovery can decrypt Internet Explorer 10 passwords both in online and offline modes. I.e., you will be able to recover Internet Explorer passwords even from unbootable PC. IE 10's passwords of the currently logged on user are decrypted instantly without any restrictions or limitations.

So, the Internet Explorer 10 password protection is just another piece of cake. The passwords can be decrypted approximately just as easily as Google Chrome ones. The best is the enemy of the good.