

## Re: A service and WTS

**Source:**

<http://www.tech-archive.net/Archive/Development/microsoft.public.development.device.drivers/2004-02/1145.html>

---

**From:** Maxim S. Shatskih (*maxim\_at\_storagecraft.com*)

**Date:** 02/20/04

Date: Fri, 20 Feb 2004 21:17:59 +0300

I would suggest you to read a great book on such (and other) cases. The book written by Microsoft's David LeBlank and Michael Howard and is called "Writing Secure Code".

ISBN 0-7356-1722-8

> *I need some user mode information in my driver before any user logs on, so that'll be a service.*

Sorry. The

– "I need some user mode information"

is one thing. But:

– "I need some information from the user input"

is another thing.

What of these two do you need? If second – then sorry, your driver will be either defunct will the user will log on, or will run in some default mode.

After the user will log on, it will run some UI app, which will call the necessary IOCTLs in your driver.

If first – then why having UI in the service?

> *What's so wrong to impersonate a logged-on user and interact with the user from a service directly?*

A potential security hole. First of all, the window manager is unprotected at all. Some malicious app will just do a couple of SendMessage to your edit control, causing buffer overrun in your code – which is the privileged code. This technique is well-described.

> *How an interaction thru a proxy application started by HKLM\..\Run is any better?*

More protected. All points where the security boundary is crossed (from the app to the service) are listed and documented (in COM's .IDL file usually).

> *Is starting an application by CreateProcessAsUser from a service a bad thing*

> *as well?*

CreateProcessAsUser requires explicit password specification. Where do you want to keep the password?

In "c:\admin\_password.txt" file? Then yes, CreateProcessAsUser is bad :-)

In DPAPI or LSA secret? Then CreateProcessAsUser is OK.

> *Should CreateProcess from a service be banned?*

No for sure.

> *I am not sure here, do you mean a driver talks to a service via inverted*

> *call path?*

> *(requesting an info from a service by completing a previously pended IRP,*

> *and obtaining this information from the next IRP to pend?)*

Yes. Exactly so.

--

Maxim Shatskih, Windows DDK MVP

StorageCraft Corporation

maxim@storagecraft.com

<http://www.storagecraft.com>