

## Re: Windows XP security concerns

**Source:** <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2001-12/0033.html>

---

**From:** David LeBlanc ([dleblanc@MINDSPRING.COM](mailto:dleblanc@MINDSPRING.COM))

**Date:** 12/20/01

Date: Thu, 20 Dec 2001 00:20:30 -0800  
From: David LeBlanc <[dleblanc@MINDSPRING.COM](mailto:dleblanc@MINDSPRING.COM)>  
To: [NTBUGTRAO@LISTSERV.NTBUGTRAO.COM](mailto:NTBUGTRAO@LISTSERV.NTBUGTRAO.COM)

> -----Original Message-----

> From: Tomasz Polus

> Sent: Wednesday, December 19, 2001 8:52 AM

> I. Problem with account locking due to fast user switching

> 1. Set the account lockout threshold to 3 attempts.

> 2. Create 10 user accounts with user level privileges

> (User1 – User10).

> 3. Logon using User1 account.

> 4. Using fast user switching, logon using User2 account.

> 5. Use fast switching to change from User1 to User2 3 times.

> 6. Attempt to logon using User3 account.

So, you'd have to have several people standing around playing musical chairs in order to have this affect anyone in a real-world scenario.

> Even switching between *\_one\_* user (logging on and logging off

> using fast user switching) results in all accounts being locked out.

Setting account lockout in general is a bit of a nuisance which normally causes more trouble for the admins than anyone else (including the hackers).

> As you can see, Microsoft admitted this to be a problem and

> recommended

> not to use fast user switching in conjunction with Account Lockout.

> We see this as a significant limitation on the new feature,

> and/or a forced downgrading of security settings.

You think this is significant? I would grant you that there's room for us to have completely different opinions on this, but, IMHO, fast user switching is most useful in the home environment, where you're not likely to have lockouts set. This seems to be a rather contrived scenario.

NT-Bugtraq: Re: Windows XP security concerns

BTW, something many people are not aware of is that in XP, if an account does have a blank password you cannot log on anywhere except the local console. It is actually safer to have a blank password than a weak one (from the network at least).

- > *First, make sure the "Minimum password age" policy is set to*
- > *a value other than 0.*
- > *Now, supposing the user forgets his password before it's age expires,*
- > *he will not be able to reset it with the disk until the*
- > *password expires.*

So you're now complaining that the minimum password age setting actually works? I'm confused.

- > *3. Remote Desktop sends recently used username in plaintext*

I believe this is configurable. I know that I've seen kiosks where the last user name didn't show up. I'll have to check into how that can be done.

---

Delivery co-sponsored by VeriSign – The Internet Trust Company

---

Protect your servers with 128-bit SSL encryption!  
Get VeriSign's FREE guide, "Securing Your Web Site for Business." You will learn everything you need to know about using SSL to encrypt your e-commerce transactions for serious online security. Click here!  
<http://www.verisign.com/cgi-bin/go.cgi?a=n016065650057000>

---

- ***Previous message:*** Eric: "Re: Windows Critical Update"
- ***In reply to:*** Tomasz Polus: "Windows XP security concerns"
- ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]