

Re: XP Less Secure than 98 for Sharing Files

Source:

http://www.derkeiler.com/Newsgroups/microsoft.public.windowsxp.security_admin/2004-04/3575.html

From: cquirke (MVP Win9x) (cquirkenews_at_nospam.mvps.org)

Date: 04/29/04

Date: Thu, 29 Apr 2004 18:50:34 +0200

On Wed, 28 Apr 2004 10:13:25 -0400, "Lanwench [MVP - Exchange]"
>cquirke (MVP Win9x) wrote:

>Inline, submitted respectfully :-)
I'm an in-liner too <g>

>> Oh, XP can be as cumbersome as hell. Ever tried chasing up settings
>> across multiple user accounts, or had to go deep into NTFS's per-file
>> permissions to fiddle with those assigned to each file? Hm.

>There is indeed a learning curve here, but I just make sure I set up my
>folders & shares such that I don't have to bother with individual
>subfolder/file permissions. And I use groups, not users, to assign
>permissions.

Yep - hence my phrasing "can be" (i.e. not that it has to be - though
to get what the original poster wanted, it's more work).

>> Note that anything other than full admin rights in XP Home will mean
>> you lose the ability to control a number of settings in that account,
>> such as "show file name extensions" etc. Swap one risk for another.

>No, you can change your display settings in Folder Options without local
>admin rights...

>>> *HOW TO Set, View, Change, or Remove File and Folder Permissions*
>>> <http://support.microsoft.com/default.aspx?scid=kb;en-us;q308418>

That wasn't my mileage. I created a new account in Home, set it up
the way I wanted it, and then changed it from Admin to limited. All
my settings were gone; it was back to hidden files, hidden extensions
etc. which I consider dangerous, from a "safe hex" perspective. It
was also back to the dancing animations etc. too.

The link you gave points to an article about file and folder
permissions. This isn't the same topic, and requires NTFS; something
that IMO is not yet ready for consumerland prime time.

>> *Requires NTFS, which forces another trade-off; no maintenance OS,*
>> *can't formally scan for malware, limited data recovery.*

> *"maintenance OS" = ?*

Yep: Maintenance OS. Something that can:

- read the file system without writing to it at all
- run without running any code off the HD whatsoever
- run without needing any HD content to be sane
- run with a minimum of hardware useage

A maintenance OS is what you'd use to pull data off sick, at-risk hard drives, do "under anaesthetic" work on the OS without the OS mother-henning along, formally scan and manage malware, run diagnostics in the presence of flaky hardware, and perform data recovery and non-automated file system repair.

DOS mode was a fair maintenance OS for Win9x, and can still be useful for XP if NTFS is avoided.

> *And re malware - you can use any of the major tools I've used for*
> *spyware scanning on NTFS volumes - the software doesn't care.*

I use the term "malware" to refer to any malicious software, whether it's a virus, worm, RAT, or any of the commercial malware. As at April 2004, you can rely on informal (i.e. hosted by the infested OS) tools to manage commercial malware, because today's commercial malware has to "play nice" to pretend to be "proper" software.

Traditional malware (viruses, worms, RATs etc.) don't have to stay within those limits, and can exploit the opportunities that "air superiority" (i.e. being active when the av tries to take off) offers.

> *Re data recovery - NTFS is less prone to errors/fragmentation than FAT, by a*
> *long shot - and a) everyone needs to make regular backups regardless of*
> *format and b) there's always NTFSDOS if needed*

Summed up as "NTFS doesn't break, if it does break you can use a 3rd-party tool, and anyway let's blame the victim for not making backups" <g> These are familiar assertions, but let's do it again...

Firstly, the assertion that NTFS is "less prone to errors".

Certain types of data corruption happen below the level of abstraction of the OS and file system, e.g. failing HD, bad RAM that corrupts what is written to disk (or where it is written to disk), malware that writes directly to disk (see Witty if you think that's impossible in NTFS). In these cases, the type of file system can do nothing to avoid the problem. The only possible factors that can mitigate the results about 10% this way or that way are the amount of redundancy to guide repair, and the surface area of each vulnerable data element.

Most discussions on file system errors assume interruption of normal (sane) file operations as the only cause, and point to NTFS's transaction rollback as evidence that the problem is licked. MS's own documentation on transaction rollback is very clear on this: the feature does NOT protect/preserve user data, it is only concerned with the structural sanity of the file system.

The other issue that's mooted is NTFS's auto-fixing of bad clusters as they arise. This is similar to what modern HD firmware does anyway, and once again, what reduces support calls is not always what is best for preserving the user's data.

>From the above I conclude that NTFS is not only as open to many times of data loss as FATxx, but it is more likely to hide these crises from the user on a "kill, bury, deny" basis.

Secondly, the eternal mantra of "backup". There's a conundrum inherent in this concept:

- the backup must be recent enough not to lose any recent data
- the backup must predate whatever happened that ate the data

So even if the mythical backup worked, there would still be data lost, and thus an ongoing need for data recovery.

Thirdly, NTFSDOS. Have you ever used it?

The free version takes around 300k of conventional DOS memory and can't recurse the directory tree properly. F-Prot will run under it, but it will tell you it's "scanned the whole drive" after, say 100 files, because of the TSR's inability to traverse the tree properly.

The fee version shells the HD installation's own NTFS code. That's great for dispelling the FUD that surrounds NTFS (given that it's undocumented, subject to change, and tends to change even within SPs of the same NT version). But if that code is infected, your av scan isn't formal anymore, and if it's corrupted, who knows what happens next. I haven't tried it, but those factors (plus cost) put me off.

For cherry-picking data off sick NTFS, I use the non-TSR tool from www.NTFS.com (it's called ReadNTFS, AFAIK). Wieldy it is not, and there's no LFN preservation (as there would be if using Odi's LFN Tools to copy an entire FATxx volume from DOS mode).

*>> As it is, adding TCP/IP-only XP to an existing Win9x LAN can weaken
>> the security of that LAN, by forcing those PCs to use TCP/IP and thus
>> requiring them to open ports in the firewalls (if you know how to do
>> that and/or your firewall supports it) or running with no firewall.*

*>If you have TCP/IP loaded at all, regardless of NetBEUI, and have Internet
>access, you need a perimeter firewall, period. What needs to be opened
>(inbound) in a firewall for basic Internet connectivity? Nothing....and*

*>relying on individual software firewalls as your sole line of defense
>against the Internet is silly on a network.*

I see. So whereas we could use software firewalls quite effectively on a pure Win9x peer-to-peer LAN (as long as F&PS was being done on a protocol other than TCP/IP), we can't do that with XP, but that's OK because we should have bought a hardware firewall anyway. Hmm.

Not all LANs connect to the 'net through a router; that's what ICS is for, remember? Many LANs still use DUN, either via ICS or with each PC doing its own DUN. The latter's quite nice as it means there doesn't have to be TCP/IP on the LAN at all... until XP comes along.

*>> XP may be more secure in its own world, as long as you do everything
>> its way, and turn a blind eye to the additional risks it opens up.*

*>Additional risks being ? Win9x has *no* security to speak of – it was not
>designed with security in mind.*

Think "safety" not "security". Too many NT fans think consumerland works the same way as their internal, professionally-administered networks (or should do). The reality is that stand-alone consumers already know and use a different security model based on the concept of "home" as a physical location where safety can be assumed:

- if you sit in the Big Chair, you have full rights of access
- if you are outside on the Internet, you have zero right of access

That's a very good, easy to understand, and appropriate security model, and MS would do well to respect it – instead of foisting per-user stuff that needs an MSCE to administer properly.

Additional risks... OK:

- that wretched defective RPC service that can't be killed
- hidden admin shares exposing entire HD volumes
- plays poorly on peer-to-peer LANs, as noted
- can't simply password-protect LAN shares
- lower number of incoming connects (nuisance, not risk)

*>> But when required to operate in the same way as existing Win9x clients
>> on a peer-to-peer LAN, it has limitations:*

>> – poor support for anything other than TCP/IP

>Not so – you can install run NetBEUI, you can run IPX/SPX, as you wish.

The assertion's been made, and believe me, I tried. Neither the hidden-on-CD NetBEUI nor IPX would work with Win9x systems that were already happily LANning; eventually I had to make the whole LAN TCP/IP for XP's benefit, with all the risks that implied.

>> – dangerous hidden "admin" shares exposing the startup axis

>*Can be disabled, but as nobody ought to have full admin rights anywhere*
>*except those who really need it, this is moot as users can't access it.*

A few things:

- loss of settings in XP Home for anything lower than admin rights
- apps that require admin rights to work, even games
- exploits that drill right through rights limitations

Yes, I do disable these damnfool shares. Even the most basic post-OpaServ "safe hex" clue knows you don't provide full access to the startup axis, which is what these shares do – and with nice predictable names, too (so what if the names end in \$?)

>> – *limit of 5, not 10, incoming connects*

>*Not so for XP Pro. And personally if there are that many computers, I vote*
>*for a domain model anyway – peer to peer does not scale well and can be a*
>*nightmare to administer.*

XP Pro is not in the same price range as Win9x; in this respect, XP (and WinME) are steps backwards in value. In fact, the only Pro I've had to sell has been forced by this issue.

As to "nightmare to administer", well, that's why one wants to avoid the overblown baggage that NT carries. Tossing domain servers around just to set more than 5 users is a serious cost overrun.

>> *It's a case of "be reasonable, do it my way" – and depending on your*
>> *requirements and limitations, the result may be far riskier.*

>*Safe Hex applies regardless of version of OS (or OS in general) or disk*
>*format. :-)*

Yes, when you can apply it. If applied to XP, there wouldn't be any RPC service mooning the Internet, and we wouldn't have to care if was patched or not <g>

Now I like XP, but I'm not going to pretend it's all steps forward on all fronts. It needs a maintenance OS before NTFS is fit for use in all contexts; it needs user control over the prototype from which new accounts are created; it needs to respect user settings when dropping an account from admin rights; it needs an interactive file system checker such as Scandisk, and it needs ways to turn off and rip out a lot of risky functionalities that are superfluous for most consumers.

I'll keep pushing for those, while others tell me I should want something else <g>

>-- *Risk Management is the clue that asks:*
 "Why do I keep open buckets of petrol next to all the
 ashtrays in the lounge, when I don't even have a car?"

microsoft.public.windowsxp.security_admin: Re: XP Less Secure than 98 for Sharing Files

>-----