

## Re: Linux and security

**Source:** <http://www.derkeiler.com/Newsgroups/comp.os.linux.security/2003-07/0492.html>

---

**From:** Nico Kadel-Garcia ([nkadel\\_at\\_verizon.net](mailto:nkadel_at_verizon.net))

**Date:** 07/28/03

Date: Mon, 28 Jul 2003 12:35:40 GMT

Johannes Halmann wrote:

>>it's  
>>possible to examine what the code actually does. Also, because the  
>>underlying UNIX *\*style\** of priveleged users do critical things,  
>>unpriveleged users are not allowed was built in long before Microsoft  
>>stole VMS from DEC and created such features in NT, it's been hammered  
>>on and tested and refined.  
>  
>  
>hmm, *MAYBE* linux/unix are better designed than windows! i believe so, but  
>how could we know??  
>the point is not *WHEN* certain features came into being used but what the  
>situation is *RIGHT* now. the actual windows-systems have user-management and  
>with ACLs even much finer in granularity then for example linux!

I assume you're referring to the NTFS file system and its subtleties of user and group ownership. Unfortunately, it's neither well documented, well understood, nor even well used by a lot of vendor software. The result is that many users give their personal accounts administrative privileges, which deletes almost the entire point.

>the never-ending stream of exploits for windows is certainly a main reason  
>for worms and even viruses to prosper, but it is my firm belief, that in  
>most of the cases the user installs a virus by accident (and if it is by  
>using Internet Explorer against all warnings) and not so much the security  
>of the OS. all the OS is supposed to do, is encapsulate the users action in  
>order to protect other users from his doings. but how can a OS protect a  
>users files from himself?

Oy. In many cases, sure. But other common vulnerabilities, such as the default exporting of the "C:" drive as a share, the overly friendly auto-opening of email attachments by various default Windows clients, and the historically poor encryption of the SMB passwords for Windows logins are fairly deeply built into the system and are their own delightful source of vulnerabilities.

Under UNIX/Linux models, the privileges of the user to touch the system files are extremely restricted, so the ability to cleverly infect the OS is limited unless someone finds a local exploit. . Windows has never really gotten this right, despite their efforts to do so. This seems to be partly because such effort may reduce funky and saleable functionality, but partly because DOS just wasn't written that way to start with, and neither was VMS (the core of the NT operating system).

> *so, the spread of viruses increases with the stupidity and technical  
> ignorance of the users and is not so strongly correlated with the OS, code  
> review, ...*

Certainly the stupidity of the users is a huge factor, I agree. But when even competent and intelligent users cannot secure the OS due to the built-in vulnerabilities, such as some of the graphic display flaws that have been exposed in the past year and the built-in MS Word and Outlook and Explorer flaws, you're in deep trouble.

> *with worms it is another topic, but these use flaws in applications and  
> against that the OS can again do little.*

Point. But the OS can make its code available and actually follow its own API's, which Microsoft is famous for not following. Adding features and improving time to market are things that get your department resources and good performance reviews. Fixing the previous group's brain-dead security stupidities does not, so is not really a priority for their development teams.