

Re: Versioning file system

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2007-07/msg01457.html>

- *From:* Erik Mouw <mouw@xxxxxxxxxxxxx>
 - *Date:* Thu, 5 Jul 2007 19:55:31 +0200
-

On Wed, Jul 04, 2007 at 04:47:59PM -0400, Theodore Tso wrote:

On Wed, Jul 04, 2007 at 07:32:34PM +0200, Erik Mouw wrote:

(sorry for the late reply, just got back from holiday)

On Mon, Jun 18, 2007 at 01:29:56PM -0400, Theodore Tso wrote:

As I mentioned in my Linux.conf.au presentation a year and a half ago, the main use of Streams in Windows to date has been for system crackers to hide trojan horse code and rootkits so that system administrators couldn't find them. :-)

The only valid use of Streams in Windows I've seen was a virus checker that stored a hash of the file in a separate stream. Checking a file was a matter of rehashing it and comparing against the hash stored in the special hash data stream for that particular file.

And even that's not a valid use. All the virus would have to do is to infect the file, and then update the "special hash data stream". Why is it that when programmers are told about streams as a potential technology choice, it makes their thinking become fuzzy? :-)

I meant valid like "not used as malware". I agree a virus could recompute the hash and go unnoticed.

Erik

--

They're all fools. Don't worry. Darwin may be slow, but he'll eventually get them. -- Matthew Lammers in alt.sysadmin.recovery

Attachment: [signature.asc](#)

Re: Versioning file system

Description: Digital signature