

Re: How will PatchGuard change kernel programming?

Source:

<http://www.tech-archive.net/Archive/Development/microsoft.public.win32.programmer.kernel/2006-10/msg00270.htm>

- *From:* "David J. Craig" <Dave@xxxxxxxxxxxxxx>
 - *Date:* Sat, 14 Oct 2006 18:36:10 -0700
-

I don't agree that McAfee has been avoiding or even inhibiting Microsoft from producing APIs to permit better add-on security products. There is a much improved registry monitoring interface. There is also a much improved file system filter stack via the minifilter model that solves a lot of problems that gave so many people using old source code versions of filemon so many problems. Just the rename interface is so much nicer than the old version that had so many variations that it was a major effort just to test them.

One decision I dislike immensely is the change that requires the system partition be NTFS. I want my FAT32. I can repair FAT32 using WinHex or even diskedit. There is no document that provides the same detail for NTFS and it keeps changing. One item I wish was better implemented is the one used to detect the initial program in a process. There is a limit on the number of users permitted and some data is not available when needed. What is the full name? Has the OS verified the crc (linker generated) and how about the digital signature – is it valid, is the certificate upon which it is based been revoked? Are there any injectors trying to insert a DLL in a new process? Are there fake system DLLs in locations other than the system directories being loaded into a process?

I see that since Microsoft hasn't released a hypervisor as a part of the standard OS, there will be many versions from VMWare, Xen, Virtual PC, etc. and many some from security companies such as Green Border. That will make getting a high quality VM such as IBM's VM for their mainframes very difficult. It will be resolved much sooner for servers, but may take several years for the consumer.

Some of the problem with security companies is that Microsoft has become a competitor. How can they ask for something without giving away their trade secrets to a competitor? Open source does have some advantages, except for how we code slingers make a living. Even Apple has an open source OS as the foundation. In the mainframe days, major customers had access to the OS source code so enhancements and changes could be done easily.

"Don Burn" <burn@xxxxxxxxxxxxxx> wrote in message <news:OjpKCE97GHA.3760@xxxxxxxxxxxxxx>

Re: How will PatchGuard change kernel programming?

You got it wrong, they have continued to say that PatchGuard will be kept and if gotten around they will fix the hole. Note: the quote from the press conference referred to in the article:

"Some security vendors expressed some concerns to the Commission, and to us, that they had previously used access to the kernel to facilitate features in their own product and that they would no longer be able to do so. We were concerned that it would be a mistake for the future of computers if PatchGuard were to be removed or eliminated. We devised a new engineering approach that will create and extend new kernel level APIs so that PatchGuard will be retained, the security of the kernel will be protected, and yet security vendors will have an opportunity to meet their needs through these kernel level API extensions. We felt that this was again the right kind of solution that meets the needs and obligations that we have under competition law, whilst also meeting the needs of computer users around the world."

That is new kernel API's, now the irony is that some of us have been arguing for additional API's to achieve some capabilities, and some of the AV guys including McAfee and Symantec refused to get behind some of this. Now that their crappy product is being cut off from hooking, do we finally get the capabilities.

Actually, the VT stuff is a bigger cause for concern, because the chip vendors did not consider security in their current efforts, so there is no way for an OS to determine it is hosted, and go "warning I wasn't in a virtual environment now I am, did you install a hypervisor?"

--

Don Burn (MVP, Windows DDK)
Windows 2k/XP/2k3 Filesystem and Driver Consulting
<http://www.windrvr.com>
Remove StopSpam from the email to reply

"David J. Craig" <Dave@xxxxxxxxxxxxxx> wrote in message
<news:OmuC2i77GHA.1188@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

I just read at:
<http://rss.slashdot.org/~r/slashdot/eqWf/~3/37127625/article.pl> that Microsoft has decided to allow PatchGuard to be bypassed. Also, the security center can be turned off by other security products so that they can choose the method of interfacing with the user. I think in corporate environments those popups should never be displayed if the domain admin so chooses, but a notification sent to IT so they can correct the problem. It permits IT to see developing problems that can be fixed for everyone at once and not have time wasted by hundreds or thousands of employees.

I see why the system needs to be locked down. Recent reviews of OneCare indicate it is not that good at detecting viruses nor is their speed of

Re: How will PatchGuard change kernel programming?

updating close to some of the other major players. Most of the major antivirus companies update every few minutes or hours depending upon what is seen on the internet.

BTW, the last I heard there are techniques to permit PatchGuard to be bypassed. Until all computers have been upgraded to the newest processors with hardware VT, I don't think many attacks can be defeated. Even then, it will probably not be a perfect solution.