

Re: The Developer Implications of Windows XP SP2

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-11/0050.html>

From: Maxim S. Shatskih (*maxim_at_STORAGECRAFT.COM*)

Date: 11/16/03

Date: Sun, 16 Nov 2003 19:56:42 +0300

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

> *Such a hardware feature has been introduced recently by intel, namely in the
> 80286 microprocessor. All Windows versions I am aware of already contain
> provisions to *circumvent* this feature!*

Yes, this is segmentation, and I can even recommend a way for MS to fix this in NT OSes:

- invent a "boundary" in user mode address spaces, like - first 1.5 GB of virtual addresses are "below" the boundary, while the last .5 GB is "above" the boundary.
- the boundary can be per-process and dynamic.
- the user-mode stacks are always located above the boundary, while the rest of user mode stuff - including mapped DLL images even for system DLLs - are below.
- the user-mode CS segment descriptor has the length which is up to the boundary.

This makes the user stacks non-executable. Implementation would be trivial - allocate user stacks (in CreateThread and CreateProcess) only above the boundary, and all other memory - including the mapped files - below the boundary. Then patch the CS descriptor in the GDT table in the kernel. If the boundary is per-process or dynamic - then SwapContext must do this.

Then - and this is the main point while only MS can do this - rebase the system DLLs to be loaded below the boundary. The system DLLs are shipped without the relocation tables, so, the 3rd parties cannot implement this.

Surely there is still a window for attacks, like when the exploit will patch the call parameters to be "tftp.exe" and so on, and the return address to be kernel32!CreateProcessA. This will not require off-stack execution. Anyway, having TFTP.EXE in base OS distro, and protected by SFP (!) so the users cannot rename it - is yet another source of holes.

Maxim Shatskih, Windows DDK MVP
StorageCraft Corporation
maxim@storagecraft.com

NT-Bugtraq: Re: The Developer Implications of Windows XP SP2

<http://www.storagecraft.com>

Marcus Ranum's new book "The Myth of Homeland Security" is now out and is available from <http://www.amazon.com/ranum> In this hard-hitting review of the homeland security business, Ranum shows us how the problem is vastly harder than it's being made to sound, and how special interests, butt covering, and bureaucracy are threatening to derail any chance of making progress.
