

## Re: thoughts on kernel security issues

**Source:** <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-01/7606.html>

---

**From:** Bill Davidsen ([davidsen\\_at\\_tmr.com](mailto:davidsen_at_tmr.com))

**Date:** 01/25/05

Date: Tue, 25 Jan 2005 10:05:47 -0500

To: [Valdis.Kletnieks@vt.edu](mailto:Valdis.Kletnieks@vt.edu)

[Valdis.Kletnieks@vt.edu](mailto:Valdis.Kletnieks@vt.edu) wrote:

> *On Wed, 19 Jan 2005 13:50:23 EST, John Richard Moser said:*

>

>> *Arjan van de Ven wrote:*

>>

>>> *Split-out portions of PaX (and of ES) don't make sense.*

>>>

>>> *they do. Somewhat.*

>

>

>> *They do to "break all existing exploits" until someone takes 5 minutes*

>> *to make a slight alteration. Only the reciprocating combinations of*

>> *each protection can protect the others from being exploited and create a*

>> *truly secure environment.*

>

>

> *OK, for those who tuned in late to the telecast of "Kernel Development Process  
> for Newbies":*

>

> *It \*DOES NOT MATTER\* that PaX and ES "don't make sense" split out into 5 or*

> *6 pieces. We merge in stuff \*ALL THE TIME\* in 20 or 30 chunks, where it*

> *doesn't make any real sense unless all 20 or 30 go in. Just today, there was*

> *a 29-patch monster replacing kexec, and another 12-patcher replacing something*

> *else. And I don't think anybody claims that many of those 29 patches stand*

> *totally by themselves. You install 25 of them, you probably don't have a working*

> *kexec, which is the goal of the patch series.*

>

> *The point is that \*each\* of those 29 patches is small and self-contained enough*

> *to review for breakage of current stuff, elegance of coding, and so on. Now*

> *let's look at grsecurity:*

>

> *% wc grsecurity-2.1.0-2.6.10-200501071049.patch*

> *23539 89686 700414 grsecurity-2.1.0-2.6.10-200501071049.patch*

>

> *700K. In one patch. If PAX is available for 2.6.10 by itself, it certainly*

> *hasn't been posted to <http://pax.grsecurity.net> - that's still showing a 2.6.7*

> *patch. But even there, that's a single monolithic 280K patch. That's never*

## Linux-Kernel: Re: thoughts on kernel security issues

> going to get merged, simply because *\*nobody\** can review a single patch that big.  
>  
> Now look at <http://www.kernel.org/pub/linux/kernel/people/arjan/execshield/>.  
> 4 separate hunks, the biggest is under 7K. Other chunks of similar size  
> for non-exec stack and NX support are already merged.  
>  
> And why were they merged? Because they showed up in 4-8K chunks.  
>  
>  
>> Split-out portions of PaX (and of ES) don't make sense. ASLR can be  
>> evaded pretty easily: inject code, read %efp, find the GOT, read  
>> addresses. The NX protections can be evaded by using ret2libc. on x86,  
>> you need emulation to make an NX bit or the NX protections are useless.  
>> So every part prevents every other part from being pushed gently aside.  
>  
>  
> Right. But if you *\*submit\** them as "a chunk to add x86 emulation of an NX  
> bit", "a chunk to add ASLR", "a chunk to add NX", "a chunk to do FOO with the  
> vsyscall page", and so on, they might actually have a snowball's chance of  
> being included.  
>  
> If nothing else, the fact they're posted as different patches means each can be  
> used as the anchor for a thread discussing the merits of *\*that\** patch. Adrian  
> Bunk has been submitting patches for the last several weeks which probably  
> total *\*well\** over the size of the PAX patch. And since they show up as  
> separate patches, the non-controversial ones can sail by, the ALSA crew can  
> comment when he hits an ALSA module, the filesystem people can comment when he  
> hits one of their files, and so on.

Unfortunately if A depends on B to work at all, you have to put A and B in as a package. There is no really good way (AFAIK) to submit a bunch of patches and say "if any one of these is rejected the whole thing should be ignored." While akpm and others do a great job of noting related parts, that's not the ideal solution. Ideally the monolithic patch should be checked in parts by the people you mention, or there should be an "all or nothing" protocol better than dropping the responsibility on the maintainer.

Adding and vetting things in stages works only when the parts work independently, and that's not always the case. You don't leap vast chasms in small cautious steps.

--  
bill davidsen <davidsen@tmr.com>  
CTO TMR Associates, Inc  
Doing interesting things with small computers since 1979  
-

To unsubscribe from this list: send the line "unsubscribe linux-kernel" in the body of a message to majordomo@vger.kernel.org  
More majordomo info at <http://vger.kernel.org/majordomo-info.html>  
Please read the FAQ at <http://www.tux.org/lkml/>