

Re: Memory Management during Program Loading

Source: <http://linux.derkeiler.com/Mailing-Lists/Kernel/2005-06/7533.html>

Valdis.Kletnieks_at_vt.edu

Date: 06/28/05

To: Sreeni <sreeni.pulich@gmail.com>
Date: Tue, 28 Jun 2005 14:58:02 -0400

On Tue, 28 Jun 2005 14:12:43 EDT, Sreeni said:

> *We have a "Bus Monitor hardware" which monitors and polices the bus at
> the specified physical address.*

What does this hardware do, exactly, in addition to the usual memory-protection capabilities of the main processor? I suspect the answer to your query will depend largely on what your monitor does, exactly, and what capabilities it has, and what threat model you're trying to secure against....

> *Basically we need to run "secure" program under the supervision of the
> Bus monitor hardware.*

Is there an actual "threat model" here, as in "the attacker might try XYZ, and this monitor is a defense because it does ABC, rendering XYZ ineffective"?

I'm unclear on how the monitor can provide any **real** security when it quite likely does **not** have access to the entire state of the system (in particular, if there's a security-critical value that's still in a CPU register or L1 cache line...)

> *Kernel can see the "secure" memory region, and kernel is responsible for enabling
> the "Bus monitor Hardware".*

The problem is that you're using an unsecured kernel to initially load the secure memory region – so an attacker is free to load broken code into the secure area. The usual "trusted system" solution for this is to ensure that the kernel **also** runs inside the tamper-proof environment....

Or is the **real** question here "We have a bus analyzer that can't see all of the physical memory, so we need the code we're interested in to be in the part of physical memory it can see"? If that's the case, totally different answers will probably apply (as we don't have to do things in a "secure" manner, we just need to get the right pages in the right frames before the analyzer is turned on).....

Linux-Kernel: Re: Memory Management during Program Loading

—

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/>

- application/pgp-signature attachment: [stored](#)