Subject: Re: [patch -mm 08/17] nsproxy: add hashtable
Posted by serue on Wed, 20 Dec 2006 06:12:03 GMT
View Forum Message <> Reply to Message

Quoting Herbert Poetzl (herbert@13thfloor.at):
> On Mon, Dec 11, 2006 at 04:01:15PM -0600, Serge E. Hallyn wrote:
> > Quoting Eric W. Biederman (ebiederm@xmission.com):
> > > "Serge E. Hallyn" <serue@us.ibm.com> writes:
> > >
> > > > Quoting Eric W. Biederman (ebiederm@xmission.com):
> > > >
> > > > > Yeah, that occurred to me, but it doesn't seem like we can possibly make
> > > > > sufficient guarantees to the client to make this worthwhile.
> > > > >
> > > > > I'd love to be wrong about that, but if nothing else we can't prove to
> > > > > the client that they're running on an unhacked host. So the host admin
> > > > > will always have to be trusted.
> > > >
> > > > To some extent that is true. Although all security models we have
> > > > currently fall down if you hack the kernel, or run your kernel
> > > > in a hacked virtual environment. It would be nice if under normal
> > > > conditions you could mount an encrypted filesystem only in a container
> > > > and not have concerns of those files escaping.
> > >
> > > Hmm, well perhaps I'm being overly pessimistic - IBM research did have a
> > > demo based on TPM of remote attestation, which may be usable for
> > > ensuring that you're connecting to a service on your virtual machine on
> > > a certain (unhacked) kernel on particular hardware, in which case what
> > > you're talking about may be possible - given a stringent initial
> > > environment (i.e. not the 'gimme $20/month for a hosted partition in
> > > arizona' environment).
> >
> > interesting, how would you _ensure_ from inside
> > such an environment, that nobody tampered with
> > the kernel you are running on?

Sorry, took awhile to find the best reference, but I guess this would be
it:

http://domino.research.ibm.com/library/cyberdig.nsf/1e4115aea78b6e7c85256b360066f0d4/459e9a2b1f668aee85256f330067589f

Another description is

http://domino.research.ibm.com/comm/research_people.nsf/pages/sailer.ima.html

I guess it was in 2004 that they did a demo of remote attestion at the
RSA conference, as described in the third to last paragraph in

http://cio.co.nz/cio.nsf/0/03943645293DB008CC256E47005D8EA2?OpenDocument
and in
http://domino.research.ibm.com/comm/pr.nsf/pages/news.20040218_linux.html

-serge

_____
Containers mailing list
Containers@lists.osdl.org
https://lists.osdl.org/mailman/listinfo/containers