

Re: IP Level Encryption (kind of long)

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-12/1084.html>

From: David Wagner (*daw_at_taverner.cs.berkeley.edu*)

Date: 12/17/03

Date: Wed, 17 Dec 2003 10:43:33 +0000 (UTC)

Robert Wessel wrote:

> "Skybuck Flying" <nospam@hotmail.com> wrote:
>> *Ofcourse a hacker could still try to overwrite other data which contains
>> pointers to executable code like Henrick mentioned.*
>
> *Trying to secure all of this in hardware inevitably leads to the
> re-re-re-re-re-re-re-reinvention of capabilities. And even then, only
> the more extreme versions of capabilities can deal fully with the
> pointer-to-function problem.*

I don't see why this requires capabilities. It seems to me that bounds-checking ought to be sufficient to deal with the kinds of failures that "Skybuck Flying" mentions. What am I missing?

> *Of course direct injection into memory is hardly the only way to
> inject code into a system. For example, just rename an executable
> image *.html, and point a link at it. It'll get downloaded and
> probably stored in the browser's cache in a disk file. Now get
> something to execute that file. Perhaps we could buffer overflow into
> a string that is to be passed to system() – not a code pointer in
> sight! OK, we can fix that by marking the cache directory as not
> allowing code execution (a feature of most OS's). But now what about
> scripts? As you said, "Ieewww... difficult problem !"*

That's one way to fix it. I believe another workable way to fix it would be to prevent the buffer overflow in the first place (e.g., using bounds checking).