

## Re: default value of security.bsd.hardlink\_check\_[ug]id

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/arch/2006-12/msg00081.html>

---

- *From:* Robert Watson <[rwatson@xxxxxxxxxxxxx](mailto:rwatson@xxxxxxxxxxxxx)>
  - *Date:* Sun, 31 Dec 2006 15:39:04 +0000 (GMT)
- 

On Sun, 31 Dec 2006, Ceri Davies wrote:

On Sat, Dec 30, 2006 at 09:08:42PM -0800, Colin Percival wrote:

FreeBSD Architects,

I'd like to make security.bsd.hardlink\_check\_[ug]id default to 1, starting with FreeBSD 7.x. This would make it impossible for a user to create a hard link to a file which he does not own.

Any objections?

One here, on the grounds that:

- a) you have provided no rationale;
- b) that sysctl does not currently seem to be documented anywhere, so changing its default value would violate POLA.

There is a longer answer in which I pine after Solaris' privileges(5) again, or wonder if this can be implemented for "system" processes only using the new priv(9) API instead.

Priv(9) provides a useful foundation for doing something like this, and is a necessary first step to do it. However, to date I've been pretty careful to avoid changing the actual privilege model, just the expression of privilege checking. It should be possible to implement a more selective privilege model using a MAC Framework policy module today. In the past, the TrustedBSD Project has fully implemented POSIX.1e privileges on FreeBSD, and having looked at the implementation, decided it was very high risk, and likely to lead to more vulnerabilities than it addressed. I think we should think very carefully before changing the OS privilege model, and make sure we're going about it in a robust and low-risk way.

Robert N M Watson  
Computer Laboratory  
University of Cambridge

---

freebsd-arch@xxxxxxxxxxxxx mailing list

Re: default value of security.bsd.hardlink\_check\_[ug]id

<http://lists.freebsd.org/mailman/listinfo/freebsd-arch>

To unsubscribe, send any mail to "freebsd-arch-unsubscribe@xxxxxxxxxxxx"