

## Re: Reflections on Trusting Trust

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-11/0090.html>

---

**From:** Kris Kennaway ([kris\\_at\\_obsecurity.org](mailto:kris_at_obsecurity.org))

**Date:** 11/30/05

Date: Tue, 29 Nov 2005 22:24:59 -0500

To: Colin Percival <[cperciva@freebsd.org](mailto:cperciva@freebsd.org)>

On Tue, Nov 29, 2005 at 06:07:29PM -0800, Colin Percival wrote:

> *Kris Kennaway wrote:*  
> > *On Tue, Nov 29, 2005 at 03:43:11PM -0800, Colin Percival wrote:*  
> >> *Even before you get to that point, you have to worry about making sure*  
> >> *that the build clients are secure. One possibility which worries me a*  
> >> *great deal is that a trojan in the build code for a low-profile port*  
> >> *(e.g., misc/my-port-which-nobody-else-uses) could allow an attacker to*  
> >> *gain control of a build client (and then insert trojans into packages*  
> >> *which are built there).*  
> >  
> > *They're closed systems that I keep up-to-date with security fixes, but*  
> > *yes, this is something that we do not defend against. As you note,*  
> > *it's not really practical to at the moment, so the best we can do is*  
> > *just keep it in mind and look for other things to fix.*  
>  
> *Yes and no. Fixing other potential security risks is good, but not if*  
> *it leads users to think that the packages are more trustworthy than they*  
> *really are. In particular, if we started distributing signed packages,*  
> *I suspect that most people would assume that the signatures guaranteed*  
> *that the packages were good, rather than simply ensuring that the packages*  
> *hadn't been modified with after they were built.*  
>  
> *If we're going to sign anything, we need to ensure not just that we're*  
> *signing what we think we're signing, but also that we're signing what the*  
> *\*end users\* think that we're signing.*

Seems to me that ignorance and a false sense of security is bad wherever it appears, so all we can do is try our best to educate users about what they're getting.

Kris

---

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