

## Re: Certification (was RE: realpath(3) et al)

**Source:** <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-08/0177.html>

---

**From:** Robert Watson ([rwatson\\_at\\_freebsd.org](mailto:rwatson_at_freebsd.org))

**Date:** 08/14/03

Date: Wed, 13 Aug 2003 23:24:51 -0400 (EDT)

To: Mike Hoskins <[mike@adept.org](mailto:mike@adept.org)>

On Wed, 13 Aug 2003, Mike Hoskins wrote:

> *i also agree with what you say here, in some sense. that is, we want*  
> *fewer bugs more than certification X. however, while 'fewer bugs' is*  
> *the better thing in the minds of most coders/admins... 'grade A*  
> *security' is often the most prominent thing in the minds of the people*  
> *with money... often the people who make the decisions. i.e. which OS*  
> *gets installed on FBI and NSA computers. ;) lots of beauracracy*  
> *there... so having 'certification X' could get fbsd in doors it would*  
> *not otherwise be allowed to enter. that's not purely a security issue,*  
> *but certainly one i'd like to consider as important. however, i fully*  
> *agree this portion of the discussion can move to –advocacy.*  
>  
> *if we can agree on a given cert that's worthwhile (in some sense, like*  
> *the one SuSe seems to have acquired)... who is the best person to make*  
> *the case to –advocacy? i haven't been subscribed in awhile, but i guess*  
> *it's time to re–subscribe. :) how hard would it be to get corporations*  
> *involved? even without massive corporate support, if the issue is given*  
> *enough visibility... i'd think getting smaller donations from a large*  
> *number of people should not be impossible. (people do buy CDs,*  
> *afterall...)*

SuSe has a low assurance (EAL2) evaluation against a custom–written evaluation criteria. I think a much better target would be a higher assurance level (EAL3) against a consumer–desired target (such as CAPP). Otherwise, it's really a press release, not an evaluation. As I mentioned before, if you want to get into the certification game, what you really want is an end–consumer in DoD (or wherever) willing to push for the evaluation of FreeBSD in their organization so that once you have it evaluated, you have someone who will use it, not to mention help you navigate the certification waters. I think smaller donations would be great, but I also think that the cost you're looking at for evaluation is probably in excess of what you'd be able to get together in small donations—to do CAPP at EAL3, I really can't imagine it costing less than 500k, which is a lot of small donations :-).

FreeBSD–Security: Re: Certification (was RE: realpath(3) et al)

The best way to get FreeBSD evaluated is to make the sell for FreeBSD in environments that require evaluation — those places are probably capable of helping to foot an evaluation bill if they decide they want to run FreeBSD. So from an advocacy perspective, that means keeping research organizations building new technology on FreeBSD, helping defense contractors use FreeBSD to solve real–world problems, etc.

I agree the certification has value, but it isn't equivalent to code review or secure development practices, at least at the lower assurance levels. I'd like to see FreeBSD receive certifications a great deal, and I'd like very much to help provide the technical pieces to make that possible. It's one of the important motivations for doing the TrustedBSD work: make sure that if an organization comes along wanting to evaluate FreeBSD, we've made it as easy for them as possible by providing the technical pieces they need.

Robert N M Watson FreeBSD Core Team, TrustedBSD Projects  
robert@fledge.watson.org Network Associates Laboratories

---

freebsd–security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd–security>

To unsubscribe, send any mail to "freebsd–security–unsubscribe@freebsd.org"