

Reflections on Trusting Trust

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-11/0070.html>

From: Peter Jeremy (*PeterJeremy_at_optushome.com.au*)

Date: 11/26/05

Date: Sun, 27 Nov 2005 09:45:30 +1100

To: freebsd-security@freebsd.org

or "How do I know my copy of FreeBSD is the same as yours?"

I have recently been meditating on the issue of validating X.509 root certificates. An obvious extension to that is validating FreeBSD itself.

Under "The Cutting Edge", the handbook lists 3 methods of synchronising your personal copy of FreeBSD with the Project's copy: Anonymous CVS, CTM and CVSup. There are two CTM modes (e-mail and FTP) and you can also download or buy ISOs. Of these six options, only CTM via e-mail has a digital signature, though the ISO checksums can be compared against the signed release announcements. Physical ISOs are a tricky subject – by trusting the content, I am implicitly trusting the vendor (Walnut Creek, Wind River in the past and (eg) FreeBSD Mall now).

The FreeBSD project appears to have three official keys:

- 1) FreeBSD Security Officer (0xCA6CDFB2)
- 2) Core Team Secretary (0xFF8AE305)
- 3) CTM e-mail (0xC380B4D8)

Of these, only the Security Officer's key has a wide assortment of signatures – providing a reasonably likelihood that an arbitrary person will be able to integrate it into their PGP web-of-trust. The Core Team secretary's key is only signed by four people other than the current secretary – this is somewhat marginal.

The CTM key has only a single signature. This is manifestly inadequate. At the very least, the key should be signed by the person who is running the CTM service.

The FreeBSD release announcements are currently signed personally by the Release Engineer. IMHO, there should be a FreeBSD Release Engineering key that is used for these announcements.

I have also been unable to locate any published information regarding

FreeBSD–Security: Reflections on Trusting Trust

the protection of or access to the private keys for the above.

Finally, FreeBSD is dependent on the protection of its DNS entries. Many years ago, I asked about the DNS servers and got a response that I found acceptable. Based on a recent check, I suspect that things have changed – it looks like ns0.freebsd.org is now part of Yahoo.

Overall, I believe FreeBSD could be improved by:

- Formulating and promulgating a policy for the protection and use of FreeBSD Project DNS, keys and certificates. (The public version of the policy does not go into explicit details but should allow an independent observer to verify its adequacy).
- Creating a FreeBSD Release Engineering key which is used to sign official e-mails from the release engineering team – in particular –RELEASE announcements.
- Tying all the FreeBSD Project keys together by cross-signing them all.
- Arranging for a wider range of signatures on FreeBSD Project keys (the SO key's already meets this).
- Investigate obtaining a X.509 certificate for the FreeBSD Project
- Signing ISO images with a Project key and/or certificate in addition to providing MD5 checksums.
- Investigate providing authenticated protocols for updating FreeBSD.

--

Peter Jeremy

-
- application/pgp-signature attachment: stored