Tails - Feature #7687
Remove ekeyd
07/29/2014 05:47 PM - sajolida

In a WhisperBack bug report, someone suggested to remove ekeyd from Tails.

Tails automatically starts up ekeyd, the Entropy Key Daemon, which looks for any attached Entropy Key device and uses it as a source of randomness for the kernel. This is all well and good, except for one fact: no one uses Entropy Key. Not only is it rare, but it's been out of stock for a very long time, and unlikely to come back soon. There are far more popular external TRNGs out there, many of which have their own daemons. That makes you think, why should Tails have an extra daemon running as root, whose purpose is to mess with the kernel entropy pool, if it's so seldom ever used? All it takes is an attacker to find a bug that allows them to fill the entropy pool with bogus data, which isn't unlikely when ekeyd has /dev/random open for writing constantly and constantly keeps looking for an Entropy Key.

Please remove ekeyd. It's unnecessary and its presence just increases the attack surface area of Tails.

Related issues:
Related to Tails - Feature #5650: rngd
Resolved
Related to Tails - Feature #11703: Consider not starting ekeyd by default
Rejected 08/23/2016

Associated revisions
Revision ef85d3c9 - 11/15/2016 10:53 AM - intrigeri
Stop installing ekeyd: it's unmaintained, very rarely used, poorly designed (dedicated daemon), and security sensitive (Closes: #7687).

History
#1 - 07/29/2014 05:47 PM - sajolida
  - Related to Feature #5650: mgd added

#2 - 08/04/2014 09:54 PM - ioerror
I use ekeyd regularly. It is extremely useful. Please do not remove it.

#3 - 08/06/2014 08:14 AM - sajolida
  - Status changed from Confirmed to Rejected

Thanks for the info.
Rejected then :)

#4 - 09/01/2016 07:23 AM - sajolida
  - Related to Feature #11703: Consider not starting ekeyd by default added

#5 - 09/01/2016 07:36 AM - sajolida
Given #11703, let’s reopen this ticket :) 

According to archive.org Entropy Keys have been out of stock since March 2013: https://web.archive.org/web/20130330233729/http://www.entropykey.co.uk/shop/.

And according to tracker.debian.org the upstream code is not available anymore: https://tracker.debian.org/pkg/ekeyd.

Still, according to popcon, the package is still installed frequently: https://qa.debian.org/popcon.php?package=ekeyd.

Maybe it's time to reconsider removing ekeyd and suggest people who still have entropy keys to install it using Additional Software Packages? This might not work for people using Entropy Key on air-gapped machines (but how many people would that be...?) Or shall we wait some more? If so, until when?

As a first step, should we disable the daemon by default, as suggested in #11703, and ask people to complain if they miss it.

#6 - 09/10/2016 07:26 AM - intrigeri
- Related to deleted (Feature #11703: Consider not starting ekeyd by default)

#7 - 09/10/2016 07:26 AM - intrigeri
I support removing ekeyd, on the grounds that it's unmaintained, very rarely used, poorly designed, and security sensitive. Given how it's (not) maintained, I bet that it'll bitrot, and sooner or later it'll be removed from Debian testing anyway.

(Nitpicking starts here ;)

But I'd rather not build this decision on top of some of the other suggested arguments, that could set precedents I'm not comfortable with:

- We go to great lengths to support various hardware, including some that's been out of stock since quite before 2013, and to do that we often accommodate ourselves of some, or all, of the drawbacks ekeyd suffers from (e.g. we ship binary firmware blobs and all kinds of mostly obsolete driver code that runs as root, when not in kernel space. By nature, these pieces of code are very dangerous, but pragmatically we have to live with it). I guess we can easily agree that we should try to support hardware even if it's 4 years old, even if this implies to ship this kind of code.
- Let's not get used to suggest Additional Software Package for hardware support, especially hardware that's particularly useful for air-gapped systems.

#8 - 09/10/2016 07:26 AM - intrigeri
- Blocks Feature #11703: Consider not starting ekeyd by default added

#9 - 09/11/2016 02:59 AM - sajolida
- Subject changed from Consider removing ekeyd to Remove ekeyd
- Type of work changed from Discuss to Code
Ok, so the rationale is that we support old hardware as long as the corresponding software is well maintained. Or actually, we include software as long as it is maintained (independently of the corresponding hardware).

Mangling this ticket accordingly then.

#10 - 09/11/2016 03:01 AM - sajolida
Or maybe intrigeri feels like this needs more discussion since he didn't close #11703...

#11 - 09/11/2016 03:48 AM - intrigeri

Or maybe intrigeri feels like this needs more discussion since he didn't close #11703...

No, that's fine, let's proceed! I did not close #11703 because I preferred us to decide something here first (and if for some reason we had decided to keep ekeyd, then we could have discussed the option suggested by #11703).

#12 - 09/11/2016 03:49 AM - intrigeri
- Assignee set to intrigeri
- Target version set to Tails_3.0

I'll do that for Tails 3.0, on the grounds that such major releases are our preferred time to deprecate support for hardware we cannot (or don't want to) support anymore.

#13 - 09/11/2016 03:55 AM - intrigeri
- Blocks deleted (Feature #11703: Consider not starting ekeyd by default)

#14 - 09/11/2016 03:56 AM - intrigeri
- Related to Feature #11703: Consider not starting ekeyd by default added

#15 - 11/15/2016 10:57 AM - intrigeri
- Status changed from Confirmed to Resolved
- % Done changed from 0 to 100

Applied in changeset ef85d3c90e20d7ee9d323593cabb4b20a1f11ab3b.