strongSwan - Issue #2494

Problems With 64bit Slot IDs With Pkcs11 Plugin

12.12.2017 11:00 - Jordan Hrycaj

Status:	Feedback	
Priority:	Normal	
Assignee:	Jordan Hrycaj	
Category:	libstrongswan	
Affected version:	5.5.3	**Resolution:**

Description

Pkcs#11 defines a (ck_slot_id_t) type as an alias of (unsigned long). Yet the pkcs11 plugin uses the type (int) in many places instead of a (ck_slot_id_t). Apart from a possible signed/unsigned clash, (int) might be 32bit while (unsigned long) has 64bit (happens on a 64bit ubuntu 14.04).

As a pkcs11 back end provider, this can only work with the StrongSwan plugin if she restricts herself to 31bit. This contradicts pkcs#11 specification (AFAIK, unless pointed out otherwise).

Example:

> pkcs11_public_key.c(853):
> static private_pkcs11_public_key find_key_by_keyid(..., int slot, ...) ..

will later call

> C_OpenSession(slot, ..)

which cannot work in general.

Sorry, no patch at the moment due to time restrictions.

History

#1 - 12.12.2017 11:15 - Tobias Brunner

- Status changed from New to Feedback

While I see the theoretical problem, are there even such large slot IDs in practice that this would become an issue?

#2 - 12.12.2017 15:45 - Jordan Hrycaj

yes it is if you run on a system with limited space.

#3 - 12.12.2017 15:51 - Jordan Hrycaj

Sorry wrong thread

Yes it is a problem unless you assume that slots have low integers. In general, an ID might be anything, maybe a hash or a pointer?

#4 - 12.12.2017 16:03 - Tobias Brunner

> Yes it is a problem unless you assume that slots have low integers.

Well, low is relative even considering 2^31. But that obviously has been the assumption and experience so far. I've no problem with using the proper type for the slot ID throughout the pkcs11 plugin, however, it will currently not be possible to configure such slot IDs (e.g. via VICI).