Tvheadend - Feature #2843

External descrambling (a plugin system using shared libraries)

2015-05-14 11:28 - B C

Status:	New	**Start date:**	2015-05-14
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	Descrambling	**Estimated time:**	0.00 hour
Target version:	999		

Description

as PowerVU is using DES instead of CSA on most channels it would be great to get support for DES aswell. vplug is doing a great job on windows but as we are all linux freaks.... :-)

History

#1 - 2015-05-14 11:56 - Petar Ivanov

yes, this is good feature if make tvh support PowerVU, i laso need if can make this feature

THx

#2 - 2015-05-14 13:33 - Jaroslav Kysela

I'm not sure, but if you compile oscam with the oscam-emu patch - https://github.com/oscam-emu/oscam-emu/ - then it should work using campt (dvbapi) without any tvh mods when you have keys. Doesn't?

#3 - 2015-05-14 13:42 - B C

I don't know how oscam-emu could decrypt the stream, it's just serving the CWs. And as these CWs are for a DES decoder and not for the standard DVB CSA decoder it won't work (maybe I got something wrong but I don't think so). Keys are widely available, and they are working fine with vplug. With vplug comes a new csa.dll which supports des beside csa. There are also a few linux receivers supporting DES, but the majority does not (eg no DB at the moment).

#4 - 2015-05-14 14:42 - Jaroslav Kysela

B C wrote:

> I don't know how oscam-emu could decrypt the stream, it's just serving the CWs. And as these CWs are for a DES decoder and not for the standard DVB CSA decoder it won't work (maybe I got something wrong but I don't think so). Keys are widely available, and they are working fine with vplug. With vplug comes a new csa.dll which supports des beside csa. There are also a few linux receivers supporting DES, but the majority does not (eg no DB at the moment).

cwc.c already uses DES functions from openssl, so it is not difficult to implement the DES descrambler, but I need to know details (initial vectors and so).

#5 - 2015-05-14 14:45 - B C

thats right.
http://colibri.bplaced.net/powervu.htm for the background. I have not yet found some source for the module or sboxes .....
maybe 007.4 can help, or it might be manio has some good connections.....

#6 - 2015-05-14 15:07 - B C

http://www.streamboard.tv/wbb2/thread.php?postid=543273#post543273

#7 - 2015-10-05 16:44 - B C

there seems to be a working solution for MuMuDVB with OSEmu. Maybe this link can help:
http://www.sat-universe.com/showthread.php?t=286651

#8 - 2015-10-05 18:52 - Jaroslav Kysela

- Subject changed from DES support for descrambler to PVU DES support for descrambler

#9 - 2015-10-05 18:55 - Jaroslav Kysela

Looking to OSEmu sources - powervu has own DES key for every video/audio PID. The descrambling itself is similar to other CSA systems. I believe we have to wait, until oscam has a support to forward these keys to the dvbapi clients.

#10 - 2015-10-05 18:58 - B C

my understanding was that osemu actually does the decryption. As PowerVU actually has no smartcard, it can only be done via emulation with the known keys. So the way to go would be with a custom Interface ot osemo, like the MuMuDVB aproach

#11 - 2015-10-05 21:47 - Jaroslav Kysela

Yes, but it's enough to know only the descrambling keys - I'm not willing to add any interface like 'push data to OSEmu and get descrambled data back - I think OSEmu calls it stream relay'. The oscam's dvbapi (with a powervu extension - multiple keys) can do exactly similar thing. Ideally, OSEmu should only provide the keys to oscam (I don't think that oscam developers will include PVU emulator) and oscam will provide keys to clients. I think that there's already a interface in OSEmu to oscam - just talk with oscam developers how handle PVU keys.

#12 - 2015-10-05 22:05 - B C

Well I don't fully agree, what is the benefit of OSEmu forwarding the keys to oscam which then can only be forward to tvheadend? There are on the one hand differnt keys for audio and video (BTW changing about every second) so this must be added to the protocol, and on the other hand PowerVU does not use CSA but DES on most channels, so tvheadend would have to add support for DES also. So I don't know how oscam can be of any help if extended. I agree that using OSEmu as a decrypting proxy might not be the best idea, but for sure a rather easy. Alternatives are embedding parts of OSEmu into tvheadend, no idea of the leagal aspect of this, but the CSA part isn't legal either.

#13 - 2015-10-06 21:36 - Jaroslav Kysela

CSA also uses DES for decryption. I looked to OSEmu sources and video PID is decoded through ffdecsa, other PIDs are decoded using unoptimized DES calls. Anyway, pipe:// allows to use any MPEG-TS source and there's possibility to get the raw MPEG-TS stream with the PID filter from TVH, too.

```
http://tvheadend/stream/mux/<muxid>?pids=0,1,2
```

#14 - 2015-10-06 22:19 - B C

yes I know I can pipe, I'm currently using DVB-Viewer Recording Service as PowerVU descrambler in tvh in a similar way and it is working great, but ugly to configure and needs a Windows VM. Maybe an interface with full acces to the stream would be an option for out of project plugins in the future. There is not only PowerVU which is not using CSA, and a lot of other DVB projects offer such an interface. As I don't think that extending the current oscam dvbapi for PVU is an option (as cardsharing is not possible with PVU anyway), I would suggest to change the request topic to a plugin extention or something like that.

#15 - 2015-10-06 22:29 - saen acro

The idea is possibility to put key as DES CCW in moment /biss/ without external software.

#16 - 2015-10-06 22:32 - B C

that won't work, keys changing rapidly and are incompatible if I did understand your suggestion right

#17 - 2015-10-07 09:38 - Jaroslav Kysela

- Subject changed from PVU DES support for descrambler to External descrambling (a plugin system using shared libraries)

- Target version set to 4.4

Only little note - a plugin system which will pass the raw mpeg-ts packets to a library and gets them back descrambled is not probably a bad idea. I just don't want to create a very specific extension.

#18 - 2015-10-07 09:47 - B C

Exactly, a general approach which is not limited to decryption alone could also be used eg for custom epg grabbers or whatever someone is up to. Thanks for taking it into account.

#19 - 2017-06-15 20:50 - Jaroslav Kysela

- Target version changed from 4.4 to 999

We have all known descrambling mechanisms in 4.4 now, so postpone this again...