Packages - Bug #647

[pacman] pacman-key is unable to fetch keys securely

2015-01-18 04:04 PM - fauno

Status:	not-a-bug		**% Done:**	100%
Priority:	bug			
Assignee:	fauno			
Category:				

Description

the secure gpg.conf we include is placed at /etc/pacman.d but pacman-keys looks for it at /etc/pacman.d/gnupg so it's ignored.

this is a problem because keys are retrieved in plain text from the keyservers and even if it's a publicly available wot i'd consider it bad practice to be mitm-prone. it's also an example configuration for users...

that said, retrieving keys from hkp + tls (hkps://) is broken since gnupg 2.1, so this bug report would have to wait until that is fixed.

History

#1 - 2015-01-28 08:53 PM - fauno

yesterday i've found the solution to using hkps with gpg. turns out dirmngr doesn't use /etc/ssl/certs to verify certificates, but symlinking this dir to /etc/gnupg/trusted-certs or ${GPGHOME}/trusted-certs works

i can implemented this solution later, unless someone thinks it's unsafe

#2 - 2015-01-30 07:12 PM - fauno

i must have reached a working server by chance, because it doesn't work anymore. the issue is this: https://bugs.g10code.com/gnupg/issue1792

#3 - 2015-01-31 04:46 PM - fauno

- Subject changed from [pacman] default gpg.conf is misplaced to [pacman] pacman-key is unable to fetch keys securely

#4 - 2015-02-02 11:59 PM - Anonymous

- % Done changed from 0 to 100

- Status changed from open to not-a-bug

reverted changes to default from pacman to solve compatibility issues against pacstrap ->
https://projects.parabola.nu/abslibre.git/commit/?id=eac23547da0bbfc69c824d21730a8a414e7e0309

#5 - 2015-02-03 02:57 AM - fauno

what does it mean? default is to fetch keys over a plain text connection