Misc infrastructure - Feature # 160: Support HTTPS for apt-cacher.lon.bitfolk.com

Status:	New	**Priority:**	Normal
Author:	garnet	**Category:**	
Created:	2017-08-18	**Assigned to:**	admin
Updated:	2019-01-23	**Due date:**	
Subject:	Support HTTPS for apt-cacher.lon.bitfolk.com		
Description:	With increased moves to have as many websites as possible using HTTPS and to make the infrastructure potentially more secure, it would be useful to be able to access the Apt-Cache server using https://apt-cacher.lon.bitfolk.com as opposed to just HTTP.		

History

2017-08-18 14:18 - garnet

For anyone wanting to use HTTPS addresses with Apt, you will need to install apt-transport-https.

2017-08-18 22:10 - admin

Not many Debian mirrors support https, as it is of limited use (briefly, the deb files have hashes which ensure they are the intended files, and traffic analysis on an https stream will tell an attacker which deb files are being downloaded).

Also, I do not think that apt-cacher-ng can be configured to cache objects downloaded by TLS. As far as I am aware the best it can do is pass through a CONNECT directly to the destination host and ignore the stream of data that comes through, i.e. it acts as a proxy. That makes sense when apt-cacher-ng is configured as a transparent proxy but we use it as an explicit proxy so I would have thought it could be technically possible for it to make its own TLS connection and store the object in cache as normal. But I can't see configuration for that.

If apt-cacher-ng can't be configured to cache objects on https mirrors then it is pointless using it and you would be better off directly putting the https mirrors in your sources.list.

I'll have a more thorough look into this when back from OggCamp next week.

2017-12-29 10:06 - halleck

It's possible to make apt-cacher-ng cache packages downloaded from a https:// source, by providing an alternative http:// placeholder path. See https://blog.packagecloud.io/eng/2015/05/05/using-apt-cacher-ng-with-ssl-tls/, and scroll down to the heading "Caching objects".

From a security point of view https:// will if nothing else make it harder for a MITM attacker to "hide" recent security updates. Yes, even without https:// there is the "Valid-Until" metadata, but that date is set with some margin.

2019-01-23 11:05 - admin

- Priority changed from Low to Normal

"Low" priority doesn't seem right after "the recent APT security issue":https://www.debian.org/security/2019/dsa-4371.

I will transition the backends to talking to https sites as described. I am convinced by the arguments in:

https://blog.packagecloud.io/eng/2018/02/21/attacks-against-secure-apt-repositories/

and not convinced by the assurances of:

https://whydoesaptnotusehttps.com/