Bip - Enhancement #350

Allow CA mode check store to be a file instead of a directory

2014-09-19 23:23 - Adam Williamson

Status:	Resolved	**Start date:**	2014-09-19
Priority:	Normal	**Due date:**	
Assignee:	Pierre-Louis Bonicoli	**% Done:**	100%
Category:		**Estimated time:**	0:00 hour
Target version:	0.9.0		
Patch Available:	Yes	**Branch:**	
Found in Versions:	0.8.9	**Security:**	
Confirmed:	No	**Help Needed:**	

Description

I use Bip on Fedora, which has a feature in the last few versions called Shared System Certificates - https://fedoraproject.org/wiki/Features/SharedSystemCertificates - which provides a system-wide store of trusted CAs, hooks into various apps and libraries, and some tools for managing it. It's a neat feature.

It doesn't provide a representation of its data in the form that Bip wants for its 'ssl_check_store' parameter when operating in CA mode, though - bip expects a directory full of .pems with a c_rehash-generated index, the Fedora system only provides bundles in various formats.

So, I fixed it. Attaching a patch which checks whether the check store is a file or a directory when activating it at the time it sets up a new server connection, and calls SSL_CTX_load_verify_locations() appropriately (the function already supports both approaches, it was only bip's use of it which restricted you to using a directory). With this applied I can set:

ssl_check_store = "/etc/pki/ca-trust/extracted/openssl/ca-bundle.trust.crt";

and it works fine. I also checked that it errors correctly if set to a non-existent file.

I am no kind of C coder so it may be possible to improve on this, but it works fine for me. st_buf is defined where it is because defining it right after case SSL_CHECK_CA: appears to be a violation of C grammar.

History

#1 - 2014-09-19 23:36 - Adam Williamson

Note - as an alternative the code could check if it's a file, load appropriately if so, then just unconditionally do the directory load otherwise, rather than explicitly checking if it's a directory and erroring out if it's neither a file nor a directory. That would more closely resemble the previous behaviour. I don't know which approach would be best...I guess there may be some odd platform or filesystem where stat() doesn't work as expected, or something, but then you'd expect to have trouble using it in that case anyway.

#2 - 2014-09-19 23:56 - Adam Williamson

Additionally, OpenSSL may be able to use a system default trust store if none is specified, so it might be appropriate for bip to continue with a warning/info that the default trust store will be used if it's in CA mode and the check_store is unspecified. I'll take a look later at how hard it'd be to do that.

#3 - 2014-09-20 05:45 - Adam Williamson

- File 0002-allow-for-certificate-store-to-be-unspecified-in-CA-.patch added

Here's a second patch that allows the value to be unspecified in CA mode. (The patches are sequential, 0002 does not replace 0001). If so, bip will try to set the default CA trust store of whatever openssl it's compiled against. If that works, it'll continue with an INFO log message; if that fails, it'll return, like the other failure paths.SSL_CTX_set_default_verify_paths() isn't documented (...thanks, OpenSSL...) but you can follow through the OpenSSL source if you want to see what it does. I believe there are cases where it can return true with a certificate store that's empty; if we want to get cute we can check the contents of the store after setting it and error/warn if it's empty, but I'm not sure it's really necessary, there's a fairly explicit log message about what's going on. The logs / documentation could explain a bit more specifically that if you have trouble using the default store you should

specify one, I guess.

Again I checked this one - I can connect to Freenode with SSL enabled fine, the log message displays correctly, the verification logs indicate the certificate being checked properly, and 'info (user) (user)' reports "SSL check mode 'ca', default or no certificate store" (I hedged because this message can also be hit in BASIC mode, where it's "no certificate store" not "default certificate store").

#4 - 2014-11-21 18:19 - Pierre-Louis Bonicoli

- Status changed from New to In Progress

- Assignee set to Pierre-Louis Bonicoli

- Target version set to 0.9.0

#5 - 2014-12-11 16:31 - Pierre-Louis Bonicoli

- Status changed from In Progress to Resolved

- % Done changed from 0 to 100

Successfully tested on Debian, with ssl_check_mode = "ca";:

- ssl_check_store unset => connection successful when ca-certificates is configured
- ssl_check_store = "/tmp/certs.pem"; (file) => connection successful
- ssl_check_store = "/tmp/certs_dir"; (directory) => connection successful
- when SSL connection fails, bip attempts to reconnect

Both patches applied:

- 89295ca4
- 88242715

Thanks a lot for these patches, the new behavior is a great improvement !

Files

0001-check-whether-trust-store-is-a-file-or-directory-in-.patch	4.36 KB	2014-09-19	Adam Williamson
0002-allow-for-certificate-store-to-be-unspecified-in-CA-.patch	4.34 KB	2014-09-20	Adam Williamson