Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by koldo on Thu, 11 Mar 2010 08:12:20 GMT
View Forum Message <> Reply to Message

kohait00 wrote on Wed, 10 March 2010 22:36http://www.winzip.com/aes_info.htm
should explain that its not trivial
Hello Kohait00

Thank you for the reference. I will use it.

Coming to the issue, look at this:

- If it is open source, I cannot put the key in the code

- If the program creates a key for the user, and he/she is not let to change it, a 32 bytes password seems too hard to use

- If we use a user defined key, we could include in AESStream:

---1. A SHA 256 possibility to convert user password in a 32 bytes key
---2. The means to avoid a brute force attack.
For example, if AES 256 with a weak user key can resist within and acceptable probability, for example, 1000000 random keys, AESStream could let the main program to enter, for example, 1000 keys per day and after that, AESStream would refuse any additional key.