Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by Mindtraveller on Thu, 11 Mar 2010 09:53:04 GMT
View Forum Message <> Reply to Message

The truth is that you MUST
1) Use strong key with AES, not password
2) Not to hardcode the key in the code in ANY way

So what is the solution? You take user password. And then you DERIVE strong key from it. Then you "forget" user password, you just don't need it at all. You do encryption with that relatively strong key (i.e. SHA from user password - see my recent comment).

Next time user enters password, you derive the key with the same function (i.e. SHA) and try to decompress AESStream. If decomression fails, then original password and the one entered is not the same (incorrect password).

It is really not that hard.