Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by kohait00 on Thu, 11 Mar 2010 09:29:39 GMT
View Forum Message <> Reply to Message

i dont know if i remember it correctly, but there are several technices combined to achieve encryption of data trggered by a user password.

1) the en/de cryption is done using a *fast* (symetrical) algorithm, like AES (they are blockorientated and relatively similar, only differ in their block functions (F functions, or Feistel Function)

2) the key used there, is the key we were speaking about, and is encrypted and stored with the data. as encryption can be used slow but really strong asymetrical (public / private key) algorithms like RSA.

3) the password thing comes into play with things like diffie hellman secure exchage of information with having it travel over the net.

but its quite a while now, and i may mix it up with things like vpn tunneling and handshaking and so on..

but in any way: encrypting decrypting to fit current standards is far from beeing trivial and involves a lot of steps, password is only a small part of it, maybe we should stick to common technologie here (means in openssl)