Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by koldo on Wed, 10 Mar 2010 20:33:18 GMT
View Forum Message <> Reply to Message

kohait00 wrote on Wed, 10 March 2010 20:54hi koldo,

as far as i got the point of mindtraveler, AES and the other symetric algorithms are not to be thought of beeing based on a "password", a user defined and therefore week combination of signs (which would be scanned first in a brute force attack), but on a statistically well distributed *binary* key (128 bit should be made wise . it is hard for a human beeing to generate one. so the computer will take over and provide some random ones(AES key generator). this key should be thought of as a "password", what it of corse isn't. everything else would diminish the stability of the key. maybe to get over it, think of it as kind a GUID which you generate once for your application (which in real world communication does not apply . dont think of AES as sort of alphanumerical password dependant encryption algorithm, it's indeed, just as mindtraveler mentioned: math. i had the luck to enjoy some lectures cryptology, and it confuses sometimes. but the first thing we learned there was to forget the idea of passwords / human readable strings as security base.
Yes yes, all of you are right

However think about for example a file encrypting software to be used by different people. How would you do it ?

Option 1: The software gives the user a 32 bytes random key
Option 2: The user enters a key

Option 1 seems much stronger. However file and hard disk encrypting software seems to choose option 2.