Subject: Encrypting password in .ini file with aes
Posted by Giorgio on Sat, 12 Sep 2015 14:46:24 GMT
View Forum Message <> Reply to Message

HI there,
I created my small application interacting with a MySQL database. Currently user and password are embedded in the source code. I would like to put them in an .ini file but I do not like to have the password in plain text. I decided to use AESstream to solve this problem. My concern is that I need the key in the source code to properly decode the password in the .ini file, so at the end of the day it is more or less the same than having the password in the source code (i.e. in the same way as a malicious user could decompile the source code to get the password, he could do the same to get the key and then decode the .ini file). What could be the right approach?
Thanks,
Giorgio

Subject: Re: Encrypting password in .ini file with aes
Posted by Mindtraveller on Sat, 12 Sep 2015 20:19:57 GMT
View Forum Message <> Reply to Message

Hi Giorgio,

According to Kerckhoffs's principle, you can't leave any kind of key in the source code, because it is almost the same "security" as unencrypted password.
It all usually means you'll have to split into parts the information needed to construct the key. At least one part of it can't be reverse engineered from source code or app data files. The truth is everything you construct programmatically will be reconstructible and reverse engineerable. The honest solution here is to make user remember the key (or part of it) himself. More dirty solution is to make this key generated by a number of algorithms wich will just separate lazy hackers.
And the last note is about the key itself. Please don't make user's password an encryption key. It lowers security level. Please use at least this formula:
key = hash(salt + password)

Thanks
Pavel

Subject: Re: Encrypting password in .ini file with aes
Posted by Giorgio on Sun, 13 Sep 2015 11:12:01 GMT
View Forum Message <> Reply to Message

Hi Pavel,
thank you for your really informative answer. Sadly, asking users to remember password is not a feasible option: they are machinists in a manufacturing company and could punch me on the face if I ask so 8) - literally, not joking. Anyway, the application is used only in our private network, the mySQL user has almost no rights on the DB and the password is known by almost anyone in the

factory, so this is more an exercise for my programming skills than a real need. Maybe an option could be using the single sign on from the operating system.
Regards,
Giorgio