

Forum:[Hack Forums](#)

Thread: [Need information on creating a secure licensing system.](#)

Pharmacist - November 17, 2016, 5:56 pm

Mainly I'm looking for feedback on what I currently have, plus I'm looking for suggestions.

1. It checks the MD5 of the EXE against the original, if it does not match, the user is banned. This happens after a successful login.
2. Remote variables, checks if the user is active and sends the variable to the client.
3. Users/passwords/HWID stored in a SQL database. Passwords are encrypted.
4. Normal's like detecting some debuggers, etc.. nothing special.

Is there anything else I can do to further secure my application?

JUSTIN - November 17, 2016, 6:06 pm

Don't use MD5? Hash passwords, don't encrypt them. Are you using a web request to access the sql server or just the client...?

BahNahNah - November 17, 2016, 6:10 pm

Using MD5 for your hashes is the first security issue. Use a stronger algorithm like SHA256.

Don't encrypt passwords, hash them with a salt.

How are you going to go about showing the login panel?

Are programs going to require to include a DLL along with their program? (If so, what's stopping someone from patching the DLL so that it unlocks all applications using the licensing system)

Is the communication between the client and server going to be encrypted? Using Wireshark (or Fiddler if you are using HTTP/HTTPS) to change the response to a successful login can be an issue.

Pharmacist - November 17, 2016, 6:14 pm

(Nov 17, 2016 07:06 PM)justinooo Wrote: [\[CITE\]](#) Don't use MD5? Hash passwords, don't encrypt them. Are you using a web request to access the sql server or just the client...?

Checks the MD5 of the main .exe so if it's modified it won't match the original.

And I'm using a web request.

(Nov 17, 2016 07:10 PM)BahNahNah Wrote: [\[CITE\]](#) Using MD5 for your hashes is the first security issue. Use a stronger algorithm like SHA256.

Don't encrypt passwords, hash them with a salt.

How are you going to go about showing the login panel?

Are programs going to require to include a DLL along with their program? (If so, what's stopping someone from patching the DLL so that it unlocks all applications using the licensing system)

Is the communication between the client and server going to be encrypted? Using Wireshark (or Fiddler if you are using HTTP/HTTPS) to change the response to a successful login can be an issue.

Well, I've got to make my thread more clear. The MD5 is for the main application to detect if it's been modified.

It won't be using an additional DLL, everything would be in the application.

The login panel is just a form, nothing special. As for the admin panel (Ban/unban/create code)

would be all done manually, this login system is for my application I'm creating.

Even if they change it to a successful login attempt, they won't be able to use the variable, and the application would be useless, because it checks if the user is registered and unbanned then sends the variable, they can't emulate that (Correct?)

mrkoolaid - November 17, 2016, 6:40 pm

-----sorry i misread the post, post removed-----

clrlslwi - November 17, 2016, 6:54 pm

(Nov 17, 2016 06:56 PM)Pharmacist Wrote: [\[CITE\]](#) 1. It checks the MD5 of the EXE against the original, if it does not match, the user is banned. This happens after a successful login.

This would be extremely obvious to anyone poking through your application, so I highly doubt this would affect anyone that's not retarded.

Patch it so it always sends the md5 that's expected when unmodified.

(Nov 17, 2016 06:56 PM)Pharmacist Wrote: [\[CITE\]](#) 2. Remote variables, checks if the user is active and sends the variable to the client.

Successfully login, check which variables are received remotely, and patch the application so they're set on startup instead.

(Nov 17, 2016 06:56 PM)Pharmacist Wrote: [\[CITE\]](#) Is there anything else I can do to further secure my application?

I wouldn't bother personally. At the end of the day, anyone who wants to bypass your licensing system is going to do it.

(Nov 17, 2016 07:14 PM)Pharmacist Wrote: [\[CITE\]](#) Even if they change it to a successful login attempt, they won't be able to use the variable, and the application would be useless, because it checks if the user is registered and unbanned then sends the variable, they can't emulate that (Correct?)

No, not correct. Like I mentioned previously, if they know what variables to send, they can emulate the server, or bypass the server entirely. To make matters worse, you can sniff plain HTTP traffic relatively easily, which means they can see what you're sending to the client.

HTTPS w/ certificate pinning would solve this.

Ninja - November 17, 2016, 7:35 pm

(Nov 17, 2016 07:54 PM)Demmonic Wrote: [\[CITE\]](#) HTTPS w/ certificate pinning would solve this. Can still be bypassed but not that easily I guess.

(Nov 17, 2016 07:14 PM)Pharmacist Wrote: [\[CITE\]](#) Checks the MD5 of the main .exe so if it's modified it won't match the original.

Where is the MD5 checked? Anything sent from client to server or backwards can be spoofed.

In case you think like this, NOTHING is uncrackable.

All you can do is make it harder. Encrypt traffic, use HTTPS, do checks, maybe IP locks, hash stuff, whatever.

Pharmacist - November 17, 2016, 7:57 pm

(Nov 17, 2016 08:35 PM)Ninja Wrote: [\[CITE\]](#) Can still be bypassed but not that easily I guess.

Where is the MD5 checked? Anything sent from client to server or backwards can be spoofed.

In case you think like this, NOTHING is uncrackable.

All you can do is make it harder. Encrypt traffic, use HTTPS, do checks, maybe IP locks, hash stuff, whatever.

I know nothing is uncrackable. But just for a licensing system, I was hoping it would make it harder for someone to crack, while still being secure for my customers/users

Aristocles - *November 18, 2016, 9:03 am*

Why would I use yours instead of NETSeal ? That's the question people will ask-themself.

Because at current stage, I can pay for a licence, extract the remote variables, remove the checks, and TADA !

Lucifer Morningstar - *November 18, 2016, 11:02 am*

Switch to a native language if you want to create a proper licensing system.