

Forum:[Hack Forums](#)

Thread: [How to ensure data is sent in my auth system?](#)

zonne - November 10, 2018, 1:37 pm

Hello,

When user is logged in, I still keep a "heartbeat" sending me information if user has opened Fiddler / Wireshark, tried modifying the program.

1. Example, user is logged in, cuts his internet connection and reverse engineer the program, how can I ensure my app send that data to auth system next time he runs the app? I thought about storing encrypted data about his activity in a file, but it can be deleted and thus no data will be sent.
2. How often should I call for heartbeat, is once per minute okay or should I do it more often?
3. How to ensure my data is not being modified / tampered? Was thinking about hashing the response / checksum the response.
4. Should I perma ban user's account if they even try to modify headers?

NOT LOOKING FOR CODE. Just need suggestions since I'm stuck right now.

Thanks

Terry A. Davis - November 11, 2018, 1:51 am

(Nov 10, 2018 02:37 PM)zonne Wrote: [\[CITE\]](#) Hello,

When user is logged in, I still keep a "heartbeat" sending me information if user has opened Fiddler / Wireshark, tried modifying the program.

1. Example, user is logged in, cuts his internet connection and reverse engineer the program, how can I ensure my app send that data to auth system next time he runs the app? I thought about storing encrypted data about his activity in a file, but it can be deleted and thus no data will be sent.
2. How often should I call for heartbeat, is once per minute okay or should I do it more often?
3. How to ensure my data is not being modified / tampered? Was thinking about hashing the response / checksum the response.
4. Should I perma ban user's account if they even try to modify headers?

NOT LOOKING FOR CODE. Just need suggestions since I'm stuck right now.

Thanks

- 1: You should check for internet as one of the first things you do, if there is no connection abort

mission and close citing no internet.

- 1.1 To aid with this called if Debugger.IsAttached and quit if it is (only once ready for release duh!)
- 2: So long as it's just a simple "are you still there?" it should be every 5-15 seconds in my books.
- 3: I'd say CRC the essential data or validate it with the server to don't trust the client with data that can be tampered with.
- 4: Kick->7 Days Ban->Permanent Ban.

Washi - November 11, 2018, 3:11 pm

(Nov 11, 2018 02:51 AM)Endless Night Wrote: [\[CITE\]](#) 3: I'd say CRC the essential data or validate it with the server to don't trust the client with data that can be tampered with.

And who is there to stop you from also updating the CRC in the packet? Such a checksum is not really hard to fake.

@OP: Look into cryptographic signatures (e.g. RSA, ECC) and secure protocols that use them (e.g. TLS). These kind of schemes allow you to sign your packets with a private key that only the sender knows, and thus only the sender can create. Everyone can verify the integrity and authenticity of the payload by using the associated public key that is available to anyone. Another option is to use message authentication codes such as HMAC, which are also built into the .NET framework itself.

Just some advice, for solid encryption and/or authentication I would suggest not to implement them yourself, but rather use existing libraries that are mature enough and make use of the best practices. Speaking from experience, the only easy thing about security is to (accidentally) do it incorrectly, especially if you are new to it. The developers of these libraries have probably worked with cryptography for a long time and have fixed a lot of errors over time.

JUSTIN - November 12, 2018, 7:44 am

If it's your own auth system, look into SafeRequest: <https://github.com/ooojustin/SafeRequest>