Security Context

Our system consists of five main components:

1. Protected (encrypted) software - identical for all users
2. Activation program - identical for all users
3. License file - unique for each user
4. Block ranges file - identical for all users
5. Dynamic jump file - identical for all users

The encryption of each basic block is implemented on the server side, making it inaccessible to regular users. Attempting to crack the software without knowing the exact implementation of block division and encryption is virtually impossible. However, if this information were to leak, a potential cracker could attempt the following:

1. Cracking the software using only the protected version is nearly impossible. The cracker would need to obtain the block ranges file to determine which key is used for each block.
2. To crack the software using both the activation program and protected software, the cracker would need to: a) Obtain the block ranges file b) Reverse engineer the activation program to find the HKDF algorithm implementation c) Somehow acquire the AES key and the PC ID for which the protected version was generated Both the AES key and PC ID would require brute force attempts unless shared by a legitimate user. In our implementation, the PC ID is 32 bytes long, and the key is 16 bytes long, resulting in 8^(48) possibilities.

3.1. If a cracker obtains all components from a paying customer, they would need to: a) Extract the PC ID from the license b) Reverse engineer the activation file to understand the HKDF implementation c) Generate keys for each basic block The cracker could also debug the program to view plaintext data after decryption. This process would be time-consuming and challenging to automate, requiring significant effort and expertise.

3.2. A cracker can also modify the activation program to get the pc id from the license instead of actually getting it from the activated machine. This will require reverse engineering of the activation program, and patching it. This is the easiest way to crack our system. And it requires buy license, reverse engenring of the activation program (which will take time to the normal hacker). Also, to distribute this cracked program will have to publish the pc id that cracked the software , which can potently lead to legal actions , or black listing some pc ids (maybe in the next version)

Protection against Man-in-the-Middle (MITM) attacks relies on the server using secure transport protocols.