An end-to-end encrypted application

1 Accomplished step

Our team has made great progress by meeting regularly and discussing project details face to face. We have completed the code part and are improving some functions. For Asymmetric encryption, we have referred to many materials, read many textbooks, and successfully reproduced the code after understanding the principles.

We conduct firewall tests, sensitive data sniffing tests, and password cracking tests according to the characteristics of the system. Among them, the firewall and data sniffing functions are well implemented. The firewall can block users in risk areas from the wall and prohibit them from accessing the server, while data sniffing can capture sensitive information sharply and accurately. Testing for encryption is still ongoing, and somewhat bumpy, showing that the encryption method still needs some improvement.

2 Obstacles and challenges you encountered

We encountered some difficulties in the reproduction of the encryption method, because it is difficult for me to realize the author's idea from the paper, and the effect is far from their work.

In addition, when writing code, I am a little unfamiliar with the principles, experiments, and implementation of the TCP protocol, so I am learning from the beginning and exploring the process. This step took us a long time and was tricky.

The important point is that the encryption method we implemented is not secure enough, because we can crack the encrypted content through the brute force method and dictionary cracking method, although it takes a long time, so we are working hard to improve the method. But the current effect is not ideal.

When defining the classes of the server and client, there are some minor troubles due to the unfamiliarity with python syntax, but these problems can be solved through python textbooks and courses.

3 Some harder steps and potential challenges you still expect

Undoubtedly, we will continue to test the security of the system, such as allowing blacklisted users to access the system through the firewall, or using some professional software, such as Brutus, to test the encryption system. This is still a big challenge for us.

Also, we still need to optimize the code. Some redundant statements are too many, so the program does not run particularly smoothly.

4 Relevant essay

In this paper, the authors address problems that are irreversible or interfere with observing and recognizing human activity, including face detection and encryption, by developing an efficient algorithm. Regarding face encryption, the author proposes a reversible hybrid encryption (decryption) scheme based on a spatial and value scrambling model.[1] We believe that the scrambling model can be properly used in our system to cause certain noise interference and cause trouble cracking the password. However, one drawback of this method is that the decoding model of my system may not be able to identify the noise in it. So how to properly use noise is a clue that we can explore next.

5 Reference

[1] Liu, S., Kong, L., Wang, H. (2018). Face Detection and Encryption for Privacy-Preserving in Surveillance Video. In: et al. Pattern Recognition and Computer Vision. PRCV 2018. Lecture Notes in Computer Science(), vol 11258. Springer, Cham. https://doi.org/10.1007/978-3-030-03338-5_14