In the course of completing the course thesis, the knowledge of two courses was supplemented: applied cryptography and computer networks.

1. Apply cryptography. Identity authentication and key exchange are very important parts of cryptography and are often the weakest parts of security. Under normal circumstances, the identity of the network connection will be introduced into the CA certificate. However, because of its particularity, it is impossible for the network agent to use the CA certificate. Therefore, the general network agent will be exposed during the authentication and key exchange process. Characteristics are also very good against man-in-the-middle attacks. The two software we studied have no identity authentication and key exchange process, and their security has greatly improved. However, we do the opposite, and confidential communication without secret key exchange is suspicious.

2. Computer network. SOCKS is a network transmission protocol that is mainly used for intermediate transmission of communication between a client and an external network server. The latest protocol is version 5. Compared to the previous version, it supports UDP, authentication, and IPv6. According to the OSI model, SOCKS is a session layer protocol that is located between the presentation layer and the transport layer. SOCKS works at a lower level than HTTP proxies: SOCKS uses a handshaking protocol to notify the proxy software that its client is trying to make a connection to SOCKS, and then operates as transparently as possible, while regular proxies may interpret and rewrite the header (for example, using Another underlying protocol, such as FTP; however, the HTTP proxy simply forwards the HTTP request to the desired HTTP server. Although HTTP proxies have different usage patterns, the CONNECT method allows forwarding of TCP connections; however, SOCKS proxies can also forward UDP traffic and reverse proxies, whereas HTTP proxies cannot. HTTP proxies are generally more aware of the HTTP protocol and perform higher-level filtering (although usually only used for GET and POST methods and not for the CONNECT method).