Contribution

By Anica Krüger

Tasks Overview:

- Research about TOR to understand project better
- worked on proxy code together with paula
- brainstromed solutions, implemented code, tested code
- wrote each method
- wrote Software Architecture and Implementation part of README for proxy
- worked on presentation slides

Contribution:

The main tasks assigned to me while working on the onion routing project were to research, develop, and provide documentation for the proxy system, which is essential to the project's fulfilment. Before working on the project's goals, I first took some time to understand the core functionality and purpose of the TOR (The Onion Router) system. This research was also fundamental in developing the detailed design of the proxy and understanding the technical requirements of our project. Cooperating with Paula, we wrote the proxy's code. We had brainstorming sessions regarding ways to implement secure communication circuit creation and what cryptographic procedures and nodes would be required during the circuit expansion stage. After testing the separate parts of the proxy, we integrated everything into the main component of the onion routing system. The practical side of the task was within my field, as I was charged with implementing and improving the techniques that ultimately worked for the proxy. This was, among other things, the designing and implementing the Diffie-Hellman key exchanges, performing RSA encryption, constructing relay cells, and finally, performing AES encryption/decryption to enable secure communication in the said network. I had additional responsibilities, too, which included coding, particularly in trying to test and debug our program to meet the performance and security requirements. All the work on the code for the proxy was done in cooperation with Paula, and we had close communication with the router team to keep track of our codes working together. I was also responsible for preparing the "Software Architecture and Implementation" section of the proxy in the README. Other information presented here includes an explanation of the directory layout and a description of each function, showing how the methods in the code facilitate the development and control of secure communication circuits. This section makes it easy for any person using our code to understand the rationale of our design and its parts. Lastly, I worked on preparing the final presentation, which summarized the report's contents, paying particular attention to the most important technical details.