SOFTWARE FOR PERFORMING END-TO-END ENCRYPTION IN THIRD PARTY SYSTEMS

Kushchevskyi D.R.
National Aviation University, Kyiv
Supervisor – Meleshko O.O., senior lecturer

Increasingly, people are wondering what information is collected about them, on which servers it is stored and how it will be used. Authorities in different countries are working on legislation to make usage of cookies and personal data by applications more transparent and clearer to users. However, there are systems that have become an integral part of our lives and the world's economies. Such systems are products of Google, Microsoft, Facebook, Amazon. The key issue is that there is no alternative for a user who is dissatisfied with privacy policies and the way the data is used. For example, when using Google Classroom in teaching students. Students must provide personal data and other information, otherwise they will not participate in the learning process. Google search engine is a monopolist. As of January 2021, the percentage of Google search use in the world is 87%. This implies that, at any time, the giant can stop showing the website of any company in search and cause serious damage to it. Facebook is having a leading position among social networks, but it is known for content filtering, censoring, suspending or banning accounts. Twitch, the largest streaming platform, is known for promoting certain values and reacting very aggressively to any criticism. Such actions on the part of technology giants should alert not only ordinary users, but also entire countries. The most dangerous are modern smartphones that have firmware from the vendor and the above giants, as well as hardware-level solutions that track geolocation, that is, collect data about places where the users go, where they live and work and send it all to servers. There are solutions that can solve some of the problems, such as: Diaspora, Thunderbird, k9mail, mutt, Tor and others. But the major challenge is that a user needs to be competent in configuring the software and have the desire to leave the usual comfort zone. It is easier for society to accept the fact that it is being monitored and interpret the problem as follows: "honest people have nothing to hide", but this can hardly be a correct statement.

Based on the arguments above, there can be proposed a solution that will use the existing infrastructure and interfaces while providing an additional layer of security. An implementation is a proxy server that encrypts the text of a user's message in real time before sending it to a Google server. The machines of both the user and the person with whom he/she shares information should have working proxy servers which coordinate the public key through the i2p tunnel and carry out end-to-end encryption of letters. Google receives and stores messages in the encrypted form. As a result, the users don’t leave the comfort zone, stay with their favorite service while receiving the necessary security. Moreover, the solution is completely free and does not require servers, white IP addresses and additional administration. The

schemes of the system and the proxy server operation are presented in Fig.1 and Fig.2.

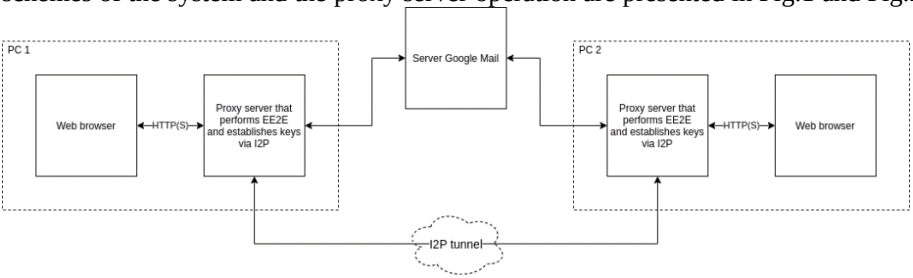

Fig 1. Scheme of system operation

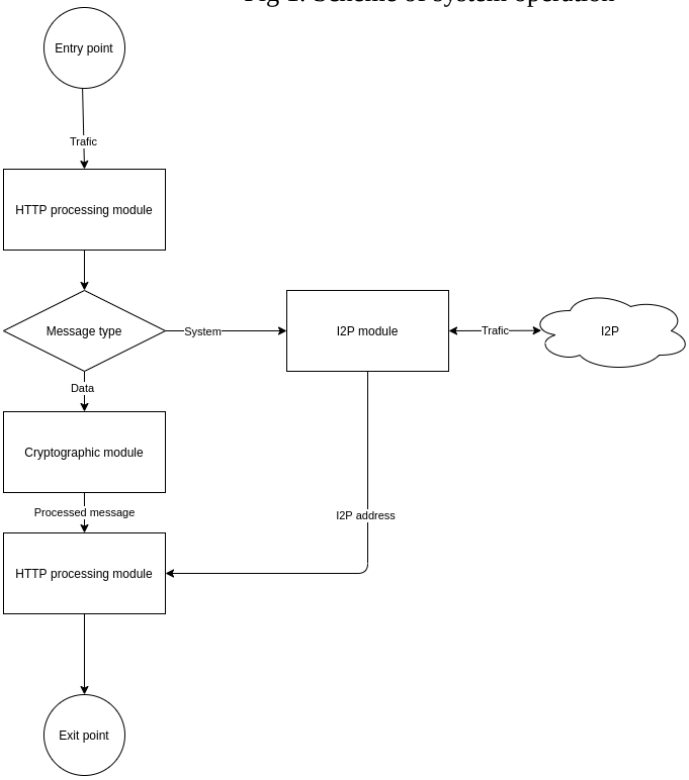

Fig 2. Scheme of proxy server operation

References:

1.The diaspora* Project [Electronic resource]. − Access mode: https://diasporafoundation.org/

2.Thunderbird free email application [Electronic resource − Access mode: https://www.thunderbird.net/en-US/

3.Invisible Internet Protocol: Network without borders [Electronic resource]. − Access mode: https://i2pd.website/