Anton Kovraiskyi
V.I. Mieshkov, research supervisor
V.V. Gubkina, language adviser
National Mining University, Dnipro, Ukraine

TOR Secure Network

So what is TOR? TOR is an anonymity network for “silent” usage by anyone who wants to stay hidden from any other secret service etc. Does it actually work as it is supposed to do? It depends on different circumstances. TOR contains nodes, which are placed all over the globe. The nodes are needed to route user traffic flows over randomly picked rows of nodes to hide which node user is getting access to. If a bad guy can track through which node the traffic is flowing, he can compare received data and confirm what destination user is connected to.

In current state, TOR cannot defend user from this kind of action, end-to-end confirmation attacks, because it overloads TOR network. On the contrary, TOR does make it harder for an intruder to even try to perform this kind of attack.

Researchers assume, based on previous attack attempts, that they are possible against TOR network, but nobody knows how effectively they will actually do against nowadays-sized TOR network.

What is a real problem for TOR users brought by end-to-end confirmation attacks? To add some spices, current research shows that TOR has its own limits before defending this kind of attacks. At this moment, we already can observe that it is not perfectly safe. We cannot rely on basic TOR defense systems in order to save users’ anonymity they are expecting from TOR network. Let us try to investigate end-to-end confirmation attacks on TOR with a score to realize the best way to prevent these threats.

By conducting real-world experiments on TOR, we can try different defensive mechanisms to secure it. According to nature’s law survival of the fittest, this will help us find out the way to help to defend ourselves.

We can try to defend our network by inserting “dummy traffic” and by examining security level that be can be provided to users. Of course, not to get into bankruptcy we are required to count our budget in order to defend ourselves. Unfortunately, in some cases it fails to help us.

Also we must consider load, put by our defense mechanisms onto the network. If the TOR network has the tendency to slow down the processing and computer activity, users are likely to stop using it. Nobody wants to crawl through the network like snails, does it?

The proposed defense mechanisms being easy to implement and deploy could potentially secure users against such kind of attacks against TOR users. Applying this defense improves the security and allows users to stay hidden and the possibilities of saving money are great.