Roman Kononov
A.T. Khar', research supervisor
I.I. Zuyenok, language adviser
SHEI "National Mining University", Dnipropetrovsk

Public Wireless Networks Vulnerability

Mobile devices make our lives much easier. But it's important to be careful when using Wi-Fi, particularly in public spaces, such as a coffee shop or in an airport.

As public Wi-Fi hotspots are lacking of security encryption, they tend to be completely open and insecure. Many users believe that public Wi-Fi hotspots are secure since they are offered from established, successful businesses. However, even the largest and most secure businesses may have security breaches. Public Wi-Fi security is in its infancy.

That is why the overall aim of my research my research is to protect the personal privacy of users, as well as their freedom and ability to conduct confidential business by keeping their internet activities from being monitored.

It would be appropriate to start with the analysis of possible wireless networks vulnerabilities. The analysis done, demonstrates that there is a variety of ways to capture your personal data.

Eavesdropping or sniffing is the process of gathering information from a network by snooping on transmitted data, where to eavesdrop or sniff is to secretly overhear a private conversation over a confidential communication in a not legally authorized way. The information remains intact, but its privacy is compromised.

The man-in-the-middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

There are different type of attack, the most common are:

- Eavesdrop Communication
- Web Sessions Sidejacking
- Evil Twin. etc.

Here the question arises: how to counter the attacks? The basic idea is to establish a secure communication channel with a server, so that attacker could not get any vital data.

I suggest the following ways of countering the attacks:

- Forcing web pages to work in "https only" mode.
- Using VPN (which is virtual private network) to create a secure "tunnel" between the machine and the remote target.
- Using onion routing.