УДК 621.326
Barylska S. ; Trush S.
Ternopil Ivan Pul'uj National Technical University

TOR- TheOnionRouter

Supervisor: Perenchuk O.

УДК 621.326
Барильська С. – ст. гр. СБ-21; Труш С. – ст. гр. СБ-21
Тернопільський національнийтехнічний університет іменіІвана Пулюя

АНОНІМАЙЗЕР TOR

Науковий керівник: викладач Перенчук О.З.

Keywords: software, Web sites, confidential
Ключові слова: програмне забезпечення, веб-сайти, конфіденційний

Tor (previously an acronym for **The Onion Router**) is free software for enabling online anonymity and censorship resistance. Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than five thousand relays to conceal a user's location or usage from anyone conducting network surveillance or traffic analysis. Using Tor makes it more difficult to trace Internet activity, including "visits to Web sites, online posts, instant messages, and other communication forms", back to the user and is intended 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. An extract of a Top Secret appraisal by the NSA characterized Tor as "the King of high secure, low latency Internet anonymity" with "no contenders for the throne in waiting".

The term "onion routing" refers to layers of encryption, nested like the layers of an onion, used to anonymize communication. Tor encrypts the original data, including the destination IP address, multiple times and sends it through a virtual circuit comprising successive, randomly selected Tor relays. Each relay decrypts a layer of encryption to reveal only the next relay in the circuit in order to pass the remaining encrypted data on to it. The final relay decrypts the innermost layer of encryption and sends the original data to its destination without revealing, or even knowing, the source IP address. Since the routing of the communication is partly at every hop in the Tor circuit, this method eliminates any single point at which the communication can be de-anonymized through network surveillance that relies upon knowing its source and destination.

Tor can also provide anonymity to websites and other servers. Servers configured to receive inbound connections only through Tor are called hidden services. Rather than revealing a server's IP address (and thus its network location), a hidden service is accessed through its onion address. The Tor network understands these addresses and can route data to and from hidden services, even to those hosted behind firewalls or network address translators (NAT), while preserving the anonymity of both parties. Tor is necessary to access hidden services.

References:

1. Official site of TOR (https://www.torproject.org)
2. Free internet encyclopedia (http://www.wikipedia.org).