- ECOMMS - ECE09433 -

T.O.R. Network

Traffic analysis attacks

Matt Delengowski
Joshua Gould
Jessica Wozniak

November 7 2018

Paper Summary

For this report, we will be addressing TOR network attacks and defense strategies as well as how the network works and improvements to these attacks.

- When was it first proposed? Who proposed it?
    - Onion Routing was first developed in the mid-1990s by U.S. Naval Research Laboratory employees, mathematician Paul Syverson, and computer scientists Michael G. Reed and David Goldschlag in order to protect U.S. intelligence communications.
    - The alpha version of Tor, developed by Syverson and computer scientists Roger Dingledine and Nick Mathewson and then called T*he Onion Routing project*, or *Tor* project, launched on September 20th, 2002. The first public release occurred a year later in 2003.
- Which groups are the leading groups?
    - Tor networks have been used by criminal and law enforcement groups alike. Agencies within the U.S. government variously fund Tor such as the U.S. State Department, the National Science Foundation, and the Broadcasting Board of Governors.
- What new techniques has been made since it was first proposed? (Defend and Attack)
    - Attack (Find IP traffic)
        - The purpose of Tor is to hide ones online presence, therefore an attack would be defined as revealing a Tor user's IP address. Tor cannot prevent traffic confirmation. Traffic confirmation is defined as when an attacker observes relays on both ends of a Tor circuit and compares traffic timing, volume, and other characteristics to determine if the relays are on the same circuit. Therefore the majority attacks are based around these traffic confirmations, and are ultimately used for exposing Tor user's IP addresses.
    - Defend (Hide IP traffic)
        - In general, Tor responds to vulnerabilities by providing updates to the infrastructure, however, when improperly handled, Tor browsing can never be perfectly anonymous
        - When properly used, the Tor browser allows for one to browse traffic without worries. At a highly secure level of browsing, as long at the user does not intercept with compromised nodes in the TOR network, the user will never be identified.