Website Fingerprinting with Website Oracles

Summary

The Tor network is an anonymity network that users typically use for anonymous browsing. To do so, they use the Tor browser, which is basically a web browser, to either avoid censorship and provide anonymous onion services. When browsing a website through Tor over the internet, a client sends traffic through three relays, that is, the guard, middle and exit relay. Traffic sent from the client to the exit is encrypted in multiple layers, which offers the anonymity to the destination of the website. However, Tor faces a number of attacks which have been discussed over the years in the literature. One of this is the Website Fingerprinting (WF) attack. This is a type of attack where a local passive attacker, for example, ISP or router, tries to analyse the encrypted traffic from the client to the guard with the aim of determining which website will a client (in this case a victim) is visiting over the encrypted network. Nevertheless, a number of challenges exist in practice for the WF attack. For example, classifier false positive rates are one of the problems. This is because an attacker who is basically performing a WF attack over the network would have a lot of false positives, which would make it harder for the attacker to easily determine the website visited. As such, to bypass and possibly make the attacker of the anonymity network capable of pinpointing the website visited by a client with significantly few false positives, the authors of the paper introduce the notion of Website Oracles (WO). WO generally answers in a binary form (YES or NO) if whether a particular website, which was being monitored by the attacker over the Tor network, was visited at time t. A number of WO exists that can be used by an attacker; however, the authors present an ideal WO, which they simulate. They use the WO with WF to confirm whether monitored website was visited. This greatly reduces false positives.

Importance of the results

Even though a number of defences exist against WF attacks, the threat model designed by Tor does not take into consideration powerful attackers. While the authors aim is not to empower the attackers, showing the possibility of a WF with WO creates the need for Tor to have defences against low cost traffic analysis attacks (as there a wide range sources of WO) that make it difficult for attackers to monitor a website with high precision.

What is good about the paper?

Generally, the report shows that the Tor browser, while it offers anonymity, still faces some privacy and security challenges. The authors show how the Tor threat model is violated as it only considers that only incoming traffic can be monitored through WF attacks, which is not the case when undertaking a WF with WO. This basically shows both the incoming traffic (due to the WF) and the outgoing traffic (due to the WO). Furthermore, the research has raised a number of possible mitigations which are recommended, for example, the user is advised to do multiple things at once with the Tor client – this would create a hard time for the attacker to perform a classification (see https://blog.torproject.org/new-low-cost-traffic-analysis-attacks-mitigations for more).

Improvements

Considering the contribution made by the authors, the paper is well structured, easy to ready and understandable. However, the mitigation section could be a little bit longer of discussed further to break down the mitigations selected for further understandability.