Eavesdropping analysis over TOR networks

Matteo Martelli, Davide Berardi

February 16, 2015

Abstract

In this document we talk about blablabla

1 Introduction

Protecting data privacy on the Web is a very hot topic nowadays. Users of the Web may want to surf without the risk that their personal informations can be read by other users. One of the most largely-used architecture for this purpose is the *Onion Routing* and its protocol implementation: *Tor*[1]. In fact, the latter is modeled with several techniques with the aim to provide communication security and data privacy to its network users. Anyway there have been recent papers pointing out the Tor's vulnerabilities.

2 Onion Routing and Tor

2.1 Tor architecture overview

2.2 Tor attacks

2.3 Eavesdropping

3 Simulation

3.1 Shadow

3.2 Autosys plugin

3.3 Analyzer plugin

3.4 Simpletcp plugin

4 Data Analysis

4.1 Netbuilder Script

4.2 Analyzer Script

4.3 Empirical Results

5 Conclusions

References

[1] R. Dingledine, N. Mathewson, and P. Syverson. Tor: the second-generation onion router. :Proceedings of the 13th conference on USENIX Security Symposium, pages 21–21, Berkeley, CA, USA, 2004. USENIX Association.