Timing Analysis Attack Simulation in Tor Networks

Matteo Martelli, Davide Berardi

March 10, 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. As the Tor community itself stages, "Tor does not provide protection against end-to-end timing attacks"[2], thus the chance for an attacker to eavesdrop a Tor communication traffic and discover the users involved in it by a timing analysis is a well known vulnerability of Tor.

In this kind of analysis, in order to identify the source of a communication, the attacker should be able to trace the outgoing traffic and the incoming traffic from both the entering and exiting node of the communication path. Clearly a timing analysis is feasible only under a certain amount of conditions that are often hard to satisfy. As instance, discovering that a generic user U is connecting to a server S over a Tor communication may require tracing the traffic of many users in the network, as the attacker cannot know which users may be interested in connecting with S. Also, there may be the need of tracing more than just the interested server because the attacker can find a better time relation between the user U and another server S' than between U and the interested server S, thus the attacker could exclude U to be a possible connection source for S. In the section 2 we will better describe how Tor works and how the end-to-end timing attack could be performed.

In order to test the feasibility and the parameters involved in a time analysis attack over the Tor network, we set up a simulation scenario in which a series of simulation runs have been performed and some interesting empirical results have been taken out and analyzed. At the end we will point out how the Tor time analysis vulnerability can be critical and we will introduce some proposals to enhance Tor with the view of preventing this kind of attacks.

2 Onion Routing and Tor

Tor is an implementation of the onion routing architecture model. The onion routing consists in a technique that provides anonymous connections over a computer network[3]. This property is achieved closing the communication data stream through a chain of encryption steps.

The figure 1 shows how a message is cyphered before the communication begins. The communication source, before sending the message, choses a communication path of nodes which the keys are known to the sender. Then the source node is able to create a stack of encryption starting with the key of the last relay node and then continuing backwards with the keys of the other relay nodes in the chain. In this way every node in the communication path can decrypt the package and read the next hop address. After that the final node receives the message, he can send the response back to the originator of the data stream. In this phase the response message is encrypted sequentially by each node in the chain.

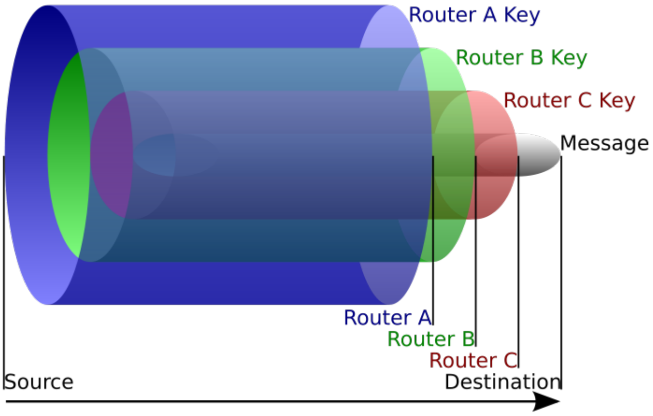

Figure 1: Message encryption layers.

2.1 Tor architecture overview

2.2 Tor attacks

2.3 Timing Attack

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.

[2] The Tor Project, Tor:Overview, https://www.torproject.org/about/overview.html.en

[3] D. Goldschlag, M. Reed, P. Syverson, Onion Routing for Anonymous and Private Internet Connections, 1999