Time analysis Based Attacks Simulation in Tor Networks.

Simulazione di Sistemi

July 17, 2015

Davide Berardi 0000712698

Matteo Martelli 0000702472

Università di Bologna.

Table of contents

Introduction

Standard *shapes* of information security:

- Confidentiality
- Integrity
- Availability

There is a new security that we want to obtain: **Anonymity**
Anonymity [...] means that the personal identity, or personally identifiable information of that person is not known.

Introduction
anonymity methods

There are a lot of anonymity driven software online, like *i2p*, *freenet* or *Tor*, we will talk about the last one because is the most used and expanded in the real world (2 million of client per day!).

Onion Routing

The onion routing model is a way to gain anonymity on the net:

- Provides anonymity
- Protects from sniffing

Introduced by David Goldshlag, Paul Syverson and Michael Reed in the 1999.

It recalls an onion because every step **peel** a layer.

Let us see an implementation.

Tor
The onion router

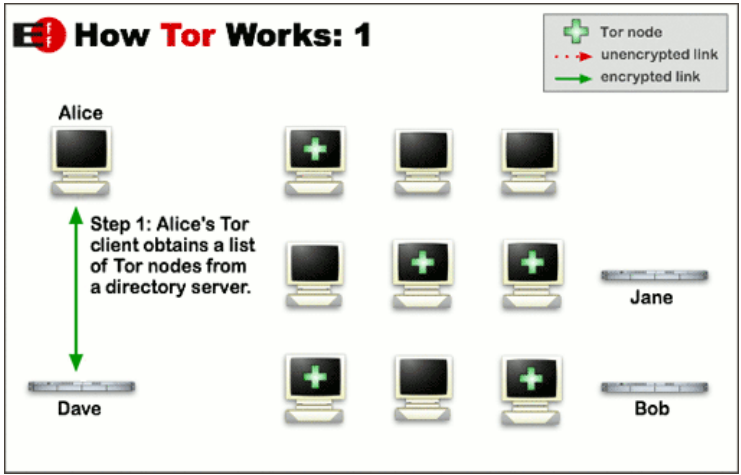
Overview

Tor is a group of volunteers that operates to defend anonymity online.
The system is based on an interconnection of machines, called **routers**.
It operates over the network level 4.

It operates as follow:

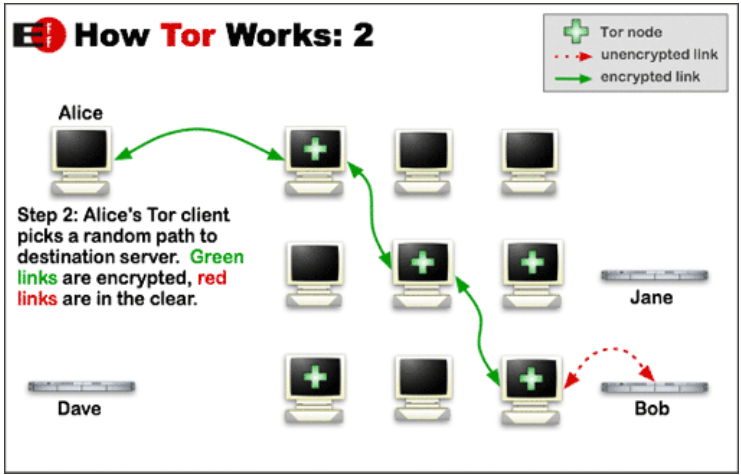
Tor

Tor workings



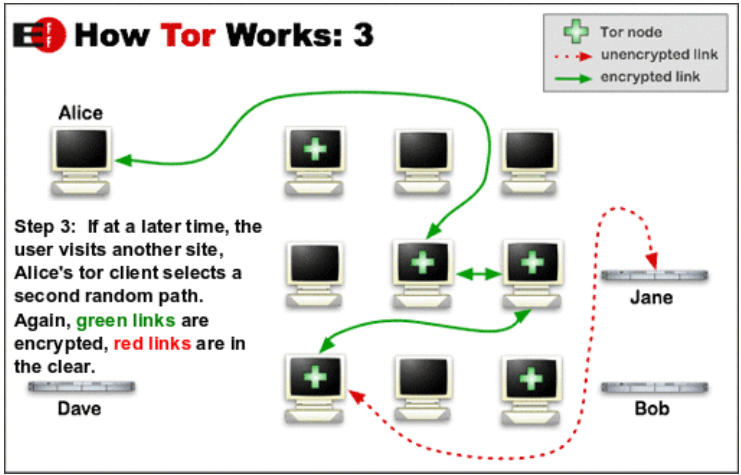
Tor

Tor workings



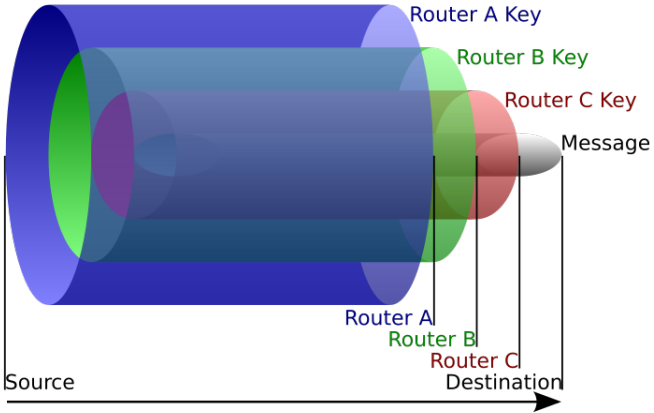
Tor

Tor workings



Tor

Tor encryption



Data Analysis

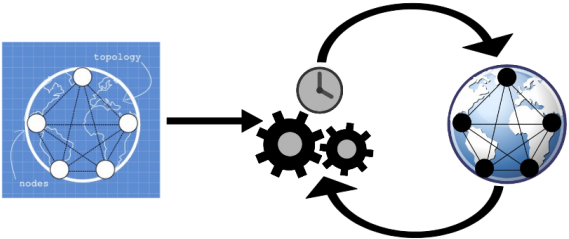
- Simulation Bunches
- Data Handler Scripts
- Empirical Results

$$score(c,s) = \frac{\sum^{N(c,s)} i = 0 pmatch(creq_i, s)}{gap_{AVG}(c,s) + 1} \quad (1)$$

Data Handler Scripts

Netbuilder

Genereates an XML file that describes the network



Netbuilder

Allow the network configuration through:

- The number of TOR exit nodes in the simulation.
- The number of TOR 4authorities[1] nodes in the simulation.
- The number of clients (simpletcp) of the simulation.
- The number of servers (simpletcp) of the simulation.
- The percentage of clients tracked by an autosys plug-in.
- The percentage of servers tracked by an autosys plug-in.
- The density of the network-requests.

[1] A 4 Authority node is simply the database that keep track of the state of the TOR network and the list of the TOR relays/exit-nodes

Netbuilder

The connection densities are the sleep time thresholds between each client connection request:

- Slow: 800 (mean) - 2000 (mean) milliseconds
- Average: 80 (mean) - 1000 (mean) millisecons
- Fast: 20 (mean) - 100 (mean) milliseconds

Launcher

Algorithm 2 Launcher script

```
for (simulation_run ← 1; simulation_run <= steps; simulation_run + +) do
    for (sim_id ← 1; sim_id <= simulations_per_step; sim_id + +) do
        for all density in (slow, fast, average) do
            if The client trace percentage is not fixed then
                client_trace_value ← sim_id/simulations_per_step
            end if
            if The server trace percentage is not fixed then
                server_trace_value ← sim_id/simulations_per_step
            end if
            if A configuration is present for < sim_id, density > And the percentages are fixed then
                Use the previous configuration
            else
                Generate a new configuration with net-builder
            end if
            Launch the Shadow Simulator with the appropriate configuration.
        end for
    end for
end for
```

Analyzer