Optimizing Tor Bridge Distribution

Michael Starzer

© 2013 The author and Karlstad University

This thesis is submitted in partial fulfillment of the requirements for the Masters degree in Computer Science. All material in this thesis which is not my own work has been identified and no material is included for which a degree has previously been conferred.

Michael Starzer

Approved, 12.12.2012

Opponent: Michael Seiwald

Advisor: Philipp Winter

Examiner: Donald F. Ross

Abstract

The Onion Router (Tor) is a good way to have privacy and anonymity while using the Internet. However there are several problems it has to deal with, because it is also possible to bypass governmental censorship, which also became goal of the Tor network. By different techniques several governments and other parties who have the capability to, try to block the network completely. One technique is to overwhelm the distribution strategies for bridges – which are an essential part of the Tor network, especially for censored users. Hereby a possible approach for distributing bridges via online social networks (OSN) is presented. It is based on the Proximax distribution but has also the capability to separate and exclude possible adversaries who managed to join the social group. Moreover trustful users get rewarded by a better status and less waiting time for bridges.

Contents

List of Figures

Chapter 1

Introduction

1.1 Motivation

These days using the Internet is daily business and there is no reason why this should change. But there is a raising demand for privacy when using it. The community wants to use the Internet in privacy or even completely anonymously and not being tracked by ISPs, the government or whoever has intention to do so. For this reason different approaches got invented to provide privacy while using the Internet. One of them is The Onion Router (Tor)[5], which is the follower of Onion Routing[7] which did not have forward secrecy, for instance. Although there were improvements to the original Onion Routing, Tor still has many issues to fight with. One of them is the distribution strategy, which is used to disseminate bridges[4] for users in blocked/censored regions. Bridges are exactly the same as onion routers but they are not public, therefore a distribution strategy is needed which should achieve that a user is able to get its addresses. At the same time she should not be able to get many bridges, otherwise they end up being blocked such as the public onion routers.

The actual distribution strategies are more or less working[1], but there are a lot of improvements possible and in this work the distribution over online social networks will be discussed and a possible distribution strategy is introduced.

1.2 Goals and Objectives

In this work a distribution strategy will be presented which is adapted towards the needs of the Tor network. The distribution strategy shall handle the distribution of bridges over online social networks. The distribution builds upon the Proximax[6] distribution but is adapted. The reason for the adaption is to separate a possible adversary from the legit user once she joined the network and banned bridges. The main goal of Proximax remains, means maximizing the user hours for bridges.

1.3 Thesis Structure

The second chapter of this paper gives an overview of Tor and how it works in detail. Afterwards the third chapter shortly explains different types of attacks and what an adversary wants to achieve with it and what an "attack" really means. The main chapter is the fourth, which gives a glance on Proximax and in the second part of it, the actual approach is explained. In chapter five and six the results are presented and a conclusion is given.

[1]The distribution works, the problem is that the adversary often can abuse it to gather the bridge addresses and ban them.

Chapter 2

Background - Tor

2.1 General Purpose of Tor

The goal of Tor (The Onion Router) is to make it for users possible, to use the Internet[1] anonymously and grant privacy. Another goal of Tor is to give censored users the possibility to skip the censorship of the government.[8]

2.2 Privacy and Anonymity with Tor

How does Tor guarantee that any user can surf in the internet anonymously? It is pretty simple; the usual way of surfing in the internet is that a user tries to connect to a server (e.g. a webserver). This webserver has an IP address which is used to establish the connection. All routers, servers and networks the request passes by can see the IP address of the user, because of the Internet protocol. There is always a source and a destination IP address in the header of it and so everyone on the way to the destination can see where the request came from and where it goes to.

[1] Tor can only be used for TCP streams and supports any application with SOCKS support.

The easiest way to "remove" the IP address of the request is to use a proxy, which does nothing less than forwarding the request to the destination. The difference is that the user opens a direct connection[2] to the proxy and the proxy opens a connection to the webserver the user wants to access. So the source IP address of the request is the address of the proxy and not of the client. But there are so called "correlation attacks"[5] where the attacker watches the connections of the proxy. So the attacker will see that after the user connected to the proxy, the proxy opens a connection to the webserver. So the attacker can estimate that the user is connecting to the webserver. That is one of the reasons why Tor uses three[1] hops to connect to the destination address. That means a client connects to the first proxy (Onion Router "OR"). The first OR will open a connection to the second which opens a connection to the third or last OR. The last OR will finally open the connection to the destination server. So if an attacker can monitor the traffic of any of these proxies, she will not find out to which destination the user is connecting, which means she can surf anonymously.[8]

Nevertheless the user has to tell each proxy to which proxy it must connect to. The last proxy needs the address of the final destination. That is one of the reasons why the whole conversation has to be encrypted; otherwise the attacker can just read the addresses the user wants to be connected with. The conversation between all participants is encrypted and therefore confidential[3] if protocols such as HTTPS are used.[5]

[2]There are seldom direct connections to a proxy, some routers will always be included
[3]The last connection to the destination is unencrypted by default.

2.3 Tor Routers

The Tor network relies on three different roles of Tor routers. The first one is the so called entry node. It is the first router the client (user) connects to. The second one is a more or less normal router which receives a connection of the entry node and opens the connection to the exit node. The exit node is the last router and opens the connection to the destination server. The last connection is unencrypted by default. Therefore if the user wants to have an encrypted connection to the server, she will have to use a proper protocol such as HTTPS.[5]

2.3.1 Entry Node

The entry node is the first OR the client connects to, therefore the client has to know about it. All Tor routers are public and the Tor client can call them from a directory. The problem is that an adversary also can call the addresses of Tor routers and can easily block them. Therefore the whole Tor network can be blocked in the adversaries controlled region. For that reason there are so called bridges which are not public and will be explained in more detail later. There are several ways to get the address of a bridge such as via HTTPS, e-mail or by social networks. But the problem still exists, because if an adversary knows many or all bridge addresses she might be able to block the Tor network again. A good example for blocking the Tor network is China.[11, 12]

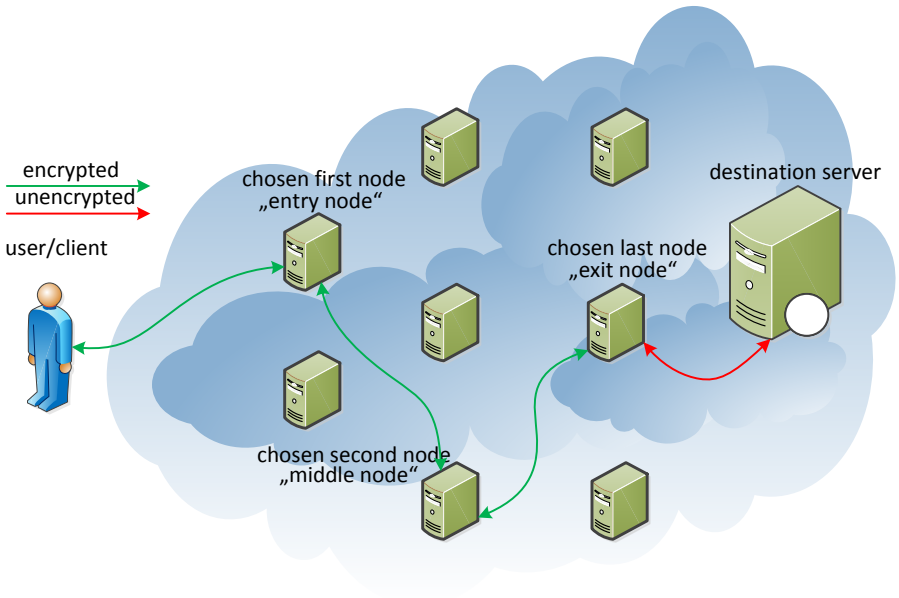

Figure 2.1: This is an overview of the Tor network. It shows the three different roles, called the entry, middle and exit node.

2.3.2 Middle Node

The router between the entry node and exit node is the middle node. There are no big requirements to become a middle node, because it just responsible for transfering the data between the other two. But still it is essential to make sure it is a ”legit” middle node what means that is not controlled by an adversary. If it is controlled by an adversary she will be able to monitor the traffic which will reveal all connected entry and exit nodes to her. Nevertheless the transmitted information (where does the connection come from, where does it connect to and what data is sent) is still secure. Means a compromised middle node is no problem for the user in respect of privacy and anonymity.[12]

2.3.3 Exit Node

The last node of the circuit is the exit node, which finally opens a connection to the destination the user wants to connect to. This last connection is not encrypted obligatory. It depends on the destination server and the protocol used. If an adversary monitors a known exit node, she will not find out the source address (the user) which wants to connect to certain destinations. But she still can monitor the traffic to find out, which connected middle node connects to which webserver. Despite the fact that there is no relation between the middle node and the user it is no problem for the privacy even if the adversary controls the middle node.[12]

2.4 Onion Routers vs. Bridges

There are no big differences concerning functionality between onion routers (OR) and bridges. The main difference is that onion routers are public to all Tor clients which also keep a full list of all available onion routers. Bridges are non-public onion routers which are distributed via e-mail, HTTP and social networks. Another difference can be the bandwidth of bridges/relays, because every Tor user can become a bridge/relay in order to give blocked/censored[4] users access to the Tor network. Bridges are essential for blocked users to access the Tor network. Therefore they must not be revealed to the adversary and it should be almost impossible for her to enumerate all or most of the bridges. An adversary will always be able to find bridges, but it should be as hard as possible for her to do so. Otherwise if the adversary can block all or most of the bridges, she might be able to block the Tor network completely.[4, 5, 8]

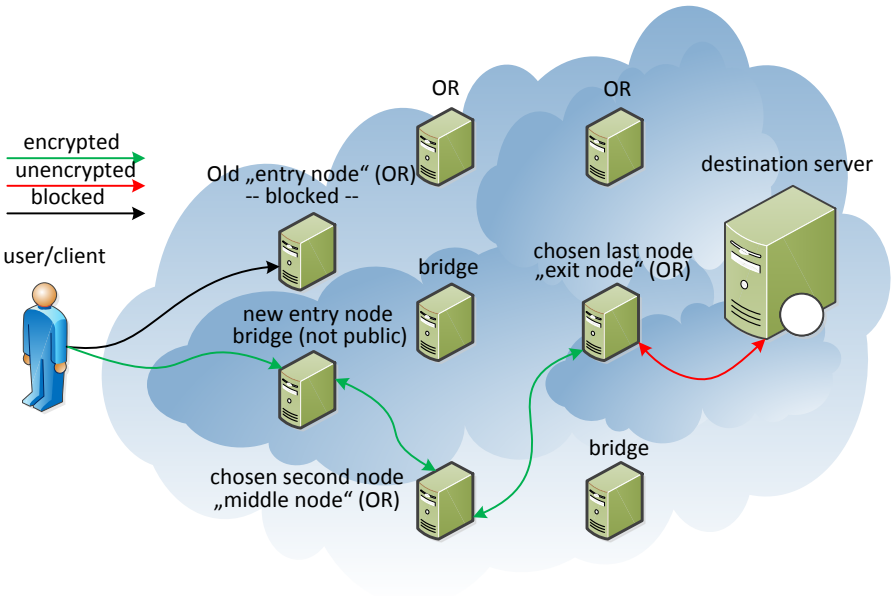

Figure 2.2: This illustrates the difference between a Tor bridge and a normal Tor relay. The relay is public and known and can be blocked easily. Therefore the user has to use a Tor bridge (which is not public) as first hop.

[4]Blocked/censored users if she decides to become a bridge. When she chooses to be a relay only, her relay will be public announced for all Tor users and will not help blocked users.

2.4.1 Tor Directories

However there are also some additional servers, which have to deal with the information about the onion routers, which are available etc.

Main Directory Authority

The main directory authority is responsible for the core network and provides a list of every known onion router.[4]

Bridge Directory Authority

The bridge directory authority provides the information of all known bridges. Clients can access the bridge information by e-mail/HTTPS servers or by social networks. It is very important that every user gets only few bridge addresses to make it more difficult for the adversary to do enumeration attacks, which will be explained in chapter three.[4]

2.4.2 All together

Onion routers but also bridges can be used for every purpose[5] (entry, middle and exit node). But it is dependent on the features they provide. The entry nodes need to provide an uptime which is above the average of similar routers and a minimum of bandwidth, if so they earn the entry guard flag. This flag means it is a reliable entry node.

Exit nodes need to allow outgoing traffic and must have at least one C class IP address space. Nodes which meet the requirements for entry and exit nodes are marked as both, means they can be used as an entry or exit node but only once in a circuit.

Middle nodes have no requirements. That means every router in the Tor network can be a middle node and will be used only for relaying the traffic. The above described routers are notated as follows:[12]

[5]It is always depending on the features the user wants to provide. Therefore if she chooses to be a relay only, she will not become an exit node.

- Pure entry guard:

  Bridges marked with the entry guard flag only.

- Pure exit node

  Bridges marked with the exit node flag only.

- EE router

  Bridges marked with both flags.

- N-EE router

  Bridges marked with none of the flags and therefore middle nodes only.

Which bridge will be chosen for a certain connections depends on the bandwidth. The algorithm tries to pick the best choice for a connection, but never picks the same routers for the same or additional connections.[3]

2.5 Functionality of the Tor Network

2.5.1 Communication and Cells

First of all, every connection is secured via TLS. The communication between Onion Proxy and Onion Router, but also between OR and OR is handled by using "cells". There are control cells and relay cells which are always 512 bytes consisting of a header (circID ...) and a payload. Control cells are interpreted by the receiving OR while relay cells are forwarded to the next OR and have an additional header for the stream ID. There are several commands for each type of cell, which will not be explained further.[5]

2.5.2 Building Circuits

A circuit is every connection between any user and any onion router. Therefore when a user starts to open a connection to any webserver the first circuit is established with one of her entry nodes (the one she choose for the path). The connection is secured by TLS using the Diffie-Hellman handshake. After a secure channel has been established to the first node, the user may extend the connection to the next circuit, sending the node a "relay extend" cell. This cell already contains the first half of the Diffie-Hellman handshake for the TLS connection between the second node and the user, which will send a "relay extended" cell with her half of the Diffie-Hellman handshake back to the user. After this, the connection has been extended to the second node of the circuit. Now the first node only transfers encrypted data to the second one and is only able to decrypt the connection between the user and itself. To distinguish between the connections, each connection between any participants of the circuit has its own circID, which can be found in the header. The connection to the third node works the same as to the second one.[5]

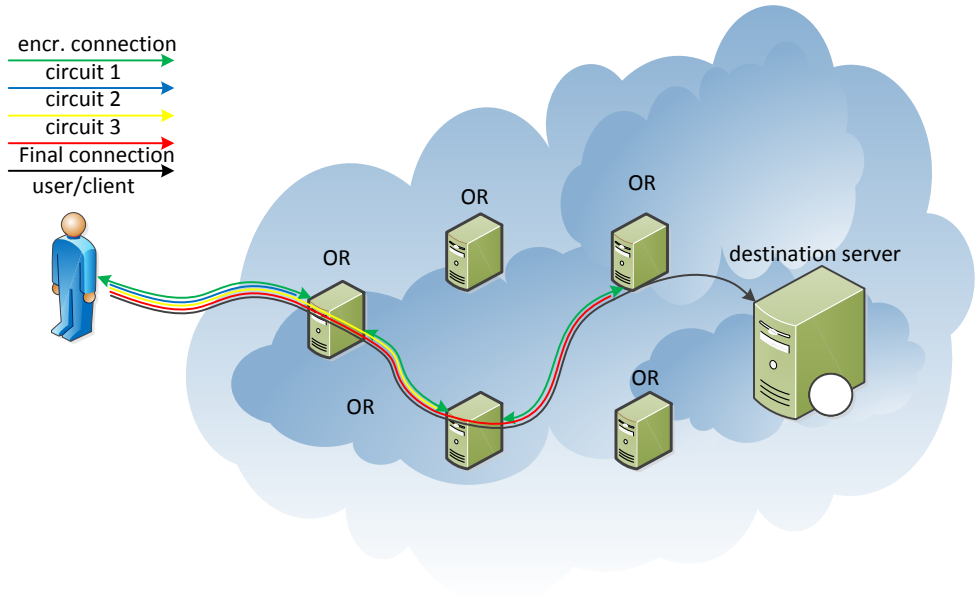

Figure 2.3: This figure shows how the circuits are created. Each node has an encrypted connection to the other node. The encrypted connection from the user to the first node gets extended one by one. The final connection to the service is by default unencrypted but can be secured for instance using HTTPS.

Chapter 3

Blocking Tor - Enumeration Attacks

3.1 Overview of the Attacks

This chapter is about attacks concerning the Tor network, but it is important to know that we are not talking about attacks against the Tor network itself. These attacks are so called enumeration attacks, which will be explained later. But first, we need to know how to block the Tor network. An adversary who wants to block Tor just has to block all its relays. If she is successful doing this, no user in her controlled region will be able to open a connection to a Tor relay and therefore she blocked the Tor network. Blocking Tor relays is quite easy, because all "normal" Tor relays are public and can be retrieved via the main directory authority. That is why bridges are already a countermeasure, because they are private Tor relays and it should not be possible to access a list of all bridge addresses. With the enumeration attacks, which mentioned before, an adversary tries to find all Tor bridges so she can block them in a region of her control. She might do this by monitoring traffic, running own bridges or just receiving bridges by the distribution strategies. There are several known enumeration attacks, which will be described shortly.[10]

3.1.1 Overwhelm the Public Address Distribution

This way to enumerate bridges is common, because it is very easy. There are several ways for a user to receive a bridge address. The problem is the adversary can do the same and pretends to be a legit user and receive a bridge address. She has to do it quite often to receive many bridges and there are already limitations for receiving addresses such as the amount of bridge addresses per IP address range or CAPTCHAs as proof that an actual human tries to receive it.[10]

Concerning the other ways of distribution such as gmail and yahoo mail, they rely on the provider to prevent mass creation of e-mail accounts with which the adversaries can gather bridge addresses. But there are also limitations such as the bridges distributed per e-mail address.[10]

3.1.2 Run a Relay to get Bridge Addresses

There are different ways to discover bridges. The adversary can simply run a (guard) relay and watch the connections. For instance, if she runs a relay that is a middle node only, then the entry nodes are the only ones connecting to it. Those can be normal (guard) relays or bridges. If you sort out the normal relays you got bridge addresses. Another way would be connecting back to all clients that connect to your relay and find out which ones are talking the Tor protocol. This is possible because the most bridges are listening on the port 443 and 9001 for incoming connections. There are some more ways with which Tor bridges can be found but will not be explained here.[10]

3.1.3 Watching Network Traffic

Since the bridge authority does reachability tests it will be very obvious that this can be used to find bridges by just observing its network connections. Even if the testing is done by using the Tor network itself, it will be a problem, because the adversary then just

watches the relays and gather bridge addresses which got tested for reachability. The next method that can be used is to "zig-zag between bridges and users"[10] which is simply watching the connections of the firewall. This approach needs some bridges so start with. The procedure is to watch who is connecting to the bridges and then monitor her for possible other bridges she connects to.[10]

It is also possible to use deep packet inspection (DPI) and look for unusual SSL flows. On the other hand active followup scanning is also possible to find out to what other destinations the original one goes to. If the final destination is ok then whitelist it. Another approach is to blindly scan the probable servers if they talk the Tor protocol. This is simply done by pretending being a normal client.[10]

3.2 Detecting blocked Tor bridges

3.2.1 Active and Passive Testing

There are two main methods of testing bridges for their reachability. Both have their advantages and disadvantages. First, passive testing does not reveal any information to the possible adversary, because the bridge is reporting statistical information about usage, utilization, etc. to the bridge directory authority. The communication is encrypted and therefore secured from eavesdropping. The information of the bridge can be accessed and used but still, a bridge which has low or no usage, need not imply it is blocked by certain regions. The other passive approach is to test the reachability via clients and let them report the results. The problem here is that they could report wrong information (for instance, an adversary might will do this) to make the BDA think the bridge got blocked. On the other side there is active testing. Active testing means that a user or tester tries to connect to the bridge and check if it is reachable. Here are problems as well, because if the user is in the non-blocked area she will just be able to test if the bridge is set up properly and no configuration mistakes are made. For real tests of the reachability, the test must be from a user or client from the inside of a blocked country.[9]

3.2.2 Statistic Information of Bridges – Passive Testing

There is a lot of statistic information which can be gathered from bridges. But it is very important to know what it means and what it may not mean. For instance a low usage rate of a bridge doesn't necessarily mean that it is blocked. There are some possible reasons for low usage:

- Bridge authority directory did not get the information about it, so it cannot be published properly
- Configuration mistakes, so the bridge doesn't work at all

- Bridges are not as "busy" as usual relays, therefore it might has a lower usage rate
- Bridge was not distributed yet, because of
  - the uptime
  - the bandwidth
  - the latency or any other reason

To get a better picture what certain information really means, it is obligatory to combine all other possible information which can be gathered. Very useful information could be the origin of users connecting to the bridge. Every bridge will know how many users come from certain regions. This information should be divided into blocked areas and non-blocked areas and the blocked areas should be divided further into all known countries which censor their users. With that information it is possible to see drops in usage and if the drops are random and in certain regions such as China. If a region such as China drops in usage it is most likely that the bridge got banned. Nevertheless if there were no or just a few users in a region anyway, it may be used to examine why there are not more users. All these information must be gathered over a period to see changes and effects of the active testing, which will be described below.[9]

3.2.3 Reachability Tests – Active Testing

The active testing should be used to test bridges which may have been blocked or don't have high usage rates. The information gathered by passive testing described above shall help to find out where the tests should be run from. That means if there are drops from China, the tests should be run from China to get accurate information about the reachability.[9]

Chapter 4

Distribution Strategies

4.1 Threat Model

The potentially adversary could be a censor and probably has access to resources of a country. The following capabilities are assumed, which will be used in order to find as many bridges as possible. Once she knows a bridge address she is able to ban it.

Network traffic

It is assumed that the adversary is able to monitor both ends of the communication and therefore she can act actively and passively. Nevertheless it is unlikely that she is able to break state-of-the-art cryptographic systems.

Control of involved parties

It is assumed that the adversary has some or full control of an involved third party. Therefore could be able to monitor, change, delete or add content to certain servers, for instance any online social network. But we also assume that there are certain third parties we can rely on.

Servers of the approach

We assume that the adversary is not capable of taking over the main servers which

will be needed for this approach to run. But she might be able to observer a fraction of the server's traffic. It is assumed the adversary can perform all possible kinds of attacks which can be run versus a server which is part of the Internet, for instance (D)DoS.

Sybil attack

The adversary could simply flood the system with benign users in order to get as many bridges as possible. It has to be mentioned that even if she just floods the system with users, each user will get the same bridge unless it gets blocked. Further more detailed attacks are described in section 4.3.7.

4.2 Related Work – Proximax

Proximax is developed for distributing proxy addresses in social networks[1], therefore a user gets a proxy address, gives it to her friends and those give it to their friends.[6]

At first they use "trusted" or "registered" users, who get the proxy address to distribute. Each of these users gets her own channel with her own unique domain name. This domain name is also used to track the amount of users for each channel. All channels get their own proxy address for distributing among the users. The amount of users and the time the proxy was online (means not being blocked by the adversary) determines how well a channel performs.[6]

Proximax does not define how to share or distribute the proxies to the end user and is therefore independent. The registration of new users is only possible by an invitation of an existing registered user. The invitation will be granted, if the performance of the inviting user, but also the performance of her already invited users is in good standing. That means, if any node or sub-tree of the inviting user performs poorly, the invitation is denied. For that reason, each user has a reputation score, which determines how well she

[1] Any social contact can be seen as 'social network'.

is performing. The reputation score of the inviter's nodes and its descendants also affects the score of the inviting user. For producing a performance score the user hours and the number of blocked resources are used. The general goal is to maximize the user hours per channel and have full utilized proxies.[6]

To protect channels from being discovered and banned, Proximax uses "fast flux". Fast flux is usually used by botnets and malware distributors.[6]

4.3 Distribution via Online Social Networks

The following distribution is similar to Proximax but includes extensions particularly targeted towards the needs of the Tor network. The differences include the distribution of proxy addresses to the users, the reputation system and a very important one is that this system splits a possible adversary from the legit users over a time period. Further differences and details will be described below.

4.3.1 General

At first there are "trusted" users, which are in the same group and share a proxy. To be equivalent to Proximax they share a channel.[6] Each user invites her friends and those again invite their friends. As long as the channel has not been blocked, they all share the same proxy address. There is some information which will be tracked of every user:

- Invitation date
- Inviting user
- "Trustworthy level"
- Last point of time her proxy got banned
- Current group
- Duration in her current group[2]

The longer a user is in the system and the longer the proxy isn't blocked, the better her trustworthy level becomes. The amount of the invited users and their trustworthy level can also be considered. There will be three major groups in which the users will be divided into:

[2]Current unblocked hours using the proxy.

- Fully trusted users "group 0"
- Trusted users "group >100"
- Unknown/untrusted users "group ≤100"

4.3.2 Invited Users

In this approach invited users will never become fully trusted users, so if the group 0 gets banned, only the original fully trusted users will join group 0. The trustworthy level of users, which got invited by other invited users, will start with the trustworthy level of the inviting user -1. That means every time a user invites another one, the invited one will be a little bit less trustworthy for the system. The following figure illustrates a new group 0 that invites several users and those invite other users. After some time the proxy of that group gets blocked and the group is split.

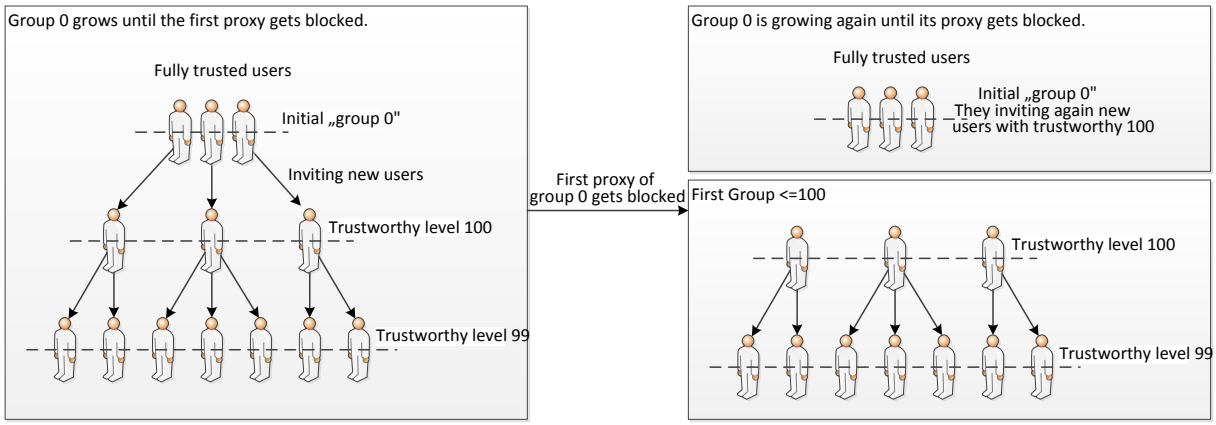

Figure 4.1: This illustrates how the initial group 0 is growing. It shows the trustworthy level of the users and how the group is split due to a proxy ban.

4.3.3 User Reputation

The group ≤100 will be divided into two new "group ≤100" groups every time a proxy gets banned. Each group gets one proxy (if necessary more are possible too). If the proxy gets banned, each user of the banned group is redirected to another group, dependent on her trustworthy level. Therefore a user with a trustworthy level below 100 will join one of the groups "≤100", any user above the group >100. All users invited by fully trusted users (group 0) will start with a trustworthy level of 100. Therefore they are not trusted at all in the very beginning. The user's trustworthy level will change in following situations (see figure 4.1 and 4.2):

- The proxy of a group gets banned → trustworthy level of all users in the group decreases by 1 ("Similar to the RICO Act[2] in the legal system, once a subnode is suspicious the whole subtree is equally suspicious."[6])
- Every time a user is in an unblocked group (=proxy did not get banned) for X hours → her level increases by 1

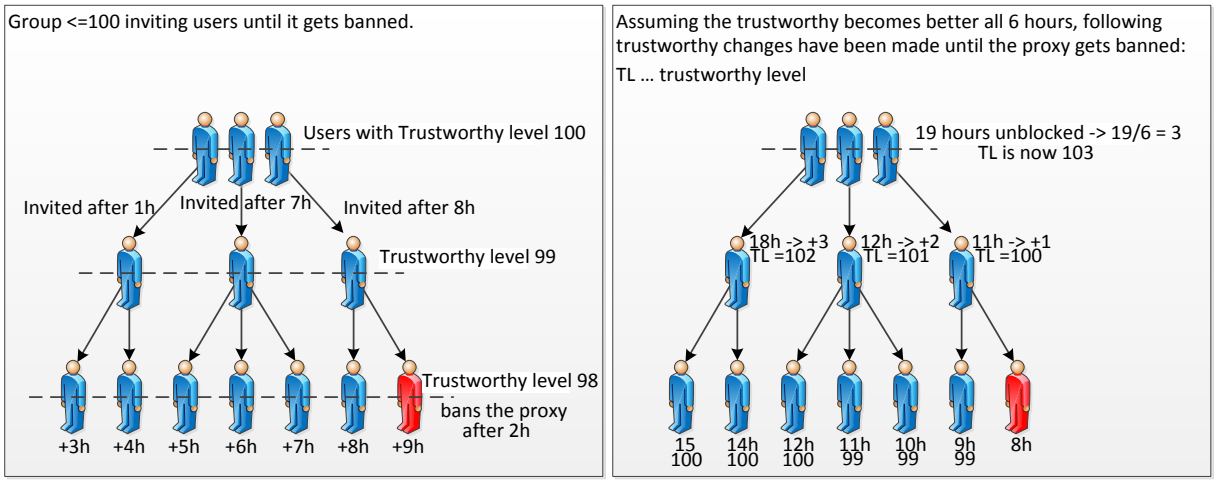

Figure 4.2: Trustworthy level changes over time, depending how long the user is in her group and how long the proxy has not been banned.

4.3.4 Adversary in Group

The problem of an adversary joining a group will be that she is able to block its proxy. That means all users of the group decrease in trustworthy level and the group splits into 2 new groups, each with its own new proxy. At least one of the proxies will be banned again, because the adversary is still in one of the new groups. She might do this until she is alone in a group and until then she will have blocked a lot of proxies. Because of the fact that the adversaries trustworthy level decreases every time she bans a proxy, her waiting time for a new proxy will increase. Therefore the ability to block a lot of proxies in a short time gets decreased. Unfortunately this will affect all users of the actual group, means legit users have to wait longer too, before they get a new proxy. Nevertheless the group becomes smaller by approximately 50% every time she bans a proxy and so fewer users are affected.

By these rules, it should be possible to reward trusted users, because they join a "more trusted" group (>100) and therefore their proxy should not be banned as quickly as in non-trusted groups. Moreover the trustworthy level determines how long it takes for a user to receive a new proxy.

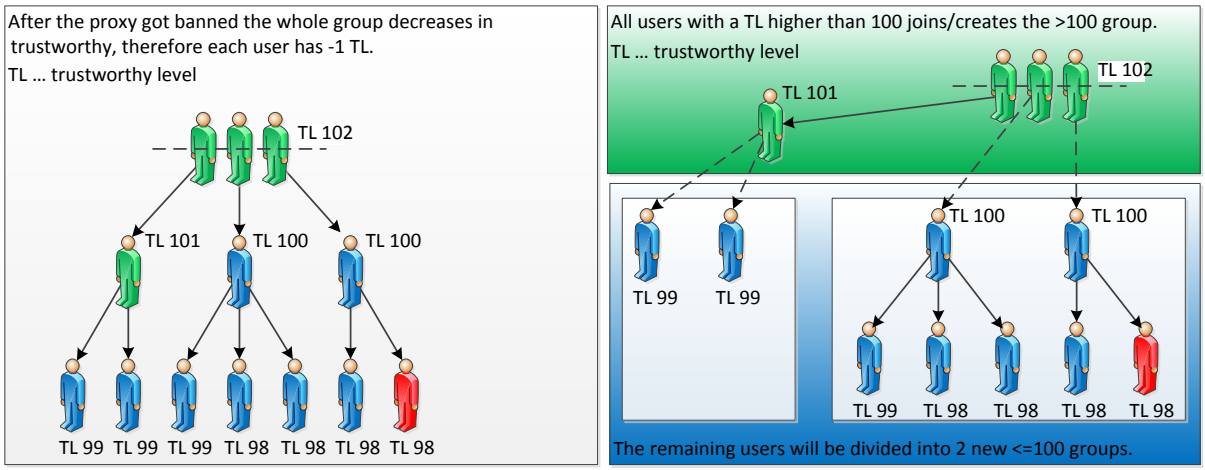

Figure 4.3: Users with different trustworthy level will join different groups whenever a proxy got banned. This is illustrated here, where users join the group >100 due to their actual trustworthy level. All other users are divided in 2 new groups.

4.3.5 Splitting Groups

Whenever a group is split, all relations between users will be kept. Nevertheless if some users are swapped to another group because of their trustworthy level, their leaf-nodes may become a new root node for their sub tree in the current group. There will be no 50:50 splitting in respect of the amount of users, but there will be a 50:50 split of all current "root"-nodes of a group. For instance, a group 100 consisting of seven users with trustworthy level 100 (the root nodes of the group) will be split into two groups of three and four users each. All sub-nodes of those users will follow their root into the group. If a group consists only of one root, the group will split 50:50 of its sub-nodes and the root follows randomly into one of the new groups, but stays as root-node of the group it follows. With this method, it is possible to split the root of a group from the adversary, so it will be protected of frequent bans of its proxies, if one of her friends or friend's descendants invited an adversary.

A group, or as we called it in the beginning – a channel, can be handled such as it is

described in Proximax.

4.3.6 Registration

At the beginning the registration is handled similar to Proximax, because there are trusted users. In Proximax the users register a channel[6] while in this approach they create a group or something equivalent on an online social network. Each of these groups will be a group 0 and is a new entity of this approach. That means they get their own proxy addresses. Those are the only real groups in online social networks, all other groups (the group >100 and all groups ≤100) will be created in the system only and are invisible for the user. Therefore the users don't know in which group they are. As mentioned before all users invited by the trusted ones will have a trustworthy level of 100, all others will start with 99, 98 etc.

Each user who joins a group 0 will be registered afterwards and her information will be tracked. To be independent from any online social network (OSN), the distribution and the information tracking/gathering will be handled on an own server which sends the proxy addresses via e-mail to the users. This means, the social network will be used only for registering users. If we take Facebook as an example, any private group/channel with invitation only can be used for that matter. The e-mail addresses can be picked up there and sent to the system. The only important issue is that the adversary must not flood such channels/groups with legit users.

4.3.7 Possible Attacks on this Approach

- **Adversary floods a channel with legitim users**

  When the adversary joins the group, she simply invites more and more "legit" users which she has under control. Doing this has no big cause to the system or at least not for all other legit users, because of the fact that the invitation tree will stay. Therefore the adversaries will be all in a group at one point of time and after this

point the group is always split into 2 groups full of adversaries. Of course they still can ban the proxies but no user will be blocked and additionally to protect the mass banning of relays the time until they get a new proxy increases as well.

- **Invite a lot of users, gain trustworthy and delayed blocking**
  This attack might work very well, but it needs some preparation. The principle is that the adversary invites a lot of users of her control and then she waits until she and the invited ones join the trustworthy group (group >100). To do so she must wait (depending on her initial trustworthy level) and ban the proxy. When she successfully joins the group >100, she can start banning the proxies until she gets another proxy address than her descendants. By this information she knows that they just left the trustworthy group and joined a ≤100 group. All her descendants are now a "root" node of the ≤100 group. If she has invited a lot, means she outnumbered the legit users, then they can start to ban the proxies of their groups. Because of the 50:50 splitting her descendants will also join groups of legit users. In the beginning the legit users are affected by this but it will not take a long time until they are separated from the adversary again. The real problem might be that the adversary creates a lot of groups and ban bridges. But still there are difficulties for her to make this approach effective:[6]
  - The adversary doesn't know her trustworthy level, means she cannot tell:
    * When her trustworthy level is good enough → a lot of time of unbanned proxies for the users, therefore the user hours will remain good.
    * If she tries to ban the proxy to join the trustworthy group (>100), she will not know if she joined the group or not, because if she and her descendants get the same proxies it does not tell her more than they are in the same group. Therefore she has to try blindly and hope she is already in there.
  - She has only one try, so if she fails and starts banning too early, she will be

quickly separated from the legit users and will have a very poor trustworthy level, therefore she will not get bridges.

  - The users will be affected only for a short time and all proxies the adversary bans will not have been distributed anyway and the legit users will be quickly in a group separated from her with a proxy she will not receive by this approach. It probably ends up that the adversary is banning the bridges just to decrease the proxy pool.

  - Every time a proxy gets banned the waiting time increases depending on the frequency of the bans and the trustworthy level of the users.

- **Adversary gets control of the operating servers of the approach**
  If the adversary gets control of an operating server, she might be able to ban all bridges the server receives for distribution. The same problem exists if the adversary takes over a bridge directory authority; therefore the server has to be run by the same party or should be protected as well. How to protect or run the server is out of the scope of this paper.

- **The online social network is controlled by the adversary, therefore can read, modify or delete social groups of it**
  It will be a problem if the adversary controls the social network and is able to read the content and modify groups, channels or private group conversations. If she is able to do this, the following things she could try to stop the distribution:

  - She might join all groups for the distribution, maybe multiple times also changing "her inviter" to many different users in the group. Therefore she will be in many groups and will not be split away from the other users because she is in many different trees.

  - She simply deletes all the groups she might thinks are used for distribution.

  - She could ban or delete all creators (the users of the so called group 0 of the approach) of such groups too. Therefore she tries to keep them out of the social network so they cannot create new groups for distribution.

  If the adversary can "only" monitor the communication between the user and the online social network, then it is probably not a huge problem, because she still has to find the groups. The groups will not be called or at least should not be called "Tor distribution group" and therefore she should have quite problems finding such groups. If she does, she has to track down the IP addresses of the users and monitor their activities to find the bridges. If she can join the group as legit user, for instance by modifying the communication, then she could try the same attack as explained above by flooding the group or whatever approach she wants to do.

- **Tracking down users of the social network**

  Because of the fact that it is a social network, the adversary can try to gather all users using this approach to get Tor bridges. There are several things she could do if she succeeds. For instance, if she gets to know the IP addresses of the users, she can try the "Zick-zack between user and bridge"[3] attack to gain all the bridges the user(s) got.[10]

[3]Based on the attack explained in section 3.4.

4.4 Summary of the Approach

In this section the differences to Proximax are described but also the goals and benefits of the approach explained above.

4.4.1 Aims and Goals

One of the most important goals is to maximize the user hours such as Proximax does.[6] For that reason, the second goal is to enhance the usability for "trusted" users and try to put them all together in a group where their proxy will not get banned as quickly as in untrusted groups. Moreover trusted users benefit from getting new proxies more quickly and enjoy therefore a better performance of the system. That is why the system aims to separate the adversary from legit users by reducing her trustworthy level. In the end the adversary should be alone in a group and will be banned out of the system. To summarize the goals:

- Maximize user hours for each group/channel.
- "More trusted" users shall be rewarded with
  - less waiting time for a new proxy,
  - more seldom proxy bans,
  - not losing their trustworthy by a proxy that gets banned if they were trusted for a longer time and
  - sharing a channel with other "trusted" users.
- The adversary shall be separated from normal users by
  - increasing her waiting time for a new proxy,
  - decreasing her trustworthy level and

  - splitting her group until she is alone.

- Giving untrusted users the chance to increase their trustworthy by
  - inviting users which don't cause a banned proxy and
  - being in an unbanned group for an amount of hours/days.
- Using online social networks as registration platform only.
- Being independent from any online social network and transparent reputation system.

4.4.2 Differences to Proximax

Distribution of the Proxy addresses

The first difference to Proximax is the distribution of the proxy addresses themselves. In Proximax they get disseminated by the users, while in the approach above they get distributed via e-mail. Therefore the social network is used to invite users and create a tree of users. Each user has an own trustworthy level. This approach speeds up the distribution of the proxies when they get banned and it is not relying on the users to distribute it.[6]

Invitation of new users

In Proximax there is a reputation score. This score is computed by the performance of the current user but also of all her invited users and theirs descendants and so on. The principle is the same as above; once a sub node is suspicious the whole sub tree is suspicious. The first difference here is the computation of the score, because the reputation of the presented distribution is derived of the invited user and is simply changed every time something happens, such as a proxy gets banned or the user is in the group for a long time not being banned. The second difference is that a user, which performed well but suddenly, is getting banned may joins the more trusted group of users. Therefore she might escape the adversary, which just got invited

by someone in her sub tree. In Proximax the reputation score is used to decide whether the invited user is allowed to join or not depending on the inviting user's performance.[6]

Groups, channels and trustworthy

The approach of this paper also uses groups, or how it's called in Proximax – a channel.[6] The groups are slightly different, because a channel in Proximax is always registered for one fully trusted registered user. This user invites her friends and those again their friends. Such channel always shares one or more proxies for its users. The actual proposal also has fully trusted registered users, but there is no channel registered for them. They may create one or more groups for inviting friends via any online social network. There are more than one of fully trusted registered users in such a group (group 0, as described earlier) possible. Each group is split into other groups (group 0, group >100 and probably more ≤100 groups), whenever a proxy gets banned. Means that new groups such as group ≤100 and >100 are created. To compare it to Proximax, each channel of Proximax consists of one group 0 (fully trusted users), one group >100 and (probably) many ≤100 groups.

Automatically distribution

Proximax is independent of any social network and the distribution is done by the users themselves.[6] That means, every time a proxy gets banned, the registered user has to distribute the new proxy addresses to her friends, those to theirs again and so on. Therefore the registered user has a higher burden to distribute the proxy addresses. The difference here is that the proxy addresses get distributed automatically via e-mail and the invited users have nothing to do with it. Additionally it can be easier to separate the adversary from the group because every group gets one (if it is a huge group maybe more) proxy address and every time the proxy gets banned the group is split in two new groups of almost 50% users each. Moreover there are

statistical information of every user, such as which proxy did she get, how long was the proxy online, when the user joined the group. This information is probably hard to gather if the users give one or more proxy addresses to their friends in any way they like.

Trustful users may join a more trusted group

A big difference to Proximax is the fact, that probably trustful users join a more trusted group to evade permanent bans from untrusted groups.[6]

Chapter 5

Results

5.1 Goals reached

The resulting approach is based on Proximax and also shares the goal of it – maximising the user hours per bridge. Moreover the trusted (core) users were used from Proximax. Those are trusted and are responsible for "their" channel, although the channel is called a group and trusted users can have more than one group where they can invite users. Also a reputation system was implemented, but it changed to give trusted or more reliable users a better status. The management of the groups should be the same as described in Proximax, using fast flux.[6]

By theory, every online social network can be used for this distribution strategy as long as it implements the following features:

- Provides private groups/channels which can be only accessed by invited users,
- it keeps track of whom invited whom and
- the e-mail addresses can be retrieved (posting in a general chat of the group is possible too).

The following goals should have been reached:

- Maximize the user hours for bridges
- Separate adversaries from legit users

Maximize the user hours for bridges

Until further evaluation the goal of maximizing the user hours should have been reached by the fact that the adversary cannot simply ban a bridge which was distributed to her. Because if she just bans the bridge, she automatically drops in the trustworthy level and will be separated and exclude soon. Additionally she will approximately affect 50% less users every time she bans one bridge. She still can do so but it should prevent her doing it. Therefore her "goal" will be gaining a better trustworthy level before she starts banning. This means she has to wait and that increases or even maximizes the user hours for bridges. Even if she waits with banning the bridge she will not get real advantages in respect of banning bridges which are used by legit users.

Separate adversaries from legit users

The separation of the adversary from the legit users is reached by splitting a group in two parts, whenever a bridge of the group got banned. Afterwards each group gets its own bridge and the adversary will be in one of them. Therefore 50% of the users are already separated and the next time she bans a bridge approximately 75% of the users are separated from her. This is done until she is alone in a group and therefore she is excluded from the legit users.

5.2 Open Issues

There are still some issues which have to be dealt with:

- Detect blocked bridges
- Testing and evaluating the approach
- Possible online social networks

Detect blocked bridges

The approach relies on the information whether a bridge got blocked or not. Therefore there should be an automated way to discover blocked bridges, because the information is important for splitting the groups. There are also open questions about the combination with fast flux.

Testing and evaluating the approach

The whole approach is a suggestion and has to be evaluated, implemented and tested for discovering the real benefits of the approach.

Possible online social networks

Another question is which online social networks can be used for this approach, which are available in which country and are they controlled by the adversary or not.

Chapter 6

Conclusion

In this paper the Tor network and how it works was described. Moreover the enumeration attacks, which try to find Tor bridges and ban them afterwards, were explained. Those attacks exploit different parts of the Tor network/protocol and one of them concerns the distribution strategies. By now the strategies can be overwhelmed by adversaries who have a lot of resources, such as China. Therefore they have to be improved or changed to make it more difficult for an adversary to use them for the enumeration of bridges. For this reason an adapted version of Proximax was shown, which shall not only maximise the user hours for bridges but also separate possible adversaries which joined the social network group. Additionally the users are less time blocked because of the separation and the reputational system. This approach has to be evaluated and tested to find out the real gains of it and possible improvements and will be done in a further work.

Nevertheless there are many battlefields Tor has to deal with. The fight for privacy, anonymity and uncensored contents will not be won by a single improvement and that is why there is still so much to do.

References

[1] Kevin Bauer, Joshua Juen, Nikita Borisov, Dirk Grunwald, Douglas Sicker, and Damon McCoy. On the Optimal Path Length for Tor. In *Privacy Enhancing Technologies Symposium (HotPETS 2010)*, July 2010.

[2] G.R. Blakey. Racketeer influenced and corrupt organizations act. Website. `http://en.wikipedia.org/wiki/Rico_act(2010)`.

[3] Roger Dingledine and Nick Mathewson. Tor path specification. Website. `https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=path-spec.txt`.

[4] Roger Dingledine and Nick Mathewson. Design of a blocking-resistant anonymity system. Technical report, The Tor Project, 2006.

[5] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[6] Damon McCoy, Jose Andre Morales, and Kirill Levchenko. Proximax: A Measurement Based System for Proxies Dissemination. In *Financial Cryptography and Data Security*, St. Lucia, 2011. Springer.

[7] Michael G. Reed, Paul F. Syverson, and David M. Goldschlag. Anonymous Connections and Onion Routing. Technical report, Naval Research Laboratory, 1998.

[8] Tor. About tor - overview. Website. `https://www.torproject.org/about/overview.html.en`;.

[9] Tor. Five ways to test bridge reachability. Website, 2011. `https://blog.torproject.org/blog/research-problem-five-ways-test-bridge-reachability`;.

[10] Tor. Ten ways to discover tor bridges. Website, 2011. `https://blog.torproject.org/blog/research-problems-ten-ways-discover-tor-bridges`;.

[11] Philipp Winter and Stefan Lindskog. How the great firewall of china is blocking tor. In *Proceedings of the USENIX Workshop on Free and Open Communications on the Internet (FOCI 2012)*, August 2012.

[12] Ling Zhen, Fu Xinwen, Lou Junzhou, and Yang Ming. Extensive Analysis and Large-Scale Empirical Evaluation of Tor Bridge Discovery. Technical report, Southeast University, University of Massachusetts Lowell and University of Massachusetts Lowell.