Network Security

Ex. 1

**CensorSpoofer**

**Article Report**

Ron Meiry 301224283   
Slava Ustinov 309930006

Contents

[Article Summary 2](#_Toc388002863)

# Article Summary

## Introduction

In the past decade, the Internet was used extensively by independent users and groups as a platform for protest and organization against oppressive governments.

These events have caused such governments, China for example, to enforce a strong censorship policy against web-sites or services that were used extensively by protesters, such as Twitter and Facebook, to share ideas that are contrary to the government's political views.

## Goal

The article proposes a new scheme to allow users access to restricted web-sites, while remaining undetected by an attacker, which is an oppressive government in our case.

## Attacker Model

Our model adversary is of government level. It's goal is to identify the rogue users and to enforce it's censorship policy. The attacker has all plausible capabilities expected from a government:

1. Full control over the network's infrastructure.
2. Ability to perform DPI, DNS hijacking, IP filtering and Packet injection.

Though our adversary is powerful, it's not omnipotent. For example, it's very unlikely that he's able to crack a modern day encryption (such as AES, RSA, etc.).

Given the capabilities described above, the attacker is motivated do avoid economic damages that may be caused by extreme actions, such as blocking all e-mail services or preventing usage of mainstream encrypted communication protocols.

## Proposed Scheme

The article's proposed scheme has 3 main entities:

* Client - Resides within the domain of a censoring authority.
  + Desires to gain access to a restricted web page, while remaining undetected.
* Spoofer server - Resides in a domain without any censorship policy.
  + Acts as a web proxy, according to the client's requests.
  + Wishes to remain untraceable and unobservable by any censoring authority, therefore it has to restrict it's identifiers to the client.
  + Wishes to be invulnerable to insider attacks (attacker agents disguised as legitimate users).
* Dummy host - An unaware machine that resides in a domain without any censorship policy, that's used as a scapegoat. The Dummy's IP address is used by the Spoofer to create a seemingly legitimate traffic.