The NetCamo Data Communication System

Ramzi A. Haraty and Bassam Zantout

Department of Computer Science and Mathematics
Lebanese American University
Beirut, Lebanon
Email: {rharaty, bassam.zantout@lau.edu.lb}

Abstract. Whenever a user tries communicating with another recipient on the Internet, vital information is sent over different networks until the information is dropped, intercepted, or normally reaches the recipient. Critical information traversing networks is usually encrypted. In order to conceal the sender's identity, different implementations have proven successful - one of which is the invention of anonymous networks. This paper presents a thorough study of NetCamo - one of the most common and existing techniques used during data communication for avoiding traffic analysis as well as assuring data integrity. The paper discusses its implementation and techniques in details. The paper also presents the benefits and drawbacks of NetCamo.

Keywords: Anonymous networks, NetCamo, and data communication systems.

1 Introduction

Since the day the Internet became a common and reliable mechanism for communication and data transfer, security officers and security enthusiasts rallied to enforce security standards on data transported over the globe. The goal was to achieve data integrity and confidentiality while using a reliable data transport medium, which is the Internet.

Whenever a user tries communicating with another recipient on the Internet, vital information is sent over different networks until the information is dropped, intercepted, or normally reaches the recipient. This information identifies where the request is coming from by revealing the user's IP; and hence, the geographical location, what the user needs from the recipient, and sometimes the identity of the user. The moment the recipient replies back, the same type of information is sent back along with a certain payload (meaningful content) for which the user had requested.

Critical information traversing networks is usually encrypted. Sometimes encrypting the payload alone is not enough for users who wish to conceal their identities while communicating with recipients over the Internet. Take, for example, a reporter working undercover and sending critical information over the Internet to a country that is at war with where the reporter is residing in. If the reporter's identity is revealed then the reporter might be convicted. Hence, concealing who is sending the information is sometimes much more important than revealing the information itself.

In order to conceal the sender's identity, different implementations have proven successful one of which is the invention of anonymous networks. Anonymous networks go beyond transferring information over the Internet, whereby theoretically, the implementations can be replicated on different communication technologies such as mobile devices, wireless networks, etc.

Before describing the details of Bit Torrent, it is important to mention that many implementations were able to achieve anonymity of the sender and receiver with some drawbacks or at a certain cost for which these implementations could, to a certain, extent prevent against traffic analysis. Anonymizer [1], JAP [2], Miximinion [3], Tarzan [4], Morphmix [5], I2P [6], TOR [7] and Bit Torrent [8] are examples of such solutions offered at the time NetCamo was being utilized.

This paper investigates the implementation of NetCamo, which is widely used today and has made a major impact on the world of networking and particularly peer-to-peer communication. The remainder of the paper is organized as follows: Section 2 describes the NetCamo system. Section 3 presents the critique, outlining NetCamo's features, advantages as well as its drawbacks. Section 4 provides a conclusion.

2 NetCamo

NetCamo, which stands for Network Camouflage, was first introduced in 1999 by team of academic researchers in the Department of Computer Science of the Texas A&M University [9]. The team, led by Yong Guan, has