Computers in Human Behavior xxx (2014) xxx–xxx

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

A collaborative-based approach for avoiding traffic analysis and assuring data integrity in anonymous systems

Ramzi A. Haraty *, Bassam Zantout

Department of Computer Science and Mathematics, Lebanese American University, Beirut 1102 2801, Lebanon

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Data integrity
Traffic analysis
Collaboration

ABSTRACT

The paper introduces a new collaborative technique for assuring data integrity while avoiding traffic analysis and other types of similar attacks (e.g., man-in-the-middle, data source fingerprinting, etc.). The new technique utilizes a quorum based approach to allow the client to validate the authenticity of the received data at his/her end by comparing different copies of the data. Similar to a reputation system, the new approach relies on the feedback of end-user communication experiences as well as a centralized entity to determine the trustfulness of nodes in the system. The new approach also is a hybrid of centralized and decentralized system that will help in keeping the system 'alive' to prevent different types of attacks that are carried out on centralized and decentralized peer-to-peer systems. The technique also accomplishes data transfer from source to destination using a distributed system, encryption, and a relatively new way for communication amongst system components.

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. 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 where the reporter is residing in. If the reporter's identity is revealed then the reporter's safety might be jeopardized. 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 (Scott, 2005). Anonymous networks go beyond transferring information over the Internet, whereby theoretically, the implementations can be replicated on different communication technologies such as mobile devices and wireless networks.

This paper presents a new technique that is inspired by many existing technologies used nowadays on the Internet. The new technique will not only use conventional methods for assuring data integrity but will also add a new approach for integrity validation that will be done on the client's end.

The remainder of this paper is organized as follows: Section 2 provides background information on anonymous systems. Section 3 introduces the new model. Section 4 presents and experimental results and Section 5 concludes the paper.

2. Background

Anonymous networks first emerged in the mid-1980s with a simple implementation of Chaum Mixes (Chaum, 1981) and the Anonymizer. Users connect to a single entity acting as a proxy that relays connections to different destinations. The identity of the sender is concealed but the destination is not; however, since hundreds of requests could be established from a single entity then pinpointing the source proved to be difficult. As adversaries gained interest in anonymous systems, many different scenarios, theories, and implementations have emerged for protecting the transmitted

* Corresponding author.
E-mail address: rharaty@lau.edu.lb (R.A. Haraty).

http://dx.doi.org/10.1016/j.chb.2014.09.031
0747-5632/

and received data (Danezis, Dingeldine, & Mathewson, 2003; Freedman, Sit, Cates, & Morris, 2002; JAP Anonymity and Privacy). Consequently, many different attack or counter-attack techniques have also emerged to challenge these security defenses. Smart deciphering, cracking of encrypted data, man-in-the-middle attacks, data replays, data-source fingerprinting, time attacks, and many others are all examples of what anonymous systems are subjected to currently (Ibrahim, Abuhaiba, & Hubboub, 2012; Ornaghi & Valleri, 2003; Whalen, 2001). Government organizations have also paid a great deal of attention to anonymous systems whereby the most commonly used anonymous system, Tor (based on second generation onion routing), is sponsored by DARPA and under the High Confidence Network Program as well the United States Navy (ONR) Haraty & Zantout, 2014. Additionally, some governments have reacted negatively to anonymous systems whereby these systems have now been banned from being used inside countries such as China, Saudi Arabia, and Germany for different reasons (China bans anonymous internet messages). As anonymous systems evolve, so is the understanding of the concept of anonymity by different computer user groups and societies in general.

The topic of anonymity has been the passion of many information security enthusiasts. However, the number was very little compared to researchers involved in other computer science topics at the time. Although the number of successful anonymous designs and implementations span to approximately 10 systems for which only two or three have been widely adopted, every system has its design flaws and features (Fernández Franco, 2012; Jansen, 2012; Ries, Panchenko, State, & Engel, 2011).

Throughout the past couple of years, scientists, researches and freedom activists have all been exposed to the topic of anonymous communication that can provide a sense of security to their identity on the Internet or during P2P communication. While public awareness has not been fully reached, research continues to take place and the topic of anonymity has been introduced as part of the curriculum to some of the leading universities in the west, as well as in Europe. To the anonymous community's surprise, some anonymous systems (like Tor, NetCamo, etc.) are being sponsored by government agencies, such as DARPA and the US Navy. This raises a lot of eyebrows and many questions to such security interests by governments in anonymous communication.

Developers of Tor, I2P, NetCamo and almost every anonymous system have clearly stated that their system cannot prevent against global adversaries, one of which are governments. Hence, should the whole concept of anonymity be cancelled and forgotten about? The question that should be asked is, how much are global adversaries interested as well as worried of concepts like anonymous communication and what is being done to strengthen/weaken or even alter this new awareness and scientific interest? More work is being put into coming up with the most advanced anonymous system that can prevent even against global adversaries and especially governments. This has lead governments such as Germany, China, Kingdom of Saudi Arabia, and others to ban the use of anonymous systems for the following reasons:

1. Governments need to monitor and control the use of the Internet communication for the sake of national security, and intelligence gathering.
2. Governments need to protect their people from being the victims of anonymous communication misuse.
3. Governments need to prevent against using anonymous systems as tools for terrorists and organized crime's undetectable communication.

The Chinese government, for example, chooses to ban Tor and other anonymous communication mainly because of national security. They simply do not wish to have information leak in or out of their country without the knowledge of Chinese intelligence agencies. There have been rumors where the Chinese government had cloned the Tor network at Internet gateways and while Chinese users think they are connecting to Tor, they are actually connecting to Chinese Tor proxies and then being routed to the outside Internet world. In addition, a Tor network is also being run inside China in order to camouflage communication between users inside the country. However, one can only wonder how secure this communication is! And whether or not it has been sponsored and introduced by the Chinese intelligence already.

The German government also banned the use of Tor as of January 1, 2008 because of the incidents and consequences inflicted by users of Tor. Since the source of anonymous communication cannot be tracked, then any message sent by a source can be completely concealed and the destination is unaware of who sent the original message, nor by whom it was relayed from, except for the last entity that delivered the message. Unfortunately, this may indicate to victims that it was the entity that delivered the message – the actual originator, which of course is not the case. As such, there have been two incidents where a bomb threat and kidnap ransom note were relayed through Tor exit nodes located in Germany which had been setup by innocent Tor enthusiasts. This had led the German authorities to accuse Tor enthusiasts of participating in such criminal acts. Accordingly, and after thorough investigations, the Tor anonymous network was to be fully banned from being used in Germany to protect the community from similar incidents.

It is clearly evident that anonymous networks have become terrorist and criminal magnets that attract malicious groups in relaying information from source to destination. It has also become used by embassies and some government agencies that choose to relay their traffic through anonymous networks in order not to be detected by any snooping party. Thus, one can deduce that an anonymous system is a two edged sword where it can be used for different conflicting purposes. Roger Dingledine, one of the core developers of Tor, had strongly argued with anonymous critics that criminals and terrorists have their own different means of communicating their plans; and hence, Tor does not present a mean for criminal use. Critics argue that as anonymous systems become sophistically complicated then Tor or other anonymous systems may become a reliable tool for criminals.

As social and government awareness arises, and as anonymous systems improve to protect against global adversaries for whom governments are part of, would anonymous systems survive? The key in anonymous system survival is to protect anonymous users from being the victims of incidents such as the ones aforementioned, and to prohibit illegal use of the system. Hence, anonymity has to be redefined to categorize different types of global adversaries for which governments, terrorists, freedom activists and/or other entities may or may not be part of. Incidents like the ones previously mentioned need to be dealt individually on a case by case basis. Then again who should define/control this categorization and release of critical information, as a terrorist in one country might be considered a hero in another; and this brings even more complication to this process where politics and national/international security become involved.

In order to encourage the use of a new anonymous system; and therefore, have it adopted and supported by all entities, one has to revisit the concept of security and freedom of communication in anonymous systems and realize that responsibilities do exist and that when a misuse occurs then malicious users need to be identified and either banned from further using the system or reported to authorities.

The methodology used in this work was inspired by four different implementations – BitTorrent (Zantout & Haraty, 2010), Tor, I2P (Zantout & Haraty, 2011), and NetCamo (Guan et al., 2001)

Please cite this article in press as: Haraty, R. A., & Zantout, B. A collaborative-based approach for avoiding traffic analysis and assuring data integrity in anonymous systems. *Computers in Human Behavior* (2014), http://dx.doi.org/10.1016/j.chb.2014.09.031