Perspectives in Science (2016) 7, 95—100

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/pisc

Whispering through DDoS attack☆

Miralem Mehic, Jiri Slachta, Miroslav Voznak*

VSB-Technical University of Ostrava, 17. listopadu 15, 708 00 Ostrava-Poruba, Czech Republic

Received 26 October 2015; accepted 11 November 2015
Available online 23 December 2015

KEYWORDS
DDoS;
Covert channel;
SIP;
Network steganography

Summary Denial of service (DoS) attack is an attempt of the attacker to disable victim's machine by depleting network or computing resources. If this attack is performed with more than one machine, it is called distributed denial of service (DDoS) attack. Covert channels are those channels which are used for information transmission even though they are neither designed nor intended to transfer information at all. In this article, we investigated the possibility of using of DDoS attack for purposes of hiding data or concealing the existing covert channel. In addition, in this paper we analyzed the possibility of detection of such covert communication with the well-known statistical method. Also, we proposed the coordination mechanisms of the attack which may be used. A lot of research has been done in order to describe and prevent DDoS attacks, yet research on steganography on this field is still scarce.

Introduction

It is obvious that the battle for the security of computer networks will be constantly present. The security agencies are trying to distance computing resources from a variety of attacks and methods of data leaks, while the computer hackers are constantly trying to find a more intuitive way for a smooth and efficient access to data. One of the challenges facing the digital forensics is the detection of channels used for data leakage and elimination of such threats. Accordingly, there is a growing interest in detecting of compromised channels and machines which were used for attack. If the attack or data leakage has occurred, any further efforts are made to collect reliable evidence about the attack. Often, it is not an easy task, especially in the case of a large number of data that have been generated by an attacker.

Network steganography is a method of hiding data in ordinary network flow in order to achieve covert communication and it was first introduced in 2003 by Deepa and Szczypiorski (Kundur & Ahsan, 2003; Szczypiorski, 2003). Szczypiorski presented basic ideas for several techniques, while Deepa examined practical applications of these techniques and the usage of Internet steganography at that time. Following these presentations, a lot of research in network steganography has been carried out, especially in the field of voice over Internet protocol (VoIP).

The idea of hiding data in network flow can be divided into two types: utilization of unused packet fields and

☆ This article is part of a special issue entitled ''Proceedings of the 1st Czech-China Scientific Conference 2015''.

* Corresponding author.
E-mail addresses: miralem.mehic.st@vsb.cz (M. Mehic), sla463@vsb.cz (J. Slachta), voznak@ieee.org (M. Voznak).

http://dx.doi.org/10.1016/j.pisc.2015.11.016

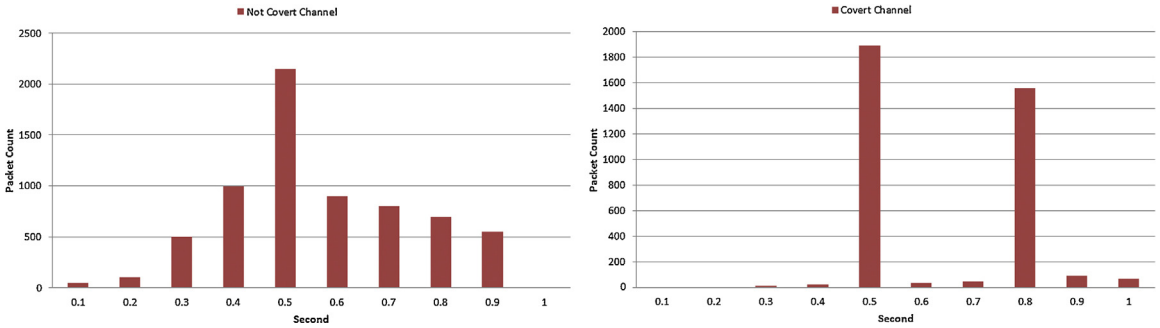

Figure 1 The figure show the number of packets received with a given delay during the experiment which is explained in Berk et al. (2005). The horizontal axis shows the inter-arrival time in seconds, and the vertical axis shows the number of packets received. Left image — two spikes show that a covert channel communication is in place, right image — represents normal communication.

information encoding in traffic behavior. The first type is a well-known technique that emerged from old Xmas packets. These packets with every single option set for used protocol are included in a well-known *nmap* network scanning tool, and they were named Xmas packets because they look like bright bulbs on a Christmas tree. These packets can be easily detected by intrusion-detection systems (IDS), or more advanced firewalls (Mazurczyk and Szczypiorski, 2008). The second type, encoding information in traffic behavior, was first presented in 2005 (Berk et al., 2005). This idea was further modified in 2008 by Mazurczyk and presented as lost audio packets steganography (LACK) solution (Mazurczyk and Szczypiorski, 2008) for VoIP communication.

Covert channels were first observed and defined in the mid-1980s as a result of the rapid development of communication networks. Lampson classified communication channels into three categories: storage, legitimate, and covert. He also gave the first definition of covert channels stating that covert channels are those channels which are used for information transmission even though they are neither designed nor intended to transfer information at all (Lampson, 1973). In the last 10 years, a large number of covert channels have been introduced, and a great development of new techniques in the following years is expected. All these techniques can significantly affect the level of security and reputation that certain communication solutions offer. Viewed from the client's side, it is reasonable to doubt the safety and quality of a particular communication solution which has weak points in the system that can be used for the undetected leak of confidential data. Because of that, covert channels are under close supervision of governments and security companies that aim to prevent these leaks.

Based on existing techniques we can define certain rules which apply to the hiding data with network steganography techniques:

1. Selected information carrier should be frequently used, which makes detection considerably difficult. If one wants to hide information in a rarely used protocol, there is a big probability that network firewalls or IDS (intruder detection system) will raise an alarm.
2. Selected carrier must create a lot of network data (i.e. VoIP traffic, IPTV or similar). This will decrease the probability of detecting information that is hidden inside the ordinary data since many IDS/IPS systems are simply not efficient enough to process huge amounts of data in real-time.
3. It is recommended to hide smaller amounts of data in the ordinary data flow and deliver it frequently rather hide large amounts of data and deliver it sporadically. If the amount of the hidden data in a package, one can assume that those data are just simple coincidence, or that they are just a random behavior of the network. If those values are quite large, there is a considerable probability they will be intercepted by firewalls or IDS somewhere in the network before reaching its destination.

In one of the first papers on this subject (Berk et al., 2005), an approach to statistical detection of covert channel embedded in network packet delays is presented. This simple technique implies the existence of clear differences between the packet delay and it is based on the probability of the existence of covert channel, which is calculated as follows:

$$P_{CovChan} = 1 - \frac{C_{\mu}}{C_{\max}} \tag{1}$$

where C_u is the packet count at the mean and $C_{\max}$ is the maximum packet-count of the histogram which is shown in Fig. 1.

The difference between a binary covert channel (left image) and regular traffic (right image in Fig. 1) is evident. The author used the calculation of the sample mean (average) value of the presented values and calculation of packet count in the histogram at that point. For covert-packet, that value should be a very low while, for normal traffic pattern, the mean value should be in the center of the highest spike. Therefore, the probability of having converted channel is inversely proportional to the ratio $C_{\mu}/C_{\max}$. If the ratio is smaller, the probability expressed with Eq. (1) is higher.

In this paper, we analyze situations where the proposed method of detection can be unsuccessful. We suggest the circumstances in which this situation can happen and we try to explain the ways they occurred.

In the following chapters, the organization and usage of DDoS attacks to hide date are discussed, continuing with the discussion of the proposed detection method and the conclusion in the last section.