Computer Communications 35 (2012) 159–169

Contents lists available at SciVerse ScienceDirect

Computer Communications

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

Hiding information in a Stream Control Transmission Protocol

Wojciech Frączek, Wojciech Mazurczyk, Krzysztof Szczypiorski *

Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland

ARTICLE INFO

Article history:
Received 21 December 2010
Received in revised form 23 August 2011
Accepted 25 August 2011
Available online 3 September 2011

Keywords:
Steganography
Information hiding
SCTP

ABSTRACT

The STCP (Stream Control Transmission Protocol) is a candidate for a new transport layer protocol that may replace the TCP (Transmission Control Protocol) and the UDP (User Datagram Protocol) protocols in future IP networks. Currently, the SCTP is implemented in, or can be added to, many popular operating systems (Windows, BSD, Linux, HP-UX or Sun Solaris). This paper identifies and presents the most likely "places" where hidden information can be exchanged using an SCTP. The paper focuses mostly on proposing new steganographic methods that can be applied to an SCTP and that can utilise new, characteristic SCTP features, such as multi-homing and multi-streaming. Moreover, for each method, the countermeasure is covered. When used with malicious intent, a method may pose a threat to network security. Knowledge about potential SCTP steganographic methods may be used as a supplement to RFC5062, which describes security attacks in an SCTP protocol. Presented in this paper is a complete analysis of information hiding in an SCTP, and this analysis can be treated as a "guide" when developing steganalysis (detection) tools.

1. Introduction

Steganographic techniques have been used for millennia and date back to ancient Greece [4]. The aim of steganographic communication in ancient times and in modern applications is the same: hide secret data (steganogram) in innocent-looking cover material and send it to the proper recipient, who is aware of the information hiding procedure. In an ideal situation, the existence of the hidden communication cannot be detected by third parties. What distinguishes historical steganographic methods from modern ones is, in fact, only the form of the cover (carrier) for secret data. Historical methods used human skin, wax tablets or letters, or other media. Today, steganographic methods use digital media such as pictures, audio, or video, which are transmitted using telecommunication networks. A recent trend in steganography is the utilisation of network protocols as a steganogram carrier by modifying content of the packets, modifying time relations between packets, or using a hybrid solution. All of the information hiding methods that may be used to exchange steganograms in telecommunication networks are described by the term *network steganography*, which was originally introduced by Szczypiorski in 2003 [8]. Many steganographic methods have been proposed and analysed, e.g., [1–4]. These methods should be treated as a threat to network security, because they may cause the leakage of confidential information. Steganography as a network threat was marginalised for a few years [20]; however, now not only security staff but also business and consulting firms are becoming continuously aware of the potential dangers and possibilities it creates [10].

Knowledge of the information hiding procedure is helpful to develop countermeasures. Therefore, it is important to identify potential, previously unknown possibilities for covert communication. Such identification is especially important when new network protocols are forecasted to be widely deployed in future networks. For example, detailed analyses of information hiding methods in the IPv6 protocol header were presented by Lucena et al. [9]. In the present paper, we perform similar analyses, except for the use of the Stream Control Transmission Protocol (SCTP) [5]. The SCTP is a transport layer protocol and its main role is similar to two popular protocols, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). The SCTP provides some of the same service features of both, ensuring reliable, in-sequence transport of messages with congestion control. Certain advantages make SCTP a candidate for a transport protocol in future IP networks; the main advantages are that the SCTP is multi-streaming and multi-homing. The popularity of the SCTP is still growing, but it has already been deployed in many important operating systems, such as BSD, Linux (the most popular is *lksctp* [13]), HP-UX, and Sun Solaris. SCTP is supported by the Cisco network device operating system (Cisco IOS) and can even be run in Windows if the proper library is installed [11].

To the best of our knowledge, there are no steganographic methods proposed for the SCTP protocol. However, information hiding methods that have been proposed for the TCP and the UDP protocols (e.g., utilising free/unused or not strictly standard-defined fields) may be utilised in the SCTP as well, due to several similarities

* Corresponding author. Tel.: +48 601268092.
E-mail addresses: wfraczek@gmail.com (W. Frączek), wmazurczyk@tele.pw.edu.pl (W. Mazurczyk), ksz@tele.pw.edu.pl (K. Szczypiorski).

0140-3664/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2011.08.009

between these transport layer protocols and the SCTP. Steganographic methods for TCP and UDP protocols were described by Rowland [1] and by Murdoch and Lewis [2], and very good surveys on hidden communication can be found in Zander et al. [3] and Petitcolas et al. [4].

The main contribution of this paper is to identify and present the most likely "places" where hidden information can be exchanged i.e. the whole landscape for the SCTP protocol. This task also includes the identification and presentation of the simplest steganographic methods, e.g., those that substitute the content of certain SCTP header fields, as these methods have been well known for years, given the state of the art. Moreover, even the simplest methods can sometimes be successfully utilised because of ambiguous standardisation, which affects later implementations. For example, padding in Ethernet frames should always be set to zeros, but due to a well-known *Etherleak* [21] effect, more than 20% of Ethernet frames have padding filled with random data [18]. This phenomenon can be utilised to mask hidden communications, even for simple steganographic methods that insert steganograms into padding. In typical cases, such methods will always be easily detectable.

However, the main focus in this paper is on proposing new steganographic methods that utilise new, characteristic SCTP features, such as multi-homing and multi-streaming. When used with malicious intentions, steganographic methods can become perfect tools to launch network attacks. Thus, knowledge about such SCTP-based information hiding solutions can be used as a supplement to RFC5062 [12], which describes security attacks in SCTP protocols and current countermeasures. However, RFC5062 does not include any information about steganography-based attacks and methods of preventing them.

For the vast majority of the presented steganographic methods, modification to the SCTP standard is enough to limit their effectiveness. Proposed in this paper, SCTP-specific steganographic methods can be divided into two groups [18]:

- *Intra-protocol methods*, which may be further divided into the following methods: (1) Modify the content of the SCTP packets, (2) Modify how the SCTP packets are exchanged, and (3) Modify both the content of the SCTP and the way the packets are exchanged, i.e., hybrid methods.
- *Inter-protocol methods*, which utilise relationships between two or more different network protocols to enable secret communication (in our case, the proposed method utilises SCTP and IP protocols).

The above classification is also presented in Fig. 1 and will be used throughout the paper to describe and analyse the proposed SCTP-based steganographic methods. This work is an extension of our previous work [19].

The remainder of this paper is arranged as follows. Section 2 gives a brief overview of the SCTP protocol. In Section 3, intra-protocol steganography methods that adopt characteristics of the SCTP protocol are presented. In Section 4, a new inter-protocol method that utilises SCTP is proposed. Section 5 provides possible detection and elimination solutions for the proposed methods. In Section 6, the implementation of one of the proposed methods is described. The methodology of an experiment based on the implemented method is explained in Section 7. Section 8 provides experimental results and analysis. Finally, Section 9 concludes our work.

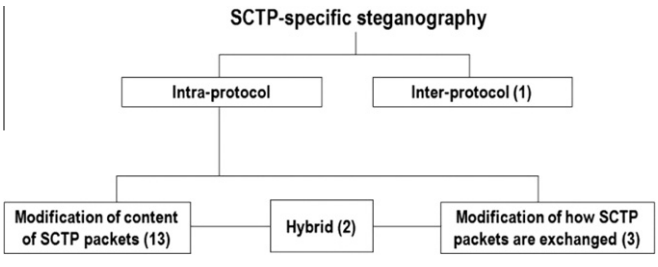

Fig. 1. Classification of SCTP-specific steganographic methods (the number of the proposed steganographic methods for each category is put into brackets).

2. Overview of the SCTP protocol

The SCTP [5] was defined by the IETF Signalling Transport (SIGTRAN) working group in 2000 and is maintained by the IETF Transport Area (TSVWG) working group. It was developed for one specific reason – the transportation of telephony signalling over IP-based networks. However, its features make it capable of being a general purpose transport layer protocol [5,6].

SCTP, like TCP, provides reliable in-sequence data transport with congestion control, but it also eliminates the limitations of TCP, which are increasingly onerous in many applications. SCTP also allows users to set order-of-arrival delivery of the data, which means that the data are delivered to the upper layer as soon as they are received (a sequence number is of no significance). Unordered transmission can be set for all messages or for only some of the messages, depending on the application needs.

The SCTP Partial Reliability Extension, defined in [7], is a mechanism that allows users to send only some of the data if all are not necessary, i.e., the data that were not correctly received but became out-of-date. The decision to not transmit some data is made by the sender. He/she has to inform the receiver that some data will not be sent, and the receiver should treat these data as though they had been correctly received and acknowledged. The Partial Reliability Extension and the order-of-arrival delivery enable the use of the SCTP in many applications that are now using UDP.

In TCP, all data are sent as a stream of bytes with no boundaries between messages. This behaviour requires that TCP-based applications have to conduct message framing and must provide a buffer for incomplete messages from the TCP agent. In SCTP, data is sent as separate messages passed by the upper layer. This feature makes SCTP-based applications easier to develop than TCP-based ones.

Each SCTP connection (called association in SCTP) can use one or more streams, which are unidirectional logical channels between SCTP endpoints. Order-of-transmission or order-of-arrival delivery of data are both performed within each stream separately and not globally. If one of the streams is blocked (i.e. a packet is lost and the receiver is waiting for the packet), this blockage does not affect other streams. The benefit of using multiple streams is illustrated in Fig. 2.

As shown in Fig. 2, User X sends four messages (A, B, C, and D) to user Y. There are two requirements concerning the delivery order of these messages. Message A must be delivered before message

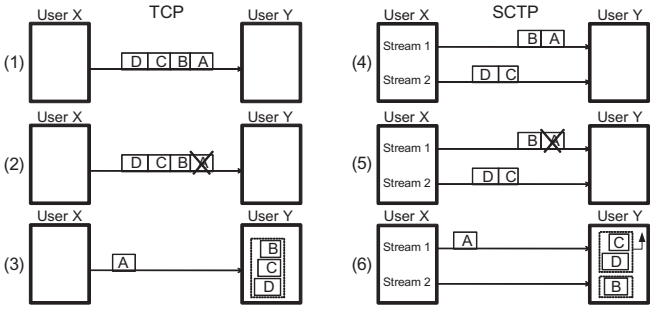

Fig. 2. Comparison of TCP and SCTP data transport using multiple streams.