International Journal of Information Technology and Knowledge Management
July-December 2008, Volume 1, No. 2, pp. 281-287

SECURITY CHALLENGES IN THE STREAM CONTROL TRANSMISSION PROTOCOL : AN OVERVIEW

Dinesh Kumar

Astract

Many protocol has been implemented for the data transmission at the transport and the most common are TCP and UDP. They have their own limitation. To avoid the deficiencies of these protocol, a new transport layer protocol i.e. stream control transmission protocol came into existence. This paper overviews the new features and different security challenges of SCTP protocol.

Introduction

The Stream Control Transmission Protocol is a unicast transport protocol for IP networks that is located at the fourth OSI [2] layer like TCP and UDP and also uses IP as the underlying network protocol. This is standardized in RFC 2960 [1] by the Internet Engineering Task Force (IETF). It was developed because the existing protocols TCP and UDP could not provide functionality and features which are needed for current and future applications of IP networks[3]. Before going forward we must flash a light on the origin of the SCTP.

There was a proposal submitted by Randall R. Stewart and Qiaobing Xie, the *Multi-Network Datagram Transmission Protocol (MDTP)* [4], which attracted the attention of the SIGTRAN working group. MDTP started to be designed in 1997, independently of the SIGTRAN work, as a solution for some of TCP's weaknesses. After getting most of the general concepts together and having a working implementation, the authors decided to submit it to the IETF for consideration in summer 1998. In its preliminary design, MDTP was an application level protocol working on top of UDP that incidentally met most of the requirements imposed by SIGTRAN. This proposal was the only one supporting multihoming and that avoided the HOL blocking, and there was even an available implementation working with a performance similar to TCP's. These were good reasons to choose MDTP it was improved and eight more versions were written. However, it never became a *Request For Comments (RFC)* and it was abandoned as well, the reason being that it was deeply modified and used as the basis of SCTP *(Simple Control Transport Protocol)* , but later on they realized that it was not that simple and that it was not limited to control messages. So the intention was firstly to change its name to *Signaling Common Transport Protocol*, but finally, that name was never used

and the protocol was renamed, in its 9th version, to the present *Stream Control Transport Protocol*. The change from MDTP to SCTP not only involved a change in the name but also a deep revision of the protocol itself. It was then when the protocol datagram header and its internal structure were almost completely modified. The 14th version of the SCTP Internet-Draft was raised to the RFC status, and was published in the IETF as RFC number 2960, a *Proposed Standard*.[7]

SCTP provides numerous advantages over user datagram protocol (UDP) and transmission control protocol (TCP). For instance, SCTP combines the datagram orientation of UDP with the sequencing and reliability of TCP. Additionally, SCTP uses multi-stream, message-oriented routing in multi-homed environments. SCTP provides applications with enhanced performance, reliability, and control functions. This protocol is essential where detection of connection failure and associated monitoring is mandatory. Furthermore, SCTP could be implemented in network systems and applications that deliver voice/data and support quality real-time services (e.g., streaming video and multimedia) [5].

MAIN FEATURE OF THE SCTP

There are many new feature have been there in the new transport layer protocol (SCTP). The main are as follows.

Multi homing

Multihoming refers to a situation where an end host have many communication paths that it can use[6]. During association initialization, each end point of the potential SCTP association advertises any IP address that are available to it. This allows the end points to create a list of addresses[8]. Ther are two types of multihoming one is host multihoming and the second is site multihoming.[9] In the Host multihoming a host have more than one IP Addresses. Ahost may have multihomed with multiple Global Ip addresses on a single interfaceor on several interfaces. Secondly in the site multihoming a site may have more han one connections to the public internet through the same ISP or multiple ISP_s. following fig shows the multihoming[9].

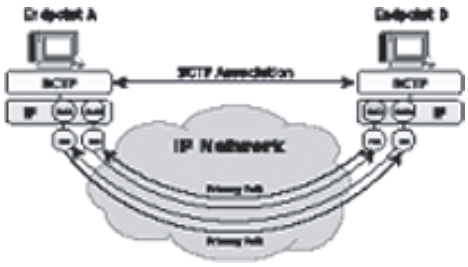


Figure 1: SCTP Multihoming[10]

If the endpoints are interconnected by two distinct networks, the connection only uses a single network for the transport (given by the address pair) . If this network fails, the connection is also broken. In order to overcome this challenge, the SCTP (Stream ControlTransmission Protocol) [16,17] – a connection-oriented and reliable Transport Layer protocol – has been designed and is now supported by all major operating systems. Its most important feature is multi-homing as long as there is at least one possible path between two endpoints, a connection stays usable.

Multi Streaming

The SCTP uses multiple streams when a host transfer data to the client instead of single stream. This set of stream is called an association. When the the association is established the number of incoming and outgoing streams is negotiated [11]. Atiquzzaman showed that multistreaming can reduce the buffer requirements at the receiver [12]. Ladha showed that using SCTP multistreaming in file transfer could improve the performance[13] i.e. the multistreaming is a very useful feature of the SCTP which is not supported by the TCP.

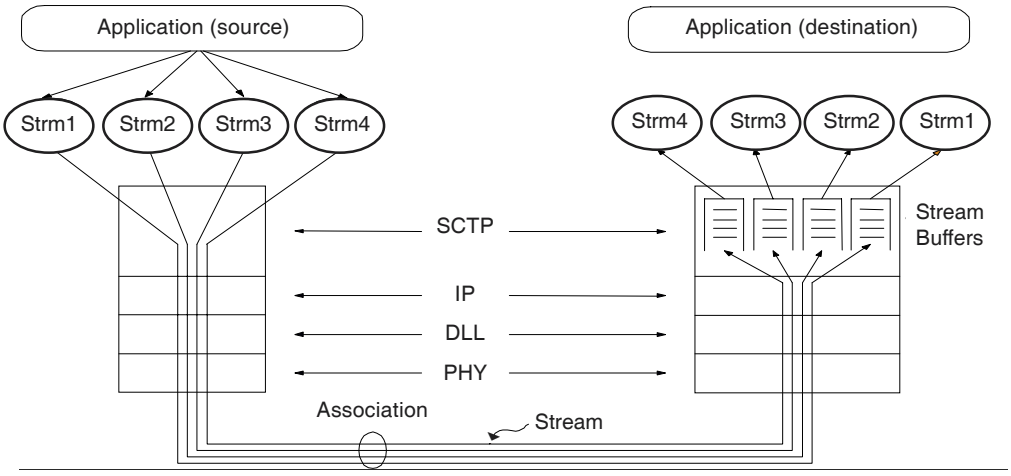


Figure 2: Multistreaming In SCTP [18]

The multi-streaming feature allows for multiplexing different data flows over a single transport association, which is in particular useful for the transport of VoIP/ multimedia trunk data[10]

Security Threats

This section describe the security threats exists that are addressed in various ways within the protocol itself. It analyses the complete attack scenarios against SCTP, which all depends on one or more protocol weaknesses [14]. The attacker can prevent data communication

between hosts by stealing their addresses, hijack the association or association redirection. Here we will flash a light on different attack or the security threats to the SCTP.

Address Camping

This attack is a form of denial of service attack[15]. In Effect, an attacker connect to a server and "camp upon" a valid peer's address. This is done to prevent the client from communicating with the server.

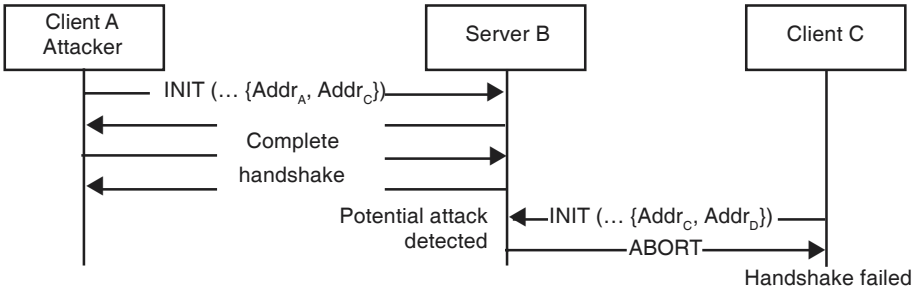
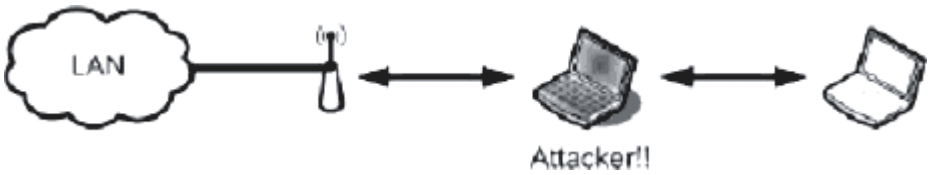


Figure 3: Address Camping in SCTP

From the figure the attacker (client A) first guess the port no. of the client (client C) and then sets up an association with the server listing the AddrA and AddrC in its initial INIT Chunk. Now the server respond and set up an association with the Attacker noting that the attacker is a multihomed and have a set of addresses addrA and addrC. When the client C sends an INIT message listing its two valid addresses AddrC and AddrD, it will receive an ABORT message i.e handshake failed. The valid client is prevented from setting up an association with the server until the server realize that the attacker does not hold the address AdrrC in future by using a HEARTBEAT mechanism. But to Succeed the attacker need to know which port no. client (C) will use when connecting to the Server (B). The guessing is not as difficult as it may appear because current implementations typically allocate port numbers sequentially. The effectiveness of the attack also depends on the timing of heartbeat requests, which varies between implementations. The address-squatting attack is perhaps the most serious threat that we discovered against the standard SCTP protocol when used for its original application. It could lead to serious denial-of-service issues when SCTP is used for transporting telephony signaling over the public Internet.

Association Hijacking

Association Hijacking is the ability of some other user to assume the session created by another endpoint.[15] An attacker that is permanently on the route between two endpoints can mount a man-in-the-middle attack and hijack the entire association[14].



Unless a strong end-to-end security mechanism is used, we cannot solve this problem. Man-in-the-middle attack is a famous attack in both wired and wireless networks[19].

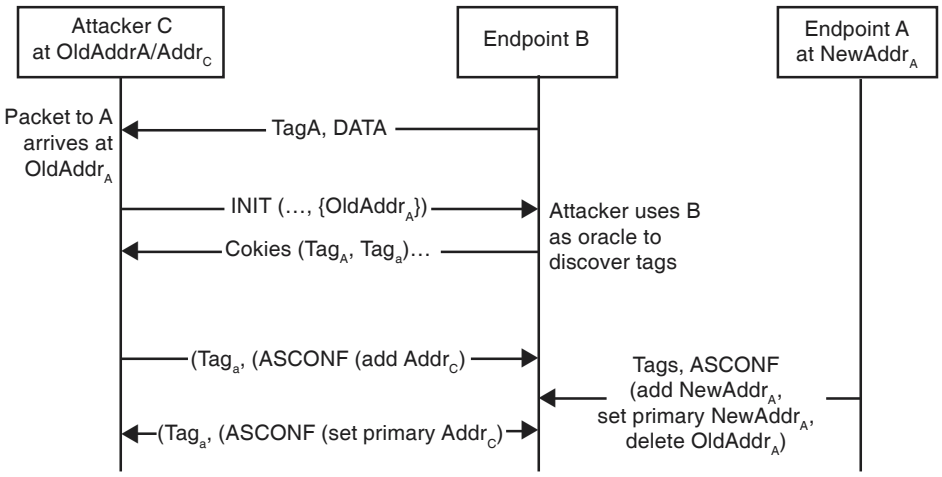


Figure 4: Association Hijacking in the SCTP

This attack can be illustrated from the above Fig as the client A has just removed the IP address oldaddrA , attacker C is the new owner of the the IP address from which the client A has just remove. The Attacker has also the IP address AddrC. The attack is triggerd when the attacker receive a packet that belongs to the *A–B* association. Now the attacker guess the verification tag of the *A–B* association. The attacker send ASCONF chunk to B to add the list of other IP addresses. As a result the attacker has managed to hijack the association from the client *A*. The *B* is communicating as usual thinking that the association is still with the Client *A*.it should be noted that this attack is possible in general whenever the attacker is able to send packets with source address oldaddrA and receive packet with destination address oldaddrA.

Bombing Attack

The idea in the bombing attack is that the attacker redirects a data flow to a target node in order to flood it with packets[14].The Bombing attack is a method to get a server to amplify

packet to an innocent victim[15]. This attack is performed by setting up an association, the attacker make a request for a large data transfer and does not acknowledge data sent to it. This cause server to retransmit the data on alternate address that is of the victim. After some time the attacker acknowledges the data for the victim. The attacker can send strategic acknowledgements so that the server can send the data continuously to the victim[15]. The bombing attack is attractive for the attacker because it can direct a large data flow from the server to the target while only sending and receiving a few messages itself. The attack is more damaging if several data streams are redirected to the same host or router[H]. There is another bombing attack (amplification) 2 this attack allows the attacker to use arbitrary SCTP endpoints to send multiple packets to a victim in response to a single packet[15]. The bombing attack (amplification) 3 allows an attacker to use an SCTP endpoint to send a large number of packets in response to one packet. The bombing attack (amplification) 4 allows an attacker to use SCTP server to send a large packet to a victim than it send to the SCTP server.

Association Redirection

This attack allows an attacker to wrongly set up an association to a different endpoints. The attacker sends an INIT from the source port "A" and directed towards port "B". when the INIT ACK is returned, the attacker sends the COOKIE-ECHO chunk and either places a different destination or source port like "A1" or "B1" this sets up association using the modified port number[DOCUMENT].like any other transport protocol, a node can act as a proxy server between two SCTP endpoints. The proxy acts as a server for a client and acts as a client for a server and forward the upper layer data between the two.[14]

CONCLUSION

This paper describes the new Transport layer protocol (SCTP) with its main feature and different security attacks. This protocol can be an alternate to the TCP and UDP as overcomes the limitations of these protocol. But still this new protocol suffer from some weaknesses like unverified peer addresses, attacker is the new address owner and security attacks like address camping, association hijacking, bombing attack and association forwarding. These attacks are very dangerous where security is concerned, but its feature like multihoming and multistreaming are of great benefit.

REFERENCES

[1] Stewart, R.; Xie, Q.; Morneault, K. RFC 2960 – "Stream Control Transmission Protocol", IETF, *Network Working Group*, (October 2000).

[2] ISO 7498:1984 Open Systems Interconnection - Basic Reference Model.

[3] Stewart, R.; Xie, Q. "Stream Control Transmission Protocol – A Reference Guide", Addison-Wesley, (November 2001).

[4] Stewart, R. R., and Xie, Q.: Multi-Network Datagram Transmission *Protocol*, *Internet-Draft*, Expired (January 1999).

[5] *http://www.iec.org*

[6] Pekka Nikander, Jukka Ylitalo and Jorma Wall. Integrating Security, Mobility and Multihoming in HIP Way. In *Proc. Ericsson Research NomadicLab.*

[7] Ivan Arias Rodriguez "Stream Control Transmission Protocol, The Design of a New Reliable Transport Protocol for IP Network" *Master's Thesis*, Helsinki University of Technology, (Feb, 2002).

[8] James Noonan, Philip Perry & John Murphy, "A Study of the SCTP Services in a Mobile-IP Network" *Performance Engineering Laboratory* Dublin City University.

[9] Naveen Gandu "Mobility Vs Multihoming" HUT T -110.551 *Seminar On Internetworking* Sjokulla (2004).

[10] Thomas Dreibholz, Erwin P. Rathgeb "Towards the Future Internet – A Survey of Challenges and Solutions in Research and Standardization" University of Duisburg-Essen, *Institute for Experimental Mathematics* Ellernstrasse 29, 45326 Essen, Germany.

[11] Sukwoo Kang And Mathhew Fields "Experimental Study of the SCTP Compared to TCP2003".

[12] Mohammed Atiquzzaman and William ivancic "Evolution of SCTP Multistreaming Over Satellite Link" *School of Computer Science*, University of Oklahoma.

[13] Sourabh Ladha and Paul D. Amer. *Protocol Engineering* Lab University of Delaware.

[14] Tuomas Aura and pekka Nikander (Cambridge and Finland) "Effect of Mobility and Multihoming on the Transport-Protocol Security".

[15] Different Security Challanges Document.

[16] A. Jungmaier. Das Transport Protokoll SCTP. PhD Thesis, University ät *Duisburg-Essen, Institute for Experimentelle Mathematik*, (Aug. 2005).

[17] A. Jungmaier, E. P. Rathgeb, and M. Tüxen. On the Use of SCTP in Failover-Scenarios. In Proceedings of the State Coverage Initiatives 2002, Volume **X**, *Mobile/Wireless Computing and Communication Systems* II, **X**, Orlando, Florida/U.S.A., July 2002. ISBN 980-07-8150-1.

[18] *www.cs.ou.edu/~atiq*

[19] Ahmed M. Al Naamany, Ali Al Shindhani, H. Bourdoucen "IEEE 802.11 Wireless LAN Security Overview" *IJCSNS International Journal of Computer Science and Network Security*, **6**(5B), May 2006.

Dinesh Kumar
Lecturer
Apeejay Institute of Management
Jalandhar (Punjab)
E-mail: dinesh_hiitm@yahoo.co.in