Research on the characteristics and blocking realization of Skype protocol

Feng LU,Xiao-Lei LIU
School of Information Engineering
Wuhan University of Technology
Wuhan, China
{lufengwut,liuxl_1986}@163.com

Zhi-Nan MA
Dept. of Electronics & Information Engineering
Huazhong University of Science & Technology
Wuhan, China
mazhinan@126.com

***Abstract*—For end-to-end encryption and special communication protocol-based Skype system, it is not feasible to recognize the Skype protocol by using traditional port-based or payload-based identification methods. By detailed analysis of Skype protocol, this paper explores the general characteristics and special behavior characteristics under certain circumstances of Skype application and proposes a connection tracking-based strategy that can efficiently recognize Skype application and in further step block it. The experimental result indicates that the proposed method can efficiently block the current popular version of the Skype application, thus, achieve the high security of network.**

Keywords-Skype; protocol recognition; behavior characteristic; blocking

I. INTRODUCTION

Skype is a kind of network telephone software based on a kind of third generation hybrid P2P technique developed by Skype Technologies S.A, which offers free and instant communications with high quality. It uses random dynamic port as most of current P2P software do. It can traverse NAT, firewall, and proxy without gap, and it adopts private communication protocol with end-to-end encryption which makes traditional port-based and payload-based recognition methods ineffective. Nowadays, there is no mature program which can effectively recognize the Skype flow.

II. RELATED RESEARCH

Reference [1] has generally explained the Skype protocol and its important functions. It shows that the Skype can not only communicate via UDP and TCP, but also choose the communication port randomly. It points out that the login process can be divided into three parts—UDP probe, TCP handshake and TCP authentication. Reference [2] goes a step further on the research of Skype communication mechanisms, and analyzes Skype partly in statistical flow characteristics and statistical payload characteristics. However, after the analysis of the latest Skype packets, we have found that some of the characteristics no longer exist. Reference [3] uses Deep Packet Inspection(DPI) to block the login process of Skype. The method checks and matches every data packet that goes through firewall, and drops or records them if they match the signature of Skype. It is simple and easy to be realized, but it's inefficient to check every data packets, and seriously influences the firewall performance.

As the methods mentioned above are flawed, the general characteristics and special behavior characteristics under certain circumstances of Skype login are detailedly analyzed in this paper, and a high effective Skype blocking strategy is proposed. Moreover, a detailed method is put forward which adopts recognition strategy of stateful connection tracking and can be more accurate and efficient to carry out management on Skype.

III. ANALYSES OF THE SKYPE LOGIN PROCESS

Due to Skype protocol communications' privacy and the end-to-end encryption, it's unlikely to obtain its public protocol criterion. The data analysis method of Skype protocol based on packet-tracking is adopted in this paper to extract payload character strings and behavior characteristics during the protocol interaction process. The principles to chose protocol are clarified as follows: Priority is given to the character strings which appears repeatedly and stably and are of high possibility to appear. In the meantime, influences on identification accuracy and identification efficiency should be considered, and the length of character strings should be moderate[4]. In the experiments, Wireshark is used to capture and analyze all of the packets entering and exiting a computer when Skpye software is running alone, then statistics analysis on those packets is conducted. Wireshark captures are conducted on different computers, at different times, with different Skype versions, Skype accounts, and different networks to ensure that all the possible circumstances were taken into account in our data collection.

In the Skype protocol establishment stage, we can accurately recognize the static characteristic group (each protocol generally includes several static characteristics) as the general characteristics through UDP's first two packets and TCP's following two packets after three-way handshake. The static fields are extracted directly to filter and recognize. For the ones we can't extract accurately, a behavior characteristic model is set up during the protocol running phase as a special behavior characteristic.

A. General Characteristics

After Skype client being installed, an Event-Sever, a Login-Sever and a list including some Super Nodes (Host Cache) will be established in the local document "shared.xml" (In

978-0-7695-4031-3/10 $26.00 © 2010 IEEE
DOI 10.1109/iCECE.2010.723

Windows XP, its in C: \Documents and Settings\<XP User>\Application Data\Skype\ shared.xml). The host cache maintains a maximum of 200 online IP addresses of Super Nodes and relevent port number of them.

During the login process, Skype node firstly connects to one of the online super nodes in HostCache. The process is described as below: After the initial connection, the Skype client attempts to retrieve information about Super Nodes through UDP first and then TCP. When the network is restricted by firewall and cannot connect, it attempts to establish the same connection through TCP 80 then TCP 433. The payloads of these packets are encrypted. Skype takes advantage of UDP to make an information connection negotiation with Super Node list addresses, and then one Super Node establishes TCP connection to maintain the communication between the Skype Client and the Skype network. Experimental verification: If the network can not transmit TCP protocol, then Skype can not login, probably because they can not use UDP protocol to transmit the key signaling. Therefore, the Skype characteristic analysis is primarily conducted by packets which using TCP protocol to log and autherticate the username and password. Statistical analysis of the experimental general characteristics about Skype protocol is shown in Table I.

TABLE I. SKKYPE LOGIN GENERAL CHARACTERISTICS

Characteristic type	Protocol	Port	Load (byte)	Data characteristic description
DNS search for the login server	UDP	53	>25	From the 13th byte to end match character strings: a*(*)skype*tom*com or tcc*skype*com.
Initialization keywords	TCP	80		Begin with “GET” and has “/getlatestversion?ver=”or “/getnewestversion”.
Login server	TCP	33033		
Special contents	TCP	any	5	Packet contain the ASCII strings: “16 03 01 00 00”

B. *Behavior characteristics*

By couting the most popular version of Skype V3.0 series and comparing different login environments, we summarized that the core signature of Skype login is: The packet begins with the ASCII strings: “16 03 01 00 ** 42 cd ef e7 40 d7 2f 1d”. But its appearing position is not fixed. The nearest one may be in the third packet after TCP’s three-way handshake. The farthest may reach to the 20th packet or even farther. Thus, if we block this kind of data packet directly, the firewall performance will be influenced seriously.

To avoid checking and matching the packet payloads in a large number, a behavior state model is established in the protocol running phase as a special behavior characteristic. Here, for hardly-recognized encrypted message which cannot be recognized in a general way, their features of Greedy Symmetric Transmission are used. Combined with TCP’s ACK, PSH flags and datalen (the lenth of application layer information), dir (dir=IP_DIR_ORIGINAL stands for client request, dir=IP_DIR_REPLY stands for sever response) etc. are considered, so that at least two packets identification is can be made.

To recognize accurately in the following special behavior characteristics, calculation of the packet whose flag is ACK and datalen is zero (ACK empty-packet) after TCP’s three-way handshake is ignored.

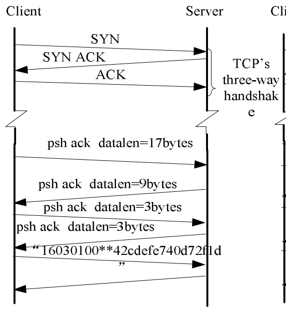


Figure 1. Behavior characteristic I

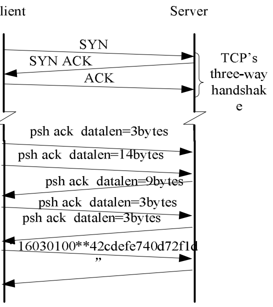


Figure 2. Behavior characteristic II

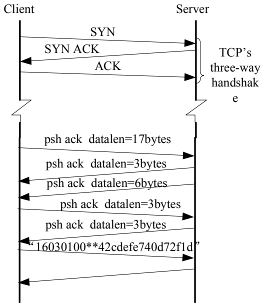


Figure 3. Behavior characteristic III

The TCP negotiation rules of Skype login which are found through our tests are shown from Figure 1 to 3. TCP negotiation rules are explained as below:

- In the Skype protocol interaction process, in the first packet after TCP’s three-way handshake, the dir is IP_DIR_ORIGINAL, ACK and PSH flag are both set to 1. What’s more, during the whole protocol interaction process, the ACK and PSH flag of tcp segments which include application layer information are set to 1. The pivotal datalen is: The dir is IP_DIR_ORIGINAL and datalen is 17 bytes, 3 bytes or 14 bytes; The dir is IP_DIR_REPLY and datalen is 9 bytes or 3 bytes. However, the Skype client ultimately sends the packet containing the ASCII strings: “16 03 01 00 ** 42 cd ef e7 40 d7 2f 1d” to Skype Login-Server. The protocol behavior state in its interaction process is the ordered and directed dynamic behavior characteristic, which made up by pivotal datalen.
- The dynamic behavior characteristic in Figure 1 is locating the packet whose dir is IP_DIR_ORIGINAL and datalen is 17 bytes. Then we make a judgment of the following packet which includes application layer information. If its next packet’s dir is IP_DIR_REPLY and datalen is 9 bytes, this kind of data flow is recognized as Skype application. From Figure 3, we

can see that Skype protocol divided the packet whose dir is IP_DIR_REPLY and datalen is 9 bytes into two parts: Firstly packet whose datalen is 3 bytes is sent and then the packet whose datalen is 6 bytes is sent. Therefore, a connection data flow which inherits the packet's state in Figure 1 whose datalen is 17 bytes and the responding datalen is 3 bytes is also recognized as Skype application.

- From Figure 2, we can see that Skype protocol also divides the packet whose dir is IP_DIR_ORIGINAL and the datalen is 17 bytes into two parts. Firstly, it sends a packet whose datalen is 3 bytes and then sends a packet whose datalen is 14 bytes. Therefore, the connection data flow whose dir is IP_DIR_ORIGINAL sends two packets orderly as above-mentioned which is recognized as Skype application.

IV. BLOCKING SKYPE THROUGH CHARACTERISTIC RESEARCH

The principle of Skype blocking considers performance firstly and then the function. For the general characteristics of Skype that can be recognized quickly, we only need to recognize the first two packets. But for the ones which cannot be fast recognized, the following packets should be analyzed further, we would handle them basing on state. Different kinds of state machines according to different protocol characteristics should be designed. If it matches a conditions of some state machine, then directly matches the state machine until the result can be obtained or it exceeds the checking number limits of packet. (Ack empty-packets are ignored).

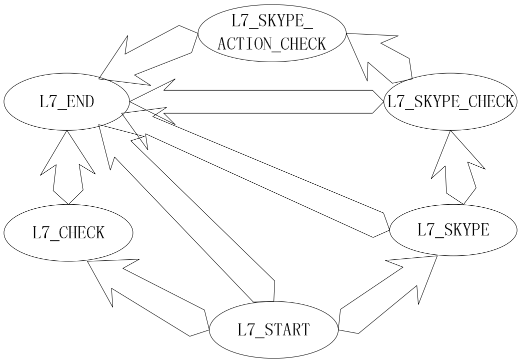


Figure 4. Skype protocol state transformation diagram

According to Skype login characteristics, several kinds of protocol identification states are defined as below, their transformation states are shown in Figure 4.

L7_START describes the non-recognized protocol state.

L7_CHECK describes the state that the first general packet is not recognized successfully and the second state should be recognized further.

L7_SKYPE describes the state that the first packet is not recognized successfully, but from the TCP flag we suspect that it may be Skype protocol and the further confirmation is needed.

L7_SKYPE_CHECK describes the state that it has been successfully passed the state of L7_SKYPE, and needs to confirm the following packets in data flow.

L7_SKYPE_ACTION_CHECK describes the state that it has been successfully passed the state of L7_SKYPE_CHECK and needs to identify the next packet to confirm.

L7_END describes recognition termination state.

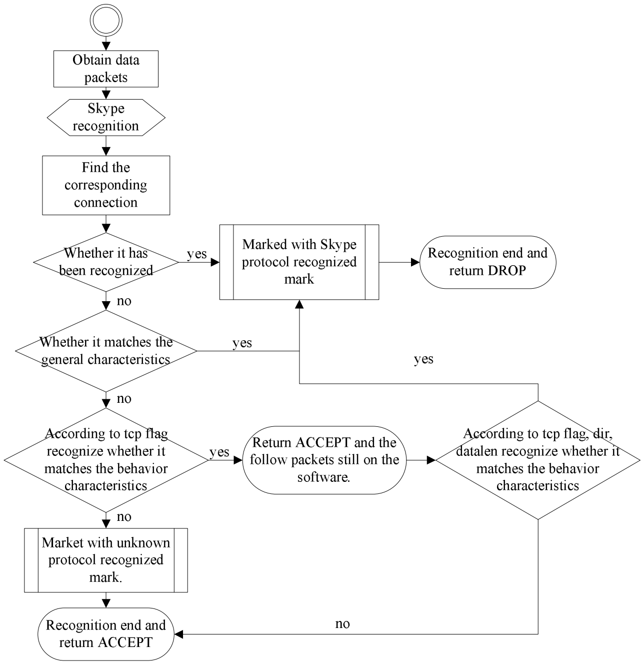

Obtain data packets
Skype recognition
Find the corresponding connection
Whether it has been recognized
yes
Marked with Skype protocol recognized mark
Recognition end and return DROP
no
Whether it matches the general characteristics
yes
yes
no
According to tcp flag recognize whether it matches the behavior characteristics
yes
Return ACCEPT and the follow packets still on the software.
According to tcp flag, dir, datalen recognize whether it matches the behavior characteristics
no
Market with unknown protocol recognized mark.
Recognition end and return ACCEPT
no

Figure 5. Flow chart of Skype protocol identification

The flow diagram of Skype protocol recognition is shown as Figure 5. And the detailed description is represented as follows:

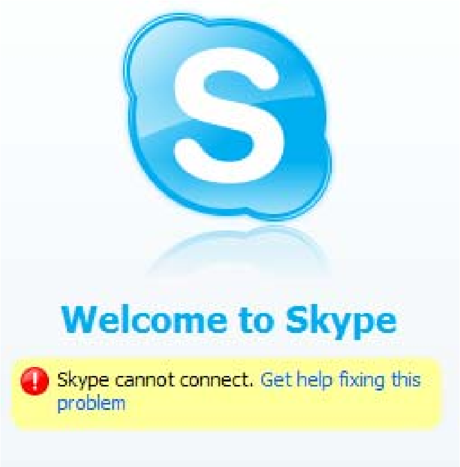
- System obtains packets from the network interface, and then the recognition of Skpye protocol is ready.
- Search for the corresponding connection record in connection tracking state table. (If the five-element group information "source IP/source port + destination IP/destination port + transportation protocol" are corresponding, we treat them as the same connection) If no one is found, create a new connection record, then move on.
- If the connection protocol has been recognized, we take it as Skype application directly and return to DROP.
- Recognize respectively according to Skype's general characteristics and special behavior characteristics of Skype. For the general characteristics, we only recognize the first two packets of UDP and the two packets of TCP after TCP's three-way handshake; For the special behavior characteristics, we recognize packets position from the following packets to the 6th packet after TCP's three-way handshake (Ack empty-packets are ignored). If it enters the state of

L7_SKYPE_CHECK, then go on checking the next packet, if it enters the state of L7_SKYPE_ACTION_CHECK, the matched characteristic conditions are recognized as Skype application and then return to DROP.

V. EXAMPLE

Local test environment, the experiment version is Skype V3.8. A Host computer is configured with dual NIC cards and operation system of Linux 2.6.26 version. The dual NIC cards are used to allow network traffic to pass through the Host computer for analysis. The dual NIC cards divide the network into two parts, outer network and inner network. The outer NIC card directly links to the internet while the inner network card links to a computer configured with windows XP operation system. And then install the Skype system on it. The inner-net computer can only connect to the internet through Linux computer, thus we can handle data packets in outer network.

After many times of experimental tests, experimental results are shown in Figure 6. (Skype V3.8 is the most widely used and the most popular version.)


Welcome to Skype

Skype cannot connect. Get help fixing this problem

Figure 6. The display of Skype cannot connect

VI. CONCLUSION

Based on detailed research of Skype protocol, this paper puts forward the general characteristics and special behavior characteristics under certain circumstances of Skype application, and proposes a connection tracking-based strategy that can efficiently recognize Skype application and then block it. For the general characteristics, this policy only recognizes the first two packets of UDP and the two packets of TCP after TCP's three-way handshake. For the special behavior characteristics, it design different kinds of state machines according to different protocol characteristics, at the farthest recognition packets loated in the 6th packet after TCP's three-way handshake(Ack empty-packets are ignored). This connection tracking-based Skype blocking strategy avoids packet deep detection so that the costs of recognition are largely reduced and the blocking efficiency is enhanced. What's more, it has been tested in the real network experiment. The result can be directly applied to the management control of Skype application. Considering some of the blemishes existed in the pure blocking Skype, more attention should be paied in research of Skype VoIP and the flow recognition of transmission in the future.

ACKNOWLEDGMENT

The authors would like to extend special thanks to Hai-tao Xiao for support in research of this paper .

REFERENCES

[1] S. A. Baset and H. G. Schulzrinne, "An analysis of the Skype peer-to-peer Internet telephony protocol," IEEE International Conference on Computer Communications. INFOCOM'06. Barcelona, Spain, pp. 1-11, April 2006.

[2] Zhen-hua Wang, Pan Wang and Shun-yi Zhang, "An analysis and identification of Skype network traffic based on integrated statistical characteristics," Journal of Nanjing University, vol. 26, pp. 1-7, January 2006 (In Chinese).

[3] P. Renals and G. A. Jacoby, "Blocking Skype through deep packet inspection," the 42nd Annual Hawaii International Conference on System Sciencs. HICSS'09. Big Island, HI, pp. 1-5, January 2009.

[4] Zhou-li Xu, Zhi-hong Jiang, Song-hai Mo and Peng-yi Fan, "Identification of P2P streaming traffic using application signatures," Application Research of Computers, vol. 26, pp. 2214-2216, June 2009 (In Chinese).

[5] R. C. Dodge, "Skype fingerprint," the 41st Hawaii International Conference on System Sciences. Waikoloa, HI, pp. 399-404, January 2008.

[6] Jun-peng Mao, Yan-li Cui, Xiang-jie Ma and Yan-feng YU, "Traffic measurement and characteristics finding of Skype network," Computer Engineering, vol. 34, pp. 142-144, September 2008 (In Chinese).

[7] S. Sen, O. Spatscheck and Dong-mei Wang, "Accurate, scalable in-network identification of P2P traffic using application signatures," the 13th International Conference on World Wide Web. New York, pp. 512-521, May 2004.

[8] Hai-bo Sun, "Protocol identification based on action character," China Network & Information Security Technology Conference(I), pp. 245-251, 2007(In Chinese).