Why and How to block Skype

Oscar Santolalla
Helsinki University of Technology
osantola(@)cc.hut.fi

Abstract

Skype has become a very popular Voice-over-Internet Protocol (VoIP) service that was designed with many smart characteristics. Nevertheless, it also has some security vulnerabilities that can be exploited by a malicious third party, and on the other hand its closed architecture generates certain distrust from many specialists about what is inside this application. This paper discusses the reasons to block the Skype service from four points of view: the telephone operator, the Internet service provider, the corporation, and the home network. Business aspects are also considered in the analysis. Finally, the paper presents and discusses the methods to block the service.

KEYWORDS: Skype, security, VoIP, P2P.

1 Introduction

Skype is a very popular peer-to-peer VoIP service [15], and has outperformed its competitors: MSN, Yahoo IM, GoogleTalk and others. Its protocol has features that allow it to traverse firewalls and network address translators (NATs). Moreover, it has been designed with many smart and efficient characteristics, including very good voice quality [1]. In addition, for the end user's point of view, it is easy to install and operate.

The main function of Skype is providing VoIP calls amongst end users but, in turn it offers some additional features: instant messaging, calls to conventional phones numbers, file transfers, and some others. Skype recommends using an Internet connection with at least 56 kbps [13], but owing to the use of wideband codecs, it guarantees reasonable quality at an available bandwidth of 32 kbps [1].

From a business point of view, the technological model of Skype has integrated the scalability of peer-to-peer (P2P) systems with the functionality and efficiency of VoIP [11].

The paper is organized in the following way. Section 2 states the methodology. Section 3 describes the service, the architecture, and the protocol. After that, it presents the most significant vulnerabilities and security flaws. However, the most important part of this document is Section 4, which discusses and analyzes the reasons why Skype service should be blocked in four different contexts. These are, from the point of view of: (1) a Telephone operator; (2) an Internet Service Provider; (3) a Corporation; and (4) a Home network. Section 5 shows in detail the methods to block the Skype service. In the subsequent section, some controversial points are presented in a final discussion. Finally, section 7 shows the overall conclusions of the paper.

2 Methodology

This paper presents a literature survey based on current analyses performed in several different research centers and by individual specialists around the world. It is not based either on new proposed methods or on own practical experiments.
The main contribution of this work is showing a comprehensive analysis about the reasons to block Skype service, from the most practical points of view, in order to unveil valuable conclusions on the matter. The work is complemented with a complete description of the methods to block Skype.

3 Description of Skype

This section describes how the Skype service works, based on [1, 4]. At the same time, it presents some of the advantages and disadvantages which will be examined in the subsequent analysis.

There are several papers dedicated to thoroughly present the characteristics of Skype. For that reason this paper only shows a basic description of the architecture needed to understand the following sections. The most important points are: (1) the elements of the Skype Network, (2) Skype functions, (3) Security vulnerabilities, and (4) Performance aspects.

3.1 Elements of the skype Network

These are the basic elements that constitute the Skype Network:

- Skype Client (SC). It is an ordinary host that is running Skype client application and has the three basic functionalities: placing voice calls, sending text messages and transferring files.

- Skype SuperNode (SN). It is a SC that additionally has a public IP address, good CPU and memory resources, and a wide available connection to Internet. Actually when a SC becomes a SN, it acquires server functionalities that contribute with the routing process of a group of hosts.

- Login server (LS). It is a special centralized server, administered by Skype, that stores all the names, passwords and buddy-lists of users.

- Host cache (HC). It is a list of supernodes IP addresses and port pairs, stored in the hard drive of each host. HC is built and updated regularly by the SC everytime it connects to the Skype network.

- Bootstrap supernodes. According to [1], there are some special supernodes that are always added by the application to the HC during the installation, and they serve to guarantee that a client will always have some basic list of available supernodes which to connect to.

Fig. 1 shows the elements in the Skype Architecture.

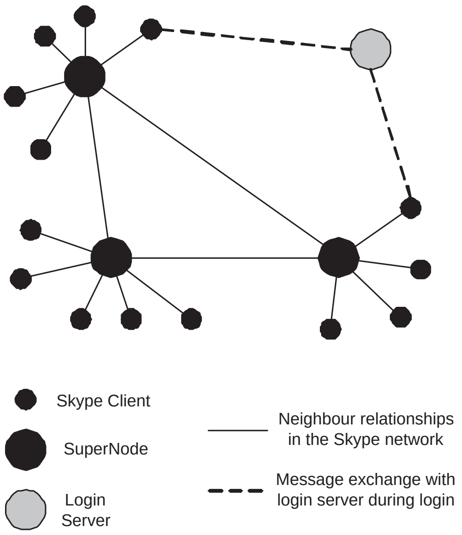
Skype Client
SuperNode
Login Server
Neighbour relationships in the Skype network
Message exchange with login server during login

Figure 1: Skype Network Elements

3.2 Main Skype functions

The most relevant functions of Skype application are:

- Login process.
  This is doubtless the most important process in the architecture of Skype, because the approaches to block the service require a thorough understanding of it.
  In order to log in, a Skype Client tries to connect to some of the supernodes stored in its Host cache. Detailed below is the Skype login algorithm.

  Step 1: SC sends a UDP packet to the HC entry.
  Step 2: If there is not response in 5 seconds, the second attempt tries to establish a TCP connection to that same host.
  Step 3: If that fails, then SC attempts a TCP connection to that IP address on port 80 (HTTP port).
  Step 4: If still unsuccessful, the fourth step is trying to connect to port 443 (HTTPs port).
  All these four steps are repeated up to four more times. If the result is still unsuccessful, in 6 seconds the application will report a login failure. This is the Skype login algorithm.
  In case of success, the SC will try to authenticate the user and password with the Skype login server.

- NAT and Firewall determination
  During the login process, Skype has the characteristic that allows to detect if the SC is behind a NAT or a firewall. The application presumably uses a special protocol called Simple Traversal of UDP through NATs (STUN) [12], or a variant of it. The result of this operation is stored in the Windows registry.

- User search
  Skype employs the Global Index (GI) technology to search for users, and assures that can find a user if it has logged in the previous 72 hours.

- SkypeIn, SkypeOut
  Skype has signed contracts with some international telephone operators in order to provide connectivity with telephone lines. SkypeOut is the service that allows using the computer to call any phone number worldwide. SkypeIn is a service that allows to reserve a phone number in order to receive phone calls from any telephone globally.

3.3 Security vulnerabilities

Skype claims to have very good security characteristics. It uses 256-bit encryption Advanced Encryption Standard (AES) for encrypting all communications, and 1536 to 2048-bit RSA to negotiate those symmetric AES keys. It also claims to be interoperable with personal firewalls and antivirus scanners.

There are different security studies related to Skype. For practical use, Skype should be more secure than conventional phone calls.

However, there are some important vulnerabilities in Skype architecture. This paper firstly defines a list of security requirements that Skype as service should offer, and after that presents the vulnerabilities related to each security requirement.

The security requirements that Skype, as a VoIP application oriented to end-users should be:

- Confidentiality. In the sense that Skype has to prevent that someone can eavesdrop the conversation.

- Authenticity. Initiating a conversation with the certainty that the speaker is the user whose username you specified.

- Availability. If the user I want to talk is connected, it should be always available from my application. Once a call is in progress, there should not be possibilities of being interrupted.

- Integrity. The possibility that some bits are lost during the conversation or file transfer, affecting the quality of voice perceived or the integrity of the received file. Another aspect regarding integrity is that Skype application can produce some harm that affects the computer or the other applications running on it

Now let us review the security vulnerabilities Skype presents.

- **Confidentiality vulnerability 1: Loss of encryption when SkypeIn, SkypeOut are used**.
  Assuming that the conversation is secure because of the encryption, these two services introduce a new vulnerability. Once the conversation reaches the public switched telephone network (PSTN), the data is decrypted and treated as regular voice traffic. After this, the conversation can be either monitored by governmental entities with legal purposes or intercepted by illegal third parties. However, this security flaw is not exclusive of Skype because is present both in telephone service and in any VoIP system that connects to PSTN.

- **Confidentiality vulnerability 2: Eavesdropping in Instant Messaging.**
  Skype allows users to login at the same time in different locations. Let us assume that there is a conversation between two users. A third party has obtained the password of one of the callers, and proceeds to login in invisible mode. He will receive all the text messages exchanged in that conversation. This attack is not possible in voice calls.

- **Confidentiality vulnerability 3: Supernode could monitor the traffic that passes through it**.
  As supernodes receive information about the clients that connect to, a security flaw could allow that someone monitor the conversations that passes through them.

- **Confidentiality and authenticity vulnerability: Monitoring program takes control of the computer**.
  One monitoring program like Netbus can be utilized to remotely and stealthily record or retransmit a conversation. Skype application does not seem to count with protective measures to these kind of threats. This vulnerability is also present in any VoIP system whose client is executed from a computer.

- **Authenticity vulnerability 1: Saved credentials in autologin.**
  In order to improve usability, Skype includes the autologin functionality. However, this implies that Skype will permanently save in the hard disk: the password, the public and private key. Despite of the fact that this information is ciphered and hashed, a hacker that succeeds in taking control of the computer can perform a brute-force attack to disclose all these data. After obtaining the two asymmetric keys, it may be possible to decrypt the conversation, depending on the strength of the Skype's cryptographic implementations. This vulnerability can be found in most of the current VoIP systems as well.

- **Availability vulnerability 1: Dependency of login server.**
  Although it is certain that supernodes help to have a distributed network, and ensure that a client will always find a supernode to perform a call, Skype infrastructure is totally dependent on login server. If this server is not available, the users cannot establish new communications. There are not studies that show what is the actual availability of the login server.

- **Integrity vulnerability 1: Unsecure file transfer**.
  Skype does not count with a built-in antivirus protection feature, that check if a file that is being transferred is harmful or not. This is a feature present in some webmail services, like Hotmail and Yahoo. Skype argues to be interoperable with antivirus and personal firewalls [13]. Nevertheless, it only allows to scan a file once is downloaded, similarly as an HTTP or FTP download. On the other hand, a network firewall is unaware of the encrypted Skype traffic is traversing through it, which represents a serious risk.

- **Integrity vulnerability 2: No integrity guaranteed when transmitting over WLANs.**
  In the case of transmitting a voice call through a 802.11 WLAN, the service does not guarantee that there will not be packet loss. This is especially relevant for file transfers [5]. Naturally, this vulnerability can be found in most of the current VoIP systems as well.

3.4 Performance aspects

Where congestion is concerned, there are some interesting characteristics of the Skype's network performance. Some studies [6] show that supernodes have a very small network cost for participating in the Skype infrastructure. In spite of being a peer-to-peer system, Skype users show diurnal and work-week behaviour, a totally different situation compared to file-sharing systems.

4 Analysis

The most important point in this paper is to find sound justifications to block Skype in a specific environment. The analysis is then, divided in four subsections, according to the environment in which the service is blocked.

The environments matter of study are: (1) a Telephone operator; (2) an Internet Service Provider; (3) a Corporation; and (4) a Home network.

4.1 Telephone operator

As the Skype service is a direct competitor to telephone calls, this subsection shows the arguments the telephone operators would have to block it. It is important to notice that the point of view of a fixed operator is different from that of a mobile operator [7]. The analysis is then, divided into these two separate contexts.

Where fixed telephone operators is concerned, in many countries Skype compete at two different levels: (1) VoIP calls, and (2) Mixed VoIP-telephone calls. In the first case, the communication is between two computers without using any telephone infrastructure. Whereas in the second case one computer is communicating with a telephone, using SkypeIn or SkypeOut features. For most of these companies, Skype represents a serious competitor that reduces their economic profits.

However, in both cases the telephone operator cannot block the service based on telephone numeration. Even in SkpeIn service, users are assigned conventional local numbers from a defined list of countries, so it is not easy to identify them as virtual phones. The only way to block the service is when the Telephone operator acts at the same time as Internet Service Provider. This case will be discussed in the following subsection.

On the other hand, some 3G UMTS operators are showing interest in including Skype as one of their applications [14]. The dynamic mobile market has been trying to find applications that exploit the potential of 3G UMTS networks. Consequently, they are not regarding Skype as a competitor but as a strategic partner. Some performance studies show that Skype is suitable for the average service levels offered by these 3G mobile networks. In these studies, the relevant parameter was the Perceptual Evaluation of Speech Quality (PESQ). If the available bandwidth of the network is above 32kbps, PESQ will vary around 2.9, sufficient to establish a good quality voice call.

Consequently, in the case of fixed telephone operators, the reasons to block Skype are principally economic.

4.2 Internet service provider

As Skype service is a direct competitor to some Internet telephony or VoIP services provided by the Internet Service Provider (ISP), this subsection shows the arguments the ISP has to block it. An ISP can work in many flavors: (1) the typical big company that gives Internet data links to home users and corporations, (2) the company who administers a paid hotspot, and (3) the company who gives Internet access in an Internet Café or an automatic machine in an airport.

An ISP can analyze all the traffic that its clients generate, and therefore can block Skype. The first apparent reasons to do this would be economic, because ISPs normally offer other paid phone call services which directly compete with Skype.

Moreover, Skype and other P2P applications tend to consume great part of the bandwidth, which is especially critical for medium and small ISPs.

On the other hand, in some countries the ISP can be forced by the government to block Skype, as well as other specific services or content. This is the case of Mexico, Oman, and United Arab Emirates [9, 16]. In these countries an ISP finds blocking Skype a justifiable and even beneficial decision. On the contrary, in the majority of countries these kind of practices will be discouraged by both the government and the general public.

Finally, for Internet Service Providers, the reasons to block Skype are either economic or political.

4.3 Corporation

For a corporation, the problem associated to Skype is that the service may introduce security vulnerabilities.

It is not possible to confine all the Skype traffic into to the corporate network, which would be more convenient from a security's point of view. By contrast, the clients always have to connect to external entities when performing a communication.

In this sense, Bergstrom [3] claims that Skype is not suitable or secure enough to be deployed in a corporate environment. The most important arguments are the following: (1) Clients inside the corporate network must connect to external entities, (2) File transfers between users are encrypted, (3) The lack of documentation especially about link encryption and key exchange.

Indeed it is impossible to locally deploy a Skype infrastructure on a corporate network without using public supernodes and Skype login servers.

On the other hand, file transfers are totally encrypted. Eventhough Skype application asks the user to accept the transfer, there is no way to analyze that file before being copied in the hard disk. The only way to protect from this threat is having installed a good personal firewall and a proper antivirus with antitrojan capabilities.

It could also exist some functionality that transmits call-statistics to the Skype centrals servers. This would compromise the confidentiality of the end users if this same process also transmits the session keys of every call.

As a consequence of this, for a Corporation, the reasons to block Skype are chiefly related to security.

4.4 Home

For a home networking environment, Skype can affect the security and privacy of the people living at home [5]. From the point of view of the user, the main concern should be loss of privacy.

Skype is more secure than phone calls over PSTN or integrated services digital network (ISDN) lines because in those cases any individual with physical access to the telephone line can monitor the conversation. Nevertheless, the case of SkypeOut and SkpeIn are exceptions. In these two cases, the conversations are in some point decrypted to be transmitted over conventional phone lines, losing their security characteristics.

On the other hand, both the buddy list and the instant messaging history are pieces of data stored in the hard disk as plaintext. Therefore, any third party who temporarily takes control of the computer can access these personal data and easily disclose information. This would clearly affect the privacy of the end users.

On the whole, the analysis of these aspects tends to favour Skype. There are not strong reasons to block it because the vulnerabilities are not related to its main function: voice calls. In practice Skype represents a convenient application, but the user has to take in consideration all the described facts throughout this analysis.

In the event that some home environment is considered critical, the reasons to block Skype are related to privacy.

5 How to block Skype?

Finally, this section presents a summary of the most reliable methods to restrict the Skype service. There are some disagreements among the authors of the approaches, as well as some methods that are not so effective enough to be included in this paper. Basically there are two possible scenarios: (1) General case for a corporate network, and (2) For Internet Service Providers.

5.1 General case for a corporate network

The general case is valid both in a network with and without a firewall or NAT [2]. For blocking the Skype service, is required to inspect the payload of the traffic (TCP or UDP) [18]. This can be done with Snort, for example.

In the login process, the client sends login messages to the login server. The first two sent messages employ the SSL header. The message sent from the SC to the login server is 0x1603010000. The value 0x16 indicates that the message type is client_key_exchange, and 0x0301 corresponds to the SSL version 3.1. As a response, the message sent from the login server to the SC is 0x1703010000. We can notice that for server to client message exchange, Skype uses a non-SSL header.

Therefore, blocking packets that have the value 0x1703010000 in their headers is the solution to block Skype without blocking any other traffic. However this is not a totally reliable solution because of some aspects. First of all, it is dependent on the login process, so it cannot block a Skype call in progress. On the other hand, it is possible to obtain false positives unless a more deep traffic identification is performed.

5.2 For Internet Service Providers

The panorama is a bit diferent for Internet Service Providers. They require more smart traffic analysis and blocking procedures. One of the most well-known cases is the application NetSpective 2.0, by the company Verso [17]. It was used to block Skype in China. In this country, VoIP is highly regulated by the government. On the other hand, Nokia has recently launched a system that can recognize peer-to-peer traffic: Nokia ISN Flexi peer-to-peer [10]. This application would allow to apply several policies once a specific traffic is recognized: for instance drop or delay packets.

Additionally, Lynanda Asynchronous Network Filter is a recent software aimed to provide a customized solution to block Skype traffic, sorting it from other P2P packets [8].

All these methods are also applied by Telephone operators that at the same time act as ISPs.

6 Final Discussion

This topic is controversial indeed, so this section presents final discussions in favor and against the use of Skype.

Some of the mentioned security vulnerabilities are related to the complementary services of Skype, rather than to the VoIP service itself. This is important to notice because in conclusion, the results of the analysis tends to favour Skype.

The closed architecture of Skype generates several potential threats that must be seriously taken into account for the network administrators and end-users. The great part of reasons to block the service are based on this black-box characteristic.

Mobile operators that are co-working with Skype should be concerned about security, especially regarding the file transfer functionality. Let us recall that the Skype encryption characteristic does not allow to analyze any file before it is downloaded to the computer, a mobile phone in this case.

Blocking Skype is a process that may alter the speed of the transmission, especially in the case of Internet Service Providers. This is critical in order to provide the offered service level to their end-users.

There are not ways to block Skype in home environments unless these networks count with a Firewall.

7 Conclusions

This paper unveils the reasons why Skype service should be blocked. Depending on which point of view we analyze from, the reasons are principally economic, security, privacy and politics related. Certainly security is largely the most important reason, as several studies claim. Only in the specific case of small ISPs, the reason could be performance of the network.

Blocking Skype requires accurate analysis and identification of the traffic. In the case of corporate networks, a firewall is required to perform this task. Whereas in the case of ISPs, some specialized companies have developed sophisticated software that fulfills these requirements. Needless to say, in the case of ISPs the blocking process must not affect the perceived bandwidth of the users.

8 Acknowledgements

Supported by the Programme Alβan, the European Union Programme of High Level Scholarships for Latin America, scholarship No. E06M103218PE.

References

[1] Baset, S. & Schulzrinne, H. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol. Columbia University, New York. September 15, 2004

[2] Baset, S. Skype. [Cited 18 April 2007]. http://www1.cs.columbia.edu/ salman/skype/

[3] Bergstrom, D. An Analysis of Skype VoIP Application For Use in a Corporate Environment. Report, Version 1.3 October 2004. [Cited 18 April 2007]. http://www.geocities.com/bergstromdennis/Skype_Analysis_1_3.pdf

[4] Berson, T. Skype Security Evaluation. Anagram Laboratories, October 18, 2005. [Cited 18 April 2007]. http://www.anagram.com/berson/skyeval.pdf

[5] Garfinkel, S. VoIP and Skype Security, Skype Security Overview. Rev 1.6, January 26, 2005. [Cited 18 April 2007]. http://www.simson.net/ref/2005/OSI_Skype6.pdf

[6] Guha, S. & Daswani, N. & Jain, R. An Experimental Study of the Skype Peer-to-Peer VoIP System. In Proceedings of The 5th International Workshop on Peer-to-Peer Systems (IPTPS ’06), Santa Barbara, CA, February 2006, pp. 1-6.

[7] Hossfeld, T. & Binzenhöfer, A. & Fiedler, M. & Tutschku, K. Measurement and Analysis of Skype VoIP Traffic in 3G UMTS Systems. 4th International Workshop on Internet Performance, Simulation, Monitoring and Measurement (IPS-MoMe 2006). Salzburg, Austria, 2006.

[8] Lynanda. Lynanda Asynchronous Network Filter - Skype & P2P. [Cited 18 April 2007]. http://www.lynanda.com/products/software-for-corporations/traffic-filtering

[9] Skype Journal. Is Telmex blocking Skype, Vonage users in Mexico?. [Cited 18 April 2007]. http://www.skypejournal.com/blog/2005/05/is_telmex_blocking_skype_vonag_1.html

[10] VoIP news. Nokia Promises An Easy Way To Kill Mobile VoIP. [Cited 18 April 2007]. http://www.voipnews.com.au/content/view/1338/107/

[11] Rao, B. & Angelov, B. & Nov, O. Fusion of Disruptive Technologies: Lessons from the Skype Case. European Management Journal. Vol.24, Nos. 2-3, pp. 174-188, 2006

[12] Rosenberg, J. & Weinberger, J. & Huitema, C. & Mahy, R. RFC 3489: STUN – Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs). March 2003.

[13] Skype Technologies. Guide for Network Administrators: How to optimize & tune networks and computers for Skype. Version 1.0.1, April 2005. [Cited 18 April 2007]. http://www.skype.com/security/guide-for-network-admins.pdf

[14] Skype. Skype Mobile partners. [Cited 18 April 2007]. http://about.skype.com/mobile.html

[15] Skype number of users. [Cited 18 April 2007]. http://share.skype.com/sites/en/news_events_milestones/

[16] TechWeb technology News. Skype Service Is Blocked In Middle East Country. [Cited 18 April 2007]. http://www.techweb.com/wire/networking/164901544

[17] Verso Technologies. NetSpective. [Cited 18 April 2007]. http://www.verso.com/products/netspective/index.asp

[18] Yu, Y. & Liu, D. & Li, J. & Shen, C. Traffic Identification and Overlay Measurement of Skype. Computational Intelligence and Security, 2006 International Conference on. Vol.2, pp. 1043-1048.