International Journal of Computer Networks and Communications Security

VOL. 6, NO. 12, DECEMBER 2018, 264–269
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Examining the Network & Security Infrastructure of Skype Mobile Application

SULEIMAN ABDULLAHI

Department of Mathematics and Computer Sciences, Faculty of Natural and Applied Sciences, Al-Qalam University, Katsina, P.M.B. 2137 Dutsinma Road, Katsina

abduljby02@gmail.com

ABSTRACT

Nowadays computer systems and other networking devices face sophisticated attackers who combine multiple vulnerabilities to penetrates networks with devastating impact. The overall security of a network cannot be determined by simply counting the number of vulnerabilities. To accurately assess the security of networked systems, one must understand how vulnerabilities can be combined to stage an attack. From this, risk mitigation options can be devised in terms of maximizing security in the networked environment as well as in on devices and minimizing cost in practice, vulnerabilities often remain in a network, even after they are discovered. Vendors may be slow to release software patches, or deployment may be delayed because of excessive cost or effort. Attackers often leverage even correctly functioning network services to gain new capabilities. An organization will often trade security risk for availability of services. Removing attack paths reduces options for an attacker, but at what cost to individual or organization? This paper describes various network and internet vulnerabilities/attacks and their mitigation techniques as they apply to modern packet transfer. This will help individuals and organizations in understanding how vulnerable or otherwise their data and information is to the attackers and decides on the most cost effective mitigation method (s) that suits them as individuals or organizations as they intend to send data from one devise to another via internet or network connectivity.

Keywords: *Network Security, Security Infrastructure, Mobile Application Security, SKYPE Mobile Application, Risk Mitigation Options.*

1 INTRODUCTION

Digitalization has transformed our world. How we live, work play, and learn have all changed. Every organization that wants deliver the services that customers and employees demand most protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation [1]. Network security is any activity designed the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network [2]. Network security combines multiple layers of defenses at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats [3,4]. Not every user should have access to your network. To keep out potential attackers, you need to recognize each user and each device. Then you can enforce your security policies. You can block noncompliant endpoint devices or give them only limited access. This process is network access control (NAC) [5]. Internet and network attackers are the criminal offenses done with use of internet and computer networks to divert money or to perform crimes [6].

Skype is a telecommunications application software that specializes in providing video chat and voice calls from computers, tablets and mobile devices via the Internet to other devices or telephones/smartphones[1]. Using Skype communication system, users can also send instant messages, exchange files and images, send video messages and create conference calls [2]. Most of the services in Skype are free but users require Skype Credit or a subscription to call landline or mobile numbers. Skype is based on a freemium model (a kind business model where you give a core product away for free and sell

premium products) [2, 3]. Skype allows users to communicate by voice using a microphone, video by using a webcam, and instant messaging over the Internet [4]. Skype-to-Skype calls to other users are free of charge, while calls to landline telephones and mobile phones (over traditional telephone networks) are charged via a debit-based user account system called Skype Credit. Unlike most other VoIP services, Skype is a hybrid peer-to-peer and client–server system [5].

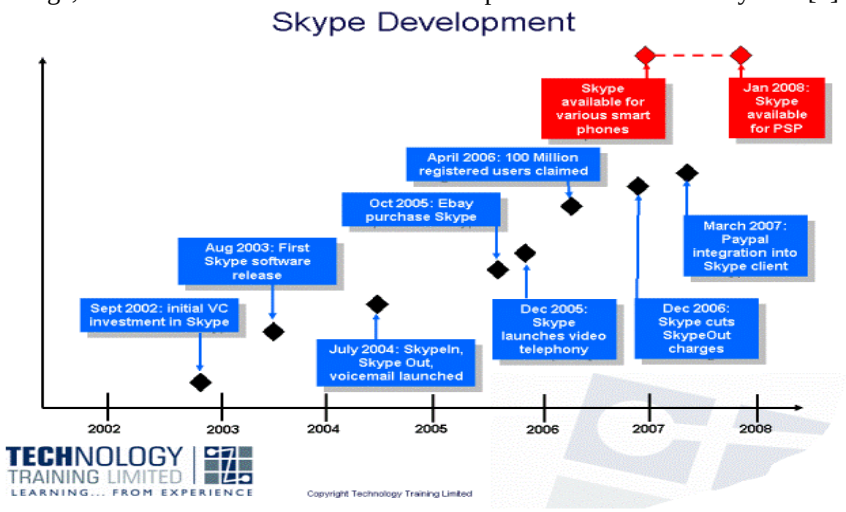


Figure 1: Skype Development [15]

Figure 1 above shows the trend at which Skype was developed. Skype was released in August 2003 [6], It was created by Dane Janus, Friis and Swede Niklas Zennström in cooperation with Estonians Ahti Heinla, Priit Kasesalu, and Jaan Tallinn, who developed the backend which was also used in music-sharing application Kazaa [7]. In September 2005, eBay acquired Skype for $2.6 billion [4]. In September 2009, Silver Lake, Andreessen Horowitz and the Canada Pension Plan Investment Board announced the acquisition of 65% of Skype for $1.9 billion from eBay, valuing the business at $2.75 billion. Skype was later acquired by Microsoft in May 2011 for $8.5 billion. Microsoft's Skype division headquarters are in Luxembourg, but most of the development team and 44% of the overall employees of the division are still situated in Tallinn and Tartu, Estonia [4, 8-10].

2 SKYPE NETWORK STRUCTURE

Garfinkel [2] concluded that Skype is related to KaZaA which is a famous P2P file sharing system and it consists of the ordinary nodes (clients), super nodes (SNs) and servers [11]. The Skype P2P network organizes participants into two layers: super nodes, and ordinary nodes. Such networks have been the subject of recent research. Typically, super nodes maintain an overlay network among themselves, while ordinary nodes pick one (or a

small number of) super nodes to associate with; super nodes also function as ordinary nodes and are actually elected from ordinary nodes. Ordinary nodes issue queries through the super node(s) with which they are associated. The findings of this suggest that Skype communication consists of three components: Skype client login, buddy lookup and file/voice/video communication [11, 12].

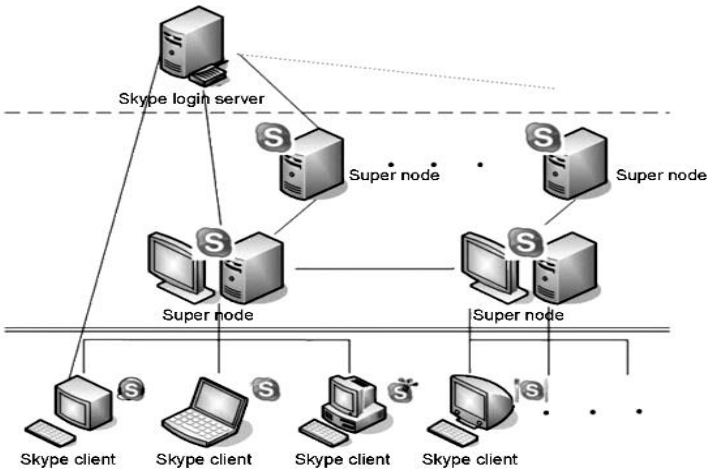


Fig. 2. Skype decentralized topology: super nodes and normal clients [18].

Skype is unique in its network structure, as shown in Figure 1. The same developing team of Skype formerly produced the well-known peer-to-peer file-sharing application KaZaa, and the Skype network is organized as a peer-to-peer overlay structure using a specific protocol. Different from other VoIP applications that are based on the more conventional centralized server model, Skype does not include central servers except for a login server, with which the Skype clients would communicate when logging in.

The function of Skype begins with a login process, when the Skype clients first register to the login server. They are then connected to a super node. Clients join the network after this process. Skype network consists of normal Skype clients and super nodes [11]. Multiple clients can connect to one super node. The strategy of selecting a Skype super node is not very clear. According to previous studies, if a client has a public IP, sufficient CPU power, memory, and network bandwidth, and stays online for a long time, it is very likely to be selected as a super node. The super nodes still run normal routines as clients, but at the same time, they are connected to each other forming the backbone of the Skype network. In the conventional VoIP process, the establishment of an audio session consists of two parts: signaling and multimedia transition. In Skype, none of these two stages involve the login server. Hence, when considering the Skype telephony functions, we can exclude the login server from the Skype network topology.[6] Skype clients and super nodes form an overlapping, peer-to-peer topology [10]. A client delivers its voice through the super node it connects to.

The peer-to-peer network infrastructure is one of the main reasons for Skype's success. On one hand, the decentralized overlay structure ensures high performance for the demanding real-time telephony service while on the other, the network is cheap to maintain and easy to scale. The Skype stores its user directory among the nodes across the network, rather than in a complex and costly centralized global server. In this manner, the network can scale very easily to a large size without too much degradation on the overall performance. The Skype application works out the efficient network path, and takes as much resource as it can access to ensure quality of service. The use of efficient audio coding with ***Internet Low Bit rate Codec[1]*** (iLBC), internet Speech Audio Codec[1](iSAC), or a third unknown codec, is another reason that the quality of Skype VoIP services is guaranteed.

Skype develops the following key feature functions, which make it very competitive among its peer VoIP software.

Connection to public switched telephone network[1](PSTN) Phones*:* Skype supports call between a client on the Internet and the traditional telephone network, including mobile network, with SkypeOut and SkypeIn. The Internet and PSTN are connected by two kinds of specialized servers, which convert the VoIP packets to the traditional telephony signals and vice versa [4].

Group Conference*:* The latest version of Skype allows users to establish audio conference containing up to nine people online at the same time. In the group conference case, Skype does not use a specialized central server either. The audio data are collected from group members, mixed at one of the end points, and then distributed to all participants [13].

NAT and Firewall Traversal: Skype's NAT and firewall traversal ability ensures that it can work behind almost all kinds of NATs and firewalls. It is conjectured that the Skype client uses a variation of STUN and TURN protocols. Moreover, as Skype can use both UDP and TCP as its transport layer protocol, it can easily switch to TCP transition if the UDP flow is blocked by some firewalls [14].

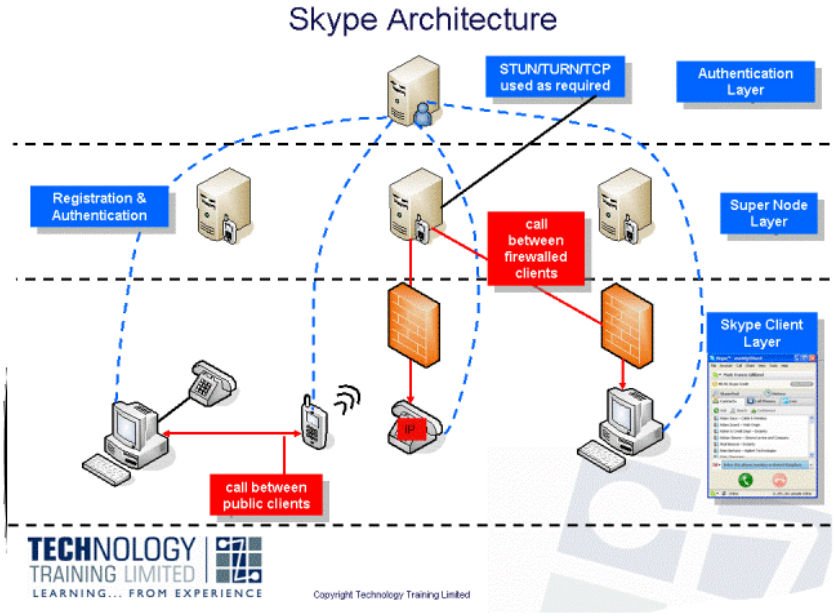


Fig. 3. Skype architecture [20] Skype login process

First, Skype client will login on to Skype and the login process could be divided into four steps:

1. Scanning super nodes
2. Connecting with super nodes
3. Connecting to update servers
4. Login on servers.

Then, Skype clients need to lookup super nodes to obtain the buddy's IP address before they conduct file transfers, chat services, voice and video communications. The lookup can be classified into distribution lookup and concentration lookup. With distribution lookup, a Skype client sends requests to three super nodes which are known alive. The super node which responds to the request will return the buddy's IP address or return the super nodes which might know the buddy's IP address. Before obtaining the IP address of interest, the lookup can repeat at most 6 rounds

The maximum number of super nodes included in the search process is 18. If the Skype client doesn't obtain the buddy's IP address using distribution lookup, it will use concentration lookup which asks the servers to find the IP address. [2]

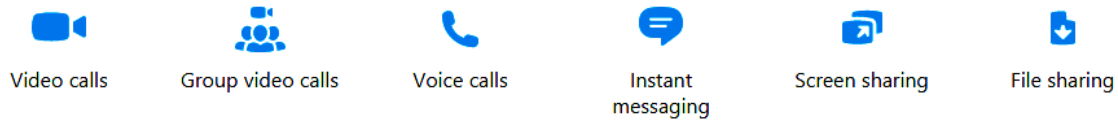
Upon learning the buddy's IP address, the Skype client can then communicate with the buddy. If it is voice communications between two Skype clients transmitted through PCs. The caller tries to establish a TCP connection after it obtains the recipient's address. If the TCP connection is successfully established, the Skype client establishes a direct connection and exchanges the secret key using UDP protocol. In the event that a direct connection fails, Skype uses reverse connection to set up communications. Suppose a caller is behind a NAT. The caller sends a request for connection to a recipient through a servant super node of the caller. The servant super node of the caller finds a servant super node of the recipient. The recipient then sets up a connection with the caller. If such NAT reversal fails or a firewall blocks Skype packets, connections between two Skype clients are relayed by a publicly reachable super node. There is no unique, fixed port for Skype traffic. [2,8,10]

TABLE I SKYPE LOGIN PROCESS AND PAYLOAD FEATURES

Time	Name	Step	Payload Feature
TI	A	scanning super nodes	UDP packets including 0x02 value
T2	B	connecting super nodes	super nodes database
T3	C	connecting to ui.skype.com	IP addresses
T4	D	login on servers	packets including 0x170301 in the head of TCP

TIME	NAME	STEP	PAYLOAD FEATURE
T1	A	Scanning super nodes	UDP packets Including 0x02 values
T2	B	Connecting super nodes	Super nodes database
T3	C		IP addresses
T4	D		

Following are some of the features available on Skype network:



Security infrastructure of Skype

Honestly speaking the real network security infrastructure of a particular company is something that is very difficult to obtain because it is their strength and revealing it is a threat to the security of the entire company and the customers as well. As a result of that, it became difficult for me gather much about the security infrastructures of Skype network.

The website of Skype claims that it uses 256-bit Advanced Encryption Standard (AES) for encryption, and yet a 1536 to 2048 bit RSA for negotiating symmetric AES keys to secure the conversations carried over Skype. [10]

As part of their ongoing commitment to continuall improve the Skype user experience and maintai high level security, they developed supernode which can be located on dedicated servers withi secure datacenters. This has not changed th underlying nature of Skype's peer-to-peer (P2I architecture, in which supernodes simply allo users to find one another (calls do not pass throug supernodes). The company believed that thi approach has immediate performance, scalability and availability benefits for the hundreds of millions of users that make up the Skype community,".[3]

As part of security measures, Skype also uses grsecurity. It is an extensive security enhancement to the Linux kernel that defends against a wide range of security threats through intelligent access control, memory corruption-based exploit prevention, and a host of other systems hardening that generally require no configuration. It has been actively developed and maintained for the past 13 years. [9]

Other company's security policy includes:

1. Usernames are unique.
2. Callers must present a username and password or other authentication credential.
3. Each caller provides the other with proof of identity and privileges whenever a session is established. Each verifies the other's proof before the session is allowed to carry messages.
4. Messages transmitted are encrypted from caller to caller. No intermediate node (router) has access to the meaning of these messages. This claim has been

undermined in May 2013 by evidence that Microsoft (owner of Skype) has pinged unique URL's embedded in a Skype conversation; this could only happen if Microsoft has access to the unencrypted form of these messages.[7,9]

1) Session cryptography

All traffic in a session is encrypted using the **AES** algorithm running in Integer Counter Mode (ICM). Skype encrypts the current counter and a salt with the session key using the 256 bit AES algorithm. This returns the key stream, which is then XORed with the message content. This produces encrypted ciphertext, which is then transmitted to the recipient. Skype sessions contain multiple streams. The ICM counter depends on the stream, and the location within the stream.

2) Random number generation

Skype uses random numbers for several cryptographic purposes, for instance as a protection against playback attacks, creation of RSA key pairs, and creation of AES key-halves for content encryption. The security of a Skype peer-to-peer session depends significantly on the quality of the random numbers generated by both ends of the Skype session. Random number generation varies by operating system.

3) Cryptographic primitives

Skype uses standard cryptographic primitives to achieve its security goals. The cryptographic primitives used in Skype are: the AES block cipher, the RSA public-key cryptosystem, the ISO 9796-2 signature padding scheme, the SHA-1 hash function, and the RC4 stream cipher.

4) Key agreement protocol

Key-agreement is achieved using a proprietary, symmetric protocol. To protect against a playback attack, the peers challenge each other with random 64-bit nonces. The challenge response is to customize the challenge in a proprietary way and returned it signed with the responder's private key.

The peers exchange Identity Certificates and confirm that these certificates are legitimate. Because an Identity Certificate contains a public key, each end can then confirm signatures created by the other peer. Each peer contributes 128 random bits to the 256-bit session key.[1,2,4,8]

9 REFERENCES

[1] Berson, T. Skype security evaluation. ALR. 2005. 31.

[2] Garfinkel, S. L. VoIP and Skype security. Tactical Technology Collective. 2005. 12.

[3] Villeneuve, N. Breaching trust: An analysis of surveillance and security practices on China's TOM-Skype platform. 2008.

[4] Watzlaf, V. J., Moeini, S. and Firouzan, P. VoIP for telerehabilitation: A risk analysis for privacy, security, and HIPAA compliance. International Journal of Telerehabilitation. 2010. 2(2): 3.

[5] Ehlert, S., Petgang, S., Magedanz, T. and Sisalem, D. Analysis and signature of Skype VoIP session traffic. 4th IASTED International. 2006.

[6] Lu, L., Horton, J., Safavi-Naini, R. and Susilo, W. Transport layer identification of Skype traffic. Proceedings of the International Conference on Information Networking: Springer. 465-481.

[7] Hayes, B. Skype: A practical security analysis. Proceedings of the InfoSec Reading Room, SANS Institute. Downloaded on 7th: Citeseer.

[8] Taylor, C. R., Shue, C. A. and Najd, M. E. Whole home proxies: Bringing enterprise-grade security to residential networks. Proceedings of the Communications (ICC), 2016 IEEE International Conference on: IEEE. 1-6.

[9] Drake, T. M. and Ritchie, J. E. The surgeon will skype you now: advancements in e-clinic. Annals of surgery. 2016. 263(4): 636-637.

[10] Bruce, T., Byrne, F. and Kemp, L. Using Skype to support remote clinical supervision for health professionals delivering a sustained maternal early childhood program: a phenomenographical study. Contemporary nurse. 2018(just-accepted): 1-17.

[11] Clarke, D. and Ali, S. T. End to End Security is Not Enough. Proceedings of the Cambridge International Workshop on Security Protocols: Springer. 260-267.

[12] Gurung, S. and Kim, Y. Healthcare Privacy: How Secure Are the VOIP/Video-Conferencing Tools for PHI Data? Proceedings of the Information Technology-New Generations (ITNG), 2015 12th International Conference on: IEEE. 574-579.

[13] Hoßfeld, T. and Binzenhöfer, A. Analysis of Skype VoIP traffic in UMTS: End-to-end QoS and QoE measurements. Computer Networks. 2008. 52(3): 650-666.

[14] Ahson, S. A. and Ilyas, M. VoIP Handbook: Applications, technologies, reliability, and security: CRC Press. 2008.