

Creating A Covert Communication Channel By Means of Skype

Aleksandr Borisovich Vavrenyuk* Michael Aleksandrovich Ivanov* Viktor Valentinovich Makarov* and Viktor Alexandrovich Shurygin*

Abstract : This paper describes how to create a covert channel using SKYPE application. Unlike the previously published methods for creating channels which in some way use SKYPE traffic, only the service characters of SKYPE are used in this case. Traffic is not used at all in this method; all manipulations with service symbols are performed strictly according to the SKYPE rules, with no interference in protocols and regulations.

Keywords : Covert channels, SKYPE traffic, SKYPE statuses, status changes, SKYPE avatars.

1. INTRODUCTION

A number of works devoted to the creation of covert channels based on SKYPE application have appeared recently [1-3].

This application allows people to communicate with each other almost in every part of the world where the Internet is available. Besides, the connection itself is very inexpensive or even free of charge. More than 600 million people use SKYPE now [4].

Clearly, it involves a huge amount of traffic. The transmitted data streams are redundant, i.e. there is a possibility to wedge in, and so there is a tempting to use SKYPE tools for creating covert channels.

All the approaches described in previously published papers, one way or another, involve SKYPE traffic, or illegally intrude in it [7-12].

We can mention, as an example, the approach for channels creating, which the developers called “SkyDe” (SKYPE Hide) [4]

This method is based on service features of silence identification. During the communication, normally only one person transmits information over the channel, SKYPE sends a coded signal of silence in the opposite direction. Its code is much shorter, and it is not monitored by the system.

If you put the disguised fragments of messages into this code, they are received in parts, and then rejoined together, so you can send messages uncontrollably.

This paper describes the alternative method of creating covert channels using service characters of SKYPE – statuses and avatars.

At this approach, traffic is not used at all, and all manipulations with special symbols are performed strictly according to the rules of SKYPE, with no interfering in protocols and regulations.

2. SKYPE STATUSES

Let us remind Skype statuses and their main idea.

When logging in SKYPE, the user sees his/her profile icon in the upper right corner (this icon is called “avatar” in SKYPE, it is a circle with a picture or photo, or without any). There is a graphical image of status under the avatar in a small circle; the same icons are near the SKYPE-users from the contact list.

* National Research Nuclear University MEPhI, (Moscow Engineering Physics Institute) 31, Kashirskoe highway, Moscow, Russia, 115409

When clicking on the avatar, its large image appears to the right of the icon. When clicking on the status icon, the list of statuses appears below the icon. These dialog boxes are shown in Figure 1.

Generally speaking, there are 10 statuses in SKYPE, but the most convenient are those shown in Figure 1. Each time your companion logs in SKYPE, he/she definitely sees one of four statuses at his/her icon, and these statuses can be easily changed.

Thus, we can see the background for transmitting data to your companion by varying statuses, in fact – the creation of a covert channel.

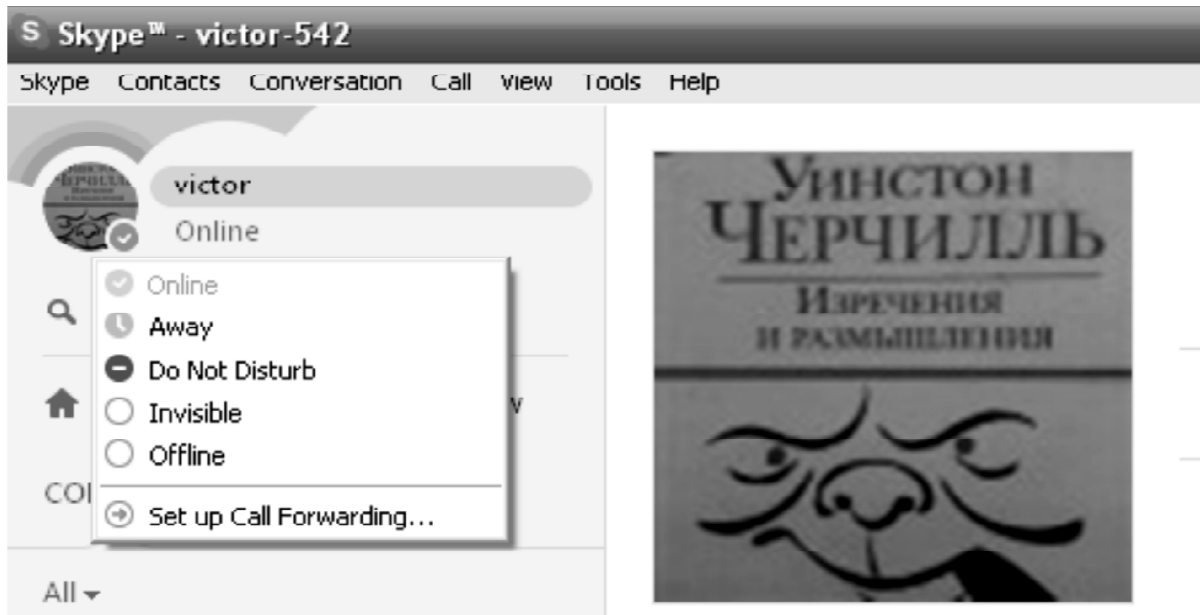




Fig. 1. Status options.


To select one of the first four statuses, you should just click on the small circle on the icon and choose the right status. This is performed manually and almost immediately (except for the “Do Not Disturb” status, as it should be confirmed).


“Invisible” and “Offline” statuses look almost the same, so further we will speak only about four statuses instead of five.

Before proceeding to the covert channel, consider the designation of statuses. When working with SKYPE application, different situations occur when you want to inform persons from your contact list, for example, that you are online, offline, or you should not be disturbed, etc. Network statuses are just for such situations, they allow to inform about the situation. Here are all these statuses:

 **“Online”**. This status is set automatically for all users by default; it means that persons from contact list can contact in any way. Subscriber immediately receives a notification about this.

 **“Away”**. This means the user has moved away from the computer, and most likely will not respond in the nearest time. However, the user can send him/her a message or call – the user is notified about that and he/she will hear that if not far from the computer.

 **“Do not disturb”**. The user is online but does not wish to be disturbed by anything. If you send a message or call him/her, these notifications are not accompanied by sound signals and can be seen only by the number next to the icon in the notification area of SKYPE app, this shows the user that someone is trying to contact.

 **“Invisible”**. This status has the same icon as the “Offline” status. Therefore, if the user does not want to contact, you cannot know for sure whether he/she is “Offline” or just “Invisible”. If you send a message or make a call, the subscriber receives the appropriate notice, but if it is not answered, you cannot know whether he/she sees the notification.

O “Offline”. It is shown automatically when the user closes the application or selects this status manually. In this case, the user cannot receive calls or text messages. He/she receives the notification as soon as selecting “Online” status.

🚫 “Blocked”. Those from the blacklist get this status. Such users do not know you have blocked them and just see your “Offline” status. If they send you a message or try to call you, you do not get any notifications. It should be noted that in the case of unblocking the user, you get all the messages and notifications for the period of blocking.

❓ “Contact request pending”. This user has not added you to the contact list and has not provided you with his/her contact information. When you try to call or send a message to him/her, the user is notified only in case this is allowed by SKYPE security settings.

➔ “Call forwarded”. This status means that the user is “Offline”, but since he/she has set up call forwarding, you can call him/her. Depending on set forwarding settings, he/she can respond from a mobile or landline phone, can receive messages and/or calls from anyone (it is a common call for the caller and a free call at SKYPE).

👁️ “Answering machine”. You are not online; callers can leave the messages on the voice mail.

📞 “Phone number”. This status is shown next to the fixed and mobile phone numbers stored in the phonebook.

It should be noted that in the recent versions of SKYPE “Offline” and “Invisible” statuses have the same icon – “empty white circle”, and cannot be distinguished by this icon, only by text.

3. STATUS CHANGING

You can change your online status in SKYPE application in one of the following ways [5]; each of them is convenient in certain situations:

- When on SKYPE main window, click on the status button and you see a list of statuses in the drop-down list (Figure 1). Select the one needed – aim a mouse cursor on it and press ENTER (left mouse button). Status text is changed to selected one.
- When SKYPE is minimized, click the right mouse button on SKYPE icon in the notification area (Figure 2.)

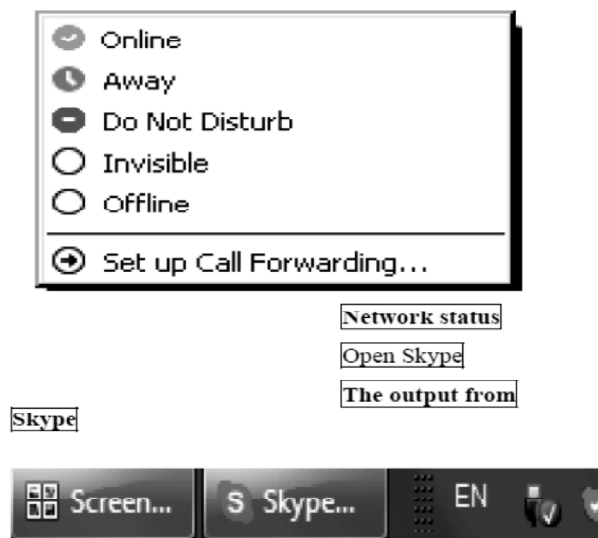


Fig. 2. Changing statuses in the notification area.

- In other cases, in SKYPE menu bar select «*Skype*» → «*Online status*» (Figure 3):

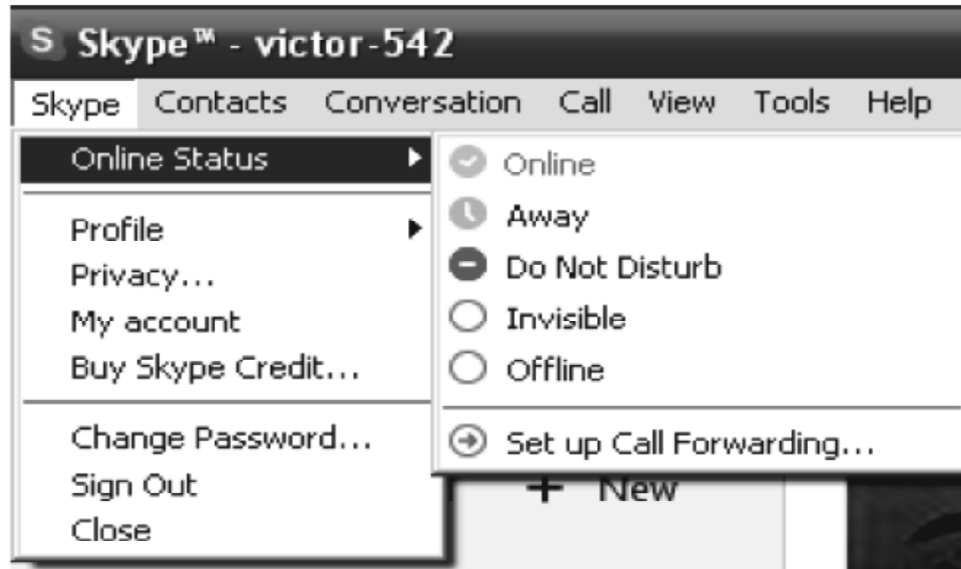


Fig. 3. Changing status from the menu bar.

- You can change the Skype online with the help of your keyboard (if the application is open). To do this, press the buttons: **Alt** + **S** + **→** and using **↑** or **↓** select status and press **Enter**.
- Let us select “**Away**” status.

The thing is, “**Away**” status is set automatically when the computer is not used for a certain time.

This is not desirable in our case, as the status changing must be performed at request.

To disable this option, or to change it in a set time, select «**Tools**» → «**Options**» in SKYPE menu bar, then:

- Select “**General Settings**” group in the “**General**” tab.
- Find the “**Change your status**”, “**Away**”, “**Show me as Away when I’ve been inactive for [x] minutes**” option and adjust as necessary. If you uncheck this option or set the value of “**0**” – SKYPE does not change the status automatically.

4. CREATING A CHANNEL

Now let us go to the issues related to the creation of a covert channel. As it was noted before, there are 10 possible statuses in Skype and the first four of them are the most convenient for our goals. They are changed easily at our request and at any time. Of course, you can use the other statuses, but they are less convenient and are not considered in this paper.

Now creating a channel let us abstract from the semantic sense of status, discussed above. We are interested only in a graphical representation of the status symbol and in the possibility of changing it at any time at request.

We define two modes of covert channels. Let us call them :

- *Signal* mode;
- “*Morse code*” mode.

The allure of using SKYPE to create a covert channel can be explained first of all be the fact, that regardless of the sender location and the receiving country, communication is possible wherever there is Internet access, at any time, by changing the skype statuses.

This reminds the classical problem about Alice and Bob [6], where SKYPE provider acts as a supervisor. Next, for short, we shall call statuses: green, orange, red and white.

Let us consider the modes.

4.1. Signal Mode

This mode is not suitable for transmitting large amounts of information, but it can be very important; moreover, it does not arouse suspicion at the frequent change of status.

The sender and the receiving parties agree in advance, that it is necessary to perform the following actions at a certain time if sender has a certain status, for example:

- “**Green**” – start some action.
- “**Orange**” – wait.
- “**White**” – stop action.
- “**Red**” – stop immediately.

It is clear that actions can be very different.

In predetermined time periods, the receiving party just logs in SKYPE and sees the sender’s status in the contact list.

There is no need to call him/her, to contact him/her with audio or video connection. You just need to see the status and react appropriately.

The above list of actions, shown as an example, can vary randomly arbitrarily, for example, the same statuses at different (pre-arranged) times may represent completely different actions.

It should be noted that the green and orange statuses are set automatically even if the sender does not change them himself/herself. So, here is a potential vulnerability of this channel. If something has happened to the sender, and he/she could not log out and close SKYPE application, the receiving party may interpret the green or orange statuses as a guide to action. The consequences can be very serious.

Therefore, if there are any concerns in this regard, use only red and white statuses. If two statuses are not enough to describe the situations, you can use (predetermined) combination of these two statuses.

4.2. “Morse Code” Mode.

In this mode, alphabet consisting of a combination of statuses is used to make messages for sending. The name is conventional, similar to Morse code. In this case, a message is transmitted online using the combinations of status symbols.

Lots of options are possible. Let us consider a specific example.

We use four statuses; “red” status is used as the separator between the letters of the alphabet. So we have three other statuses for the letters of the alphabet. It is obvious that the number of letters in the alphabet is determined by the number of 3^n , where n is code size of one letter. Let $n = 3$. A possible number of letters in such alphabet is 27.

The following restrictions are introduced in the case of the Russian alphabet :

- The letters “**е**”, “**е̇**”, “**э**” are denoted by a single character.
- The letters “**й**”, “**й̇**” are denoted by a single character.
- The letters “**д**”, “**д̇**” are denoted by a single character.

Each of these letters is determined when reading a message, implicitly.

It is obvious that any letter can correspond to any (predetermined) combination of the three statuses, such as BZZH, ZBB, etc.

Next, the sender types the message at the appointed time of the communication session, and the receiving party tracks of the status of the sender and writes the text.

For safety reasons, it makes sense to change the alphabet in a predetermined time intervals.

Now the question arises, how much data can be sent in this mode, for an hour for example.

Let us make a rough estimate. The time of manual status change is about 1s. In the case of the “**red**” separator, the time is about 2s (to be confirmed). Thus, about 20 letters are transmitted in one minute, and 1,200 letters in one hour, respectively.

One can send approximately 28,800 letters per day; this corresponds to approximately 2,000 to 3,000 letters per page or 14 pages per day (Times New Roman – 12).

Clearly, the amount is small, but in some cases it is sufficient. These examples illustrate the principle of the proposed method. By changing the connection time and alphabets lots of options become possible, as well as the use of other statuses. This increases significantly the volume of transmitted messages.

5. USING AVATARS

Let us return to Figure 1. There is a drawing, a kind of your representation in the upper left corner, in a circle. This can be your photo, or a drawing, some picture or no pattern at all. You can change picture arbitrarily at any time; therefore, together with the status, this can be used for creating a covert channel.

Changing avatar.

Refer to Figure 4. It shows a screen with the avatar. A large image of avatar appears when clicking on the circle with the avatar. There is a sign **“Change Avatar”** below. After clicking on this link, go to the avatar selection mode (Figure 5).

In this mode, you can change the avatar to any other in the following way:

- Take a picture using the computer camera;
- Take an image from your pictures;
- Use a picture from your computer’s memory;
- Use pictures from external memory (*e.g.* flash memory).

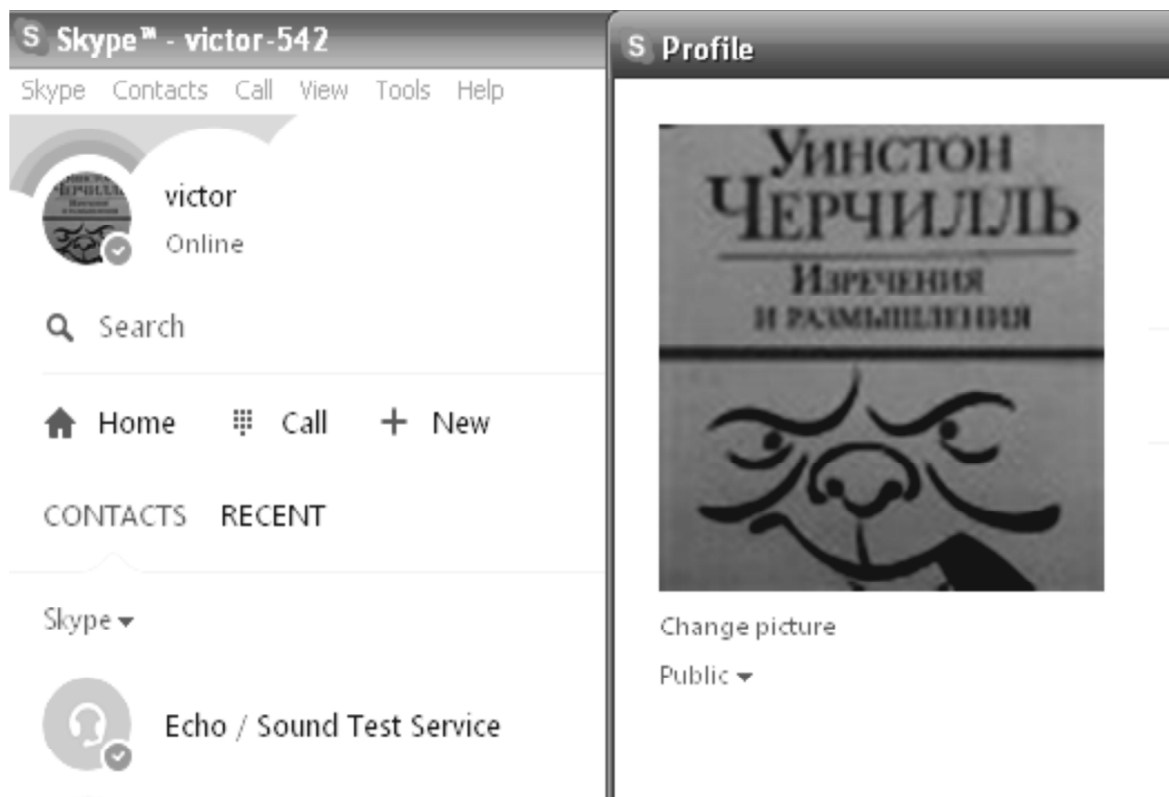


Fig. 4. Screen with avatar.

To take a picture, put the object in front of the computer camera and click on the **“Take a picture”** button, then the image appears on the small screen.

To use the previously taken pictures, just click on the appropriate image in the **“Your previous pictures”** film, and it appears on the small screen. There are arrows to the left and to the right of the film, with the help of which you can shift the film, searching the image.



Fig. 5. Avatar selection mode.

To remove the image from the internal or external memory, click on the **“Browse”** button, select the file in the appropriate section and pick it.

The image appears on the small screen, then click **“Open”** and our image appears in the avatar selection mode on the small screen (Figure 6).



Fig. 6. electing an image from memory.

Click on the **“Use this picture”** button, no matter which way you selected the image, and a new avatar appears (Figure 7).

There can be lots of avatars and combined with statuses they can significantly enhance the channel's characteristics both in signal mode and in “Morse code” modes.

This is especially true concerning the signal mode. In contrast to four statuses, there can be a number of avatars, therefore; it is possible to provide a great number of situations.



Fig. 7. Screen with a new avatar.

Naturally, the receiving party should have the means to automate the search for correspondence between the picture and description of necessary actions.

The avatar can be used as an additional symbol to increase the number of letters in the alphabet when using “Morse code” mode.

But it seems more appropriate to use it as a sign of a particular alphabet. The receiving party sees a new avatar and understands it should switch to another predetermined alphabet.

6. CONCLUSION

Thus, the use of SKYPE service symbols allows creating a covert communication channel in several ways, not intruding in traffic and, thus, without breaking all existing protocols and agreements.

The possibility to use one SKYPE on two computers is of a particular interest.

Consider the following situation: there are two computers with Internet access in two different countries; they run the same SKYPE with the same account, login and password. Let it be Moscow and Bulgaria.

If the person in Moscow logs in SKYPE, he/she sees the avatar in the upper left corner. If he/she clicks on it, a large image of avatar appears to the right of it. If the other user enters SKYPE in Bulgaria, he/she see the same thing.

But the thing is you can easily change your avatar, SKYPE allows it (see. Section 5 of this article), and when your companion in Moscow logs in his/her SKYPE account, he/she sees a new avatar.

In other words, in this case, there is no need to have your own SKYPE account; you can communicate with each other without any traffic at all as if communicating to yourself, but in different parts of the world.

At the same time, if one of the parties changes its status, his/her companion sees it immediately.

As for the time of appearing of a new avatar on the other side from the moment of its changing, there is some uncertainty.

We have conducted a series of experiments and in some cases this happened immediately, and in other cases – in few minutes, sometimes it took several hours, but change always occurred. In order to find out what is the reason of such variation, it is necessary to conduct a separate study.

7. REFERENCES

1. J. Zhai, & M. Wang, “SkyLen: A Skype-Based Length Covert Channel”. *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 6, No. 3, 2015, pp. 106-110.
2. W. Mazurczyk, M. Karac̆, & K. Szczypiorski, “SkyDe: a Skype-based Steganographic Method”. *International Journal of Security and Its Applications*, Vol. 9, No. 3, 2015, pp. 353-362.
3. R. McPherson, A. Houmansadr, & V. Shmatikov, “CovertCast: Using Live Streaming to Evade Internet Censorship”. *Proceedings on Privacy Enhancing Technologies*, Vol. 3, 2016, pp. 1-14.
4. Naskol’ko bezopasen Skype? [How Safe is Skype?]. 2016. Retrieved October 9, 2016, from <http://medbe.ru/news/interesnoe/naskolko-bezopasen-skype/>.
5. Setevye statusy v Skaype [Network Statuses in SKYPE]. 2013. Retrieved October 9, 2016, from <http://www.skaip.su/setevye-statusy-v-skaype>.
6. R.L. Rivest, A. Shamir, & L. Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”. *Communications of the ACM*, Vol. 21, No. 2, 1978, pp. 120-26.
7. L. Xiang, Y. Xie, G. Luo & W. Wang, „On the Existence of Subliminal Channel in Instant Messaging Systems”. *International Journal of Security and Its Applications*, Vol. 9, No. 3, 2015, pp. 353-362.
8. K. Kohls, T. Holz, D. Kolossa & C. Popper, „SkypeLine: Robust Hidden Data Transmission for VoIP”. In *ASIA CCS’16*, May 30 – June 3, 2016, Xi’an, China, pp. 877-888.
9. W. Mazurczyk & J. Lubacz, “LACK: a VoIP steganographic method”. *Telecommunication Systems: Modelling, Analysis, Design and Management*, Vol. 45, No. 2-3, 2010, pp. 153-163.
10. K. Kohls, T. Holz, D. Kolossa & C. Popper, „Skypeline: Robust Hidden Data Transmission for VoIP”. Technical Report TR-HGI-2016-001, RUB, 2016.
11. A. Janicki, W. Mazurczyk & K. Szczypiorski, “On the Undetectability of Transcoding Steganography”. *Security and Communication Networks*, Vol. 8, No. 18, 2015, pp. 3804-3814.
12. Zielińska, W. Mazurczyk & K. Szczypiorski, “Trends in Steganography”. *Communications of the ACM*, Vol. 57, No. 2, 2014, pp. 86-95.