How dangerous is Skype?

Skype is a peer-to-peer (P2P) application, meaning users can connect directly to each other without going through a central server. There is a lot of information (many of which are inaccurate) about the level of risk

There is a lot of information (including a lot of inaccurate information) about the danger of Skype for corporate networks and personal users. So how dangerous is it really? In this article we will learn.

Understand the basic structure of Skype

Skype is a peer-to-peer (P2P) application, meaning users can connect directly to each other without going through a central server. Initially Skype used Internet-based servers to authenticate users when logging in and monitoring their status. But when 'chat' or instant messaging (Instant Message) forms, voice calls and file transfers are born, communication is transferred to direct P2P connectivity. If one or both users are behind a firewall that interprets an enterprise network address (Network Address Translation or NAT Firewall), communication can be relayed through a Supernode. Because direct P2P connection cannot be established after NAT firewall. In the case of file transfer, you will see a message given saying that the transfer process is being relayed.

One of the security experts' top concerns about Skype is that a Skype client can find its way around secure, comprehensive firewall configuration. Skype uses ports 80 and 443, which are included in most open firewalls for Web links. Moreover, Skype can also reroute traffic if the initialization port assigned during Skype installation is unavailable. That makes it very difficult to remove Skype at the firewall level, because the Skype ports used can be changed if needed.

Skype also encrypts each contact with a 25-bit AES key, which means that each contact will have a different key every time you make it, making it impossible to eavesdrop on communications.

One of the notable points about Skype security is its 'Super nodes' (Supernote), which has Skype traffic routing function. A Super node is a computer with its own configuration, connected directly to the Internet and cannot be behind a NAT firewall. They must have a 'real' routable IP address. In addition to some of these limitations, the super node can be any Skype user computer that meets the minimum hardware and configuration requirements.

There are many things you can learn about Skype's security structure. See details on the website: Skype Security Resource Center.

Skype FUD

You have a rough understanding of how Skype works, now we will see how dangerous and dangerous it is. There are many misconceptions about Skype that are still floating in the online world. Here are the 5 most common misconceptions:

1. Skype uses a lot of bandwidth on a network.
2. Any computer can be a Super node.
3. Skype is like any IM application program and vulnerable to IM worms and viruses.
4. Skype can hardly be removed online.
5. Skype is encrypted, unable to query IM messages.

Let's see how bad these issues really are.

First problem: Skype uses a lot of bandwidth on the network

In fact, Skype uses very little bandwidth, only approximately 30Kbit / sec for a conversation. If a user's computer becomes a Super node, of course it will consume a large amount of extremely high bandwidth. But remember, your computer must be directly connected to the Internet to become a Supernode. Most computers in the enterprise or personal computer must be connected to the Internet through intermediate servers. Therefore, this issue is not really worrying.

Second problem: Any computer can become a Super node

We already know that a computer must have a routable IP address and live directly on the Internet to become a Super node.

If the computer is on a typical corporate network, protected by a firewall providing NAT, using a 192.168.xx or 10.xxx private IP address frame, it cannot become a Super node. NAT firewalls and even home routers prevent many computers from becoming Super nodes.

Third problem: Skype is easily vulnerable to IM worms and viruses

Last year, according to Akaonix Systems statistics, by the beginning of December, there were 1,355 worms and viruses attacking IM clients, but none of them affected Skype. Although Skype received two security warnings in 2006, four for 2005 and one in 2004, no warnings have been made into exploited vulnerabilities.

The main vulnerability of instant messaging applications (IM) is the file transfer function, which can be

exploited, allowing someone to send files containing malware. Virus scanners are constantly updated, running in the 'auto-protect' model that can handle this activity. In addition, many applications have their own IM scanning options. If you have the latest updated anti-virus software, run in the 'auto-protect' model, you don't need to worry much about worms or viruses. Or you can disable Skype's file sending function if you want to be completely secure.

Problem 4: Skype can hardly be removed online

Skype is only difficult to remove if you do not know it is on your network or if you do not have a good configuration management program for clients. There are many ways to remove Skype, from using scripts to use network management software to removing them directly at the network layer.

Problem 5: Skype is encrypted, unable to query IM messages

This is not really wrong. Skype sessions are encrypted, so you cannot package or query Skype communications. The same is true for many other IM applications. So Skype is no less secure than any other instant messaging (IM) program that uses encryption.

Conclude

Until now, Skype has not encountered some unpleasant troubles about viruses and worms like other IM applications. The only frequently mentioned problem is some warning signs before a hole is discovered and exploited. Any application that allows file transfer, instant messaging, or computer calls that cannot be monitored, stored, or recorded is subject to a certain level of danger.

However, Skype's structure is more difficult to crack than some IM applications open on the Internet. So it can be said that it is the safest among IM applications. But there are also some application programs that do not serve Internet connections like Jabber is even safer for internal IM contacts. But, so far, if you question whether Skype is more secure than MSN Messenger, Yahoo Messenger, AIM or ICQ, the answer is 'Yes'.