An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol

(Salman A. Baset e Henning Schulzrinne)

Prof. Dr. Célio V. N. Albuquerque

Etienne César R. de Oliveira
Doutorando em Computação

Objetivo e Motivações

O objetivo deste trabalho é identificar o funcionamento do cliente para VoIP Skype, descrevendo o processo de autenticação, a transferência de arquivos de mídia, o estabelecimento da chamada, CODECs etc, além do comportamento desta ferramenta quando executado em redes com NAT e/ou firewall.

A principal motivação dos autores baseia-se no fato do Skype prover uma qualidade de voz superior a produtos similares, tais como Yahoo IM e MSN.

Proposta

O Skype é um cliente de VoIP, desenvolvido pelo KaZaa, que atua sobre uma rede sobreposta ponto-a-ponto e possui dois tipos de nós: nós comuns (*ordinary host*) e SN (*Super Nodes*). Os nós comuns representam aplicações Skype que podem estar estabelecendo ligações telefônicas ou enviando mensagens de texto; já os SNs atuam como ponto de conexão da rede Skype, além de executarem as mesmas aplicações que os nós comuns. Nós comuns conectados à Internet através de IPs públicos e que disponham de recursos de processamento, memória e rede disponíveis são candidatos a SNs. O processo de autenticação ocorre entre os nós da rede Skype e um conjunto de servidores específicos, denominados Skype *Login Server*. A figura 1 descreve esse ambiente.

Os autores acreditam que os nós Skype usam uma variação do protocolo STUN (*Simple Traversal of User Datagram Protocol Through Network Address Translators* – RFC 3489) com intuito de determinar o tipo de NAT ou de *firewall* que possa estar entre o cliente Skype e a Internet.

Cada cliente Skype (SC – Skype *Client*) mantém uma tabela denominada *host cache* (HC) com nós que encontram-se ao seu alcance, relacionando os endereços IP e porta dos SNs. O protocolo TCP é utilizado para sinalização e tanto o protocolo TCP quanto o protocolo UDP podem ser utilizados para transporte do fluxo de mídia.

O cliente Skype, ao ser instalado, gera uma porta aleatória, que será utilizada para a conexão. Além desta porta, as portas 80/TCP e 443/TCP podem vir a ser utilizadas. Após a

conclusão da instalação e o início do uso do cliente Skype, a tabela *host cache*, que é implementada através da inserção de informações no *Windows Registry*, passa a ser incrementada com informações (endereço IP e porta) de outros usuários. A lista de contatos também é armazenada, de forma criptografada (AES), no *Windows Registry*, o que constitui um problema na versão avaliada do Skype. Os autores afirmam que o sinal de voz na faixa de 50 à 8.000 Hz é codificado com base em 3 codificações distintas: iLBC, iSAC e um terceiro codificador não reconhecido.

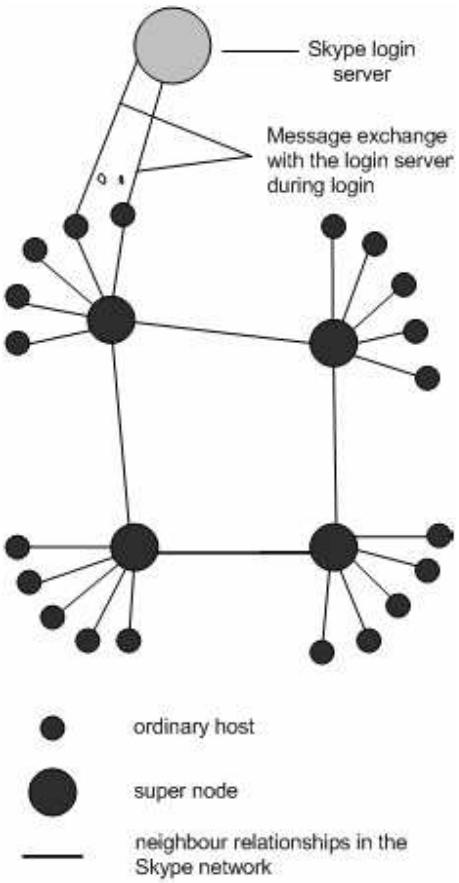

Figura 1 - Rede Skype

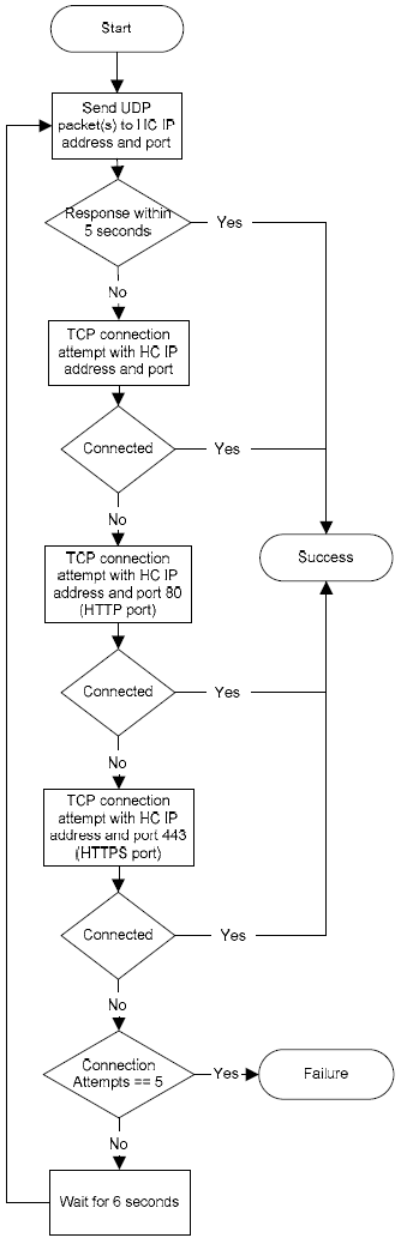

Figura 2 – Algoritmo de Autenticação

Os testes foram realizados com a versão 0.97.0.6 do Skype em máquinas instaladas com Windows 2000, entre fevereiro e abril de 2004.

Durante o processo de login, o cliente Skype envia, inicialmente, um pacote UDP para um SN e aguarda por uma resposta por 5 segundos. Caso não obtenha sucesso, tenta, então, estabelecer uma conexão na porta 80; caso não obtenha sucesso novamente, tenta estabelecer uma conexão na porta 443. Este processo é repetido até 4 vezes. Após o cliente Skype contatar um SN, é necessário efetuar a autenticação no *Login Server*. O algoritmo de autenticação (*login*) encontra-se na exemplificado através da figura 2. Após o primeiro login, a tabela *host cache* é populada com 7 entradas.

Os autores acreditam que o cliente Skype é capaz de identificar, no processo de login, se o mesmo se encontra sobre a proteção de um sistema de *firewall* ou sobre a ação de NAT. A forma de comunicação entre o cliente Skype e o SN pode variar em função da presença ou ausência de um *firewall* ou de NAT.

A localização de usuários no Skype é baseada na tecnologia Global Index. A pesquisa garante a localização de qualquer usuário que tenha se conectado nas últimas 72 horas. Após o estabelecimento de uma chamada entre dois usuários Skype, inicia-se a troca de dados, que pode ser a transferência de dados ou uma chamada VoIP. Os dados são transmitidos através do protocolo UDP se ambos os clientes Skype estiverem na Internet com endereços IPs públicos; caso um dos clientes esteja sob NAT, serão enviados pacotes de dados com protocolo UDP através de um *host* Skype intermediário; por fim, se ambos os clientes Skype estiverem sob NAT, os pacotes de dados com o protocolo TCP serão enviados através de um *host* Skype intermediário.

Vantagens

A proposta de identificar o funcionamento e a arquitetura do Skype foi bastante interessante e, embora o trabalho tenha sido prejudicado pela ausência de informações ou pela incompreensão de algumas situações, o resultado final foi capaz de elucidar, de forma genérica, o comportamento do Skype.

Desvantagens e Limitações

Os autores fazem referência à figura 15 que, na realidade, é a figura 16 do artigo. O mesmo fato ocorre quando os autores fazem referência à figura 16, que na realidade é a figura 17. A numeração das figuras está incorreta, passando da figura 14 para a figura 16.

Como os autores não conseguiram, nas experiências realizadas, forçar um SN para um cliente Skype, a análise foi prejudicada, pois não foi possível determinar efetivamente o papel do SN. Os autores não descreveram como algumas informações foram obtidas, tais como o algoritmo de criptografia (AES), os CODECs utilizados (iLBC, iSAC) etc.