Analysis and Signature of Skype VoIP Session Traffic

Sven Ehlert

Sandrine Petgang

Fraunhofer FOKUS, Berlin, Germany

July 25th, 2006

Students :Amine.Boukioud@ensimag.fr
Lamya.Boumert@ensimag.fr

Course Link : https://ensiwiki.ensimag.fr/index.php/4MMSR

Authors

- **Sven Ehlert :**
  - ✓ Fraunhofer Society
  - ✓ Engineering, Networks & Communications, Security & Privacy,SIP/Voip Security and research
- **Sandrine Petgang :**
  - ✓ Fraunhofer Society
  - ✓ Skype research
  - ✓ http://www.cs.columbia.edu/~salman/skype/

Skype ?

- A peer-to-peer (P2P) overlay network for VoIP launched in 2003.
- Skype allows its users to place voice calls and send text messages to other users of Skype clients
- similar to MSN and Yahoo IM but it has better voice quality and uses different protocols

Introduction

Analyzing network traffic with the goal to detect patterns that are intrinsic to the Skype protocol

Creating a security operator to detect , monitor or filter Skype traffic

Table of contents

I. Introduction
II. Skype network entities
III. Analysis methods
IV. Skype components
V. Skype message flow
VI. Detection limitations
IV. Conclusion

Skype network entities

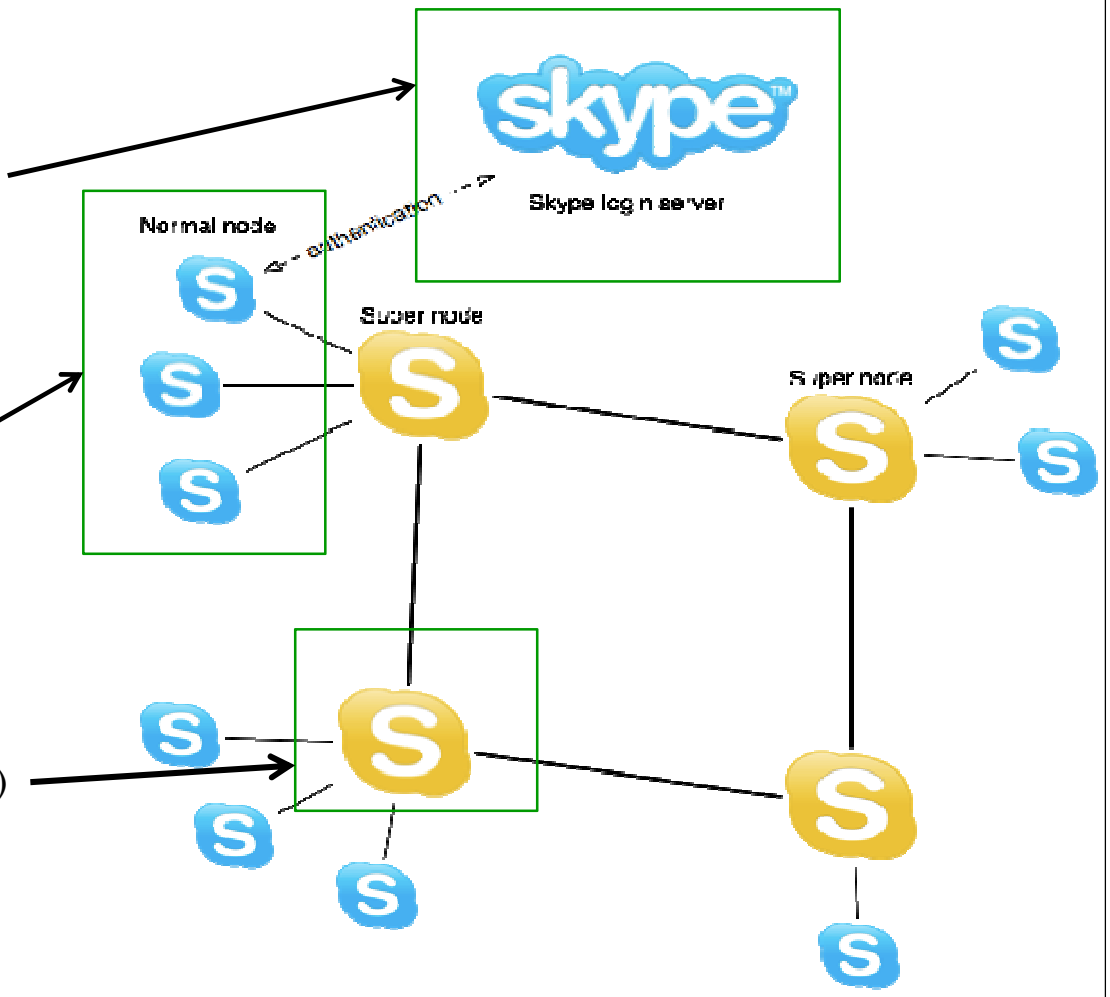
Skype Login server (LS):

✓ manages the creation of Skype usernames
✓ handle user authentication

Skype Client (SC): a participating user

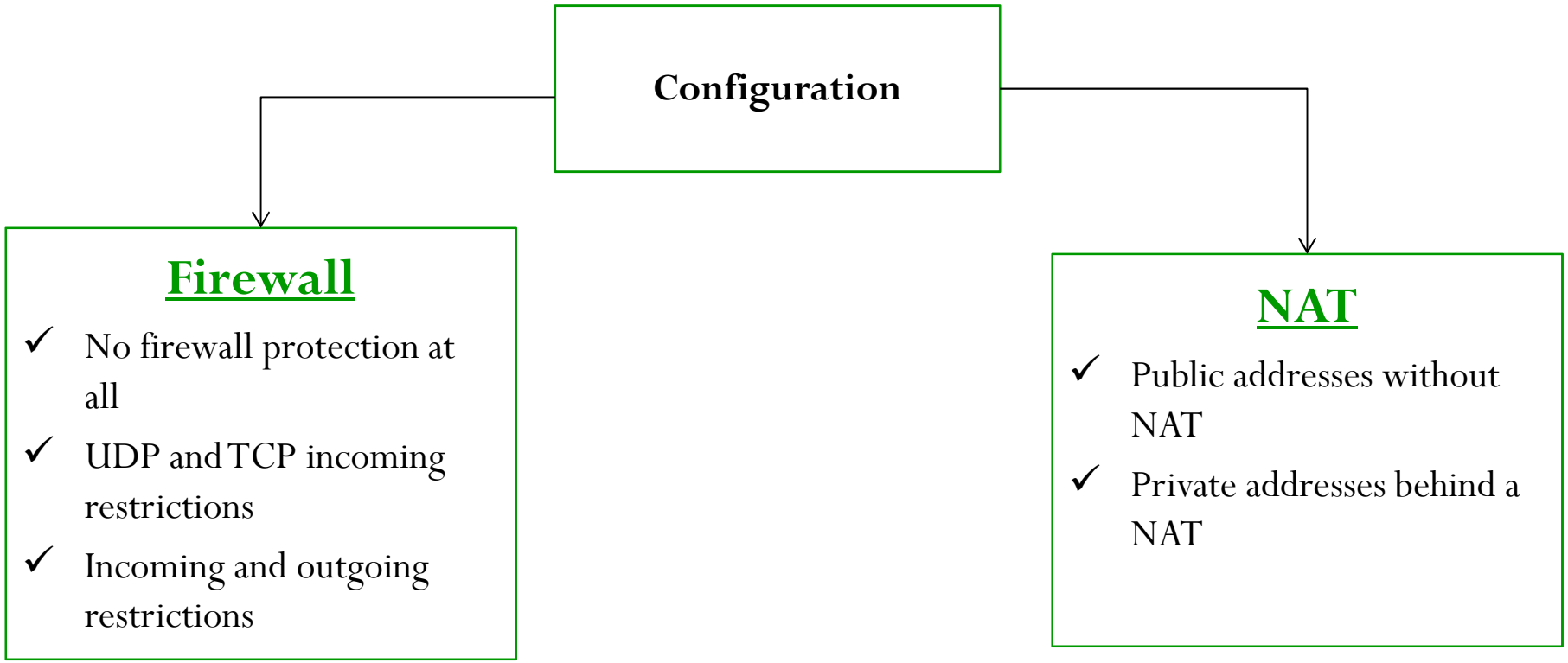
Super Node(SN): is a SC that has a public IP and enough CPU ,can perform:

✓Routing tasks (forwarding requests)
✓Forwarding login requests
✓Providing media proxying capabilities

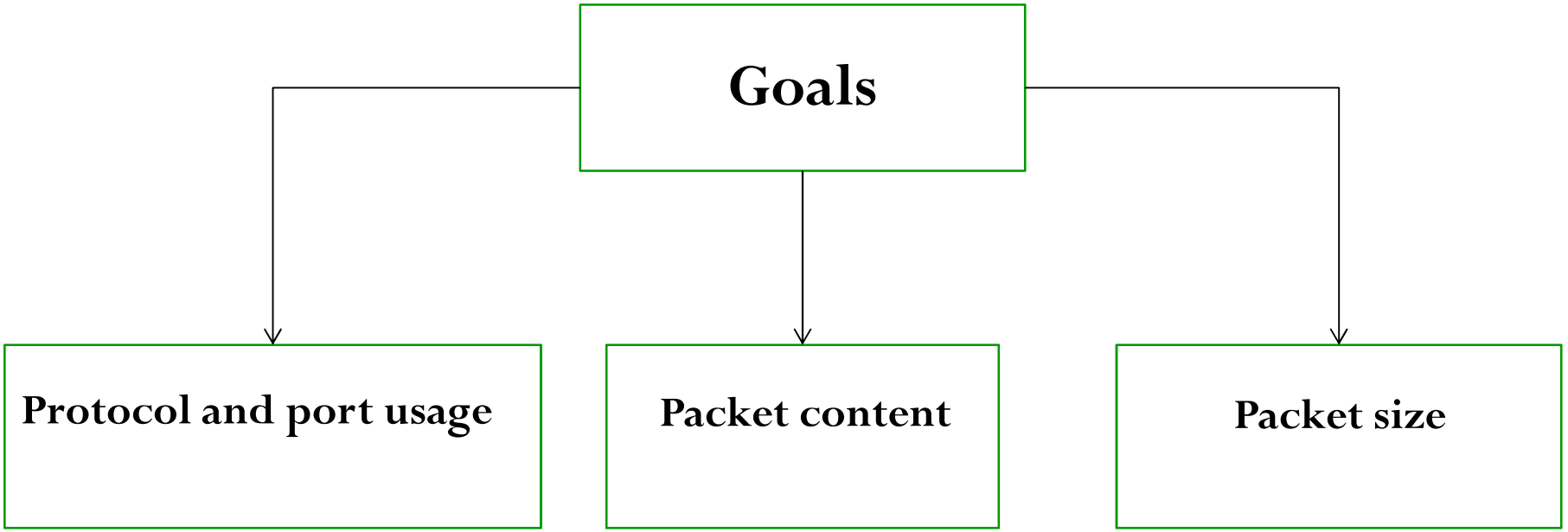


Analysis Methods (1/2)

To detect characteristics of Skype's network behavior, they have modified firewall and Nat at both nodes to gain a broader data set



Analysis Methods (2/2)



Skype's components (1/3)

- **Ports :**

A Skype client (SC) opens a TCP (signalization) and a UDP (media streaming) listening port configured in its connection dialog box

- **Host Cache (HC)**

A list of super node IP address and port pairs that SC builds and refreshes regularly

- **Codecs**

A wideband codec [1] allowing frequencies between 50-8KHz

Skype's components (2/3)

- **Buddy List**
  - ✓ In Windows XP, Skype stores its buddy information in an XML file
  - ✓ In Linux, Skype stores the 'config.xml' file in $(HOMEDIR)/.Skype/<skypeuserid>

- **Encryption**
  - ✓ Skype uses 256-bit AES encryption
  - ✓ Skype uses 1536 to 2048 bit RSA to negotiate symmetric AES keys

- **NAT and Firewall**

  SC uses a variation of the STUN and TURN protocols to determine the type of NAT and firewall

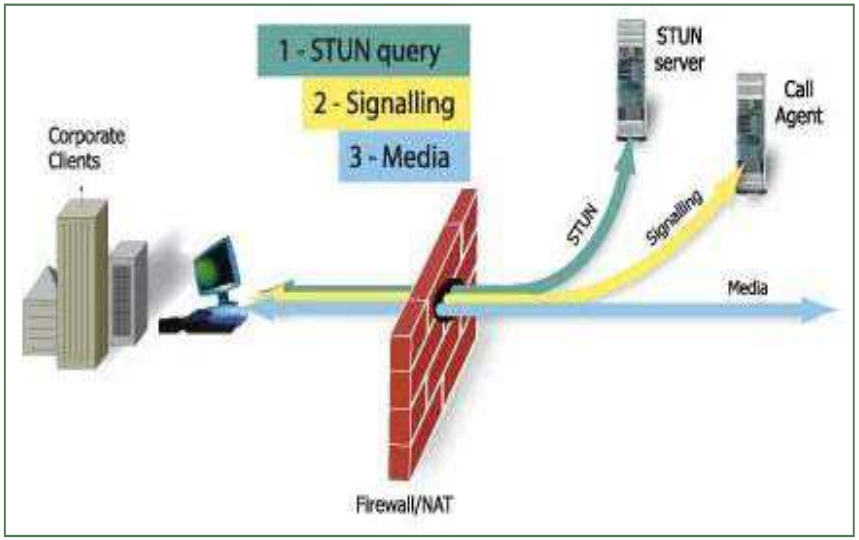
Skype's components (3/3)

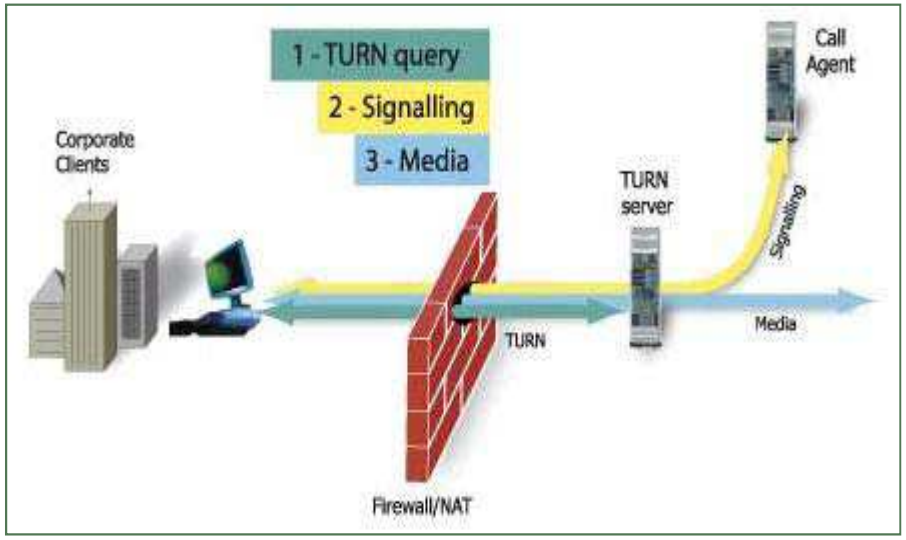
STUN:

- Simple Traversal of UDP through NAT

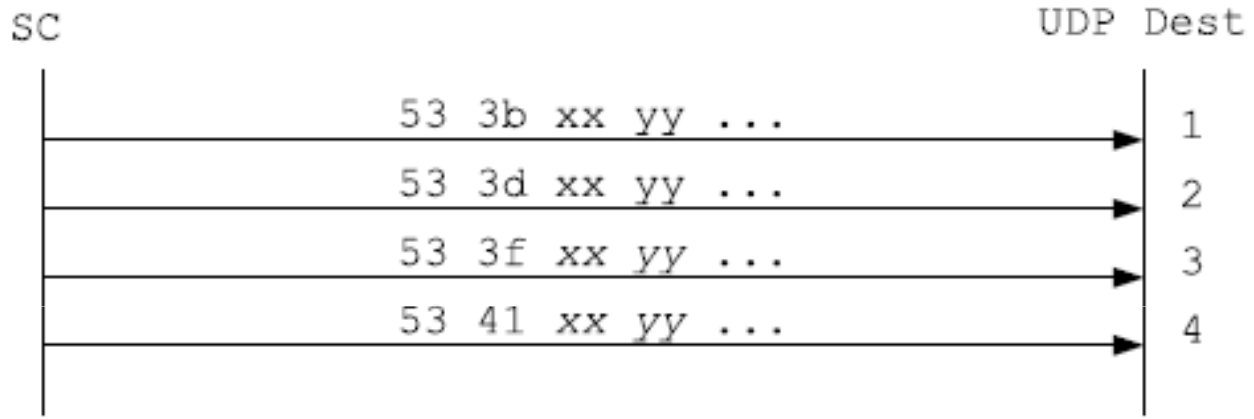
TURN:

- Traversal Using Relay NAT





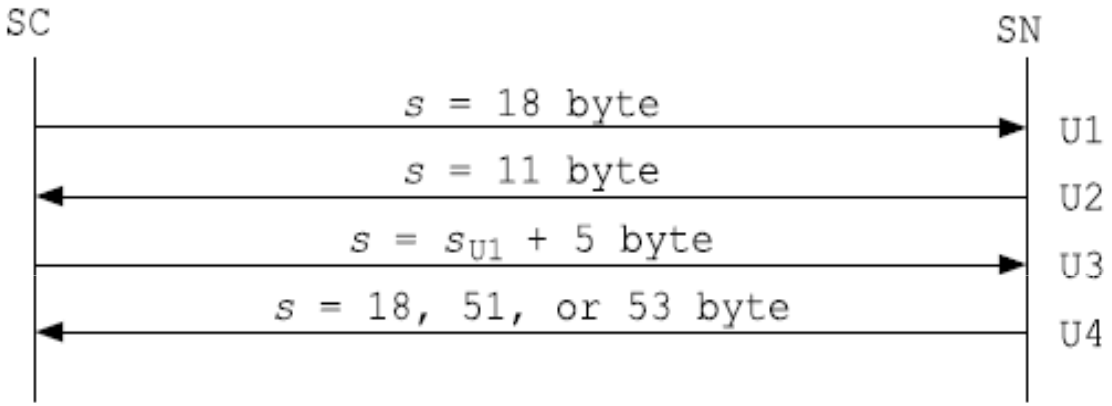
Skype message flow analysis



- Three distinct tasks :
  - ✓ UDP Probe
  - ✓ TCP SN Handshake
  - ✓ TCP Authentication

Skype message flow analysis

UDP Probe



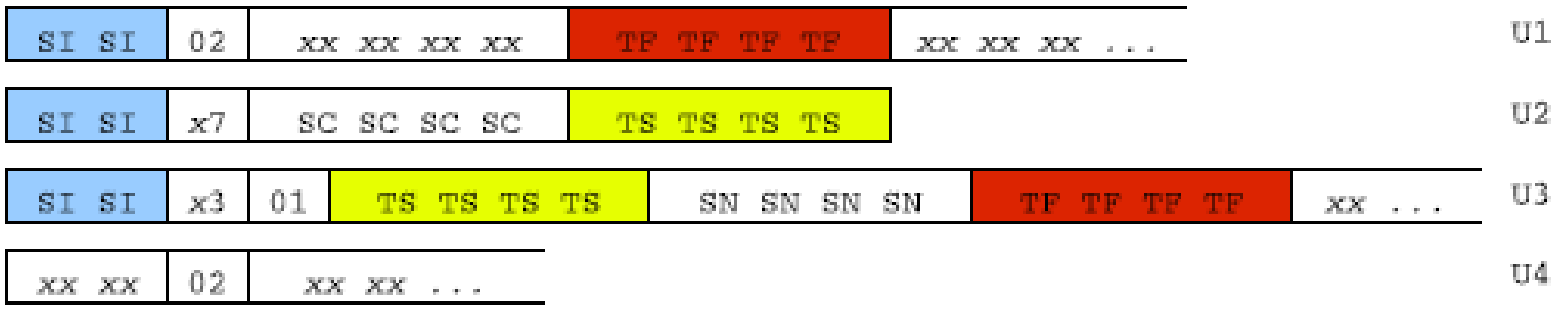
Skype 1.4	Skype 2.0
Su1 = 18 bytes	Su1 varies.
Su2= 11 bytes	Su2= 11 bytes
Su3=Su1+5	Su3=Su1+5
Su4=18,51 or 53 bytes	Su4=18,51 or 53 bytes

Skype message flow analysis

UDP Probe

Session identifiers :

- U1 is a initiating message
- the first two bytes contain a session identifier

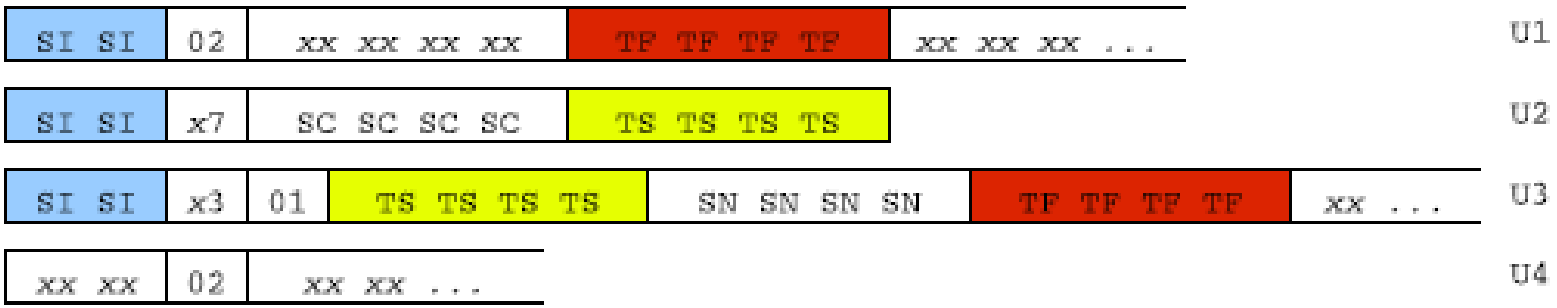


Skype message flow analysis

UDP Probe

Function parameter :

- The third byte of a message seems to be a message type encoding.

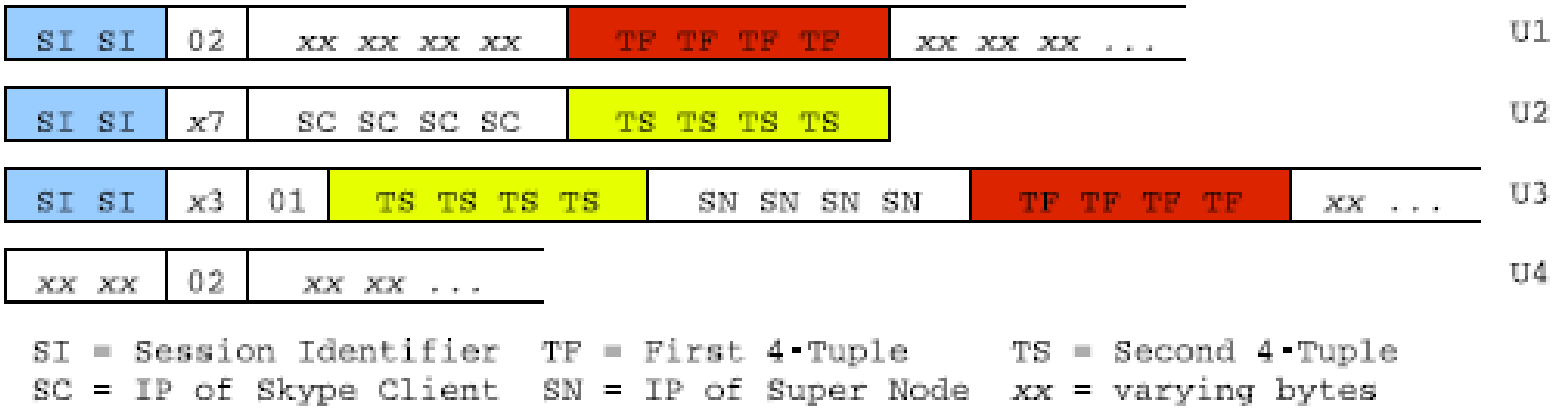


Skype message flow analysis

UDP Probe

IP Address exchange :

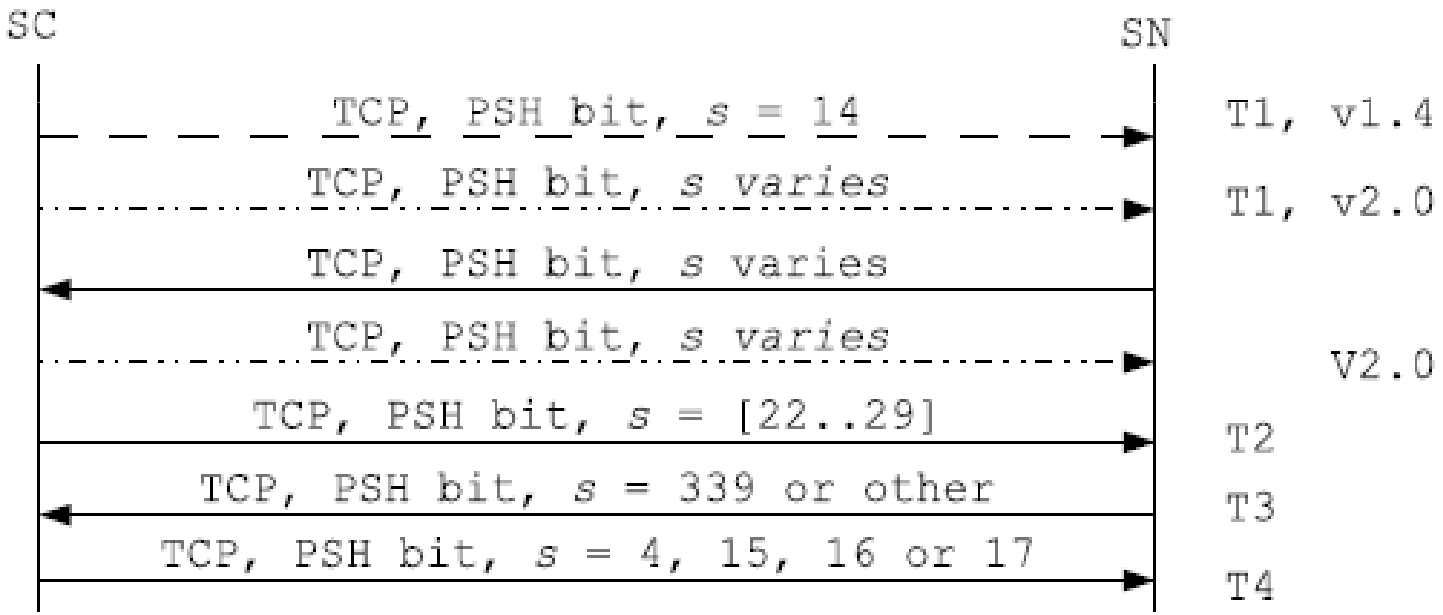
- U2 (4-7) contains the SC's IP address
- U3 (9-12) contains the SN's IP address.



Skype message flow analysis

TCP SN Handshake

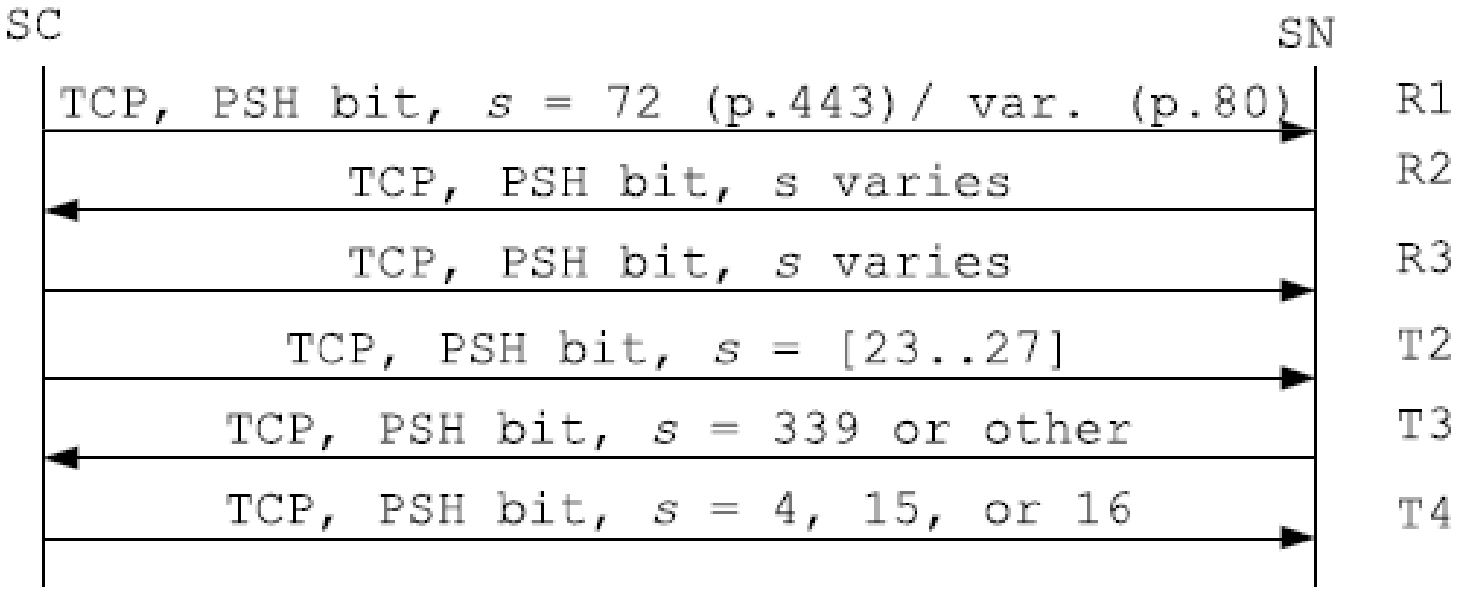
TCP SN signalling :



Skype message flow analysis

TCP SN Handshake

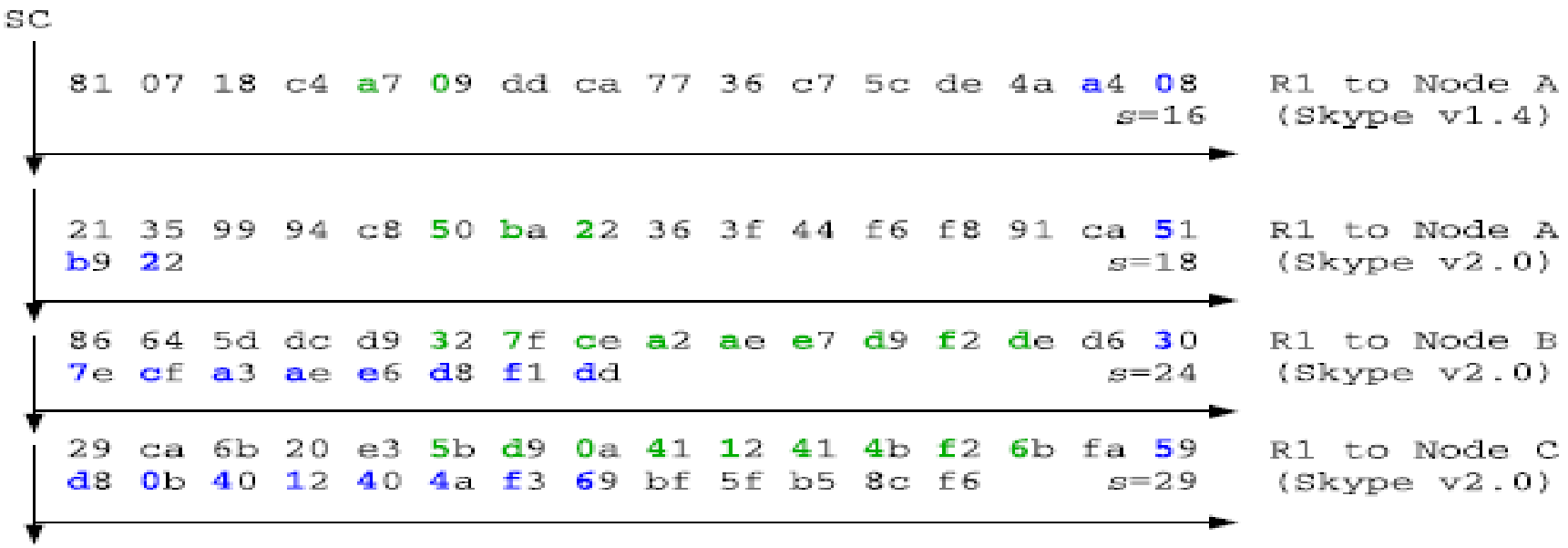
TCP Restrictions Applied :



Skype message flow analysis

TCP SN Handshake

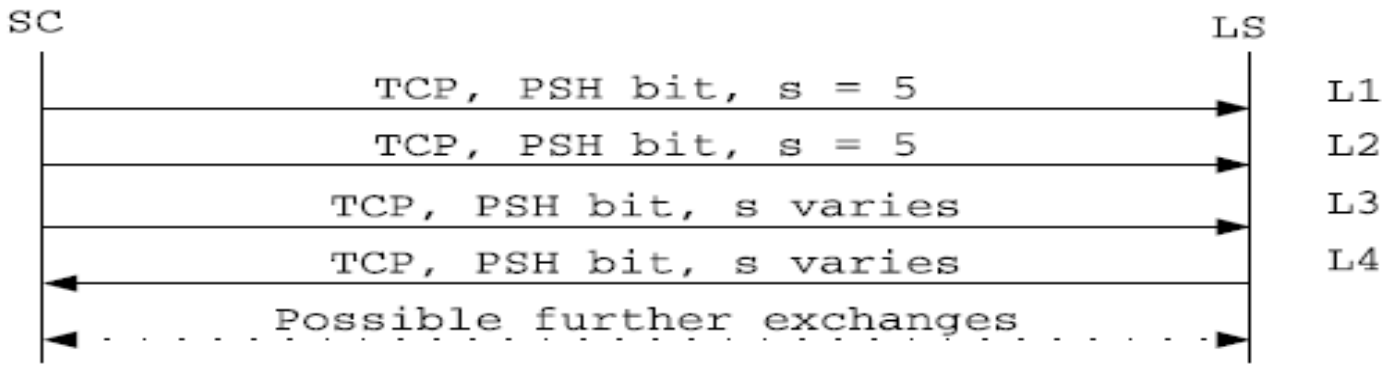
- **Port 80 Operation :** it does not use HTTP
- **Port 443 Operation :** use a modification of the Transport Layer Security (TLS) protocol



Skype message flow analysis

TCP Authentication

- **Restricting Access to LS :** detect messages L3 and L4 exchanged with a randomly selected
- **SN Restricted TCP Access :** TCP access over port 1024 was not allowed, the SC initiated the same handshake over ports 443 and 80.
- **Automatic Login :** the Skype application stores the informations and retrieves it the next time the user starts up the application. The users does not have to enter his credentials again for further login attempts.



Detection limitations

- Skyp's Peer-To-Peer character, the security network has to install monitoring systems at all network points
- Detection of Skype usage in high traffic scenarios requires powerful monitoring hardware
- Patterns differ between the versions ,so the detection requires continuous monitoring

Conclusion

- **Skype is a P-2-P technology**
- **Skype architecture:**
  - ✓ Skype client
  - ✓ Super nodes
  - ✓ Login servers
- **Skype components:**
  - ✓ Ports
  - ✓ Host cache
  - ✓ Codecs
  - ✓ Body list
  - ✓ Nat firewall(STUN-TURN)
- **Skype message flow:**
  - ✓ UDP Probe
  - ✓ TCP Handshake
  - ✓ TCP authentication

References

- [1] **a)** iLBC codec. http://www.globalipsound.com/datasheets/iLBC.pdf **b)** iSAC codec.http://www.globalipsound.com/datasheets/iSAC.pdf **c)** iPCM codec. http://www.globalipsound.com/datasheets/iPCM-wb.pdf
- [2] Global IP Sound. http://www.globalipsound.com/
- Google talk (beta). http://www.google.com/talk.
- Yahoo messenger with voice. http://messenger.yahoo.com.
- Skype - the whole world can talk for free. http://www.skype.com.
- H. Schulzrinne. Session initiation protocol. *RFC 3261, 2002.*
- V. Paxon. Bro: A system for detecting network intruders in real-time. *Computer Networks, 31(23-24), 1999.*
- A. Valdes and K. Skinner. Adaptive, modelbased monitoring for cyber attack detection. *RAID 2000, 2000.*
- M. Fiedler K. Tutschku T. Hossfeld, A. Binzenhoefer. Measurement and analysis of skype
- J. Kurose D. Towsley K. Suh, D.R. Figueiredo. Characterizing and detecting relayed traffic: A case study using skype. *UMass Computer Science Technical Report 2005-50, 2005*
- N. Daswani S. Guha and R. Jain. An experimental study of the skype peer-to-peer voip system. *5th International Workshop on Peer-to- Peer Systems (IPTPS '06), 2006.*
- H. Schulzrinne S. A. Baset. An analysis of the skype peer-to-peer internet telephony protocol. *IEEE Infocom, 2006*
- D. Fabrice. Skype uncovered, 2005. http://www.ossir.org/windows/supports/listewindows- 2005.shtml.

Analysis and signature of skype voip session traffic

At least One ☺