Skype

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

ENDS reading group, 12/03/07

Stephen Strowes

Purpose of paper

- Analysis of widely used p2p application, Skype
  - The paper presents some information gleaned from packet traces
    - How often does Skype write home…?
- Paper focuses on functions required for PC-to-PC calls
  - login, user/buddy lookup, call establishment & teardown
  - brief look at call conferencing

Brief background...

- VoIP: conceptually simple...
- Certain barriers to easy deployment:
  - Centralisation (costly)
  - User location
  - NAT boxes & firewalls
  - Conferencing

Methodology

- Authors performed analyses using different versions of Skype over different operating systems to track its behaviour
  - Packet traces
  - Shared library and system call interception
  - Experiments using different network setups
    - No NAT
    - 1 machine behind NAT
    - 2 machines behind NAT & UDP-restricted firewall

Skype

- Skype doesn't make analysis easy
  - Closed source, no information released about protocols from parent companies
  - Packet contents are encrypted end-to-end
    - Can follow where some packets go, but can't easily see the contents
  - The binary is encrypted
    - And employs fairly smart techniques to try and stop people from figuring out more information at runtime...

Skype

- Super nodes vs. ordinary Skype clients
  - Any client can become a super node, given a public IP and enough network bandwidth, cpu time, etc
    - University machines can make great super nodes :-)
- Nodes use TCP for signalling, UDP or TCP for data, depending on network

Skype: NAT/Firewall traversal

- Variation of the STUN (RFC3489) protocol?
- No global server to traverse NAT and firewall; clients use super nodes
- Skype nodes do behave very differently in almost all interactions depending on their public network connectivity
  - In essence, greater restrictions == greater reliance on super nodes

Skype: User Lookup

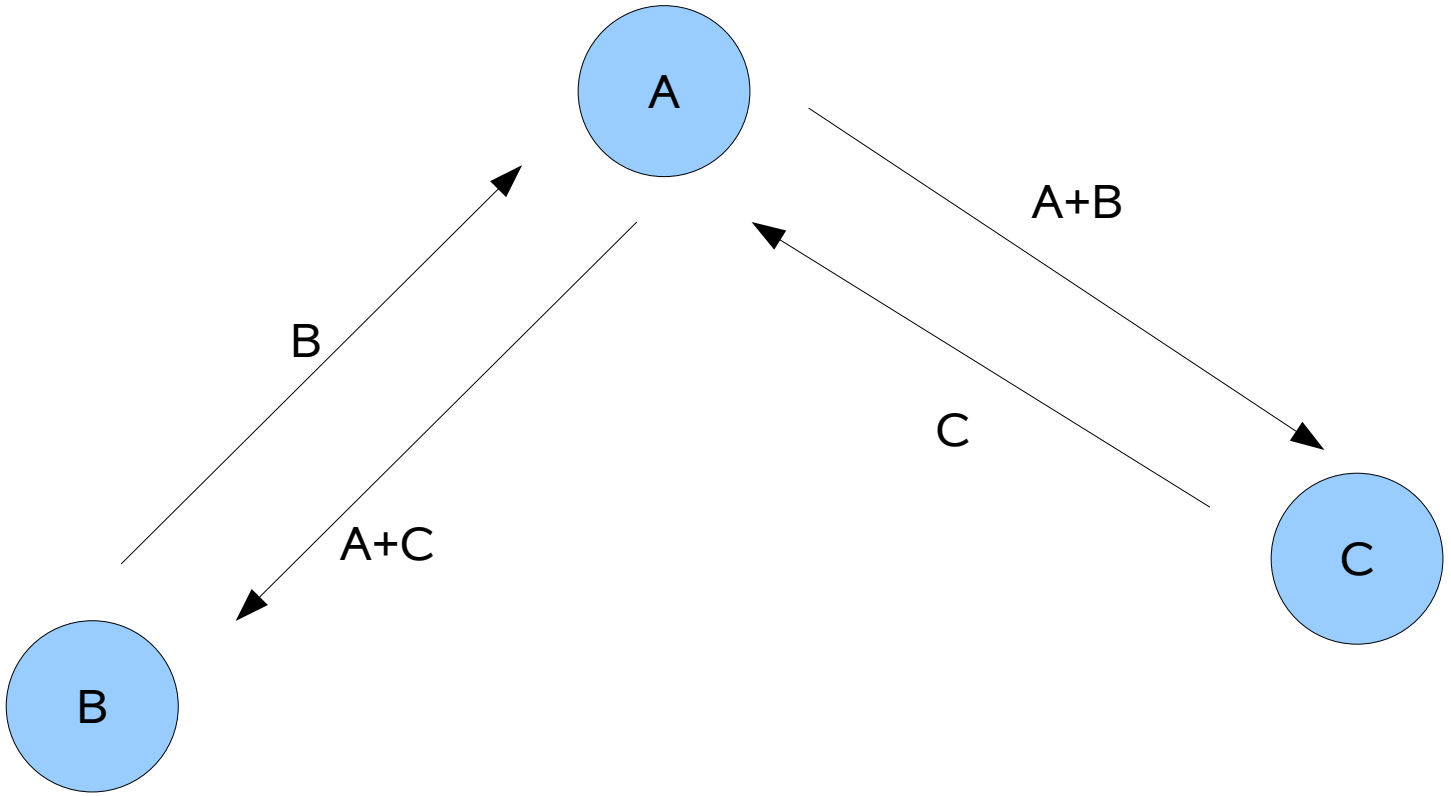
- Skype seems to use some sort of distributed hash function to locate users
  - Client/super node queries 8 clients, then 16, etc, until the user is found or declared to have not existed (within the last 72 hours)
- Actual algorithm used is unclear...

Skype: Data transfer

- Call data passes directly between hosts over UDP if possible
  - If not, then via a super node over UDP
  - If that's not possible, then via a super node over TCP...

Skype: Conferencing

- Paper spends a little time on conferencing
  - (not enough)



Skype: Slightly surprising

- Doesn't use silence suppression
  - Why not?
    - Maintains UDP bindings at NAT, or maintains a TCP flow

References

- There's a bunch of stuff on Skype out there

[1] An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol, Salman A. Baset and Henning Schulzrinne, IEEE Infocom 2006

[2] “Silver Needle in the Skype”, Philippe BIONDI and Fabrice DESCLAUX, Black Hat Europe 2006

[3] “An Experimental Study of the Skype Peer-to-Peer VoIP System”, Saikat Guha, Neil Daswani and Ravi Jain, IPTPS 2006