Skype

Skype is an amazing cross-platform application that averages a whopping 30 million concurrent users. It allows communication between users through video chat, voice over IP, as well as messaging. Though the application has been around for nearly a decade it is now just hitting its stride over the last year. In 2012 over 70 million Android users's downloaded the application and later that year Skype would hit its all time high of 36 million simultaneous users running the application. Skype has needed to take great precautions in its security as well as its server hardware in order to keep up with such a jaw-droopingly large user base. The technology behind Skype does exactly this in a most impressive way.

Tech

Skype networks its operations in a variation of the peer-to-peer format. In its most basic form peer-to-peer is a network design that deviates from the normal user to host format (which requires a sturdy server to host the traffic) by making every connected user a host. So instead of downloading a file from a central server a user will download bits of the file from a handful of other users that have the requested data. In the past Skype twisted this format by designating certain users "Super Nodes". These would normally be users on huge pipes such as universities. This process has now been removed from Skype in favor for their own Linux-based servers to act as the Super Nodes. Microsoft (who purchased Skype in 2011 for $8 billion) backed up this change by saying it allowed them to have more control over Skype's system as a whole.

The transport protocol underlying Skype is referred to as, simply, Skype protocol. This was designed specifically for Skype and is not open source. Though the basic steps of the protocol are known and are as follows.

1. The user logs into the Skype network and a TCP handshake between the two establishes the connection.
2. The user's login data is confirmed at one of the various Skype servers.
3. Skype initializes the users private, public, and session keys (detailed below in the security section)
4. Two users are connected via a super node on the network .The keys from step 3 ensure validity of the two users.
5. The Skype video/audio stream is handled using UDP. Any other form of communication is handled by TCP.

Security

Skype encodes any transferred data on its network using primitive encryption techniques that are still highly effective. These primitives include the AES block cipher, the RSA public-key cryptosystem, the ISO 9796-2 signature padding scheme, the SHA-1 hash function, and the RC4 stream cipher.

The encryption process as a whole follows (all Greek for any non-tech security savvy readers)
On each login session, Skype generates a session key from 192 random bits which is then encrypted with the login server's RSA key to form an encrypted session key. Skype also generates a 1024-bit private and public RSA key pair. An MD5 hash of the constant string, username, and password is used as a shared

secret with the login server. The session key is used to encrypt the session's shared secret and the public RSA key. These keys are sent to the login server.

On the login server side, the plain session key is obtained by decrypting the session key using the login server's private RSA key. The plain session key is then used to decrypt the session's public RSA key and the shared secret. The login server will sign the user's public RSA key with its private key upon the match of the shared secret. Finally the signed data is dispatched to the super nodes. The mentioned RSA key is used to create a session key once two users begin a session. All traffic during a session is encrypted by XORing the plaintext with key stream generated by 256-bit AES (also known as Rijndael).

Overall Skype is an amazing feat of network design. Its ability to scale according to its user base while still maintaining the sheer amount of traffic is inspiring. The people behind Skype are some of the best minds in the industry.

References

Berson, Tom. "Skype Security Evaluation." N.p., n.d. Web.
"How Does Skype Technology Work?" Small Business. N.p., n.d. Web. 18 Feb. 2013.
"Skype's Network Ditches P2P Tech for Linux Boxes." Tom's Hardware. N.p., n.d. Web. 18 Feb. 2013.
"Protecting Your Online Safety, Security and Privacy." Skype Security. N.p., n.d. Web. 18 Feb. 2013.