

Skype Steganography

Thomas Paul Carlson

August 17, 2007

1 Intro

So. I was thinking. Skype is a global Voip client with encryption, firewall breakingness / avoidance and is generally a rather neat little bit of software. Recently some unscrupulous ISPs have worked on cracking down on skype traffic so they can offer their own voip service which, conveniently enough, just works. This little lump of text describes hiding messages inside of a skype stream and a few ways this might be accomplished. Disclaimer: I'm not a cryptographer and do not know a great deal about cryptosystems and those that work to crack them. What I say may well be total rubbish :-).

2 The Premise

People paranoid about security are likely to use some form of encryption to shift around their data, often using public key security like that found in ssh (And scp). But what if you were to let Skype handle the crypto for you and hide messages in the audio stream? Anyone listening in on your Skype conversation (Which would in itself be quite a feat - 2048 bit RSA for AES key exchange and 256 bit AES encryption for the call itself) will just hear you and a friend talking away as normal. So hiding something else inside of this already heavily encrypted stream sounds like a fairly good plan.

3 How?

As far as I can make out, there are a couple of ways this could be done. Firstly, you could record samples of your voice and modify those to include data translated into sound somehow and included in a low frequency part of the spectrum. To an eavesdropper, the noise could just look like noise on your microphone. Fairly obviously, some amount of care would be needed to take out low noises from your mic and replace with data so a low pass filter (For example a cutoff at 60hz) could be employed. The data rate on this would be pretty low. The audio codec used by skype allows for frequencies between 50hz and 8khz, unsure of the sample rate (Possibly 16khz). Either way, the data rate here is going to be

fairly low. Consider that Skype itself will use either very small or rather large amount of bandwidth dependent on the quality of the line. Also remember that the Skype audio codec allows for massive packet loss along the way - some way of signaling between sender and receiver of secret hidden data would be needed.

The second way of hiding messages in Skype conversations might be to modify the raw bitstream that skype is transmitting. This is probably next to impossible. I assume that Skype keeps the AES key used to encrypt conversations somewhere, whether it be resident in memory or stored in the windows registry, /tmp on linux or anywhere really. The basic idea would be to intercept the outgoing communication, decrypt this bit of the stream, flip a few bits and encode a message without totally breaking the audio, re-encrypt the stream, transmit across the internet. On the other end, a similar process would be used. Something to intercept packets headed for skype and decrypt the stream, retrieve the message (Hopefully intact!), re-encrypt and pass on to Skype.

4 Why?

Why on earth would you want to do this?! What kind of lunatic would want this kind of craziness? Skype already includes an instant messaging service which is encrypted. However skype is closed-source, proprietary and nobody really knows what is going on under the hood...although it seems lots of smart people have analysed it thoroughly. With the advent of skype video, higher bandwidth is available for larger (hidden) transmissions. You could tunnel ssh over skype over an ssh tunnel over TOR for total lunacy. Or do an exchange of one-time pads hidden in a skype conversation, followed by further exchanges of actual messages. The possibilities are only limited by how twisted you think!

5 End Stuff

This is all crazy ramblings. It is 2am and I am tired. I have no idea how well if at all any of the stuff I described would work. I expect badly. I sleep now.