Skype – gaping security hole or wünderapp?

By Randolph Osterroht

Ok, so what do we know about this p2p, voice application?

- We do know that it's letting users around the world (well, SOME parts of the world anyway) make local AND international calls at one HELLUVA reduced rate (thereby taking business away from and annoying bloated telecoms companies)
- It uses peer-to-peer technologies to allow connections based on Kazaa (the creators of skype are Niklas Zennström and Janus Friis, none other than the boys responsible for Kazaa and Joost).
- Call encryptions, when established use strong encryption, making listening in on conversations almost impossible (thereby irritating certain governments)
- By using it's own protocol and peer-to-peer technologies, it circumvents many firewalling and NAT issues (thereby irritating many security conscious sysadmins)

With about 170 million users (and growing) skype has come under fire lately from many sysadmins claiming that because they cannot effectively block or monitor the traffic, that it may be one HUGE security hole. Skype runs on its own proprietary protocol, the code for which, is jealously guarded by its creators. Attempts to reverse engineer this protocol have so far proved fruitless. Reverse engineering the program is also proving to be problematic. The skype executable refuses to load if certain debugging programs are running in the background. Some programmers believe that the executable itself is suspicious at a whopping size of 12Mb *what else is in there??*

In a nutshell, the skype network is made up of a number of nodes and supernodes, because of the nature of peer-to-peer, the only "centralized" servers are the login authentication servers which are hardcoded into skype and hidden in the code. Once a user is logged in, skype will look for skype "supernodes" a supernode is ANY skype user that has good bandwidth and is not sitting behind a firewall. From this supernode, he will receive the list of peers and can become part of the skype network.

Skype's protocol is proprietary and jealously guarded, all traffic is encrypted using at least 128-bit encryption using RC4 method, server login is encrypted at 256-bits with an MD5 hash check added to the username, random node checks using 64-bit encryption, so, this is all good and well, but… what's in the traffic exactly? If an exploit is found, what could stop skype's infected p2p traffic? Would we end up with a net that looked like kazaa in it's later days? Like taking a walk in the dark woods?

The Darkside…

If one takes a close look at the Skype EULA (end user license agreement) take note of section 2.4 which states:
"You acknowledge and agree that the Skype Software may be incorporated into, and may incorporate itself, software and other technology owned and controlled by third parties."

Why does skype want to run other companies software on your system? Shouldn't skype be enough? The likely scenario is that skype is referring to codecs and technologies not owned by skype, but… who knows. No one can really know what is going on until the code is cracked. Will skype make the program open source? Not so according to it's founder, Niklas Zennström, who claims they simply don't have the time.

Section 4.1 states:
"You hereby acknowledge that the Skype Software may utilize the processor and bandwidth of the computer"

By its peer to peer nature, skype uses your bandwidth to facilitate communications between other skype users. By as much as 5Kb for normal nodes (normal users) and up to 10Kb for supernodes. Imagine this… you are the sysadmin of a company. You have users that run skype. Perhaps three of them might be normal nodes, and one of them is a supernode. This could mean a possible 25Kb of your bandwidth out the window.

The good, the bad and the downright nasty

So, is this program all bad? I must admit, that before I took a deep look into this program, I was vehemently anti-skype due to its subversive nature, but… let me step back a moment and take a look at the bigger picture here. Skype is offering a viable alternative for low-cost local and international calls forcing fat cat telecoms companies from around the world to reduce prices. That is indeed its biggest calling card to users in third world countries where the cost of using the traditional high cost old technology. For the business-cost savvy, skype offers many options for reducing cost of calls, for example, the skypein feature, allows a user to create a telephone number in Helsinki that will ring on a skype device in Tokyo, the Helsinki landline caller only paying local telephone rates. Skype also offers a voicemail feature, ideal for having an answering machine follow you around the world (or wherever internet access is available).

Halt! Spy!

So, why would any sysadmin, of sane mind and body even DARE run this application that sits behind your firewall, can figure out a way of getting PAST your firewall (it can connect through port 80 or 443, what corporate firewall today does not allow these out?) AND has HEAVILY encrypted its traffic so that we have no way of knowing what’s coming into or going out of our corporation? I certainly would not have my network running such an app, especially one that uses p2p as the backbone of its technology. There are many apps out there that can duplicate skype’s functions such as Google talk and msn messenger that has long ago had voice capabilities built in. heck, msn messenger even has video facilities built in! Most other voice over IP programs run with a server-client model that a sysadmin can track and keep an eye on, and I like keep an eye on. It lets me sleep at night.

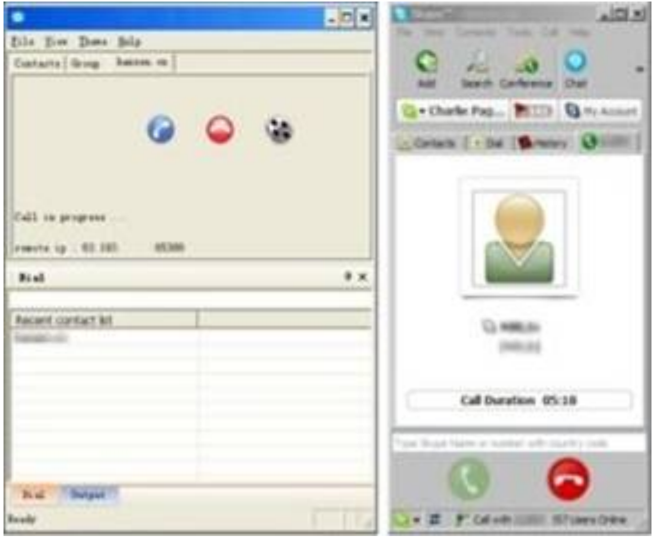
Although skype is a great app for what it is, at the end of the day, it’s just not worth the risk running such a subversive app on your network, and as in any I.T. problem, there is always more than one way to skin a cat. There are other apps out there, USE THEM, be AWARE, that's all for now folks!

--UPDATE--

According to sources, a Chinese info-tech company has cracked skype.

I'm not in the know if they are doing this for fun or financial, (most likely financial) but, there it is, someone has gotten past skype's MASSIVE encryption. This could possibly mean free telephone calls on the skype network, and I'd love to see skype techs try pick out this foreign traffic from their legitimate traffic, hahaha. But most likely, this company will collaborate with skype and the Chinese government and sell this serivce as a controlled service (i.e. No political naughtyness!). From what I hear as well, it can do IP address resolution regardless of what firewall you are sitting behind, so you can be tracked down if you are being politically naughty.

Screenshot of the hack skype version vs. Legitimate skype.



As far as I know. This software is not yet out.