Skype tells surveillance alarm-raisers they got it all wrong

July 30 2012, by Nancy Owano

(Phys.org) -- Skype, the famous and widely used voice-over-Internet protocol service and software application that in 2011 became Microsoft's online message, phone and video chat service, is fighting off assumptions and reports that its parent Microsoft has made it loosen up and roll out a welcome mat to law enforcement for surveillance purposes. Skype has issued flat denials that it has changed its policy about outside surveillance of users' Skype communications. Skype insists that any technical upgrades to its system have not been with surveillance in mind.

The reports have suggested that Skype infrastructure upgrades may make it easier to hand over users' chat data to eager legal agencies wanting access to conversations over the Skype service. The reports were largely

based on a recent addition of supernodes in the data centers of Skype's new corporate parent, Microsoft. Skype moved its supernodes into Microsoft's data centers for the purpose of reliability, not to please legal surveillance agents, assured the company in its statements.

Earlier this month, Mark Gillett, Skype's corporate vice president of product engineering and operations, described all claims that Skype was bending its policy rules as false. In contact with ExtremeTech, Gillett said any changes in infrastructure were to improve user experiences.

"As part of our ongoing commitment to continually improve the Skype user experience, we developed supernodes which can be located on dedicated servers within secure datacenters. This has not changed the underlying nature of Skype's peer-to-peer (P2P) architecture, in which supernodes simply allow users to find one another (calls do not pass through supernodes). We believe this approach has immediate performance, scalability and availability benefits for the hundreds of millions of users that make up the Skype community."

More recently, he decided to pen a detailed explanation of what Skype has done and why on Skype's own, The Big Blog. He was concerned that reports could mislead the Skype community about how Skype handles user security and privacy.

"It has been suggested that Skype made changes in its architecture at the behest of Microsoft in order to provide law enforcement with greater access to our users' communications," he said, which he repeated as false.

Regarding the supernodes, he said that even before Microsoft came into the picture for acquisition of Skype, the latter was already in the process of moving supernodes to cloud servers.

“Skype first deployed 'mega-supernodes' to the cloud to improve reliability of the Skype software and service in December 2010,” he said. The nodes were deployed at Skype's data centers, in third-party infrastructure such as Amazon's EC2, and most recently in Microsoft's data-centers and cloud.

The move was made to improve platform reliability and “to increase the speed with which we can react to problems,” he added.

Gillett said reports of changes to facilitate law enforcement’s access to instant messages were false too. He acknowledged that some messages are stored temporarily on Skype/Microsoft servers for immediate or later delivery to a user, “to provide for the delivery and synchronization of instant messages across multiple devices, and in order to manage the delivery of messages between clients situated behind some firewalls which prevent direct connections between clients.”

Skype does make an exception to cooperate with law enforcement, he said, “if a law enforcement entity follows the appropriate procedures and we are asked to access messages stored temporarily on our servers,” and he said that will happen “only if legally required and technically feasible.”

Meanwhile, the China-only version of Skype remains a glaring exception to privacy. The China-only version is provided locally through Skype’s joint venture partner operating “tom.com” which contains a “chat filter” in order to comply with local laws.

The Chinese government monitors communications in and out of the country. TOM Online, like other communications service providers in China has an obligation to comply in order to operate in China.

Skype traditionally has been credited with its use of strong encryption

and complex peer-to-peer network connections as a safeguard against interceptions.

What fed on recent alarm and speculation were reflections on the supernode move in the light of how Microsoft had filed in 2009, before the acquisition of Skype, an application to the U.S. Patent and Trademark Office, which was later published in 2011, describing "recording agents" to legally intercept VoIP phone calls.

Microsoft's application noted that "Sometimes, a government or one of its agencies may need to monitor communications between telephone users. To do this with POTS, after obtaining the appropriate legal permission, a recording device may be placed at a central office associated with a selected telephone number. Electrical signals corresponding to sound to and from the telephones at the selected telephone number may be monitored and transformed into sound. This sound may then be recorded by the recording device without the telephone users being aware of the recording. With new Voice over Internet Protocol (VoIP) and other communication technology, the POTS model for recording communications does not work." This "Legal Intercept" patent application discussed an idea for how communications on VoIP networks can be silently recorded.

Skype serves 250 million active users each month and supported 115 billion minutes of person to person live communications in the last quarter alone, according to numbers cited by Gillett on the Skype blog.