skype Tips.com

Five Reasons, OK six, NOT to block Skype

By Michael Gough Updated June 2006

Being a computer security consultant I am always amazed when I read articles like the one I recently found in an Australian paper on blocking Skype. The firm **Info-Tech Research Group** in Canada cites in their report "Five Reason's To Ban Skype"

- **Nov 8, 2005 -** www.infotech.com **(see main points at the end of this article)**

claiming that the popular VoIP technology is just too insecure for business use. These blanket statements are grossly inaccurate as each business is different and has the responsibility to set their own policy to match their specific need. Many very intelligent Fortune 500 companies use and approved Skype for internal and external use.

First and foremost a company should create a policy for any and all new technologies that ban their use until they are specifically allowed, this should be the policy for most organizations that try to manage, control and secure their IT resources. So from this perspective, Info-Tech is correct, Skype should be treated like any other IM product which many companies allow, but do have policies that state "Not for company sensitive business use". This means chatting is fine, discussing mergers is not. Most of us know the difference. Info-Tech estimates that roughly one-third of Skype's 53 million registered users are business users. Gartner also came out again and warned of Skype's use, but mostly as a warning to use configuration management and understand your risk which any good security practitioner should already be doing.

So here are my six reasons NOT to block Skype…

#1 **–** Skype does not use either of the two most popular VoIP standards, H.323 or SIP. This is because Skype was not designed to interact with these systems so there is no need. If there is, gateways can be used (like Uplink Skype2SIP) to connect the two systems together as several vendors are now developing. SIP has been known in the past to have many security issues and no solution is "totally secure", especially SIP. To think Skype is or should be goes against that no application is 100% secure and that includes H.323 and SIP which have had many vulnerabilities over the years and you do not see companies banning these devices, VoIP based on SIP is being adopted at a very fast rate. If you want to see how insecure your VoIP solution is, just download either VOMIT or VoiPong and run it against a SIP or H.323 system, with approval of your Information Security manager of course. You will find you can record anyone's voice call without permission if you have access to the voice data network that the IP phones reside on. I saw a presentation a few years ago by Ofir Arkin on VoIP security and he demonstrated how insecure SIP could be, so do not begin to think SIP or H.323 are any more or less secure than Skype – they are just different. Skype was not designed to be the corporate IP telephone infrastructure, SIP and H.323 were, so Info-Tech is comparing Apples to Oranges.

Skype is incredibly firewall friendly, but there are ways to block the use of Skype, both from a commercial appliance perspective as BlueCoat and Verso claim to do and in fact China has purchased Verso appliances to block Skype. You can also use your software inventory or asset management solutions or just write a script that goes out on your network, discovers any Skype clients and whose system they reside and disable or delete Skype as needed. If you do not know how, let me know, and you can hire me to show you. Info-Tech's blanket statement by creating "FUD", Fear Uncertainty and Doubt about Skype to block it in the enterprise is unwarranted.

#2 **–** The recently announced Buffer overflow vulnerabilities and URI vulnerability found by Auzzie Secuirty-Assessment.com:

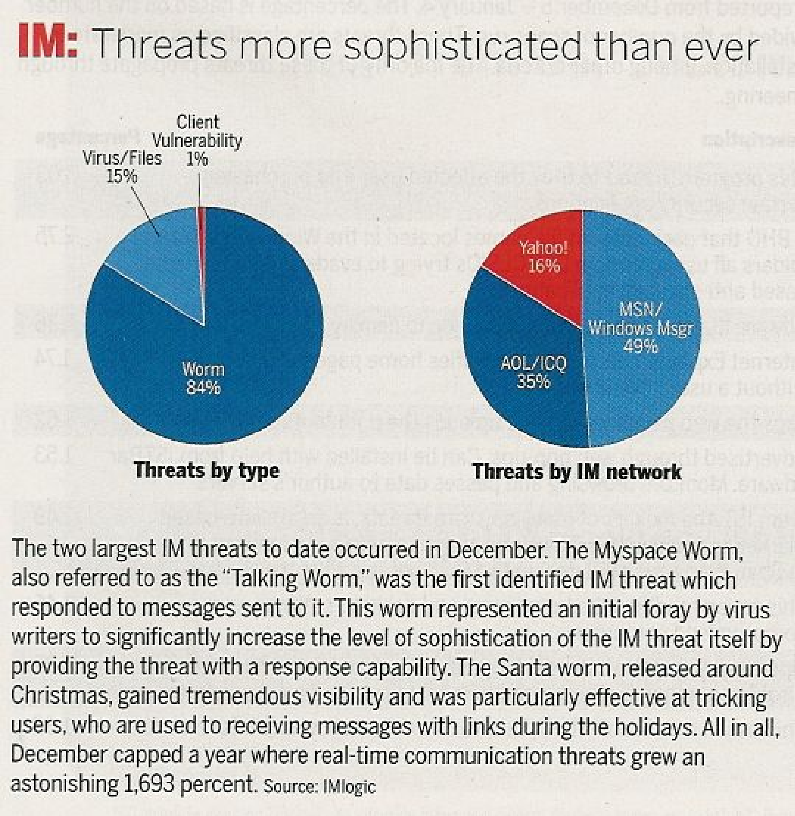
- www.security-assessment.com/Advisories/Skype_URI_Handling_Vulnerability.pdf

are no different than any application and that includes the Windows operating system that inherently runs on 90% plus of the systems in worldwide enterprises. This logic with all the worms, damage and financial loses companies have already suffered, they should also ban the Microsoft Windows operating system as a viable option, clearly a much higher risk to organizations than Skype's vulnerabilities which were identified and patched just as any application vendor does. You could between the time a vulnerability is announced to the time it is patched, do exactly what I suggested in #1, scan your network and disable Skype until it has been updated, simple and easy. Also Info-Tech did not seem to acknowledge the 'Skype Security Evaluation" whitepaper Skype released by Tom Berson of Anagram Laboratories in October 2005 :

- www.skype.com/security/files/2005-031%20security%20evaluation.pdf

that discusses most of the security aspects of Skype and answers many concerns IT security professionals would have. Also as in any software, bugs are inherent and unavoidable that is why we recommend to practice 'defense in depth' to avoid the risks associated with any and all applications and especially the operating system they run on. Worms do not need Skype, they do just fine on the Windows operating system alone. Info-Tech's logic applies to a corporate VPN as well that is used to secure a connection between home and work for example. Worms have been seen and proven to pass through this encrypted channel and I do not see Info-Tech warning anyone of this threat. It all comes down to 'defense in depth' and protecting the asset that runs any operating system and any and all applications running on each asset.

With hardware devices in the home, like a Cable/DSL router and firewall and anti-virus software on the mobile systems, a client is fairly secure from worms. Might I also point out that Microsoft is the leader in IM with over 250 million users, far more than Skype and also has voice capability, it is just not as flexible or good as Skype and I do not see Into-Tech warning anyone about this application that is used far more worldwide than Skype. They did say "should be treated like any other IM product" and they are correct in this statement. Treat Skype as you would AIM, YIM, MSN or any other IM product. Here is a recent fact from the December 2005 Secure Computing Magazine on IM vulnerabilities:



IM: Threats more sophisticated than ever

The two largest IM threats to date occurred in December. The Myspace Worm, also referred to as the "Talking Worm," was the first identified IM threat which responded to messages sent to it. This worm represented an initial foray by virus writers to significantly increase the level of sophistication of the IM threat itself by providing the threat with a response capability. The Santa worm, released around Christmas, gained tremendous visibility and was particularly effective at tricking users, who are used to receiving messages with links during the holidays. All in all, December capped a year where real-time communication threats grew an astonishing 1,693 percent. Source: IMlogic

Notice Skype is not even on the chart as of December 2005, but know the threats and attacks are basically the same.

#3 **–** Yes, companies and countries have blocked Skype, some for fear of economic damage to their telco industry as China has done. British Telecom specifically lowered their long distance fees to match or beat those of Skype due to this economic threat. Others block it to avoid file sharing that leads to lawsuits and sharing of copyrighted material. Company policy should dictate how to treat applications that can transfer files and that includes Email, Web based email and Web surfing which many companies allow. There is nothing Skype can do that Web based email can do for example as far as files. They are both encrypted channels, Web email over HTTPS or SSL and Skype with AES, so there is no difference. Company policy should dictate what to do and anti-virus solutions today that are received with Skype using the 'auto-protect' capability that scans all files as they are saved. Companies have the same issue with copyrighted or inappropriate material that can be transferred over Skype or any IM product that they do over Email , Web based email or Web browsing and downloads. Skype does not increase this risk at all. Set a company policy on all file transfers and how the company will look for any and all inappropriate materials on all company systems regardless of how they get there, the rules and actions are the same. Did I point out you can disable the File Transfer capability of Skype making it less of a risk that email or Web surfing?

- HKLM\SOFTWARE\Policies\SkypePhone\"DisableFileTransfer"=dword:00000001
- For Windows version 2.0 and later

Setting the DisableApi key to 1 will completely disable the Skype public API interface.

- HKLM\SOFTWARE\Policies\Skype\Phone\"DisableApi"=dword:00000001
- For Windows version 2.0 and later

This could be helpful when enforcing an enterprise policy concerning the use of software plug-in modules. Setting the DisableFileTransfer key to 1 will disable file transfer. In this case, inbound file transfers will be automatically rejected (the remote user will see a "Cancelled" message) and outbound file transfers will cause a messagebox to pop up containing an error message. (At present, these controls are available only on Skype for Windows.)

***#4* –** Yes, some companies that do trading of stock for example have a requirement in the United States by the SEC and OCC to monitor all transactions of these individuals to avoid any insider trading and issues as Martha Stewart are all too familiar with. These institutions also ban Web based email, scan and monitor email and approved IM solutions and yes, can even can monitor internal telephone calls. There are some organizations with these requirements that should ban and control any and all communication as a part of their jobs, but these companies are in the minority and not the norm. Also the users of these companies would just go outside and use their cell phone with text messaging to conduct this sort of risky business and businesses are not required to monitor cell phone or text messaging. So what applies to these companies does not apply to 90% of all companies. Did I mention that there are recording solutions that can record Skype calls?

***#5* –** If the regulatory people, of which Info-Tech forgot to mention CALEA can not decide what to do about all of the solutions, then how are companies suppose to cope with this? Again, a company should set a communication policy of what to use and when so that an employee uses the correct communication device for the correct communiqué. New solutions are being developed all the time and just because it is new does not mean it should not be considered. A company should have a new technologies policy that states “any and all technologies are banned until a policy is created on the proper use of these technologies”. Then determine the proper use and allow the technology and monitor its use.

Another concern that The Butler Group says that Info-Tech missed, a key reason for corporations not to use Skype – the hijacking of bandwidth. That issue is the Supernode technology inside of Skype that was specifically designed to let Skype punch through network address translation (NAT) and firewalls.

***#6* –** The Butler Group is incorrect in this statement as a general statement. This should be little to no concern to a business that uses an enterprise firewall device like a Cisco PIX, NetScreen, CheckPoint or other true firewall. Home users that have a Cable/DSL router or any business that uses a NAT or firewall product cannot become a Supernode. Only systems that are open on the Internet with a true routable IP address, the Skype client loaded and has enough CPU, memory and storage can become Supernodes and most if not all corporate enterprises worldwide use these types of devices and so losing bandwidth to a Supernode is a non-issue. If a company sees this behavior, then they are misconfigured and have bigger issues than Skype. This is something you should verify, but in reality should not find. Just check your CPU utilization with the Windows Task Manager and network bandwidth utilization with a tool like NetPeeker to see what Skype is using. It should be obvious if you are acting as a Skype Supernode.

In summary, you cannot apply the same logic for a company that has strong policies or regulatory requirements to control communication to every company. Each company is different and should set a policy, evaluate the advantages, support, risks and costs to decide how to if at all to apply a communication tool like Skype. Do not take Info-Tech's or The Butler Group's recommendation as absolute fact as it does not apply to 90% of you our there. If you properly secure your clients and infrastructure with 'defense in depth', the risk of using Skype is far less that using Microsoft Windows or laptops without encryption.

The Gartner Group just came out with a report due to the latest URI vulnerability from May 2006:

- www.gartner.com/DisplayDocument?doc_cd=140991

Again, a generic statement does not apply to all companies. Yes, Skype has and will have vulnerabilities like any other application, but it should not stop you from considering if Skype as a softphone is a good fit for your company and needs. I feel Skype is only getting the attention because it is Skype and not because it is truly causing issues in companies by worms and infestation. Remember that Skype has yet to be exploited like the other IM tools or Windows itself and thus far is safer than most applications being heavily used today.

Lawrence Orans is correct in saying that Skype, like any other application on a Security experts radar should be managed and controlled with whatever technologies and options available to a company and to use your configuration management solution like SMS, Radia, Tivoli, etc. will easily take care of this issue, or of course well crafted batch files and login scripts like I have used in the past.

Companies unable to manage their clients have a far larger issue than Skype. I tell my clients if you cannot look for something on your network and find it and invoke a change within an hour, you have far larger problems than Skype. Your number one concern should be to figure out how to and actually manage your clients. If you can do this, then Skype is of little concern if you just watch the alerts and take appropriate action.

May 2006 Gartner Report:

A recent bug in Skype, discovered by Australia security research outfit Security-Assessment has prompted industry analyst firm Gartner to speak out against the peer-2-peer (p2P) software once more.

In an online research note, Gartner analyst Lawrence Orans said corporates need to “Act Now to Combat the Growing Skype Security Threat”.

He wrote that the 19 May security issue was tagged as "medium risk" by the broadband phone provider. It was recommended that users and customers to upgrade to the most recent version of the softphone client to fix the problem. The vulnerability notice notes that a flaw in the software would allow an attacker to transfer a single, named file from a victim’s PC.

However, the victim must first be tricked into visiting a malicious Web site under control of the attacker, and the attacker must know the location of the requested file on the victim’s machine.But Orans correctly notes that this follows three vulnerabilities discovered last year two of which were classified as high-risk (one was rated only as low-risk).

Orans says that the string of vulnerabilities “highlights the risk of not establishing and implementing an enterprise policy for Skype. Although the VoIP software has become very popular amongst users, some network security administrators are more cautious about the free IP Telephony software.

“Because the Skype client is a free download, it is widely used and most businesses have no idea how many Skype clients are installed on their systems or how much Skype traffic passes over their networks,” he wrote.In part Orans’ problem with Skype was the handling of the issue.

When users with a vulnerable client sign on to Skype, they receive a prompt suggesting they upgrade to the most recent version, but are not warned about the vulnerability or the associated risks, he notes saying that they are still allowed to access the service even though they have a vulnerable client.“

In contrast, Microsoft immediately restricted access to its MSN Messenger instant messaging (IM) service in 2005 when it discovered a vulnerability in its IM client.

Only users with an updated and non-vulnerable client were allowed to access the service, which meant Microsoft essentially performed the vulnerability management process on behalf of businesses.“

Skype provides no such protection”, he wrote.

Among the list of Skype’s dangers according to Info-Tech are:

1. It’s too firewall-friendly. Skype's proprietary closed-source VoIP protocol - which does not employ accepted VoIP standards like H.323 and Session Initiation Protocol (SIP) - allows it to traverse corporate firewalls and symmetric NATs. An unknown and unsanctioned VoIP protocol freely roaming the network - without IT's approval or assessment - poses an unacceptable transgression of IT's authority over the corporate network and computing resources.

2. It has too many vulnerabilities. Buffer overflow vulnerabilities are known to exist in Skype. And since Skype travels the network as data packets, conversations are prone to capture. Problems also exist with Skype's encryption format: First, it doesn’t prevent a man in the middle attack and secondly, if it becomes infected with a worm (which it one day will), the worm could hide in the encryption during transmission, undetected by anti-virus software. Because the encryption is closed source, there are some unanswered questions about how well the keys are managed. Finally, Skype recently announced that all of its VoIP clients – including Windows, Linux, Mac OS X, and Pocket PC – suffer from bugs that leave PCs prone to crashes and open computers to takeover by a hacker.

3. It poses a communication barrier with other countries or institutions. Countries like China and Oman have banned Skype already, as has the rest of the United Arab Emirates. Many post-secondary institutions in North America have banned Skype as well, in addition to most other P2P and file sharing applications.

4. It violates established legal requirements. For example, securities brokers operate under a mandatory requirement to record and track all telephone calls. Unsanctioned usage of an application like Skype would put a brokerage at severe risk of prosecution if caught using telephony that is undetectable, untraceable, and un-auditable.

5. It's one more type of communication to secure, monitor, store, and archive. Enterprises are already struggling with records retention rules imposed by HIPAA, Sarbanes-Oxley, and other laws. In addition, the question of whether VoIP calls constitute a business record or not is a legal quagmire in and of itself. Throwing Skype into the communications mix will only further cloud the issue.