Is Skype Secure?

What You Need to Consider
Before Using Skype in Your Business

9-19-2011
Kenneth G Hartman
www.KennethGHartman.com

Contents

Background

Skype offers a free solution to communicate via instant message, voice and video with anyone, virtually anywhere in the world. The Skype website boasts that it has more than 145 million connected users per month [1]. In May of 2011, Microsoft announced that it was buying Skype. Overshadowing all of the great functionality, potential, and media buzz are lingering questions regarding the security of Skype.

Businesses face pressure to allow their customers, clients, vendors, and staff to communicate with each other via Skype and other social media tools. This has many business decision makers grappling with questions regarding what to do about Skype. This is good. Each business need to make a decision for itself regarding Skype, based on the information security needs of that business. Ignoring the issue or failing to make a decision is not leadership.

This article will facilitate your decision making process by demonstrating the application of security management fundamentals and will allow you, as the decision maker to feel at ease with the decision you make. The article is written in two sections. The first section presents a decision making framework,[1] while the second part of the article will provide important security considerations and resources that can be used as inputs to the decision.

A Decision & Management Framework

1. Understand What You Are Protecting

We are all familiar with the concept of governments protecting their “Top Secret” information thanks to many fascinating spy stories in the entertainment media. The US Federal Government actually uses different levels of classification based on the damage that leakage of the information would cause to national security. This classification is called ***Labeling***, and it is done because higher levels of sensitivity require more effort to safeguard.

While most private businesses do not handle classified government information, they do have secrets to protect. Secrets create competitive advantage and come in two general forms—*intellectual property* and *personally identifiable information.* Mature, well-managed businesses label their sensitive information, and have formal programs to appropriately protect it. These organizations also know which information systems contain their secrets. All businesses are different, so it certainly makes sense that different businesses will make different decisions—and that includes the position that they take on the business uses of Skype.

2. Understand the Risks

We all long for binary decisions, such as yes/no and right/wrong. And unfortunately, the answer to “is Skype secure?” is *it depends.* Perhaps a better question is, “under what conditions can I accept the risks

[1] There are a variety of formal frameworks, such as the NIST Risk Management Framework and the ITIL Security Management Process. Our purpose here is not to prescribe a formal model but to discuss how application of the security fundamentals common to all models yields the correct decision for the business.

that Skype introduces to the information that we protect?" A proper answer to this question, implies that the risks are understood. The formal mechanism for this is a ***Risk Assessment***, which is performed by a technically competent individual that has an appropriate understanding of the operating environment of the business. Risk Assessment is an important component for all change management. Once a risk assessment is performed, management can either:

- accept the risk,
- transfer the risk (such as via an insurance policy), or
- reduce the risk to an acceptable level.

The majority of businesses that have a compelling business need to use Skype will choose to reduce the risk to an acceptable level. Risk mitigation solutions emerge once the risks are identified, understood and ranked. The second section of this document suggests various topics that should be considered in a Skype risk assessment.

3. Take a Position

After considering the organization's secrets and fully understanding the risks as well as how those risks can be reduced to an acceptable level, management must articulate its decision. This is typically done via a written policy. ***Security policies*** document the specific requirements and rules that must be met by the organization's members for a given system or process to be considered secure. Clear policies enable the staff of the organization to understand what the organization expects and should reflect the organizational culture and business climate.

4. Implemention

After management has decided "what" to do, procedural and technical work will need to be performed by resources with the proper skills to implement the new technology in a secure manner. ***Security controls*** are safeguards or countermeasures to avoid, counteract or minimize security risks. Documents that describe "how" employees are expected to comply with policies are called ***Procedures*** while documents that describe how systems need to be configured so as to be secure are called ***Standards.***

The second part of this article will provide suggestions for implementers that want to mitigate Skype risks in a business environment based on consensus best practices.

5. Inspect What You Expect

After publishing the decision to the affected parties and after implementing the new technology such that the risks are acceptable, it is very important to make sure that the security controls stay in place and remain effective. This activity is called a ***Security Audit***. For example, if your security policy states that Skype will not be installed on a computer system that contains protected information, it is very important to make sure that expectation is followed by a periodic inspection of those systems.

Companies are very dynamic because they must respond to rapidly changing markets. New people are hired and experienced people leave the company. No company can remain secure, if they do not audit their security controls.

6. Stay Tuned

Technology changes rapidly. Software evolves and new vulnerabilities are discovered all the time. Skype is no different. Skype is considered to be very well-designed software, but it will keep changing, especially now that Microsoft owns it and starts to integrate it into their portfolio. Changes can introduce new risks. True security requires vigilance.

Considerations Regarding the Business Use of Skype

Several security considerations have been raised by the various authors listed in the References section. The authors discuss each of these considerations as well as the associated risks and how to mitigate them. Table 1 contains a summary of some of these risks; however this information is presented only to provide an overview of the issues that warrant analysis by a detailed risk assessment that is tailored to the needs of your business.

The mitigation strategies that are designed to reduce Skype risks will depend on the business environment, but will likely involve the security principles of ***Least Privilege*** and ***Reluctance to Trust.*** The principle of Least Privilege states that *every Program/System/User should operate using the least set of privileges (access rights) necessary to complete its task* [2]. The principle of Reluctance to Trust states that one should assume that external systems are insecure and that the operating environment is insecure as well. "Trust, whether it is in external systems, code, people, etc., should always be closely held and never loosely given." [3]

For some organizations, applying these two concepts might mean that they operate Skype on dedicated computer systems on isolated network segments and are careful about the sensitivity of information they communicate on the systems. Other organizations may decide that they do not want Skype on their networks. In that case, they should implement security controls to prevent and detect against Skype. [4] [5]

Conclusion

This article has attempted to illustrate how solid security management fundamentals provide a framework to introduce potentially risky software to an organization, using Skype as an example. It is assumed that the business benefits of the software warrant the effort.

Once sensitive information is labeled and stored in secure systems, the risks introduced by changes can be assessed and mitigated with proper security controls. Audits and vigilance are required to ensure that the security controls remain effective.

Skype, like any other software, can be implemented in a manner that does not compromise an organization's security and still provides business value, but only if the risks are understood and properly addressed.

Consideration	Security Implication (Risk)	Mitigation Techniques
Bandwidth Usage	Excessive bandwidth consumption can cost money and make bandwith unavailable for more critical purposes	Disable the following three configuration settings: HTTP Ports, Super Node, Disable TCP Listen. [4]
Firewall Traversal	Skype innovatively traverses firewalls to reduce administrative burden, however Firewalls are an important security control to manage what traffic enters or leaves the organization's network	Usage of Skype can be detected/blocked on a network with an Intrusion Prevention System or specific firewall rules. [4]
Closed-Source Binaries	The Skype software uses obfuscation and other techniques to actively prevent analysis and reverse engineering. Lack of transparency causes suspicion. "It can be very difficult to know exactly what Skype is doing on your system, or what data about your system is being transmitted..." [4]	Run Skype on a dedicated system. Because Skype continues to operate on the P2P network after the user closes the application, train users to fully quit the application. Do not use Skype on a sensitive network
Attack Vector for Spam, Phishing, and Malware	Users can be tricked into running malware or divulging information when using the instant messaging and file transfer capabilities of Skype	User training and awareness is needed to prevent this attack, the same way it is needed with other software that offers similar features. [4] Configure Skype to limit communications to only people on the user's contact list. [7] Configure AV to run in "auto-protect" mode to scan file transfers. [7]
Misuse of the Skype API	Third party applications can use the Skype API to completely control the Skype application	Third party applications can be prevented from using Skype on windows by a registry key setting. [4]
Data Exfiltration	"Skype presents a simple to use, highly encrypted channel for sensitive data exfiltration that can be difficult to detect and hard to block" [4]	Do not use Skype on sensitive data networks or systems. Disable File Transfer.
Lack of Anonymity	Forensic analysis of the system running Skype will yield user's contact lists, logged instant messages, and other potentially sensitive details. In Addition, as the communication is primarily direct peer-to-peer the IP address of both sides of the communication can be determined. [4]	Maintain physical control of the system; use countermeasures to prevent unauthorized forensic examnation of the computer system, such as Full Disk Encryption
Not Able to Audit Transmissions	Because Skype is a P2P application, there is no ability to log Instant Messages or Files that have been transmitted in a centralized manner.	Either do not use Skype in business situations that are subject to the logging requirement or use a limited number of systems and create a work-around technique to collect logs.
Conversations can be recorded	Recording of conversations is most likely subject to Wiretapping laws which may vary among the different jurisdictions represented by the parties to the communication	Like with other telephony situations, it is highly recommended that legal advice be sought before recording any Skype communications.
Evesdropping Malware	Symantec announced the appearance of trojan source code (Trojan.Peskyspy) on the Internet that uploads encrypted MP3 audio recordings of Skype traffic. This is not a vulnerability of Skype itself, but an interception of the Windows API calls to the sound drivers. [9]	Keep virus definitions and IPS signatures up to date.
Software Vulnerabilities	All software is vulnerable to software bugs that can be exploited upon discovery	Keep virus definitions and IPS signatures up to date. Keep the Skype Software up to date. Monitor vulnerability alerting services
Interception of Communications	Microsoft applied for a patent for a technology called "Legal Intercept" that provides for the silent recording of communications. In addition, human-rights activists discovered that Tom-Skype (a Chinese Joint Venture with Skype) was intercepting and modifying messages. Lastly, it must be recognized that if you do not completely control the encryption keys, you do not completely control the security of the messages.	Do not use Skype for highly sensitive communications.

Table 1 – Summary of Risks Discussed in Reference Literature

References

[1] "About Skype," [Online]. Available: http://about.skype.com/. [Accessed 10 September 2011].

[2] "Least Privilege," Homeland Security - Build Security In, 14 September 2005. [Online]. Available: https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/351-BSI.html. [Accessed 10 September 2011].

[3] "Reluctance to Trust," Homeland Security - Build Security In, 15 September 2009. [Online]. Available: https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/principles/355-BSI.html. [Accessed 10 September 2011].

[4] B. Hayes, "Skype: A Practical Security Analysis," 9 October 2008. [Online]. Available: http://www.sans.org/reading_room/whitepapers/voip/skype-practical-security-analysis_32918. [Accessed 10 September 2011].

[5] M. Gough, "How to Protect Your Network Against Skype," Computerworld, 6 March 2007. [Online]. Available: http://www.computerworld.com/s/article/9012243/How_to_protect_your_network_against_Skype. [Accessed 10 September 2011].

[6] S. Baines, "Is Skype secure enough for businesses?," Silicon.com, 2 April 2007. [Online]. Available: http://www.silicon.com/legacy/research/specialreports/voipsecurity/0,3800013656,39166609,00.htm. [Accessed 10 September 2011].

[7] M. Gough, "How Dangerous is Skype?," Computerworld, 6 March 2007. [Online]. Available: http://www.computerworld.com/s/article/9012239/How_dangerous_is_Skype_. [Accessed 10 September 2011].

[8] J. Markoff, "Surveillance of Skype Messages Found in China," New York Times, 1 October 2008. [Online]. Available: http://www.nytimes.com/2008/10/02/technology/internet/02skype.html?_r=1&scp=1&sq=Surveillance. [Accessed 10 September 2011].

[9] Symantec Security Response, "Trojan.Peskyspy—Listening in on your Conversations," 28 August 2009. [Online]. Available: http://www.symantec.com/connect/blogs/trojanpeskyspy-listening-your-conversations. [Accessed 10 September 2011].

[10] J. Vijayan, "Microsoft seeks patent for spy tech for Skype," Computerworld, 28 June 2011. [Online]. Available: http://www.computerworld.com/s/article/9218002/Microsoft_seeks_patent_for_spy_tech_for_Skype. [Accessed 2011 September 2011].