NCSC

Guidance Regarding Skype and Other P2P VoIP Solutions

Ver. 1.1

June 2012

Guidance Regarding Skype and Other P2P VoIP Solutions

Scope

This paper relates to the use of peer-to-peer (P2P) VoIP protocols, with specific reference to the use of Skype, on New Zealand government information systems.

Background

Official information, as defined in the Official Information Act (1982), as amended, requires a degree of protection to be exercised in order to ensure its on-going confidentiality, availability and integrity. This implies that systems used to create, process and store official information should have similar levels of protection and security.

The appropriate levels of protection must be adopted to protect information in accordance with the designated classification levels and handling instructions.

The New Zealand security classification system as agreed by Cabinet is detailed in the Protective Security Manual (PSM), published and distributed by the NZ Security Intelligence Service (NZSIS), and also the Security in the Government Sector (SIGS) national policy document, authorised by the Interdepartmental Committee on Security.

The use of peer-to-peer (P2P) protocols in information systems has become widespread and can offer particular functionality. P2P protocols are often designed to circumvent or by-pass firewall, network address translation tables (NAT) and other security measures using a technique described as “hole punching”.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

This technique is described in several Internet Engineering Task Force (IETF) standards, such as RFC 5389 - Session Traversal Utilities for NAT (STUN). In addition, P2P protocols are often proprietary and not open to inspection by an organisation's intrusion detection system.

NZISM Policy

The New Zealand Information Security Manual (NZISM)[1], published by the Government Communications Security Bureau (GCSB) provides guidance on the use of P2P protocols in Section 9.4 - Using the Internet:

> **Peer-to-peer applications**
>
> ***System Classification(s): R, C, S, TS; Compliance: should not***
>
> Agencies should not allow personnel to use peer-to-peer applications over the Internet.
>
> **Receiving files via the Internet**
>
> ***System Classification(s): R, C, S, TS; Compliance: should not***
>
> Agencies should not allow personnel to receive files via peer-to-peer, IM or IRC applications.

While this guidance specifically relates to systems classified RESTRICTED and above, many agency systems process SEEMAIL and are therefore classified RESTRICTED as this is the highest level to which SEEMAIL operates.

[1] The New Zealand Information Security Manual is UNCLASSIFIED and is available from http://www.gcsb.govt.nz

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

Certification and Accreditation

The Certification and Accreditation of NZ government systems is described in Section 5 of the NZISM and covers roles, responsibilities and authorities for ensuring systems properly protect official and classified information.

Risk Assessment

Agencies are required to conduct a risk assessment prior to commissioning new applications, conducting infrastructure changes or security arrangements, to ensure that additional risk is not introduced and that existing risks are properly managed. A risk assessment also contributes to documentary evidence of due process.

Any decision made regarding the protection of information systems and data rests with the respective agencies, except in cases where the GCSB is the Accreditation Authority. Decisions must be based on the completion of a full risk assessment and the subsequent implementation of appropriate controls.

Risk assessments should be repeated after an appropriate time interval or when a significant system change occurs. Risk assessments should include consideration of:

- Continued protection of official and classified information throughout its entire lifecycle, including the destruction of classified material in accordance with NZ national policies;
- NZ legislation such as the Official Information Act (1982) and the Public Records Act (2005);
- Compliance with national policies, including the NZISM, PSM and SIGS.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

Risks

The risks and effects of peer-to-peer application usage are often not considered by agencies seeking to adopt P2P applications. Known risks include:

- Extensive file sharing from workstations. In some cases P2P applications will scan workstations for common file types and share them automatically for public consumption;
- When personnel receive files via peer-to-peer file sharing, IM or IRC applications, security mechanisms put in place by the agency to detect and quarantine malicious code are often circumvented;
- Some P2P applications, such as Skype, use proprietary protocols and make use of encrypted tunnels to bypass firewalls. As a result, their use is extremely difficult to regulate or monitor. It is important that agencies choose applications based on protocols that are open to inspection by intrusion detection systems;
- While Skype encrypts user sessions, other traffic, including call initiation, can be monitored by unauthorised parties;
- New Zealand's Internet infrastructure allows the routing of domestic traffic outside New Zealand. Routing cannot be pre-determined;
- Skype packets containing advertisements are unencrypted and can be linked to several sources, creating a potential cross-site scripting vulnerability;
- By default, Skype records call data (but not message content) which is saved in a "history" file on the user's workstation. If the workstation is compromised, call histories will be exposed;
- Skype's file transfer function does not currently integrate with all anti-virus products;

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

- Skype does not record all Skype communication activities, so a complete log of activity is possible only through the use of additional logging systems;
- Skype creates a file named "1.com" which is capable of recording BIOS data from a PC. According to Skype, this is used to identify computers and provide DRM protection for plug-ins;
- The Skype client for LINUX has been observed accessing the /etc/passwd file during execution. This file contains a list of all user accounts on the systems and may also include hashed passwords;
- The Skype client for Mac has been observed accessing protected information in the system Address Book, even when integration with the Address Book is disabled in the Skype preference settings;
- Skype maintains user data on the user's machine, on Skype servers and in the P2P network. There is no inherent Skype security for chat logs, transfer files or voicemail messages stored at the client;
- Skype can be "bandwidth hungry", consuming other users' bandwidth and consuming network bandwidth, even when idle. This is documented in the Skype license agreement (EULA). The use of uncontrolled network bandwidth provides an attack vector for security compromises and breaches.

Skype Architecture[2]

Skype's installation package includes several management tools that interact directly with Microsoft's Active Directory and a web-based Skype Manager. Skype has three peer nodes, ordinary nodes, supernodes and relay nodes, included in the installation package. Relay nodes exist outside the corporate network to relay media and signalling information between nodes that cannot communicate directly.

[2] Skype IT Administrators Guide, Skype for Windows version 4.2, Version 2.0, copyright © Skype Limited 2010

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

The Skype client requires TCP connectivity for signalling information, by default UDP connectivity. Skype offers three methods of firewall and NAT traversal:

- Native firewall NAT traversal;
- A SOCKS5/HTTP proxy server; and
- TCP/UDP relays with direct Internet access.

Skype automatically traverses most firewalls and NATs using UDP “hole punching”, allowing Skype clients to pass networking parameters (remote node IP address and source port) to other hoists and relays.

Encryption

The NZISM requires the use of the following encryption algorithms for new systems and applications:

- AES 256 or better;
- SHA-2 family (SHA-256, SHA-384 and SHA-512);
- ECDH for agreeing on encryption session keys (curves P-256 and P-384 (prime moduli), field/key size of at least 160 bit);
- ECDSA for digital signatures (curves P-256 and P-384 (prime moduli), field/key size of at least 160 bit);
- Other algorithms are permitted ONLY in legacy systems – this does NOT include new applications, upgrades, major version changes etc.

Skype provides the following encryption:

- AES 256 block cipher data encryption;
- SHA 1 hash function;
- 1024 RSA public key cryptosystem;
- RC4 stream cipher.

UNCLASSIFIED

P O Box 12-209, Wellington, New Zealand | incidents@ncsc.govt.nz | Phone: +64 4 498 7654 | Fax: +64 4 498 7655

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

7

Skype does not meet the current cryptographic standards as described in the NZISM.

Some Mitigating Measures

This is not an exhaustive list of mitigating measures and agencies should complete their own risk assessment, considering all risks, including those discussed in this guidance, and select the appropriate controls to provide effective risk mitigation.

Important steps include measures to prevent or mitigate the effects of:

- Password misuse, including social engineering;
- Cross-site scripting and phishing;
- Malware, adware and spyware;
- False identity and spoofing;
- Spam and Spam over Internet Telephony (SPIT);
- Multiple logins;
- Skype editing.

In addition the following specific controls may be implemented:

- Implement application white listing;
- Prohibit classified conversations over Skype;
- Use a separate, “air-gapped”/stand alone environment for Skype;
- Use only verifiable, authentic copies of the application. Where necessary, download from an authenticated source. Verify application checksums;
- Use only the Business Version of Skype;
- Rigorous patch management;
- Ensure version consistency (only the latest version in use);
- Remove user administrator rights;
- Use anti-virus and anti-malware tools;
- Use strong authorisation processes;

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

- Ensure user profiles are current;
- Use strong authentication for third parties;
- Implement strong password controls;
- Ensure system policies are rigorously enforced. Use Windows Group Policy Objects (GPO) to secure and manage configuration and technical policy;
- Disable “remember my password” as a matter of policy;
- Enable logging and auditing.

Skype Business Version Configuration

Skype offers an Administration Template for configuring Active Directory group policies, controlling many functions in Skype. When configured, these templates can be pushed out to, and enforced on, all workstations in the domain.

For further information you can search for and download the latest Skype PDF manual, “Skype-IT-Administrators-Guide.pdf”. This can be downloaded here: http://download.skype.com/share/business/guides/skype-it-administrators-guide.pdf)

Additionally, you can download a Group Policy Object (GPO) template for Skype. The file format is Skype-Vx.x.adm (where x.x refers to the file version).

The following are the minimum recommendations for the configuration of the Skype Business Version:

- Disable File Transfer;
- Disable API;
- Enable Memory Only;
- Enable Listen Port Policy;
- Set the Listen Port and ensure it is blocked on the border firewall;
- Disable Listen HTTP Ports Policy;

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

- Enable Disable Supernode Policy;
- Disable Screen Sharing.

Locking Down Functionality in Other P2P VoIP Solutions

There are many other P2P VoIP applications on the market. Some minimum hardening and mitigation actions that should be considered for all applications, includes, but is not limited to, the following:

- Disable file transfer;
- Disable API;
- Block or limit file system access;
- Lock down functionality as much as possible.

Queries

Any queries regarding any aspect of Skype, or any other P2P VoIP application, can be directed to: liaison@ncsc.govt.nz

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.