Whitepaper: Skype for Business

A Brief Security Analysis of Microsoft Skype for Business

Date: December 2015

Doc Ref: SOS-WP-SFB-1215A

Author: Fatih Ozavci

Author Title: Principal Security Consultant

Table of Contents

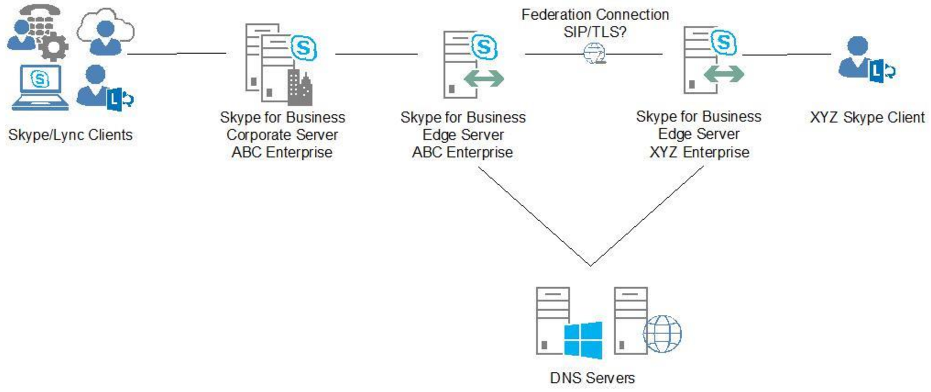
Prologue

Larger organisations have complex communication requirements including video conferencing, office collaboration through meetings and cost effective international communication between branches. Unified Communications (UC) is a technical term that describes a next-generation communication infrastructure that supports instant messaging, presence information, content sharing, and audio and video calls through various communication services. Larger organisations have already started using UC for their corporate communication, although it brings with it some major security challenges. Call-centres, LTE service providers, VoIP subscriber services and enterprise meeting solutions are just some examples of UC in the enterprise environment. Skilled attackers may target UC services for toll fraud, cyber intelligence gathering and financial profit. This whitepaper aims to highlight the security concerns related to UC, and discuss them specifically with respect to Microsoft Skype for Business (a.k.a. Microsoft Lync), which is becoming a popular UC solution in corporate environments. It also offers solutions for known security issues, providing methods to secure UC services otherwise susceptible to toll fraud, denial of service and eavesdropping attacks.

Microsoft Skype for Business

After acquiring Hotmail, Microsoft started offering instant messaging services using Microsoft Live Communications 2005. This path evolved during the communication era with Microsoft Office Communicator and Lync services. Microsoft Skype for Business (SFB) is a new product recently announced by Microsoft to provide enterprise communication services using a combination of Microsoft Lync and Skype environments. SFB supports all UC services, including instant messaging with file and screen sharing, office collaboration through office servers, audio and video meetings as well as traditional IP phone services.

Federation-based UC is another emerging trend which is supported by SFB to improve multi-national and enterprise communications with partners, service providers and cloud services. Federated UC between enterprise organisations can be configured using Session Border Controllers (SBC) and edge servers which are responsible for managing trust relationships, authorisation and security.


Skype/Lync Clients
Skype for Business Corporate Server ABC Enterprise
Skype for Business Edge Server ABC Enterprise
Federation Connection SIP/TLS?
Skype for Business Edge Server XYZ Enterprise
XYZ Skype Client
DNS Servers

Federated Unified Communications

Although SFB has modern collaboration features and security improvements for UC services, it still retains security challenges due to design flaws, backward compatibility issues and flexible configuration options.

Modern Unified Communications Threats

Although they do not utilise the same degree of security technology and features as web services, UC services also carry critical and sensitive information. This provides an opportunity for skilled attackers to collect cyber intelligence and financial information from their victims. Even non-skilled attackers can use traditional attacks such as toll fraud and call spoofing to obtain financial benefit.

Moreover, larger organisations can also be affected by advanced attacks such as the impersonation of an important executive (e.g. CIA managing director, CEO of a Fortune 100 corporation) caller identity spoofing, an attacker targeting a call centre to collect credit card and Personally Identifiable Information (PII) using IVR recordings, toll fraud using auto-diallers, or blackmail of a call centre with a Telephony Denial of Service (TDoS) attack.

Larger organisations may be liable for security breaches regarding privacy, PII or financial information stored or transmitted through UC services. Government guidelines on communication, lawful interception, financial regulations and compliance standards may require additional security precautions for enterprise communication and services. Although the attacks above may not initially seem dangerous, financial losses after such attacks may ensue as a result of liability issues and a loss of reputation. Thus the cost of securing UC services is likely to be lower than the cost of managing the financial and regulatory impact of a security breach.

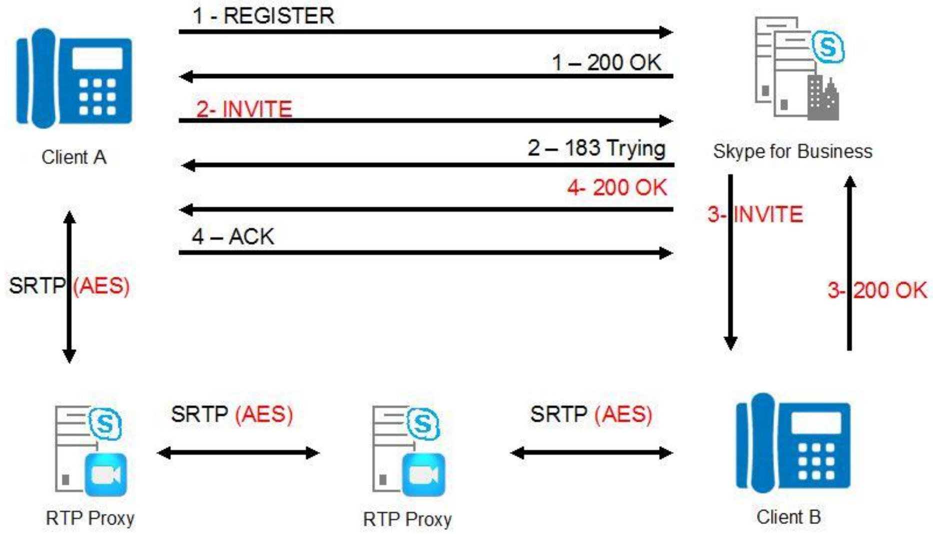
Design Security of Skype for Business

The Microsoft Skype for Business (SFB) platform supports interconnectivity for federated connections, multi-vendor services and cloud integration requirements. IP phones and teleconference devices in use on SFB platforms are also manufactured by other vendors. As a result of this, SFB supports several types of clients including mobile platforms (e.g. iOS, Android, Windows Phone), desktop platforms (e.g. Mac OS X, Windows), web services and third-party clients. Microsoft Lync clients available on other platforms are also compatible with the new SFB features after software upgrades.

As a result of the compatibility requirements of various designs, the initial configuration of SFB is fairly insecure. Insecure SIP trunk connections, potential encryption issues, weak communication policy enforcement and federation configuration are some of the security concerns that affect SFB networks.

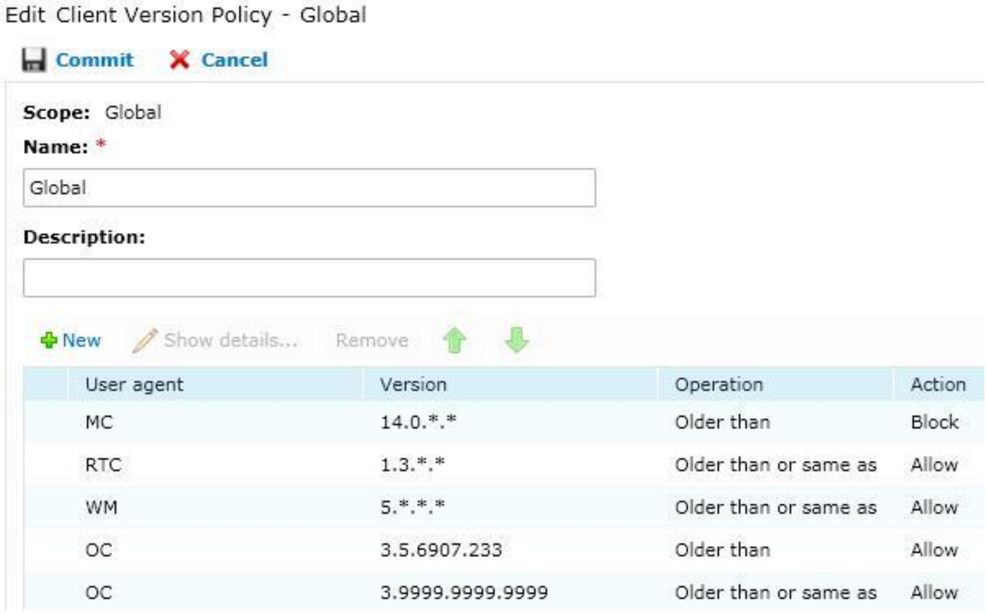
SFB has a mediation service to provide connectivity with SIP trunks and PSTN gateways for third-party connections. The mediation service running on SFB does not support authentication schemes such as x.509 digital certificate-based authentication, digest authentication or OAuth. It is assumed that the connection between the mediation service and third-parties is restricted and secure. Therefore, it only relies on the IP address restriction which may allow attackers to bypass security restrictions using IP spoofing or Man-In-The-Middle (MITM) attacks.

Encryption enforcement on SFB is fairly tight, for example SIP over TLS connections are enforced for official Microsoft clients. SFB also enforces AES symmetrical encryption-based SRTP for call transport to secure audio, video, files and content transmitted through RTP streams. Symmetrical encryption keys for an SRTP connection are exchanged through SIP over TLS signalling. However, if the mediation service is configured over TCP without TLS, signalling services may disclose the encryption keys used during the calls through the call signalling which is plain-text. When the encryption keys are exposed, intercepted SFB calls can be decrypted or eavesdropped on to conduct further attacks.



Sample Call Flow with SRTP Encryption Keys

Enterprise communication and good governance requires security policies and procedures to be implemented on the technologies used. SFB offers a set of corporate communication policy options through a web-based management interface. However, it is difficult to enforce security policies for such a large variety of clients which do not support all the SFB features and impose some limitations. A client software version management policy should be used by SFB to avoid client-based vulnerabilities and to manage software versions on clients. Pre-configured secure meeting invitations and external authentication for the services connected should also be enforced to avoid unauthorised connections to the SFB environment.



Edit Client Version Policy - Global

Commit Cancel

Scope: Global

Name: *

Global

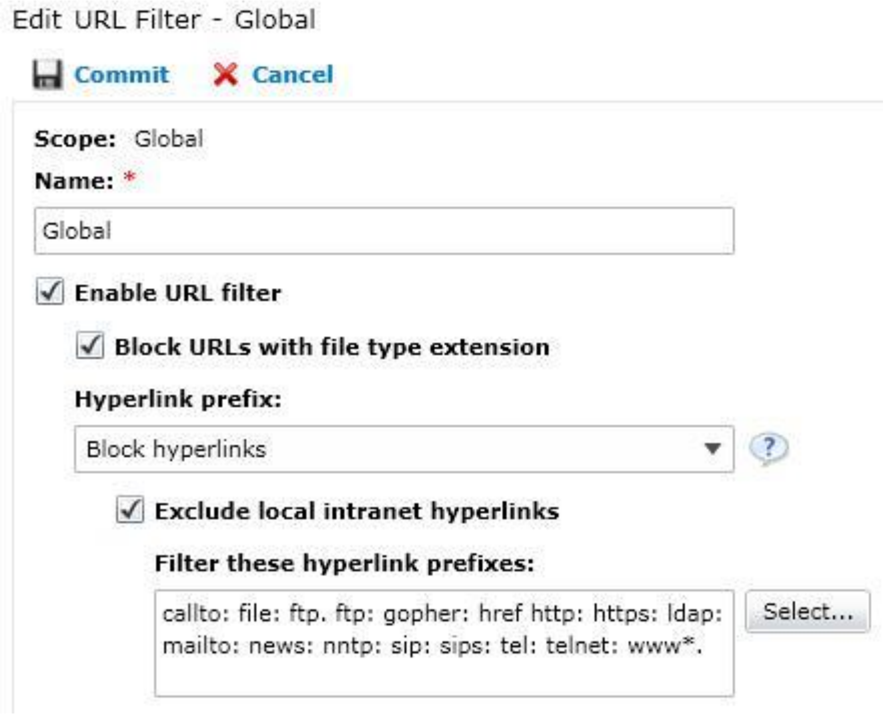
Description:

New Show details... Remove

User agent	Version	Operation	Action
MC	14.0.*.*	Older than	Block
RTC	1.3.*.*	Older than or same as	Allow
WM	5.*.*.*	Older than or same as	Allow
OC	3.5.6907.233	Older than	Allow
OC	3.9999.9999.9999	Older than or same as	Allow

Client Version Policy

Moreover, the security features of SFB should be enabled and configured to improve instant messaging security. URL and file filtering features should be enabled to avoid forbidden content being shared between clients. It is also possible to restrict instant messaging content types (e.g. disabling HTML or RTF communication) using the `Set-CsClientPolicy` command. This is required to minimise the attack surface and could be abused to exploit client-side vulnerabilities, such as memory corruption through invalid fonts, graphic content or file types.



Scope: Global

Name: *

Global

☑ Enable URL filter

☑ Block URLs with file type extension

Hyperlink prefix:

Block hyperlinks

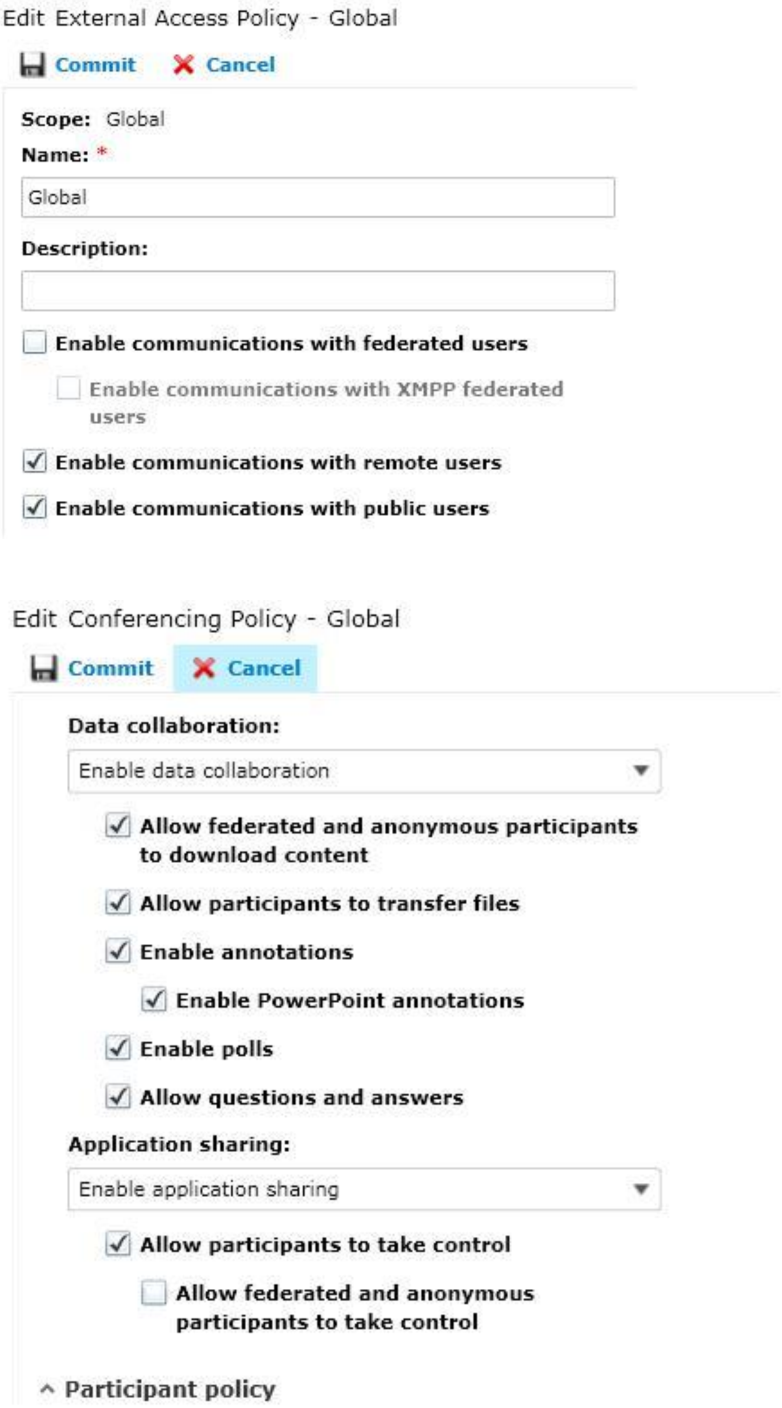
☑ Exclude local intranet hyperlinks

Filter these hyperlink prefixes:

callto: file: ftp. ftp: gopher: href http: https: ldap: mailto: news: nntp: sip: sips: tel: telnet: www*.

URL Filter Settings

Finally, external authentication, public meetings and third-party federation connections should be secured in conjunction with a secure network design. Enterprise communication services should be isolated from non-corporate networks using SFB edge servers. Edge servers may apply additional layers of security and enforce policies to disable unnecessary features. SFB networks should not accept authentication requests or calls coming from untrusted parties, clients or service providers. Federation connections should be configured on edge servers and existing SFB policies enforced should not be bypassed or disabled for multi-vendor compatibility.



Edit External Access Policy - Global

Scope: Global

Name: *

Global

Description:

- ☐ Enable communications with federated users
  - ☐ Enable communications with XMPP federated users
- ☑ Enable communications with remote users
- ☑ Enable communications with public users

Edit Conferencing Policy - Global

Data collaboration:

Enable data collaboration

- ☑ Allow federated and anonymous participants to download content
- ☑ Allow participants to transfer files
- ☑ Enable annotations
  - ☑ Enable PowerPoint annotations
- ☑ Enable polls
- ☑ Allow questions and answers

Application sharing:

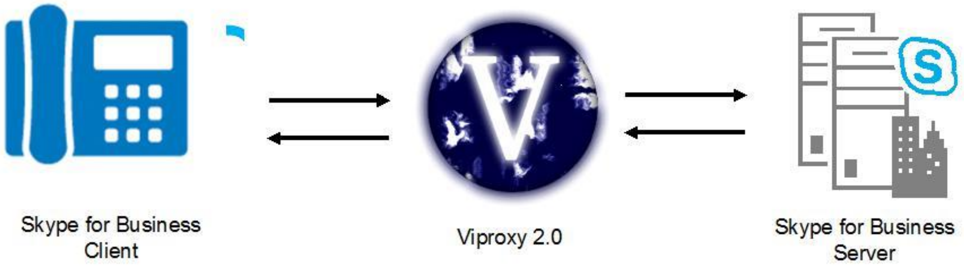
Enable application sharing

- ☑ Allow participants to take control
  - ☐ Allow federated and anonymous participants to take control

External Access and Conference Policies

Security Research and Development Process

Sense of Security consultant, Fatih Ozavci, who is also the author of Viproy VoIP Penetration Testing Kit[1] and VoIP Wars research series, developed a new security testing tool using the existing features of Viproy. This was required to analyse all Microsoft Skype for Business (SFB) features using the official clients. The new security testing tool, named Viproxy, is a Man-In-The-Middle (MITM) attacking proxy which uses existing connections to attack clients and servers. Viproxy supports TCP/TLS interception to debug data traffic between SFB clients and servers. It also disables compression support requested by clients to keep the connection in human-readable plain-text.

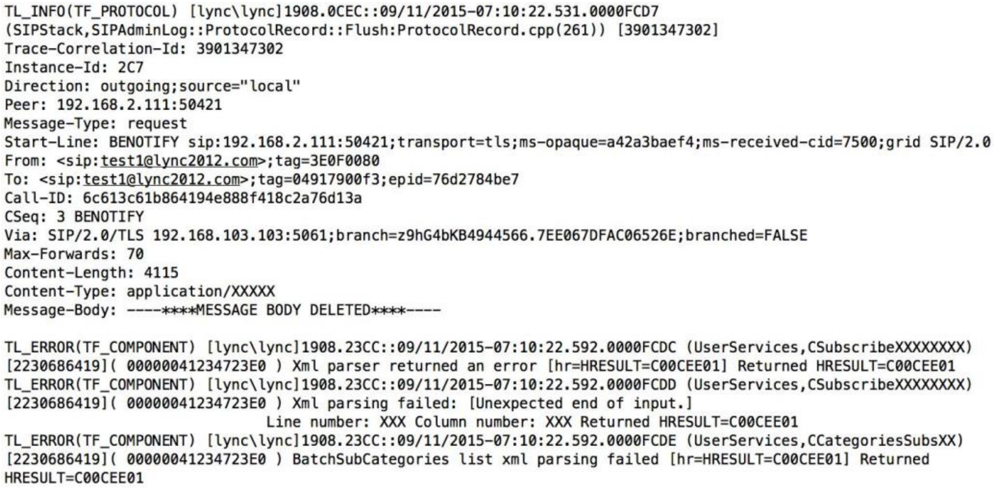


Sample Debugging with Viproxy

Viproxy can debug and change the content transmitted to test the target software through manual fuzzing, content manipulation and feature-unlocking attacks. Basic search and replace, content injection, “dumb” fuzzing, message content injection, custom header injection and manipulating responses by request are the essential features of Viproxy. It provides an online command console to execute attacks as well as importing an attack configuration file during start-up.

It was identified that SFB has multiple programming errors and exceptions resulting from the parsing and handling of invalid content sent during tests. Although the exceptions detected are not yet marked as exploitable, the programming error messages leak sensitive information about server components.

[1] http://viproy.com



```
TL_INFO(TF_PROTOCOL) [lync\lync]1908.0CEC::09/11/2015-07:10:22.531.0000FCD7
(SIPStack,SIPAdminLog::ProtocolRecord::Flush:ProtocolRecord.cpp(261)) [3901347302]
Trace-Correlation-Id: 3901347302
Instance-Id: 2C7
Direction: outgoing;source="local"
Peer: 192.168.2.111:50421
Message-Type: request
Start-Line: BENOTIFY sip:192.168.2.111:50421;transport=tls;ms-opaque=a42a3baef4;ms-received-cid=7500;grid SIP/2.0
From: <sip:test1@lync2012.com>;tag=3E0F0080
To: <sip:test1@lync2012.com>;tag=04917900f3;epid=76d2784be7
Call-ID: 6c613c61b864194e888f418c2a76d13a
CSeq: 3 BENOTIFY
Via: SIP/2.0/TLS 192.168.103.103:5061;branch=z9hG4bKB4944566.7EE067DFAC06526E;branched=FALSE
Max-Forwards: 70
Content-Length: 4115
Content-Type: application/XXXXX
Message-Body: ----****MESSAGE BODY DELETED****----

TL_ERROR(TF_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDC (UserServices,CSubscribeXXXXXXXX)
[2230686419]( 00000041234723E0 ) Xml parser returned an error [hr=HRESULT=C00CEE01] Returned HRESULT=C00CEE01
TL_ERROR(TF_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDD (UserServices,CSubscribeXXXXXXXX)
[2230686419]( 00000041234723E0 ) Xml parsing failed: [Unexpected end of input.]
                              Line number: XXX Column number: XXX Returned HRESULT=C00CEE01
TL_ERROR(TF_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDE (UserServices,CCategoriesSubsXX)
[2230686419]( 00000041234723E0 ) BatchSubCategories list xml parsing failed [hr=HRESULT=C00CEE01] Returned
HRESULT=C00CEE01
```

Sample XML Parsing Error Message

Viproxy[2] can also be used to alter server responses to bypass client feature restrictions and policies. This feature is required to test the corporate policies used, meeting options and enforcements relying on the restrictions of official clients. It is a standalone Metasploit Framework[3] module and can be downloaded through the Sense of Security homepage.

[2] https://www.senseofsecurity.com.au/sitecontnt/uploads/2015/11/viproxy-2.0.zip

[3] http://www.metasploit.com/

Security Vulnerabilities

Microsoft Skype for Business (SFB) supports rich Instant Messaging (IM) using HTML, RTF and content sharing. It is possible to send HTML content or to share a file or client desktop using the IM sessions established between the clients. This may allow attackers to exploit client-side vulnerabilities through IM sessions, such as sending an invalid graphic or font to trigger a memory corruption on client software. Basically, almost all font, graphic or office file vulnerabilities released for Microsoft products can be exploited through the SFB environment because of the use of shared libraries.

Sense of Security identified that it is also possible to attack clients or the environment using IM session content as well as shared libraries. Current versions of SFB servers and clients are vulnerable to content manipulation, multiple Cross-Site Scripting (XSS) injections and URL filter bypass vulnerabilities below.

1. IM URL filter bypass using content obfuscation

SFB Server has a security mitigation known as IM URL filtering which is disabled by default. This feature can be enabled by administrators to avoid URL injections in IM messages such as call, HTTPS and SIP URLs. Attackers can bypass the IM URL filter using JavaScript content or content obfuscation. This allows attackers to inject valid URLs to the IM sessions for phishing or social engineering attacks.

PoC exploit to bypass IM URL filter:

```
<script>var u1=“ht”; u2=“tp”; u3=“://”;o=“w”; k=“.”; i=“”;
u4=i.concat(o,o,o,k);
window.location=u1+u2+u3+u4+”senseofsecurity.com”</script>
```

2. Unauthorised execution of HTML/JavaScript in SIP MESSAGE requests

SFB clients use the lynchtmlconv.exe component for parsing HTML based IM sessions. Lynchtmlconv.exe allows attackers to execute HTML and JavaScript content in the IM context without user interaction. Attackers can invite a victim user to an IM session using a SIP INVITE request. Even if the victim user does not answer that invitation, attackers can send another SIP MESSAGE which contains malicious JavaScript content in the same context. Lynchtmlconv.exe parses and executes the JavaScript in the message without user interaction or approval. Attackers can use this vulnerability to open a malicious web page using the default browser, to execute a browser exploit, to open another IM session with someone else, or to trigger other URIs defined on the client’s system for another application.

PoC exploit can be injected as a SIP INVITE header:

```
Ms-IM-Format:       text/html;       charset=UTF-8;       ms-
```

```
body=PHNjcmlwdD53aW5kb3cubG9jYXRpb249Imh0dHA6Ly93d3cuc2Vuc2
VvZnNlY3VyaXR5LmNvbS5hdSI8L3NjcmlwdD4K
```

Base64 decoded ms-body content used:

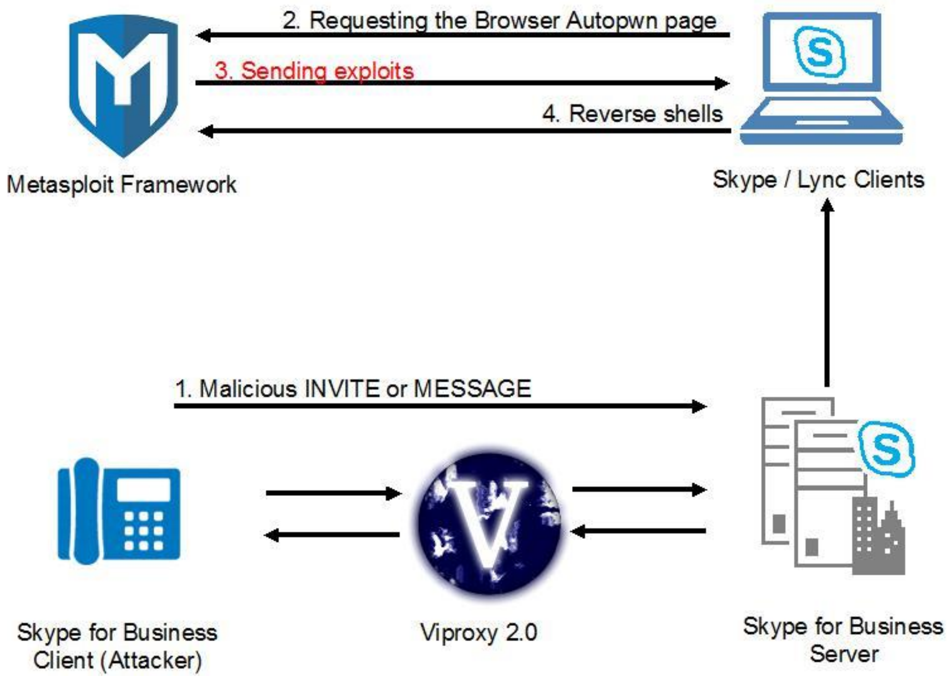
```
<script>window.location="http://www.senseofsecurity.com.au"
</script>
```

3. Unauthorised execution of the HTML/JavaScript in SIP INVITE requests

SFB clients use the lynchtmlconv.exe component for HTML based IM sessions, but it is also used for HTML based INVITE request subjects. Lynchtmlconv.exe allows attackers to execute HTML and JavaScript content in the SIP INVITE header without user interaction. Attackers can invite a victim user to an IM session using a malicious SIP INVITE request. It is irrelevant whether the victim user accepts the invitation or not, and the malicious content will be executed. The INVITE subject is a header that contains the malicious content, and it can also be forwarded by the SIP trunks or proxies. Attackers can use this vulnerability to open a malicious web page using the default browser, to execute a browser exploit, to open another IM session with someone else, or to trigger other URIs defined on the client's system for another application.

PoC exploit can be injected as SIP MESSAGE content:

```
<script>window.location="http://www.senseofsecurity.com.au"
</script>
```


2. Requesting the Browser Autopwn page
3. Sending exploits
4. Reverse shells
Metasploit Framework
Skype / Lync Clients
1. Malicious INVITE or MESSAGE
Skype for Business Client (Attacker)
Viproxy 2.0
Skype for Business Server

Sample Exploitation Scenario

The vulnerabilities detected allow authenticated attackers to inject malicious content into the IM messages and SIP INVITE requests that are delivered through the MS Lync, Skype for Business or Office 365 platforms. They can be also exploited through federated connections, meeting requests, SIP trunks and PSTN gateways without authentication. Malformed IM messages or SIP INVITE requests can be used to compromise multiple clients without user interaction. Exploitation vectors of these vulnerabilities depend on the corporate communication design and implementation. Clients of the federations connected, public meeting invitation requests, open meetings, bulk IM messages and SIP trust relationships can be used for mass compromise attacks.

Remediation of the vulnerabilities reported:

Install the security patches released by Microsoft and follow the instructions contained in the security advisory below.

Microsoft Security Bulletin MS15-123 – Important Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)

https://technet.microsoft.com/library/security/ms15-123

Securing Unified Communications

Secure design is the foundation of secure Unified Communications (UC). Federation bridges should be established with only trusted parties, with limitations such as simplifying instant messaging content or creating call-only links. SIP trunks and PSTN gateways are other possible third-party connection types and they should also be configured with a proper authorisation scheme and restricted network level access.

Moreover, encryption requirements should be analysed with respect to potential ensuing liability stemming from non-compliance with regulations, PCI compliance and the Australian Privacy Act. Transport security should be designed with asymmetrical encryption such as ZRTP[4] or MIKEY[5] to avoid possible disclosure of symmetrical encryption keys. It is also required to enforce SIP over TLS for all clients, trunks and third-party connections.

Furthermore, the design of authentication and authorisation schemes used for clients, trunk connections and services is an important area to be considered. Authentication should be enforced for all UC connections including clients, third-parties and even access-restricted internal networks. The authentication types can be adjusted with network layer protection, client types and trust levels, for example using digital certificate pinned mutual TLS connections for trunks, and using alphanumeric usernames and passwords with strong policies for clients. This may reduce unauthenticated calls, dictionary attacks or the easier forms of toll fraud. In addition, authorisation within the voice services should be improved to avoid call spoofing, dial-plan bypass and denial of service attacks.

Finally, security procedures should be improved to support management of security updates, IP phones, user restrictions and conference call security. This may assist administrators in solving challenges with interoperation between departments and third-parties as well as reducing the attack surface in the UC environment.

[4] https://tools.ietf.org/html/rfc6189

[5] https://tools.ietf.org/html/rfc3830

Security Testing Methodology

Sense of Security provides a vendor and provider-independent VoIP audit service for Unified Communications (UC) services. The key elements of testing include VoIP clients, IP phone and softphone management services, signalling, media streaming, tenant service management interfaces, tenant sandbox and privacy/confidentiality, jailbreak tests for tenant sandbox security, federation services, network design and wide area network communication. Signalling analysis covers tests of authentication and authorisation, call and dial-plans, call spoofing, and bypass tests for call data records and billing. Media streaming tests cover media encryption, proxy features and analysis of interception protection. VoIP client analysis tests cover official clients, essential devices or embedded software vulnerabilities. Furthermore, VoIP client management service assessments, voicemail analysis, network design analysis, database analysis for CDR and voice recordings, VoIP client analysis and essential network services analysis are the key components of the testing service.

Awareness – Conclusions

Communication is not conducted only by voice anymore. File sharing, voice and video conferencing, collaboration and entertainment streaming are vital elements of any current communications solution. The business world may require branches in different countries, employees working from home or servicing of geographically diverse customers. The bridge between modern communication and the business world is Unified Communications (UC), and voice is not the only asset to protect within it. Confidential presentations, persistent surveillance, management meetings and expensive international connections are a prime target for contemporary attackers.

Microsoft Skype for Business is a solution aimed at supporting the modern enterprise's growing communication requirements, but it also comes with security concerns that need to be handled carefully. Sense of Security has completed extensive security research in the UC field with significant results highlighting the critical areas of risk to secure corporate communication. The security issues investigated and the vulnerabilities reported for this environment may lead to full compromise of corporate communications. It is possible to attack subscribers, employees and managers as well as infrastructure.

Unified Communications security starts with a secure design, continues with strong management practices, and ends with improved monitoring of the services used. Therefore, Sense of Security offers a next-generation UC penetration testing methodology as well as consulting services to secure enterprise communications.

About Sense of Security

Sense of Security Pty Limited is an Australian based information security and risk management consulting practice delivering industry leading services and research to organisations throughout Australia and abroad. Our strategic approach to security provides our clients with a capability to understand the security risks relevant to their organisation and knowledge to protect their information assets. We provide expertise in governance & compliance, strategy & architecture through to risk assessment, assurance & technical security testing.

For more information please contact us:

Web: www.senseofsecurity.com.au

Email: info@senseofsecurity.com.au

Phone: 1300 922 923

Sense of Security - Compliance, Protection and Business Confidence