VoIP Wars: Destroying Jar Jar Lync

Fatih Ozavci

13 November 2015

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000 Australia

Melbourne
Level 15, 401 Docklands Drv
Docklands VIC 3008 Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Speaker

Fatih Ozavci, Principal Security Consultant

- VoIP & phreaking
- Mobile applications and devices
- Network infrastructure
- CPE, hardware and IoT hacking

- Author of Viproy, Viproxy and VoIP Wars research series
- Public speaker and trainer
  Blackhat USA, Defcon, HITB, AusCert, Troopers, Ruxcon

Previously on VoIP Wars

```
Program received signal EXC_BAD_ACCESS, Could not access memory.
Reason: KERN_INVALID_ADDRESS at address: 0x00000000
[Switching to process 6787 thread 0x3e03]
0x327bc26c in ?? ()
(gdb) info registers
r0             0x0      0
r1             0x40     64
r2             0x55d13de        89986014
r3             0xa86b6  689846
r4             0x11fd214        18862612
r5             0xeeb50  977744
r6             0x11fd214        18862612
r7             0x55d11a8        89985448
r8             0x9cfd10 10288400
r9             0x0      0
r10            0x9d0914 10291476
r11            0x55d1b98        89987992
r12            0xdf450  914512
sp             0x55d11a8        89985448
lr             0x122e1  74465
pc             0x327bc26c       846971500
cpsr           0x10     16
(gdb)
```

```
Trust Analysis : SCAN |
t Target SIP Server
Target SIP Server
 interface
The SIP Server
er
ytes to capture
form Trust Sweep.
erform Trust Sweep
oncurrent threads
econds to wait for new d
ata
   TO           701             yes       Destination Number at Target SIP Server

msf auxiliary(vsiptrust) > run
[*] Auxiliary module execution completed
msf auxiliary(vsiptrust) > 
```

```
RPOR
TARG
TELN
VHOS

msf aux
```

```
ion completed
usage) >
*]    Display Name: 2000 ]
*] Line is open for Call Forward to 1011
```

Ready to load or capture

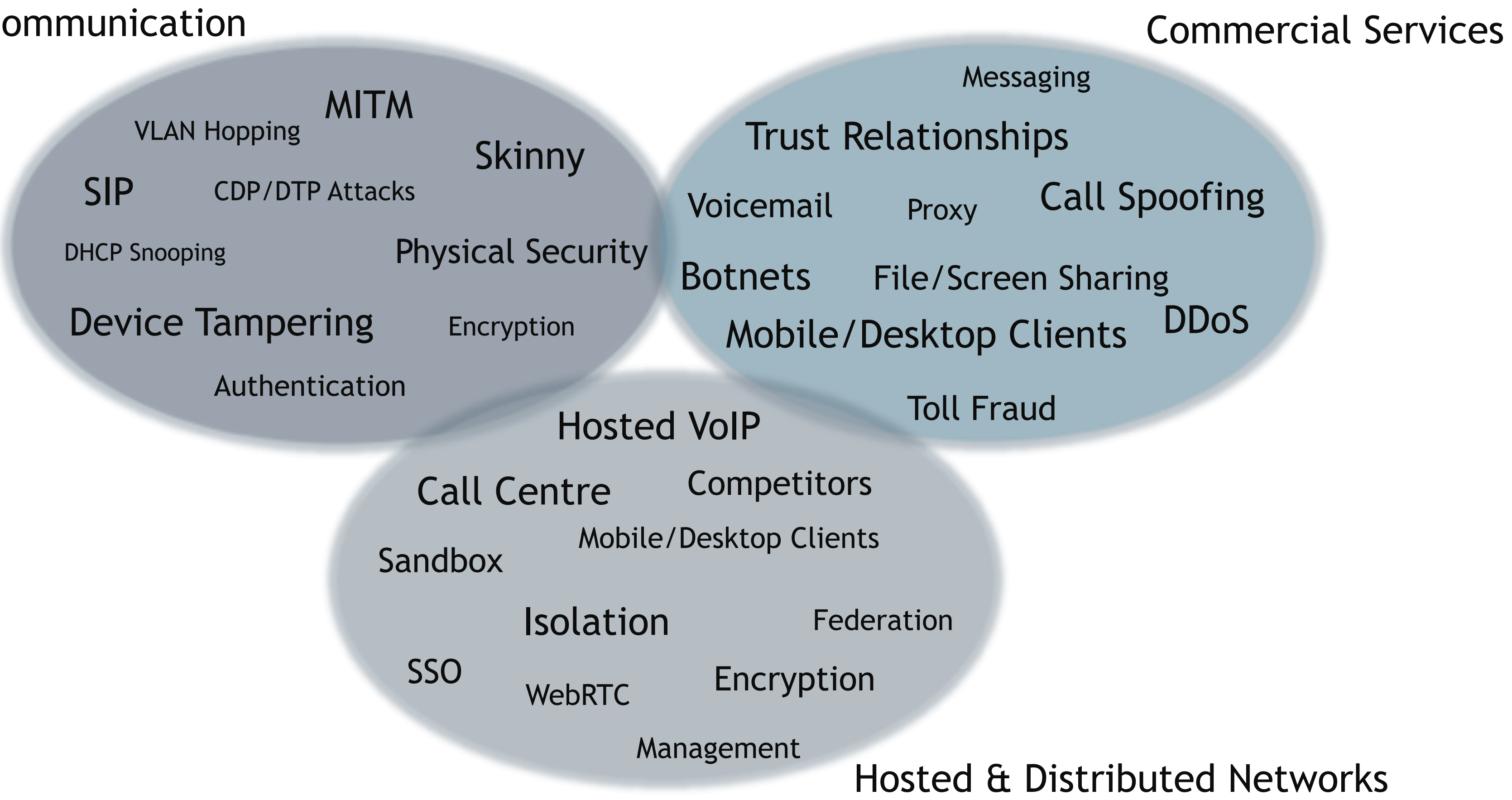
Current research status

- This is only the first stage of the research
  - Analysing the security requirements of various designs
  - Developing a tool to
    - assess communication and voice policies in use
    - drive official client to attack other clients and servers
    - debug communication for further attacks
- Watch this space
  - Viproy with Skype for Business authentication support
  - Potential vulnerabilities to be released

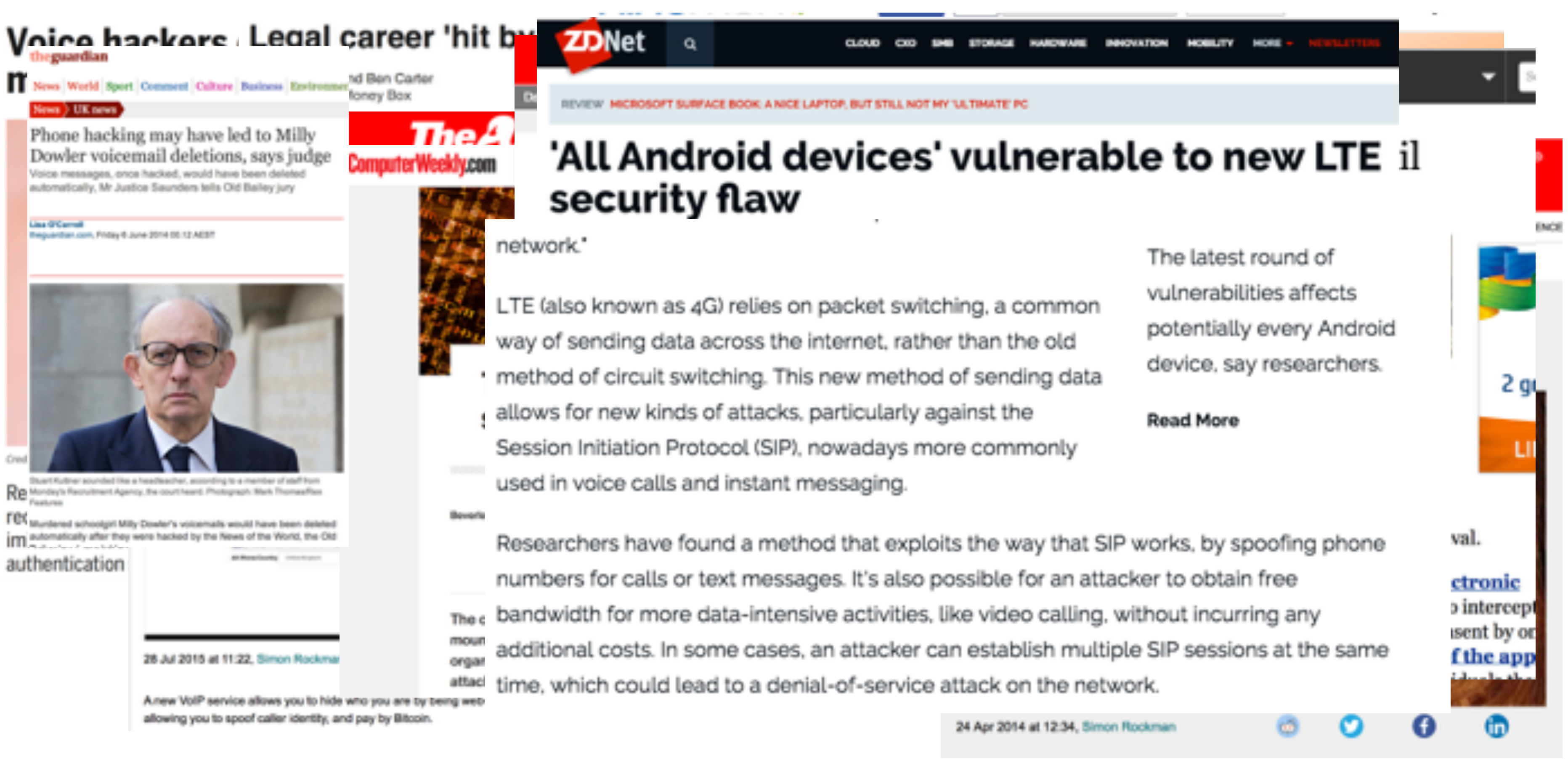
Agenda

1. Modern threats targeting UC on Skype for Business
2. Security requirements for various implementations
3. Security testing using Viproxy
4. Demonstration of vulnerabilities identified

Security requirements for UC



Modern threats targeting UC



Voice hackers

Legal career 'hit by

theguardian

News | World | Sport | Comment | Culture | Business | Environment

News › UK news

Phone hacking may have led to Milly Dowler voicemail deletions, says judge

Voice messages, once hacked, would have been deleted automatically, Mr Justice Saunders tells Old Bailey jury

Lisa O'Carroll
theguardian.com, Friday 6 June 2014 00.12 AEST

Stuart Kuttner sounded like a headteacher, according to a member of staff from Monday's Recruitment Agency, the court heard. Photograph: Mark Thomas/Rex Features

Murdered schoolgirl Milly Dowler's voicemails would have been deleted automatically after they were hacked by the News of the World, the Old

authentication

nd Ben Carter
Money Box

ComputerWeekly.com

28 Jul 2015 at 11:22, Simon Rockman

A new VoIP service allows you to hide who you are by being web allowing you to spoof caller identity, and pay by Bitcoin.

ZDNet

CLOUD CXO SMB STORAGE HARDWARE INNOVATION MOBILITY MORE NEWSLETTERS

REVIEW MICROSOFT SURFACE BOOK: A NICE LAPTOP, BUT STILL NOT MY 'ULTIMATE' PC

'All Android devices' vulnerable to new LTE security flaw

network."

LTE (also known as 4G) relies on packet switching, a common way of sending data across the internet, rather than the old method of circuit switching. This new method of sending data allows for new kinds of attacks, particularly against the Session Initiation Protocol (SIP), nowadays more commonly used in voice calls and instant messaging.

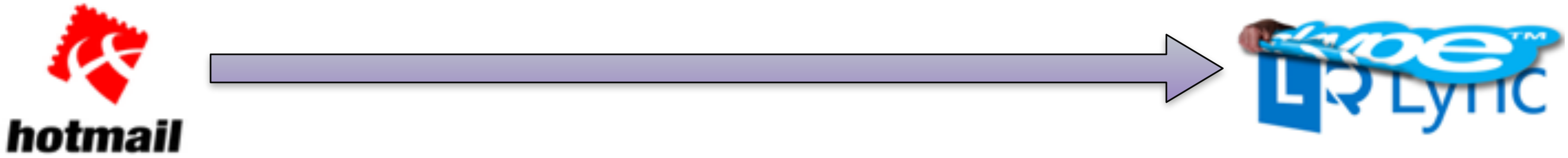
Researchers have found a method that exploits the way that SIP works, by spoofing phone numbers for calls or text messages. It's also possible for an attacker to obtain free bandwidth for more data-intensive activities, like video calling, without incurring any additional costs. In some cases, an attacker can establish multiple SIP sessions at the same time, which could lead to a denial-of-service attack on the network.

The latest round of vulnerabilities affects potentially every Android device, say researchers.

Read More

24 Apr 2014 at 12:34, Simon Rockman

Skype for Business



Microsoft Live Communications 2005

Microsoft Office Communicator 2007

Microsoft Lync 2000 - 2013

Microsoft Skype for Business 2015

Microsoft Office Live Communications Server 2005

Microsoft Office Communicator 2007

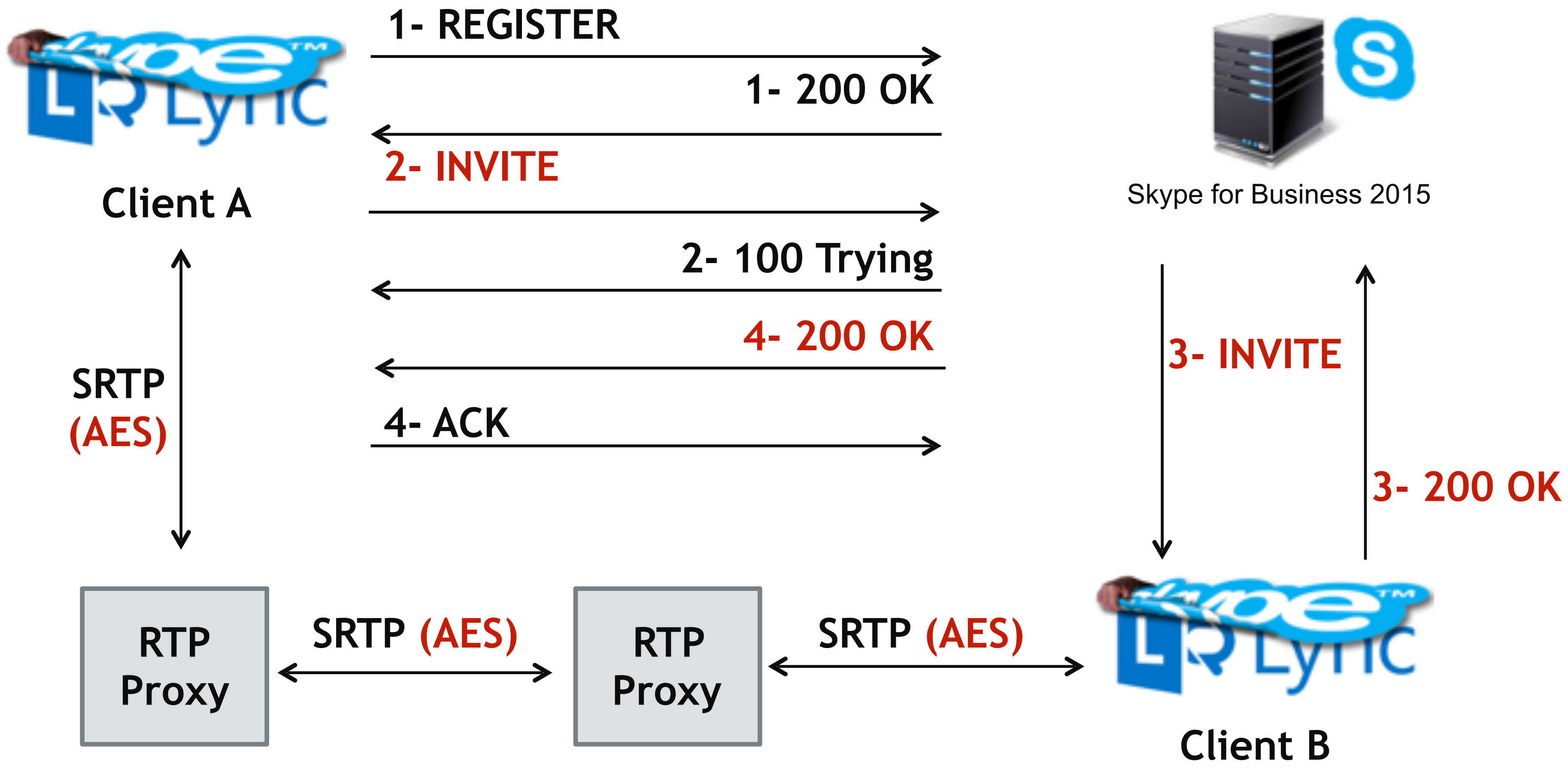
Microsoft Lync

Skype for Business

UC on Skype for Business

- Active Directory, DNS (SRV, NAPTR/Enum) and SSO
- Extensions to the traditional protocols
  - SIP/SIPE, XMPP, OWA/Exchange
  - PSTN mapping to users
  - Device support for IP phones and teleconference systems
  - Mobile services
- Not only for corporate communication
  - Call centres, hosted Lync/Skype services
  - Office 365 online services, federated services

VoIP basics



1- REGISTER

1- 200 OK

2- INVITE

2- 100 Trying

4- 200 OK

4- ACK

Client A

SRTP (AES)

Skype for Business 2015

3- INVITE

3- 200 OK

Client B

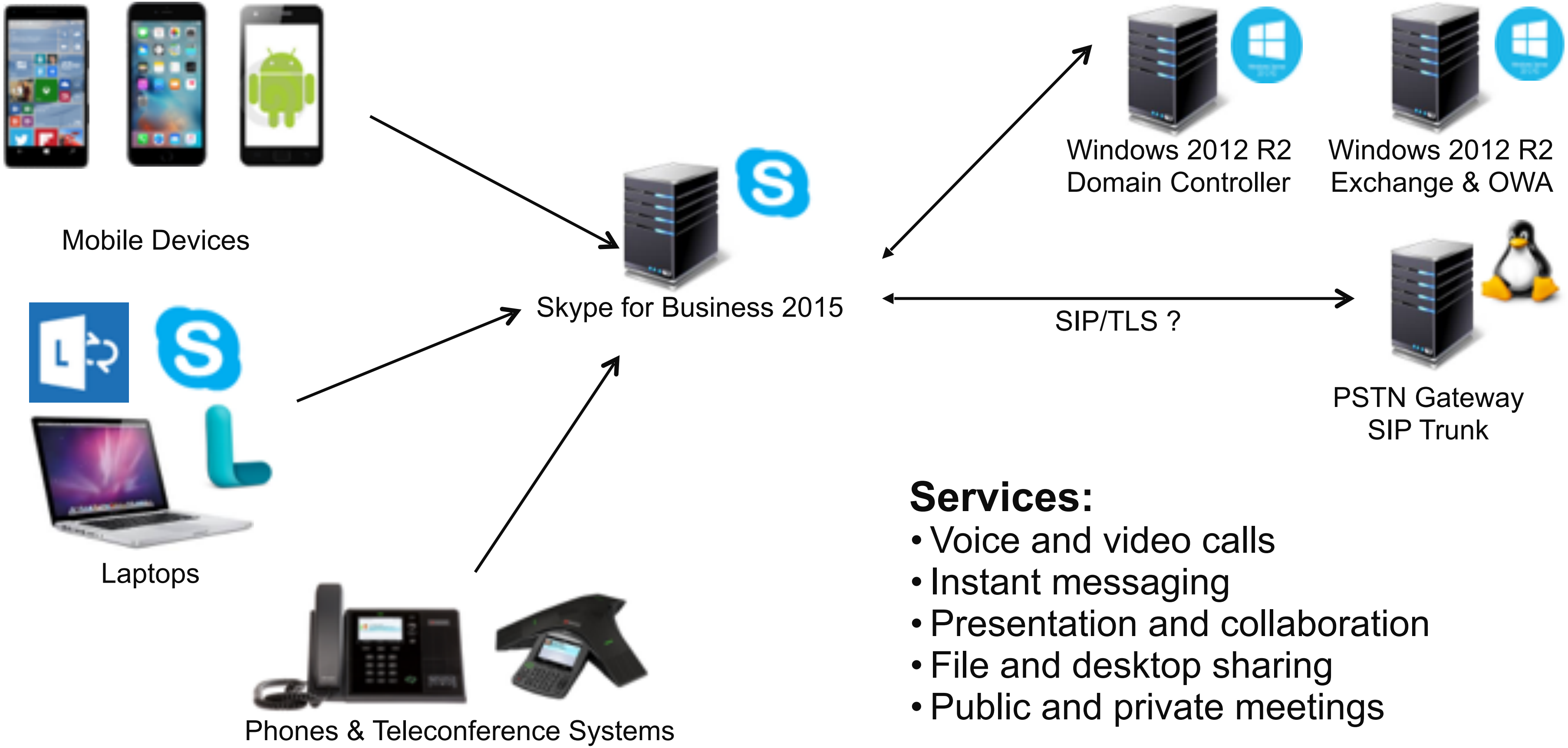
RTP Proxy

SRTP (AES)

RTP Proxy

SRTP (AES)

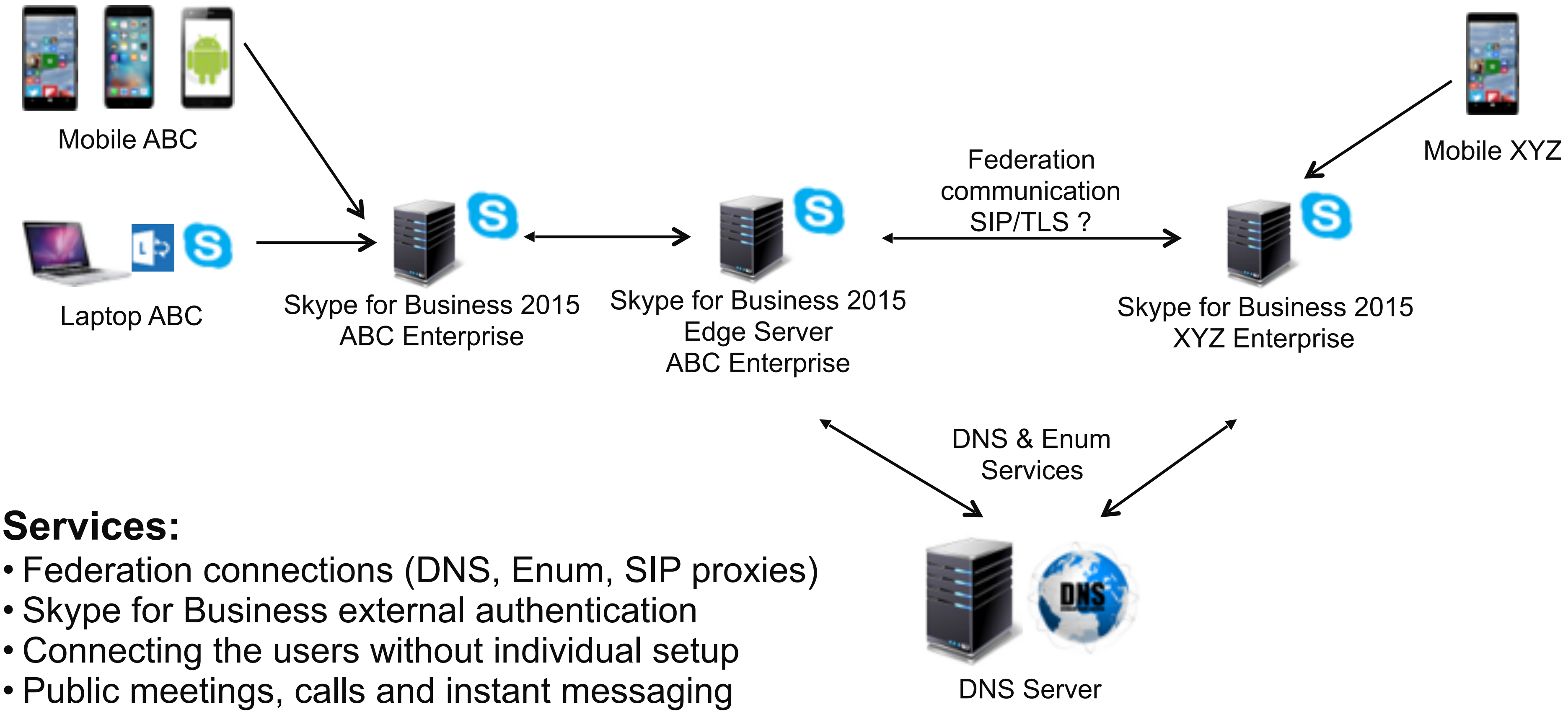
Corporate communication



Services:

- Voice and video calls
- Instant messaging
- Presentation and collaboration
- File and desktop sharing
- Public and private meetings

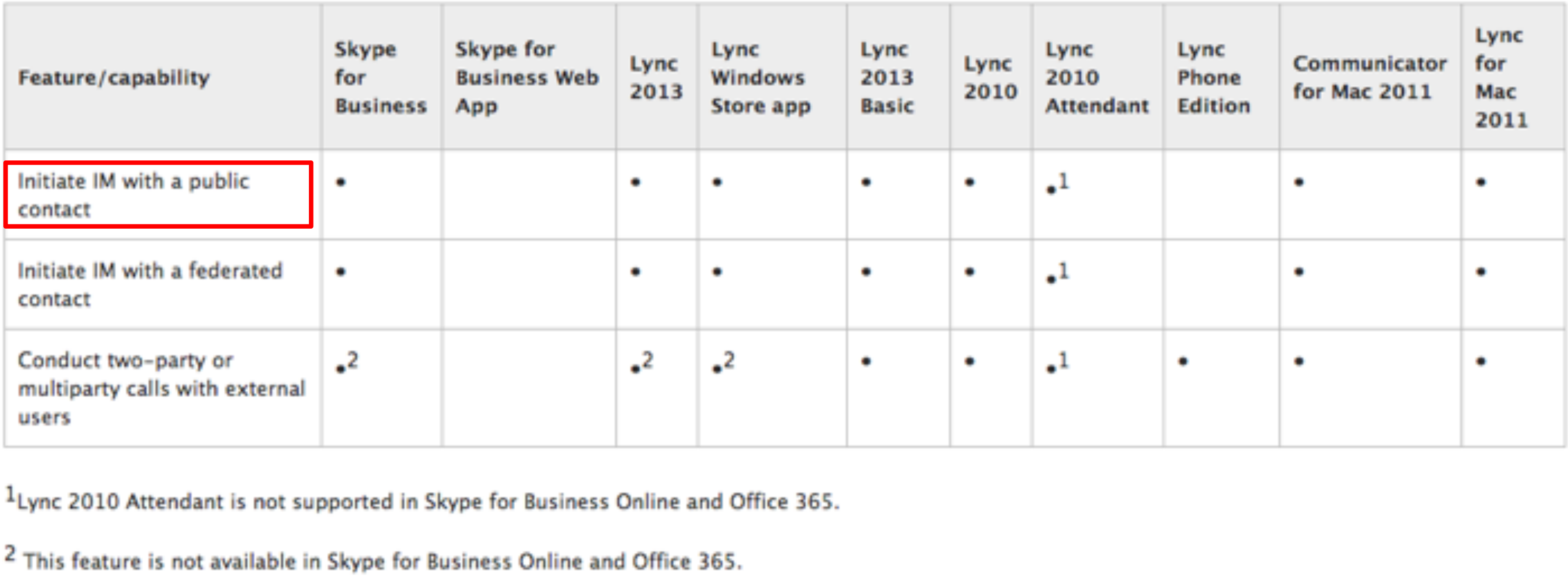
Federated communication



Services:

- Federation connections (DNS, Enum, SIP proxies)
- Skype for Business external authentication
- Connecting the users without individual setup
- Public meetings, calls and instant messaging

Supported client features



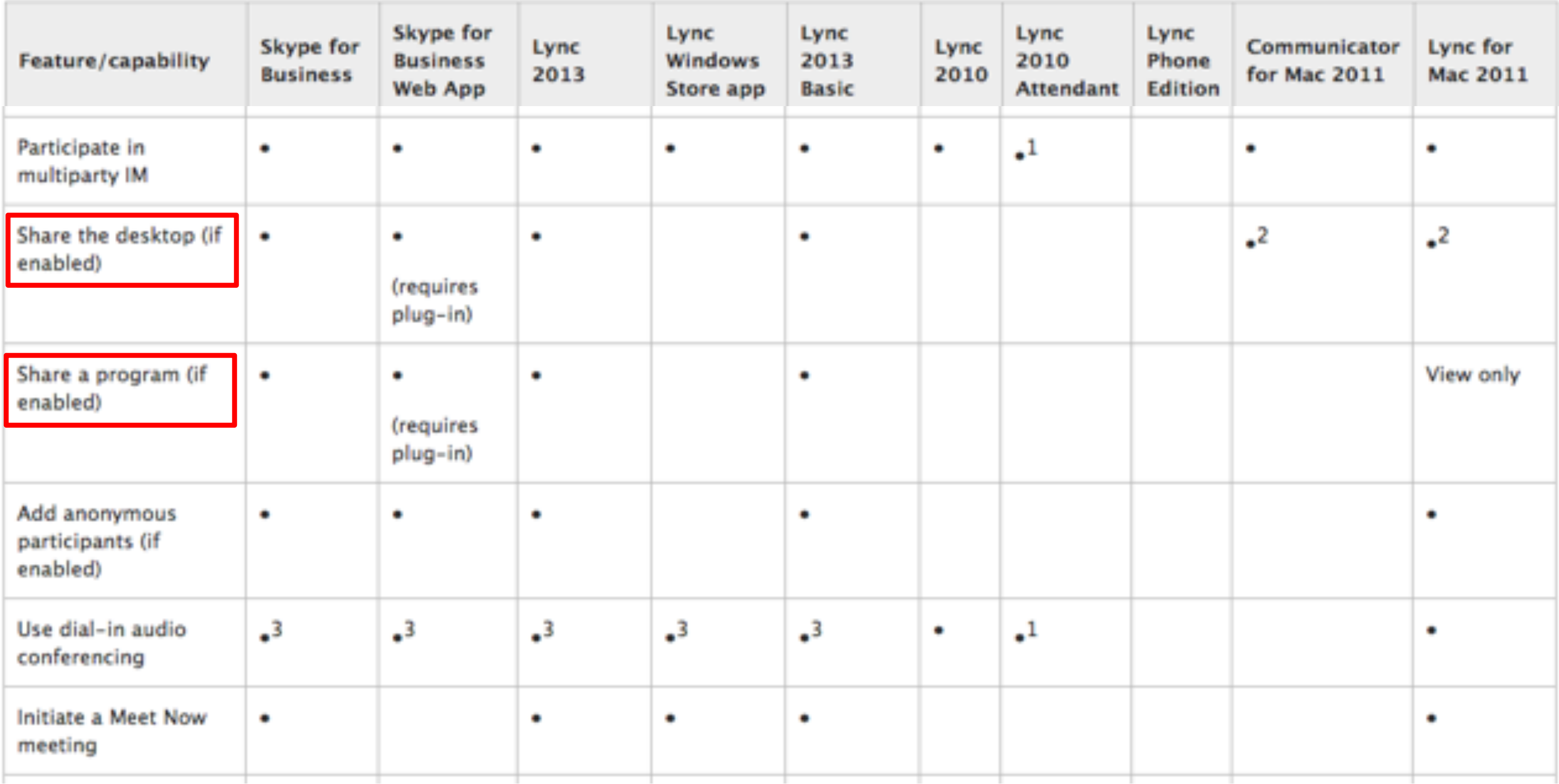
Feature/capability	Skype for Business	Skype for Business Web App	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync 2010	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Initiate IM with a public contact	•		•	•	•	•	•[1]		•	•
Initiate IM with a federated contact	•		•	•	•	•	•[1]		•	•
Conduct two-party or multiparty calls with external users	•[2]		•[2]	•[2]	•	•	•[1]	•	•	•

[1] Lync 2010 Attendant is not supported in Skype for Business Online and Office 365.

[2] This feature is not available in Skype for Business Online and Office 365.

https://technet.microsoft.com/en-au/library/dn933896.aspx

Supported client features



Feature/capability	Skype for Business	Skype for Business Web App	Lync 2013	Lync Windows Store app	Lync 2013 Basic	Lync 2010	Lync 2010 Attendant	Lync Phone Edition	Communicator for Mac 2011	Lync for Mac 2011
Participate in multiparty IM	•	•	•	•	•	•	•[1]		•	•
Share the desktop (if enabled)	•	• (requires plug-in)	•		•				•[2]	•[2]
Share a program (if enabled)	•	• (requires plug-in)	•		•					View only
Add anonymous participants (if enabled)	•	•	•		•					•
Use dial-in audio conferencing	•[3]	•[3]	•[3]	•[3]	•[3]	•	•[1]			•
Initiate a Meet Now meeting	•		•	•	•					•

Give control?

Give control?

https://technet.microsoft.com/en-au/library/dn933896.aspx

Security of Skype for Business

- SIP over TLS is enforced for clients by default
- SRTP using AES is enforced for clients by default
- SIP replay attack protections are used on servers
  - Responses have a signature of the critical SIP headers
  - Content itself and custom headers are not in scope
- Clients validate the server response signatures
- SIP trunks (PSTN gateway) security
  - TLS enabled and IP restricted
  - No authentication support

Research and vulnerabilities related

- Defcon 20 – The end of the PSTN as you know it
  - Jason Ostrom, William Borskey, Karl Feinauer
  - Federation fundamentals, Enumerator, Lyncspoof
- Remote command execution through vulnerabilities on the font and graphics libraries (MS15-080, MS15-044)
- Targeting Microsoft Lync users with malwared Microsoft Office files
- Denial of service and XSS vulnerabilities (MS14-055)

Security testing

- 3 ways to conduct security testing
  - Compliance and configuration analysis
  - MITM analysis (Viproxy 2.0)
  - Using a custom security tester (Viproy 4.0 is coming soon)
- Areas to focus on
  - Identifying design, authentication and authorisation issues
  - Unlocking client restrictions to bypass policies
  - Identifying client and server vulnerabilities
  - Testing business logic issues, dial plans and user rights

Discovering Skype for Business

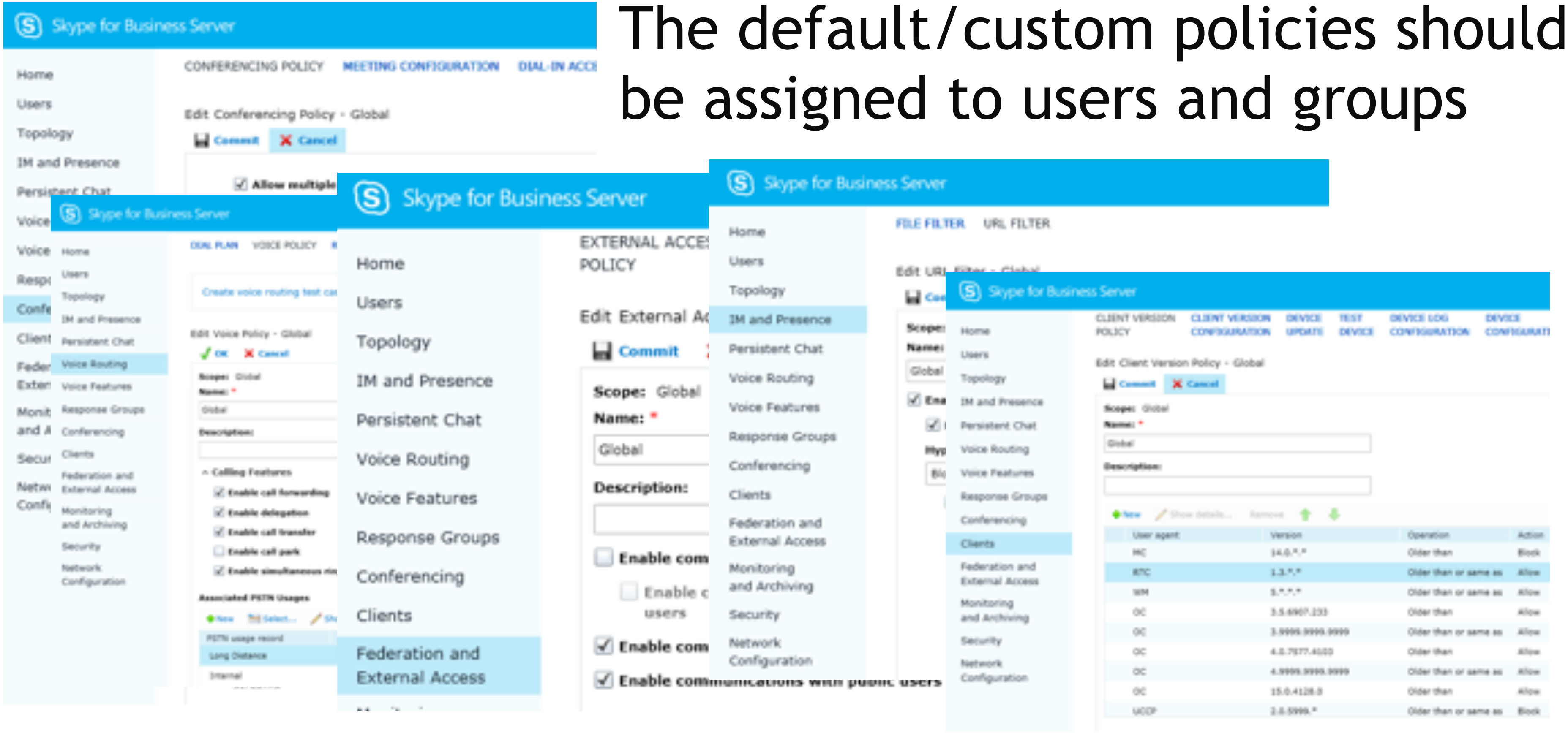
- Autodiscovery features
  - Autodiscovery web services
  - Subdomains and DNS records (SRV, NAPTR)
- Web services
  - Authentication, Webtickets and TLS web services
  - Meeting invitations and components
  - Skype for Business web application
- Active Directory integration
- Information gathering via server errors

Corporate communication policy

- Design of the communication infrastructure
  - Phone numbers, SIP URIs, domains, federations, gateways
- Client type, version and feature enforcements
  - Meeting codes, security, user rights to create meetings
  - Open components such as Skype for Business web app
  - Feature restrictions on clients
  - File, content and desktop sharing restrictions
- User rights (admin vs user)
- Encryption design for signalling and media

Corporate communication policy

The default/custom policies should be assigned to users and groups



Edit Conferencing Policy - Global

☑ Allow multiple

Create voice routing test ca

Edit Voice Policy - Global

Scope: Global

Name: *

Global

Description:

Calling Features

☑ Enable call forwarding

☑ Enable delegation

☑ Enable call transfer

□ Enable call park

☑ Enable simultaneous rin

Associated PSTN Usages

PSTN usage record

Long Distance

Internal

Edit External Ac

Scope: Global

Name: *

Global

Description:

□ Enable com

□ Enable c users

☑ Enable com

☑ Enable communications with public users

Edit URL Filter - Global

Scope:

Name:

Global

☑ Ena

Edit Client Version Policy - Global

Scope: Global

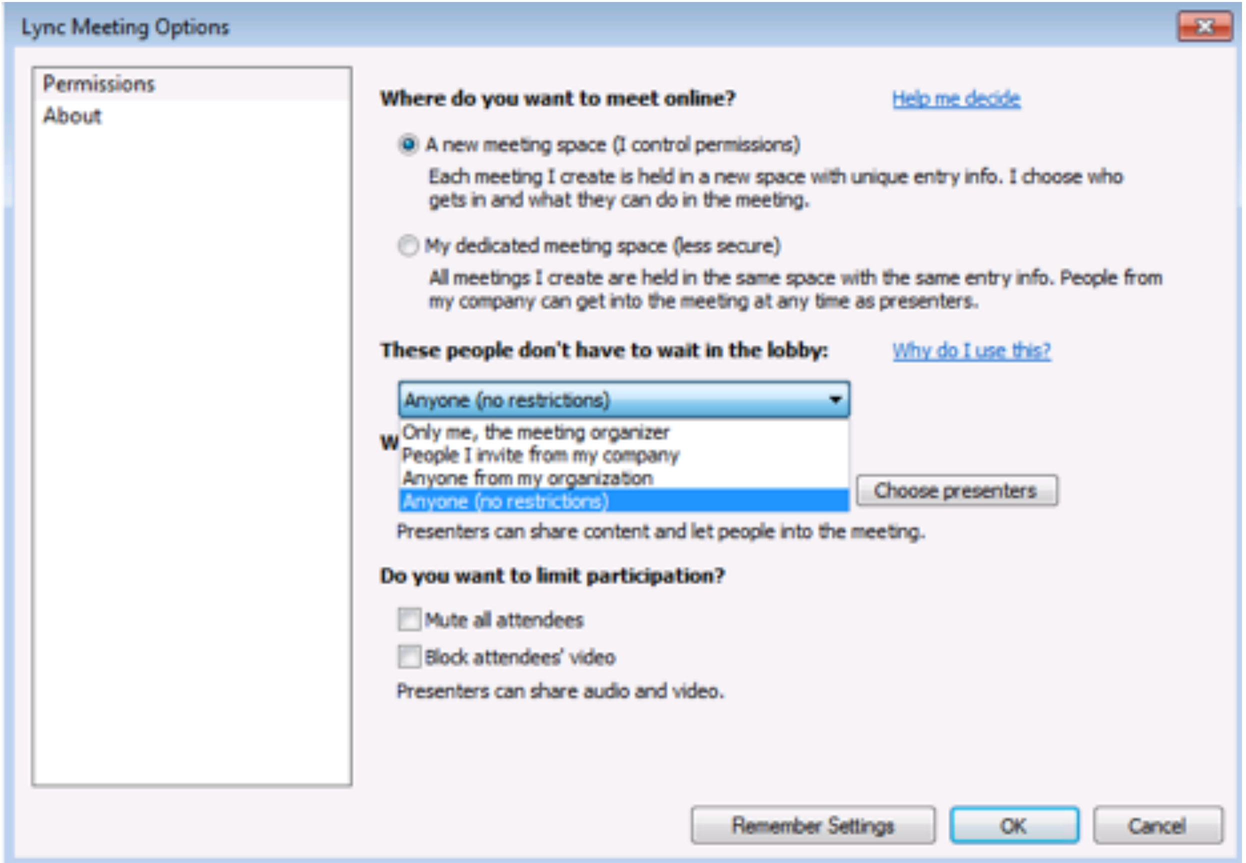
Name: *

Global

Description:

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
OC	4.0.7577.4103	Older than	Allow
OC	4.9999.9999.9999	Older than or same as	Allow
OC	15.0.4128.0	Older than	Allow
UCCP	2.0.5999.*	Older than or same as	Block

Corporate communication policy



Lync Meeting Options

Permissions
About

Where do you want to meet online? Help me decide

● A new meeting space (I control permissions)

Each meeting I create is held in a new space with unique entry info. I choose who gets in and what they can do in the meeting.

○ My dedicated meeting space (less secure)

All meetings I create are held in the same space with the same entry info. People from my company can get into the meeting at any time as presenters.

These people don't have to wait in the lobby: Why do I use this?

Anyone (no restrictions)
- Only me, the meeting organizer
- People I invite from my company
- Anyone from my organization
- Anyone (no restrictions)

W

Choose presenters

Presenters can share content and let people into the meeting.

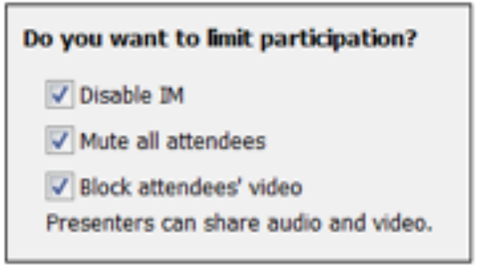
Do you want to limit participation?

□ Mute all attendees

□ Block attendees' video

Presenters can share audio and video.

- Meeting rights to be assigned by users
- Policies assigned are in use



Do you want to limit participation?

☑ Disable IM

☑ Mute all attendees

☑ Block attendees' video

Presenters can share audio and video.

SRTP AES implementation

- SRTP using AES is enforced for clients (No ZRTP)
- SIP/TLS is enforced for clients
- SIP/TLS is optional for SIP trunks and PSTN gateways
  - Compatibility challenges vs Default configuration
  - SIP/TCP gateways may leak the SRTP encryption keys

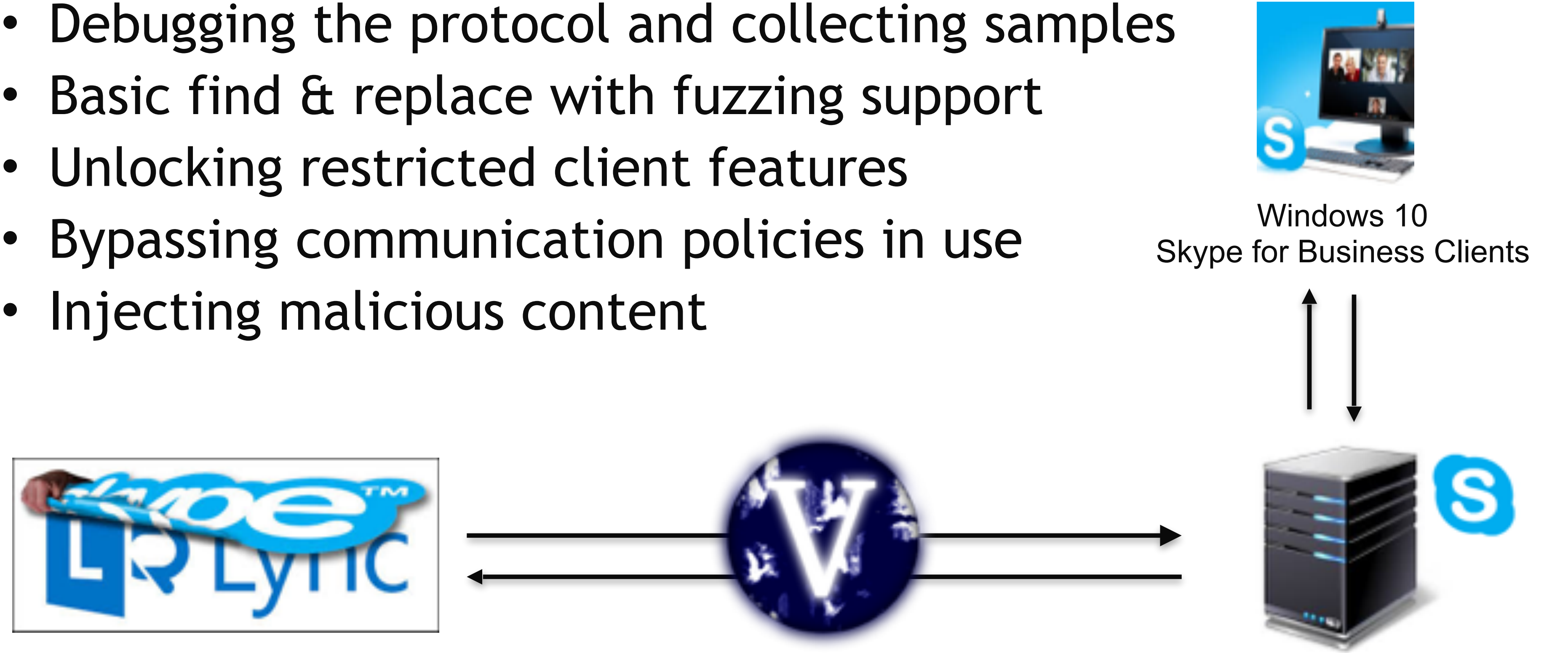
```
a=ice-ufrag:x30M
a=ice-pwd:oW7iYHXiAOr19UH05baO7bMJ
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:Gu
  +c81XctWoAHro7cJ9uN6WqW7QPJndjXfZsofl8|2^31|1:1
```

MITM analysis using Viproxy

- Challenges
  - SIP/TLS is enabled by default
  - Microsoft Lync clients validate the TLS cert
  - Compression is enabled, not easy to read
- Viproxy 2.0
  - A standalone Metasploit module
  - Supports TCP/TLS interception with TLS certs
  - Disables compression
  - Modifies the actions of an official client
  - Provides a command console for real-time attacks

Viproxy test setup

- Debugging the protocol and collecting samples
- Basic find & replace with fuzzing support
- Unlocking restricted client features
- Bypassing communication policies in use
- Injecting malicious content



Windows 10
Skype for Business Clients

MS Lync for Mac 2011
Client to be used for attacks

Viproxy 2.0

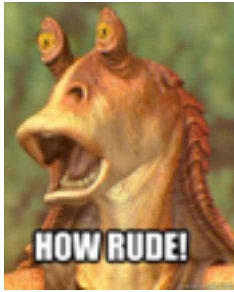
Windows 2012 R2
Skype for Business 2015 Server

Analysing the corporate policy

- Instant Messaging (IM) restrictions
  - File type filters for the file transfers
  - URL filters for the messaging
  - Set-CsClientPolicy (DisableEmoticons, DisableHtmlIm, DisableRTFIm)
- Call forwarding rights
- Meeting rights
  - Federated attendees
  - Public attendees
  - Clients’ default meeting settings
- Insecure client versions allowed

Attack surfaces on IM and calls

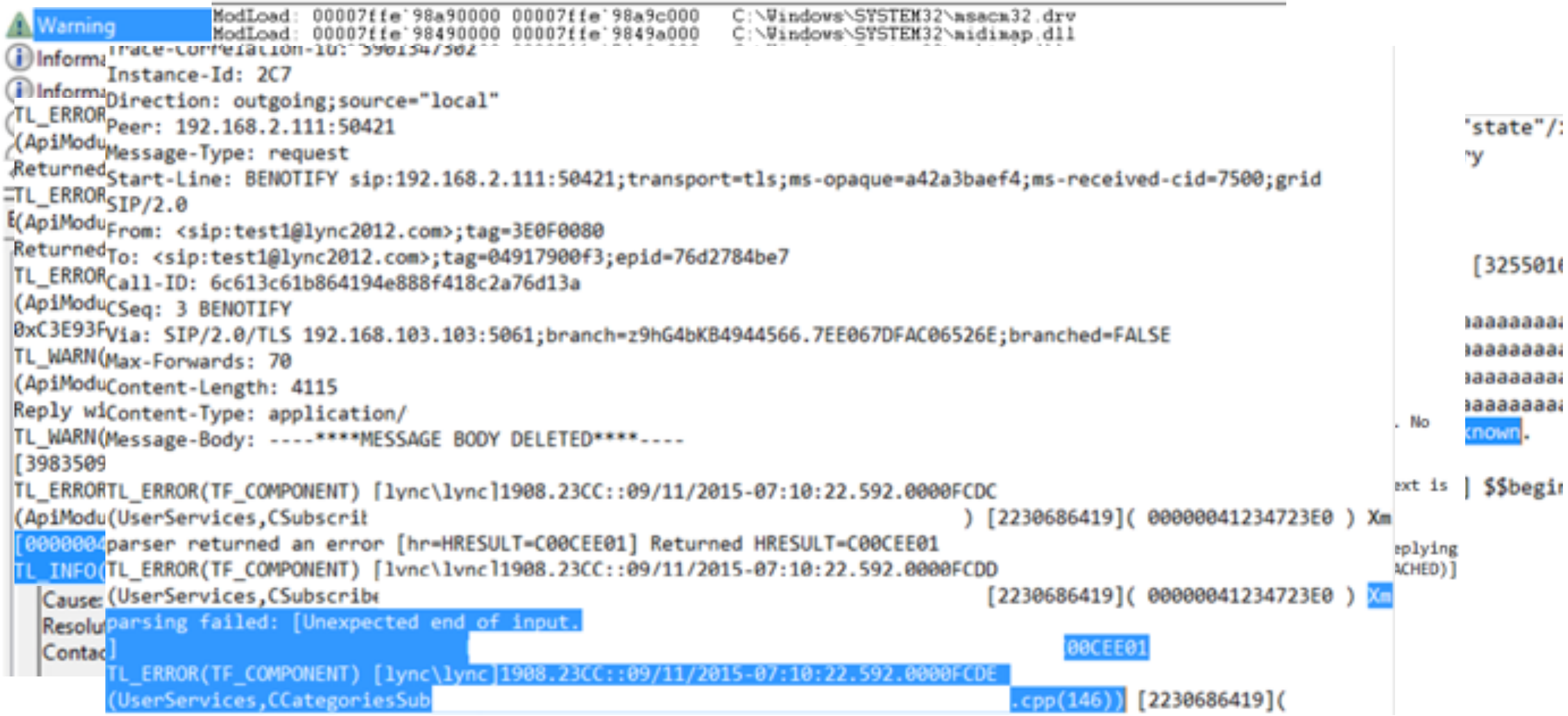
- Various content types (HTML, JavaScript, PPTs)
- File, desktop and presentation sharing
- Limited filtering options (IIMFilter)
  - File Filter (e.g. exe, xls, ppt, psh)
  - URL Filter (e.g. WWW, HTTP, call, SIP)
  - Set-CsClientPolicy (DisableHtmlIm, DisableRTFIm)
- Clients process the content before invitation
  - Presence and update messages
  - Call and IM invitation requests
  - Mass compromise via meetings and multiple endpoints



How Skype for Business sees VoIP

- Custom SIP extensions
- XML based INVITE and SUBSCRIBE content
- HTML/Javascript based messaging (IM)
- Instant and unusual disconnects
- C# and C++ combination for apps
- File and desktop sharing through RTP sessions

Parsing errors and exceptions



```
ModLoad: 00007ffe`98a90000 00007ffe`98a9c000   C:\Windows\SYSTEM32\msacm32.drv
ModLoad: 00007ffe`98490000 00007ffe`9849a000   C:\Windows\SYSTEM32\midimap.dll
```

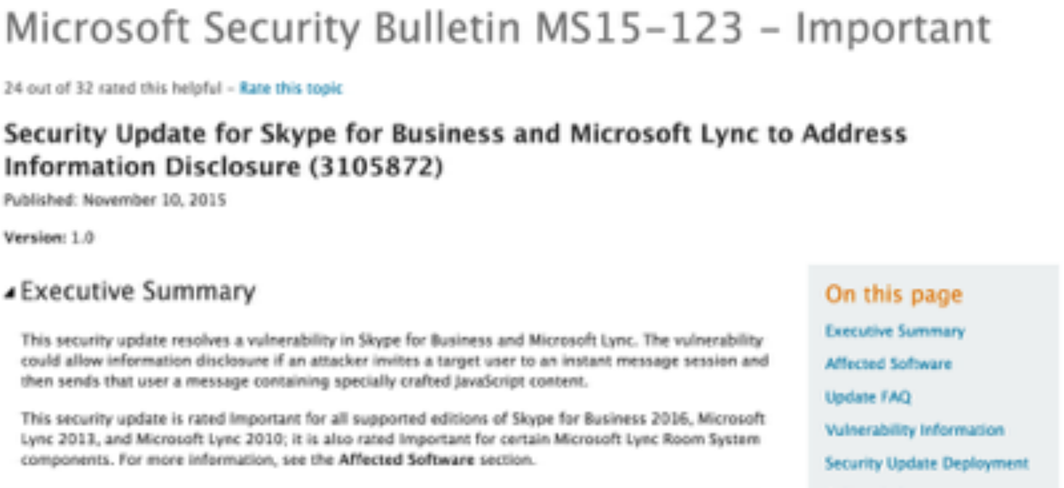
```
Trace-Correlation-Id: 3961347362
Instance-Id: 2C7
Direction: outgoing;source="local"
Peer: 192.168.2.111:50421
Message-Type: request
Start-Line: BENOTIFY sip:192.168.2.111:50421;transport=tls;ms-opaque=a42a3baef4;ms-received-cid=7500;grid
SIP/2.0
From: <sip:test1@lync2012.com>;tag=3E0F0080
To: <sip:test1@lync2012.com>;tag=04917900f3;epid=76d2784be7
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/
Message-Body: ----****MESSAGE BODY DELETED****----

TL_ERROR(TF_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDC
(UserServices,CSubscrit                                        ) [2230686419]( 00000041234723E0 ) Xm
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,CSubscribe                                        [2230686419]( 00000041234723E0 ) Xm
parsing failed: [Unexpected end of input.
]                                                          00CEE01
TL_ERROR(TF_COMPONENT) [lync\lync]1908.23CC::09/11/2015-07:10:22.592.0000FCDE
(UserServices,CCategoriesSub                                   .cpp(146)) [2230686419](
```

Microsoft security advisories

CVE-2015-6061 (MS15-123)

Impact:

- Unauthorised script execution
- Security bypass



Microsoft Security Bulletin MS15-123 – Important

24 out of 32 rated this helpful - Rate this topic

Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)

Published: November 10, 2015

Version: 1.0

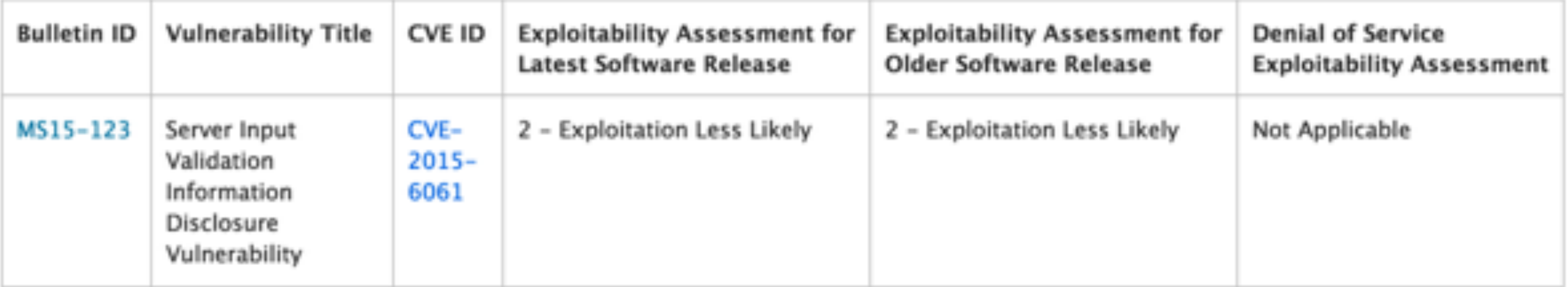
Executive Summary

This security update resolves a vulnerability in Skype for Business and Microsoft Lync. The vulnerability could allow information disclosure if an attacker invites a target user to an instant message session and then sends that user a message containing specially crafted JavaScript content.

This security update is rated Important for all supported editions of Skype for Business 2016, Microsoft Lync 2013, and Microsoft Lync 2010; it is also rated Important for certain Microsoft Lync Room System components. For more information, see the **Affected Software** section.

On this page

- Executive Summary
- Affected Software
- Update FAQ
- Vulnerability Information
- Security Update Deployment
- Acknowledgments
- Disclaimer
- Revisions



Bulletin ID	Vulnerability Title	CVE ID	Exploitability Assessment for Latest Software Release	Exploitability Assessment for Older Software Release	Denial of Service Exploitability Assessment
MS15-123	Server Input Validation Information Disclosure Vulnerability	CVE-2015-6061	2 - Exploitation Less Likely	2 - Exploitation Less Likely	Not Applicable

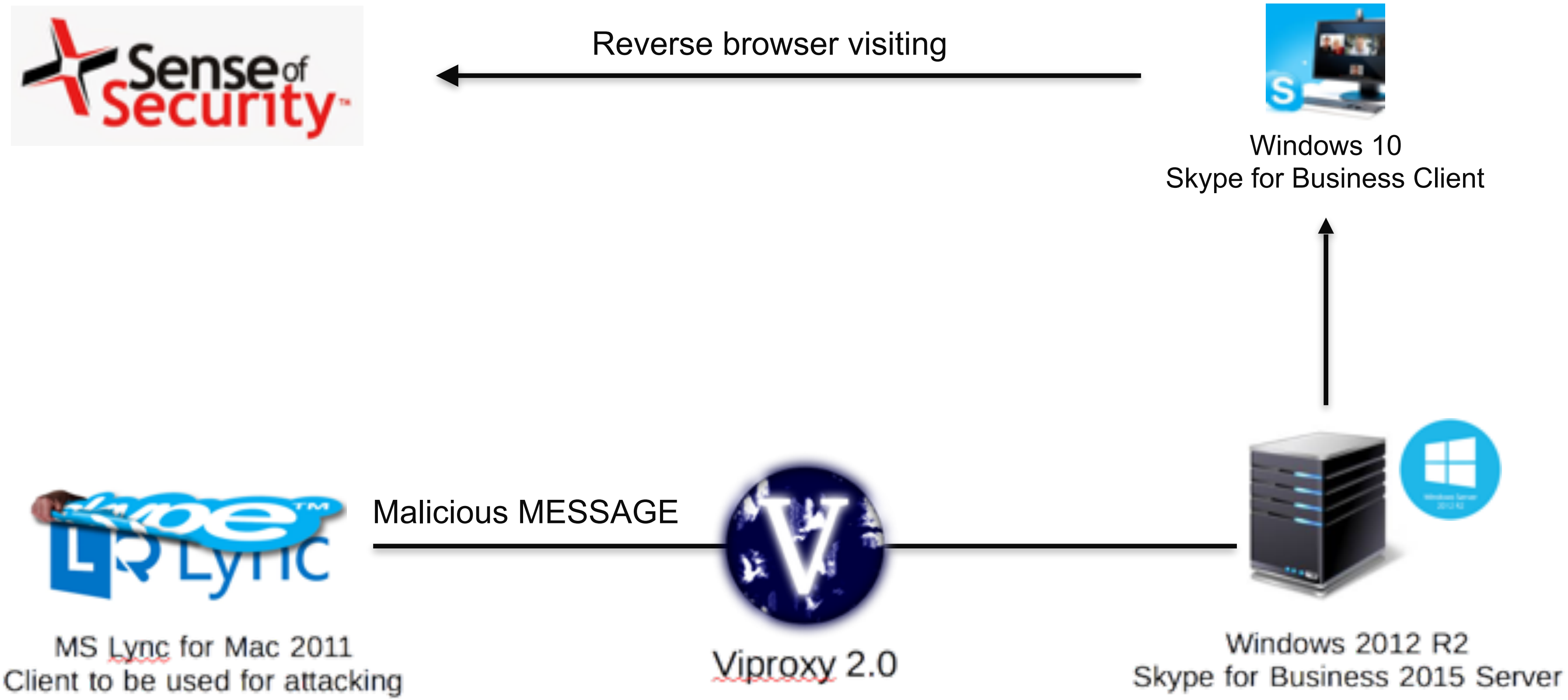
https://technet.microsoft.com/en-us/library/security/ms15-123.aspx
https://support.microsoft.com/en-us/kb/3105872

Bypassing URL filter in IM

IM URL filter for Microsoft Skype for Business 2015 (Microsoft Lync 2013) server can be bypassed with content obfuscation

```
<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>
```

URL filter bypass



Reverse browser visiting

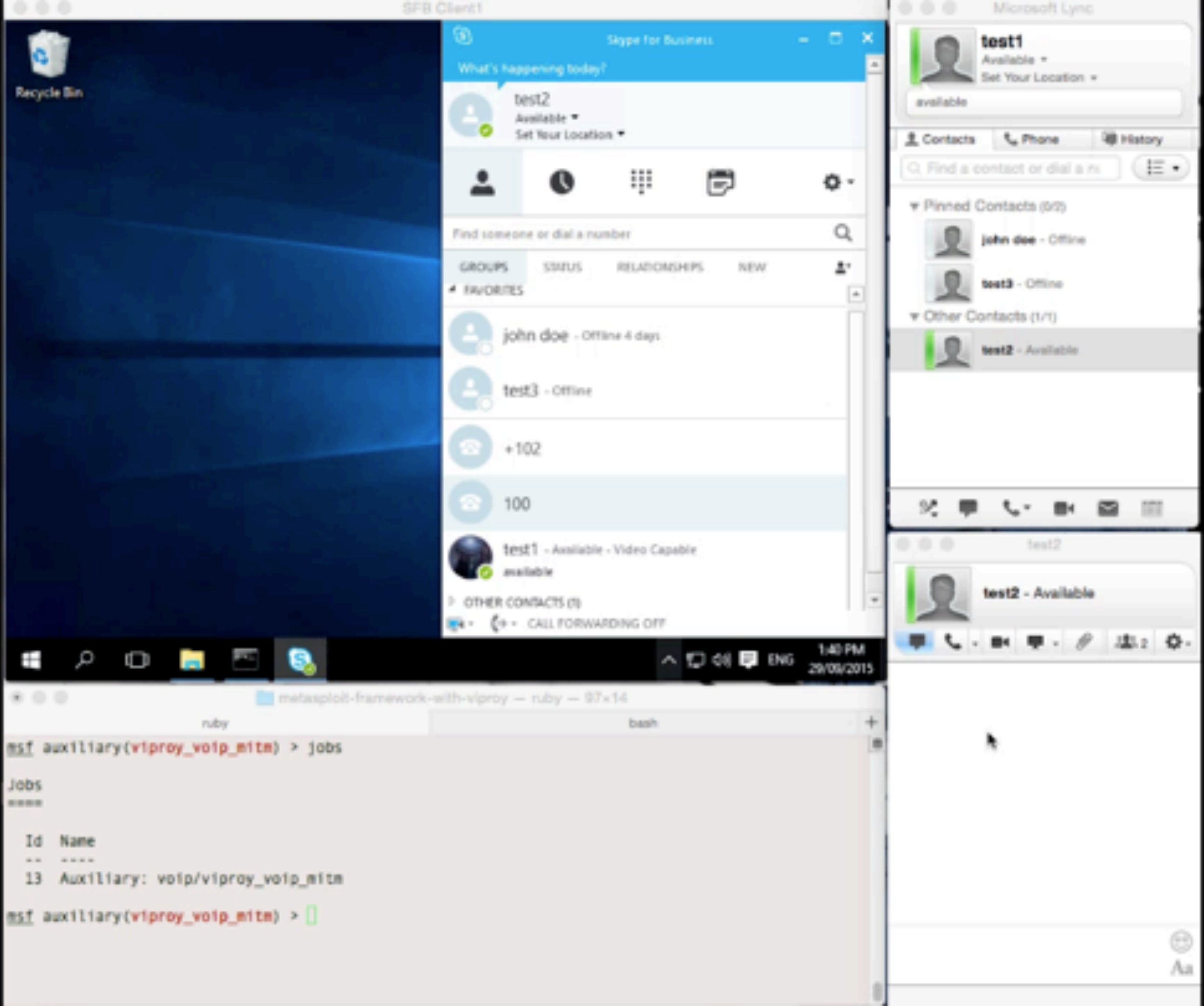
Windows 10
Skype for Business Client

Malicious MESSAGE

MS Lync for Mac 2011
Client to be used for attacking

Viproxy 2.0

Windows 2012 R2
Skype for Business 2015 Server



```
msf auxiliary(viproy_voip_mitm) > jobs

Jobs
====

  Id  Name
  --  ----
  13  Auxiliary: voip/viproy_voip_mitm

msf auxiliary(viproy_voip_mitm) > 
```

Sending INVITEs w/ HTML/XSS

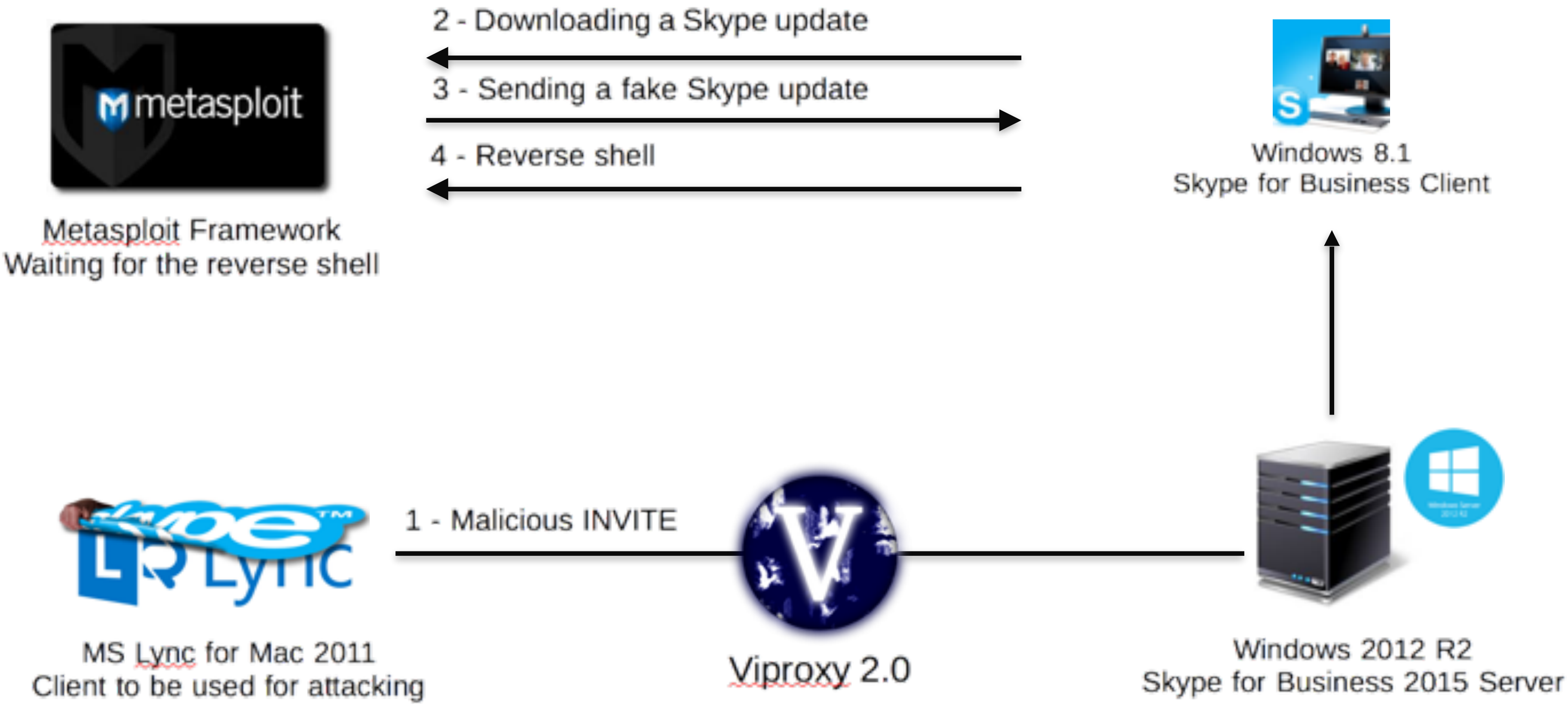
Microsoft Skype for Business 2015 (Microsoft Lync 2013) client executes HTML and JavaScript content in the SIP INVITE request headers without user interaction

- No user interaction required

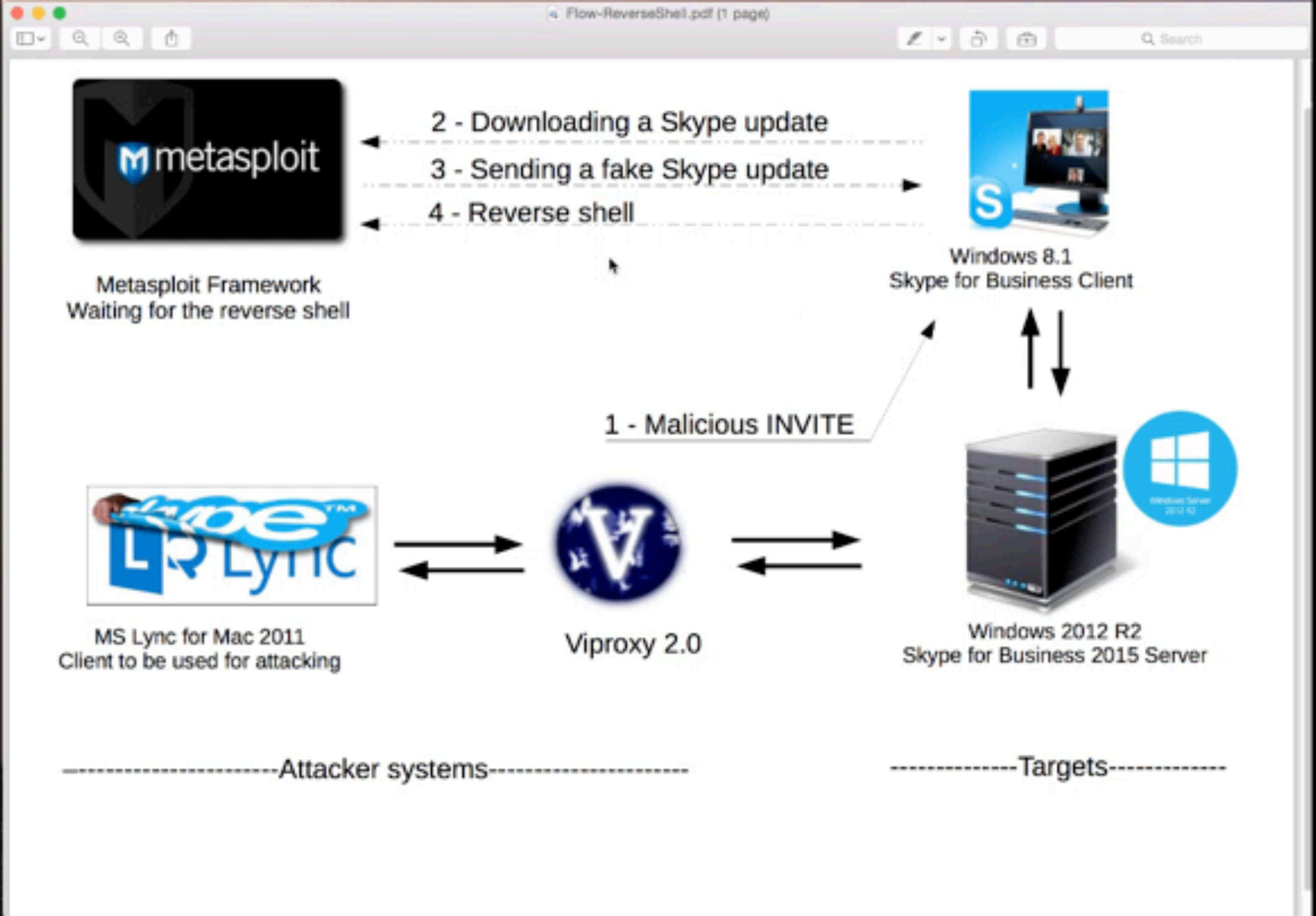
```
Ms-IM-Format: text/html; charset=UTF-8; ms-
body=PHNjcmlwdD53aW5kb3cubG9jYXRpb249Imh0dHA6Ly93d3cuc2Vuc2VvZnNlY3VyaXR5LmNvbS5hdSI8L3NjcmlwdD4K
```

```
Base64 decode: <script>window.location=“http://www.senseofsecurity.com.au"</script>
```

Fake Skype update via INVITE



2 - Downloading a Skype update
3 - Sending a fake Skype update
4 - Reverse shell
metasploit
Metasploit Framework
Waiting for the reverse shell
Windows 8.1
Skype for Business Client
1 - Malicious INVITE
Lync
MS Lync for Mac 2011
Client to be used for attacking
Viproxy 2.0
Windows 2012 R2
Skype for Business 2015 Server



2 - Downloading a Skype update

3 - Sending a fake Skype update

4 - Reverse shell

Metasploit Framework
Waiting for the reverse shell

Windows 8.1
Skype for Business Client

1 - Malicious INVITE

MS Lync for Mac 2011
Client to be used for attacking

Viproxy 2.0

Windows 2012 R2
Skype for Business 2015 Server

-----------------------Attacker systems---------------------

-------------Targets------------

Multi endpoint communication

- Meeting requests
  - Private meetings, Open meetings, Web sessions
- Multi callee invitations and messages
  - Attacks do not need actions from the attendees/callees
- Injecting endpoints to the requests
  - XML conference definitions in the INVITE requests
  - INVITE headers
  - Endpoint headers
- 3rd party SIP trunk, PSTN gateway or federation

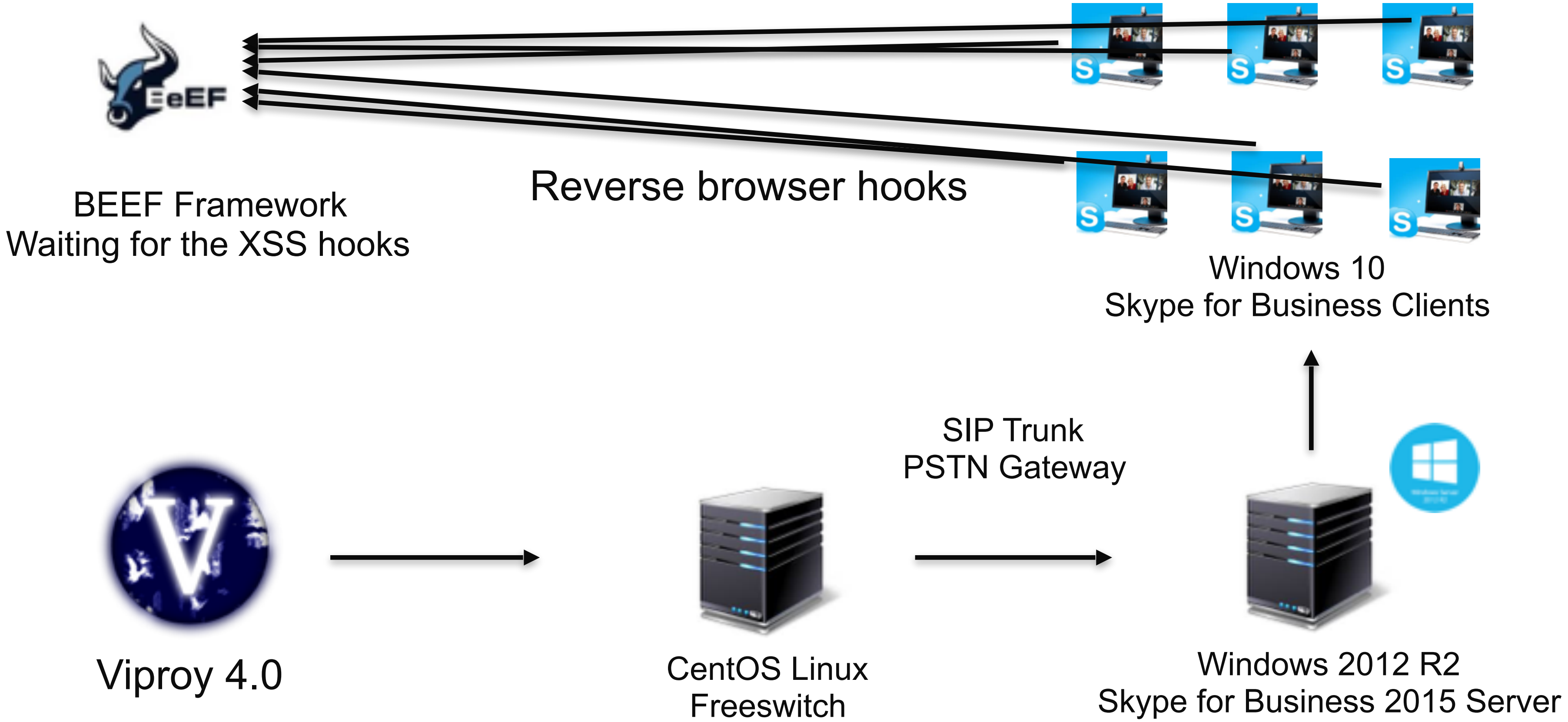
Sending messages w/ HTML/XSS

Microsoft Skype for Business 2015 (Microsoft Lync 2013) client executes HTML and JavaScript content in the SIP MESSAGE requests without user interaction

- No user interaction required

```
Content-type: text/html

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

Mass compromise of clients



BEEF Framework
Waiting for the XSS hooks

Reverse browser hooks

Windows 10
Skype for Business Clients

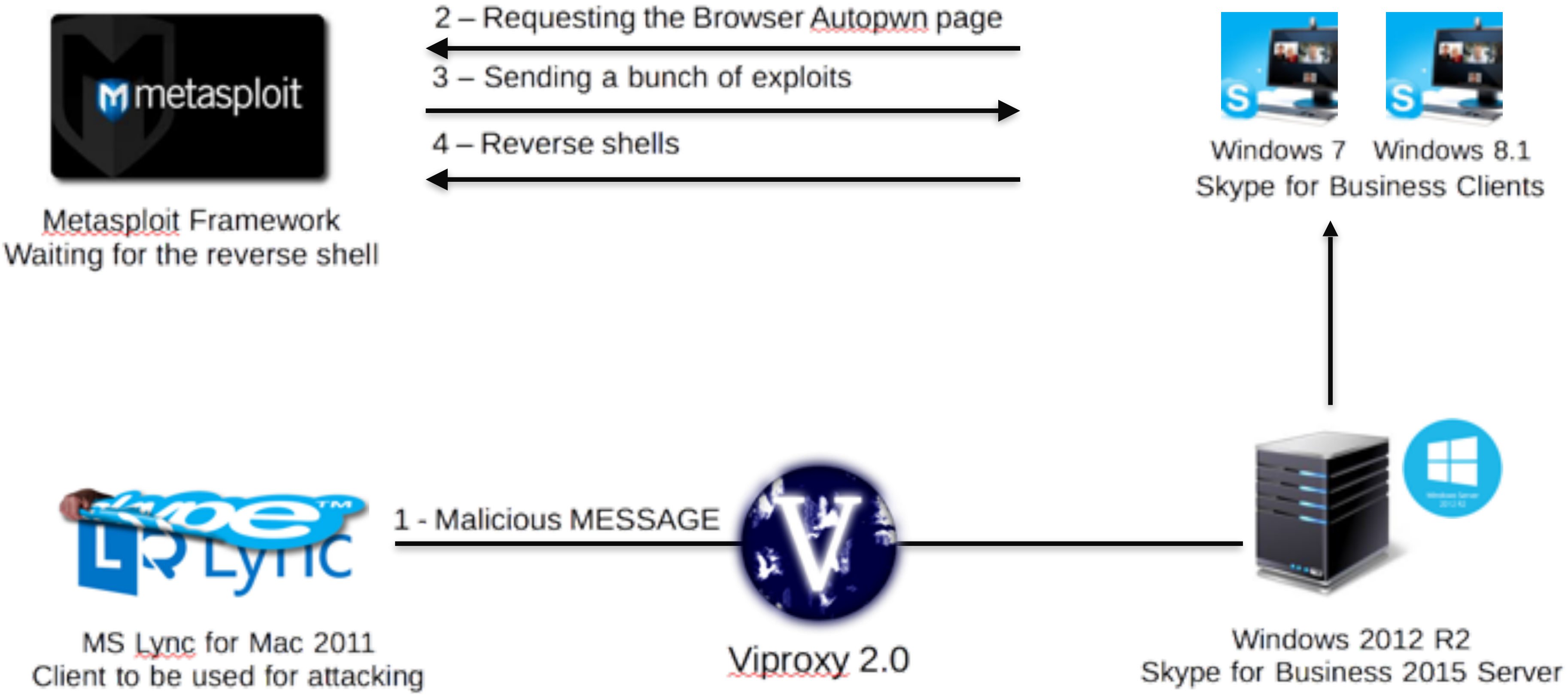
SIP Trunk
PSTN Gateway

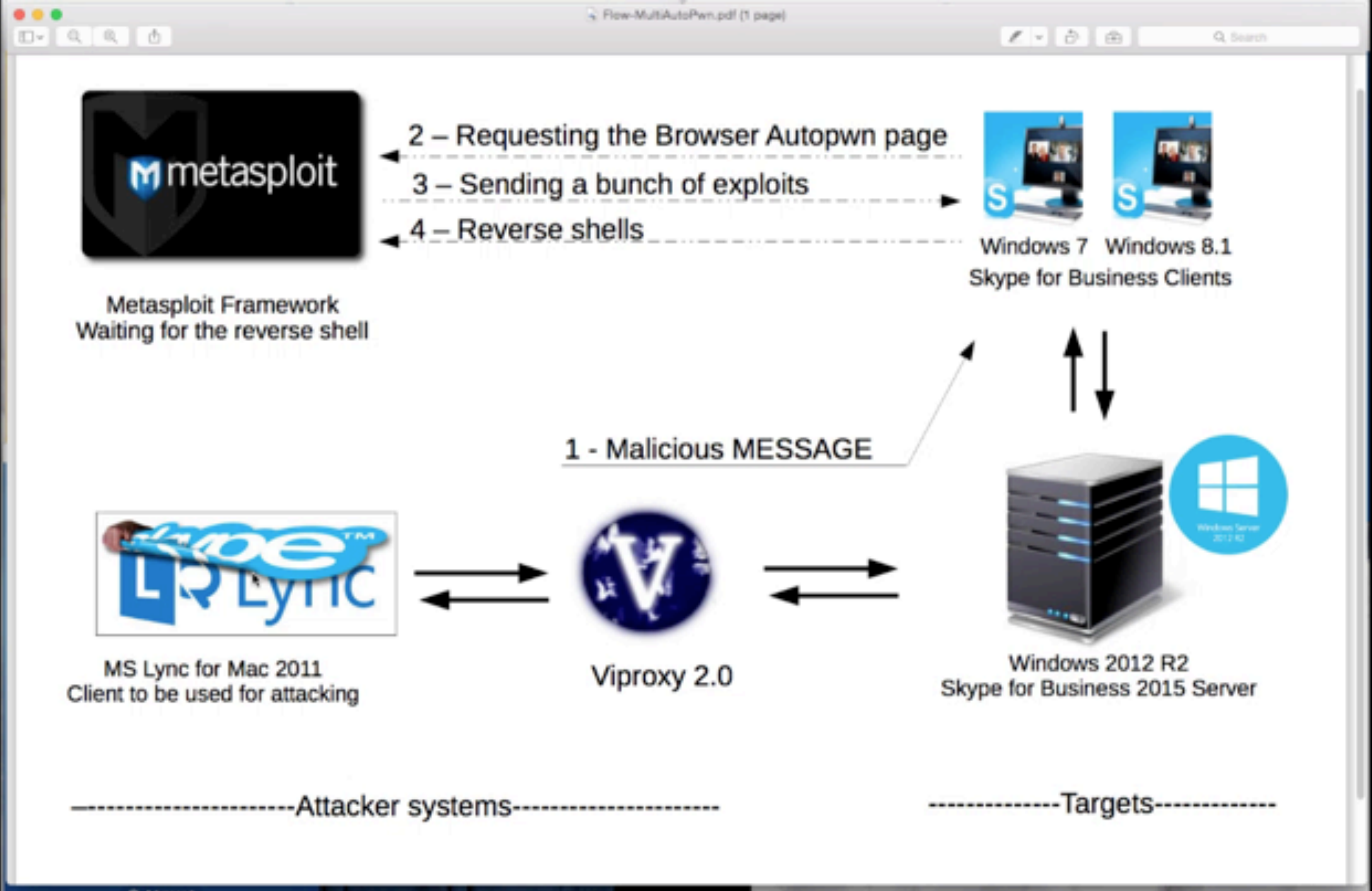
Viproy 4.0

CentOS Linux
Freeswitch

Windows 2012 R2
Skype for Business 2015 Server

Mass compromise of clients


2 – Requesting the Browser Autopwn page
3 – Sending a bunch of exploits
4 – Reverse shells
metasploit
Metasploit Framework
Waiting for the reverse shell
Windows 7
Windows 8.1
Skype for Business Clients
1 - Malicious MESSAGE
MS Lync for Mac 2011
Client to be used for attacking
Viproxy 2.0
Windows 2012 R2
Skype for Business 2015 Server



2 – Requesting the Browser Autopwn page

3 – Sending a bunch of exploits

4 – Reverse shells

Metasploit Framework
Waiting for the reverse shell

Windows 7 Windows 8.1
Skype for Business Clients

1 - Malicious MESSAGE

MS Lync for Mac 2011
Client to be used for attacking

Viproxy 2.0

Windows 2012 R2
Skype for Business 2015 Server

---------------------Attacker systems---------------------

-------------Targets------------

Second stage of the research

Analysis of

- mobile clients and SFB web app
- SFB meeting security and public access
- federation security and trust analysis

- Further analysis of the crashes and parsing errors identified for exploitation
- Social engineering templates for Viproxy and Viproy
- Viproy 4.0 with Skype for Business authentication, fuzzing and discovery support

Securing Unified Communications

Secure design is always the foundation

- Physical security of endpoints (e.g. IP phones, teleconference rooms) should be improved
- Networks should be segmented based on their trust level
- Authentication and encryption should be enabled
- Protocol vulnerabilities can be fixed with secure design
- Disable unnecessary IM, call and meeting features
- Software updates should be reviewed and installed

Black Hat Sound Bytes

- Microsoft Skype for Business 2015 is the next-generation Unified Communications system, though it still has legacy vulnerabilities and design issues.
- There are new security testing tools to test it with new vulnerabilities and techniques which are Viproxy and Viproy.
- Secure design is the foundation for securing Unified Communications, and it reduces the attack surfaces.

Previously on VoIP Wars

VoIP Wars I: Return of the SIP (Defcon, Cluecon, Ruxcon, Athcon)

- Modern VoIP attacks via SIP services explained
- SIP trust hacking, SIP proxy bounce attack and attacking mobile VoIP clients demonstrated
- https://youtu.be/d6cGlTB6qKw

VoIP Wars II : Attack of the Cisco phones (Defcon, Blackhat USA)

- 30+ Cisco HCS vulnerabilities including 0days
- Viproy 2.0 with CUCDM exploits, CDP and Skinny support
- Hosted VoIP security risks and existing threats discussed
- https://youtu.be/hqL25srtoEY

The Art of VoIP Hacking Workshop (Defcon, Troopers, AusCERT, Kiwicon)

- Live exploitation exercises for several VoIP vulnerabilities
- 3 0day exploits for Vi-vo and Boghe VoIP clients
- New Viproy 3.7 modules and improved features
- https://www.linkedin.com/pulse/art-voip-hacking-workshop-materials-fatih-ozavci

References

Viproy VoIP Penetration and Exploitation Kit

Author	: http://viproy.com/fozavci
Homepage	: http://viproy.com
Github	: http://www.github.com/fozavci/viproy-voipkit

VoIP Wars : Attack of the Cisco Phones

https://youtu.be/hqL25srtoEY

VoIP Wars : Return of the SIP

https://youtu.be/d6cGlTB6qKw

https://www.senseofsecurity.com.au/aboutus/careers

Questions

Thank you

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au