

VoIP Wars: Destroying Jar Jar Lync

Fatih Ozavci

25 October 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



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

RPOR
TARG
TELN
VHOS

msf aux

```
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 0x35d13de 89986014  
r3 0xa86b6 609846  
r4 0x11fd214 18862612  
r5 0xeeb58 977744  
r6 0x11fd214 18862612  
r7 0x35d11a8 89985448  
r8 0x9cfd10 10288400  
r9 0x0 0  
r10 0x9d0914 10291476  
r11 0x35d1b98 89987992  
r12 0xdf450 914512  
sp 0x35d11a8 89985448  
lr 0x122e1 74465  
pc 0x327bc26c 846971508  
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.  
perform Trust Sweep  
oncurrent threads  
econds to wait for new d
```

73-8521-02 Rev.A9

Speaker Power

```
ion completed  
usage) > |  
*) Display name: 2000 |  
*) Line is open for Call Forward to 1811
```

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

To 701 yes Destination Number at Target SIP Server

- 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

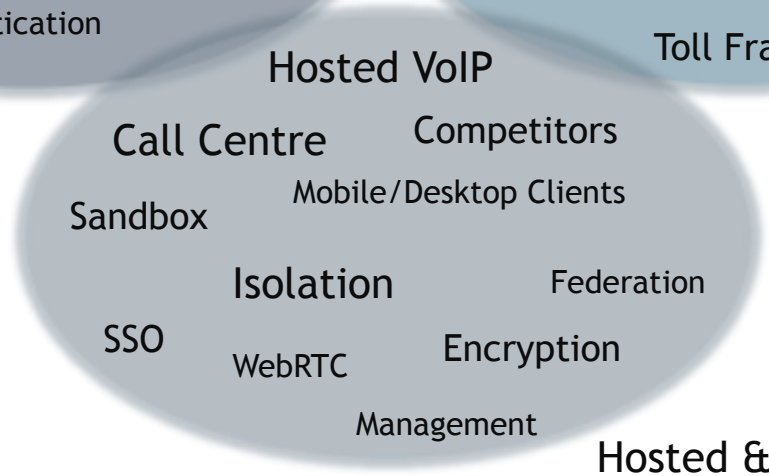
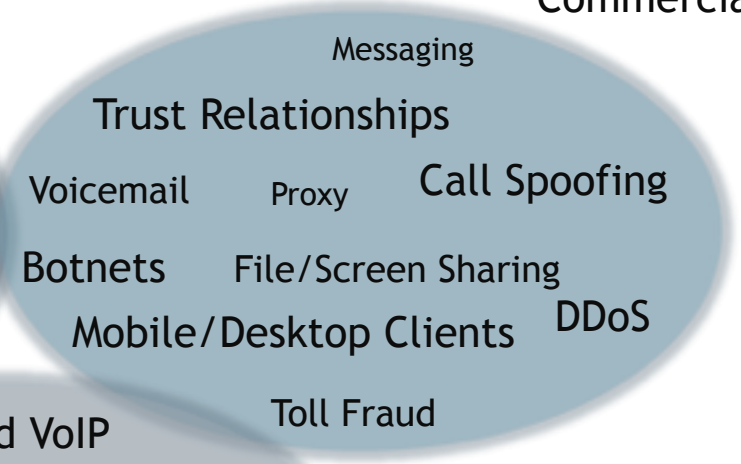
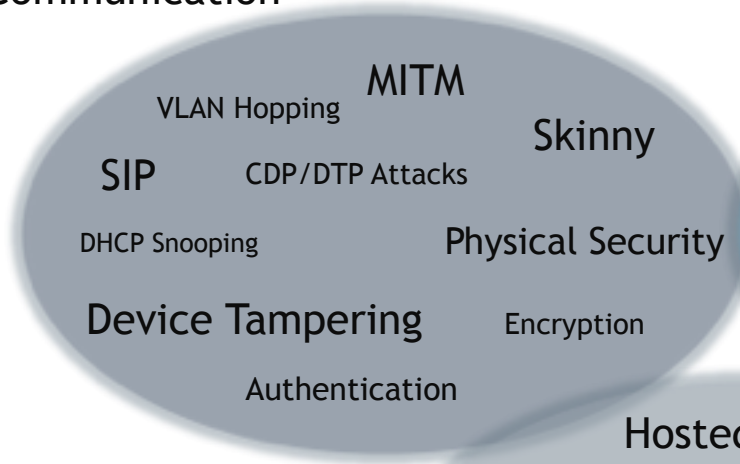


loading...

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
 - CVE-2015-6061, CVE-2015-6062, CVE-2015-6063

Corporate Communication

Commercial Services



Hosted & Distributed Networks

Voice hackers: Legal career 'hit by wiretapping'

the guardian
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'Connell
theguardian.com, Friday 6 June 2014 05:12 AEST



David Butler sounded like a headteacher, according to a member of staff from Monday's Recruitment Agency, the court heard. Photograph: Mark Thomas/PA
Milly Dowler's voicemails would have been deleted automatically after they were hacked by the News of the World, the Old Bailey jury has heard.

authentication

28 Jul 2015 at 11:22, Simon Rockman

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

The A
ComputerWeekly.com



Th
se
By Simon
Share

RELE
STORIE

We'd switch mobile net but we can't be bothered - survey

The costs mount up as organisational attacks in

Australian government access smartmobs but don't

Forbes Your Secret Weapon in Business: Culture Active on LinkedIn
Data Center



Marc Weber Tobias
Contributor

FOLLOW

I am an investigative attorney and physical security specialist.
Full bio →

Opinions expressed by Forbes Contributors are their own.



without permission, but one of the strange things about it all is that at no stage have



It's Too Easy To Hack Voice Mail

TECH | 7/25/2011 @ 12:32PM | 9,228 views
Comment Now Follow Comments

While there's been [extensive coverage](#) of the [News Corp.](#) phone hacking [cases](#) during the past few weeks, nobody has really addressed two relevant elements of the story: the legal liability (both criminal and civil) for such conduct and the underlying problem which allowed the media to gain access to confidential information: the insecurity of most voice mail systems.



Image by apDuchamp via Flickr

All voice mail platforms, regardless of vendor, are simply stored digital information systems. The law makes little distinction between emails and digital voice messages; they are both stored for later retrieval.

In the United States, the Wiretapping Act, found in [Title II](#) of the [Electronic Communications Privacy Act of 1986 \(ECPA\)](#), makes it illegal to intercept aural communications except with a Court order or where there is consent by or both parties to the communications (depending upon the [state law of the applicable jurisdiction](#)).

24 Apr 2014 at 12:34, Simon Rockman
Social media icons



Microsoft Live Communications 2005

Microsoft Office Communicator 2007

Microsoft Lync 2000 - 2013

Microsoft Skype for Business 2015



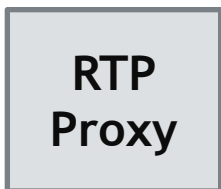
- Active Directory, DNS (SRV, NAPTR/Enum) and SSO
- Extensions to the traditional protocols
 - SIP/SIPE, XMPP, OWA/Exchange
 - PSTN mapping to users
 - Device support for IP phones and teleconference systems
 - Mobile services
- Not only for corporate communication
 - Call centres, hosted Lync/Skype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



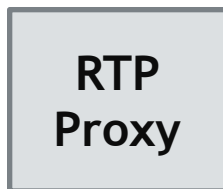


Client A

SRTP
(AES)

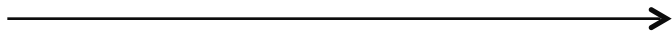


SRTP (AES)



SRTP (AES)

1- REGISTER



1- 200 OK



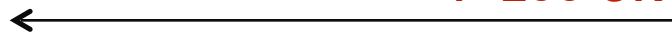
2- INVITE



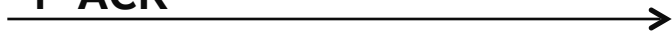
2- 100 Trying



4- 200 OK



4- ACK



Skype for Business 2015

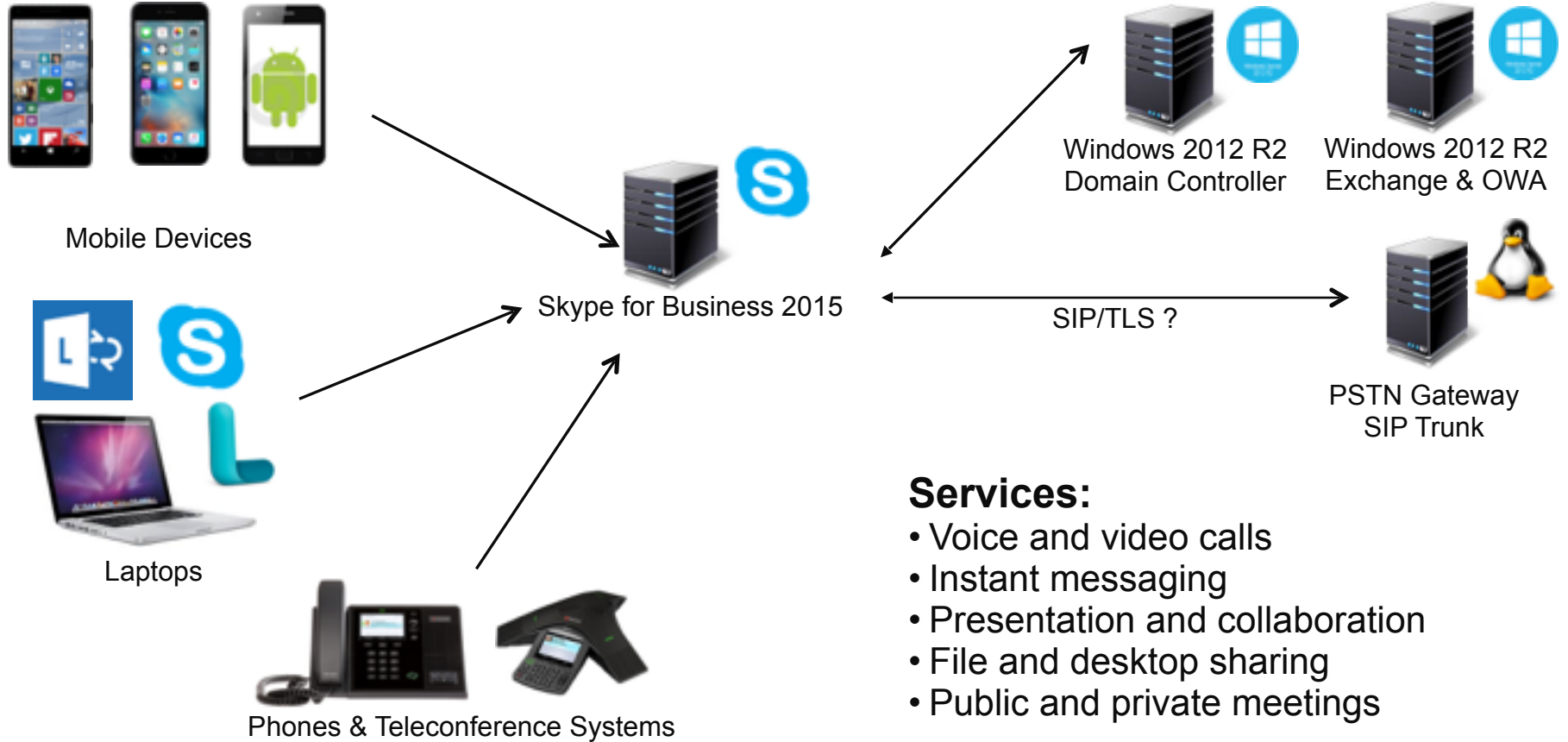
3- INVITE



3- 200 OK

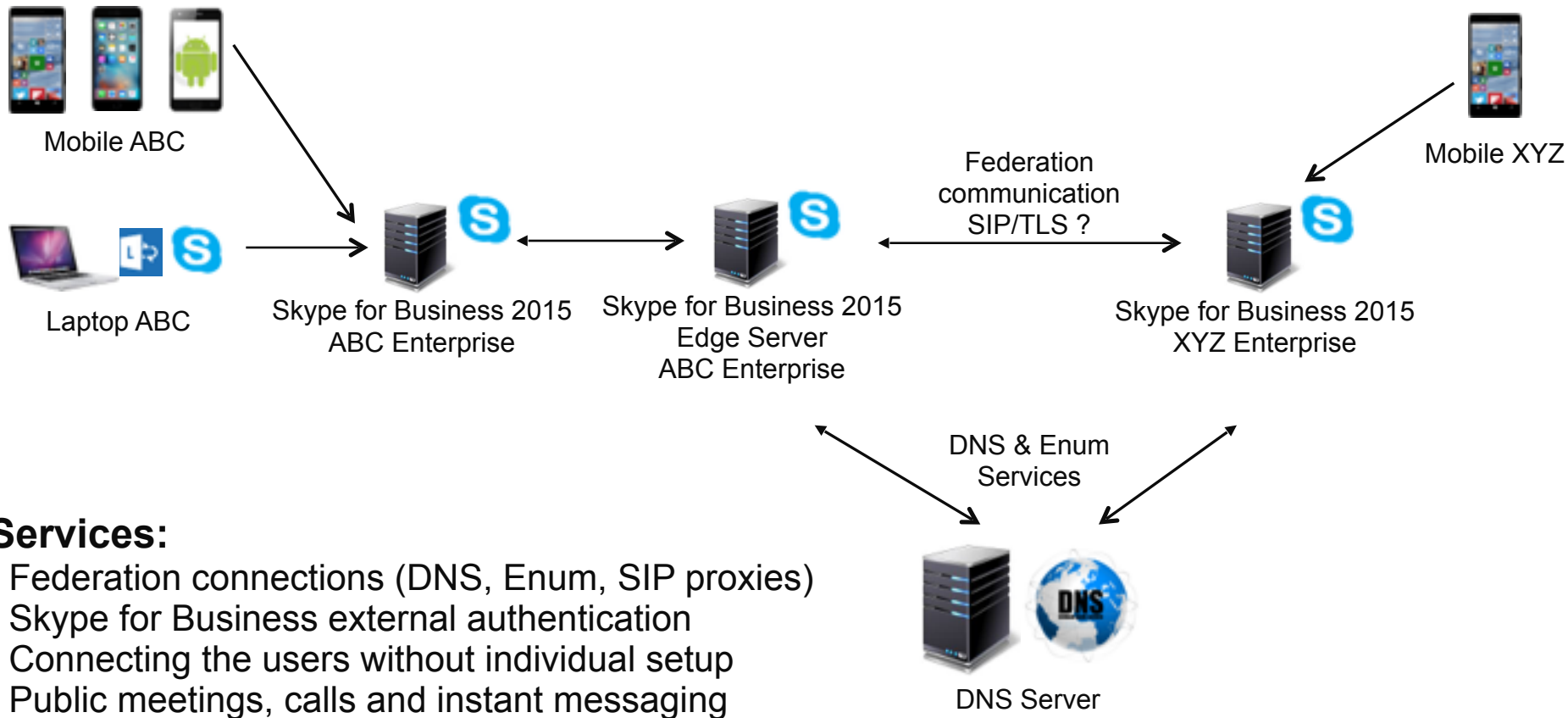


Client B



Services:

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



Services:

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

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	•	•	•

¹Lync 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.

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>

- 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



- 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)

- 3 ways to conduct security testing
 - Compliance and configuration analysis
 - MITM analysis (Viproxy 2.0)
 - Using a custom security tester (Viproxy 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

- 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



- 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



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

Skype for Business Server

CONFERRING POLICY MEETING CONFIGURATION DIAL-IN ACCESS

Edit Conferencing Policy - Global

Commit Cancel

Allow multiple

Skype for Business Server

Home Users Topology IM and Presence Persistent Chat Voice

Skype for Business Server

Home Users Topology IM and Presence Persistent Chat Voice Routing Voice Features Response Groups Conferencing Clients Federation and External Access Monitoring and Archiving Security Network Configuration

EDIT VOICE POLICY - Global

OK Cancel

Scopes: Global

Name: Global

Description:

Calling Features

- Enable call forwarding
- Enable delegation
- Enable call transfer
- Enable call park
- Enable simultaneous ring

Associated PSTN Usages

PSTN usage record

- Long Distance
- Internal

Skype for Business Server

EXTERNAL ACCESS POLICY

Edit External Access Policy - Global

Commit

Scope: Global

Name: Global

Description:

Enable communications with public users

Enable communications with public users

Enable communications with public users

Skype for Business Server

FILE FILTER URL FILTER

Edit Client Version Policy - Global

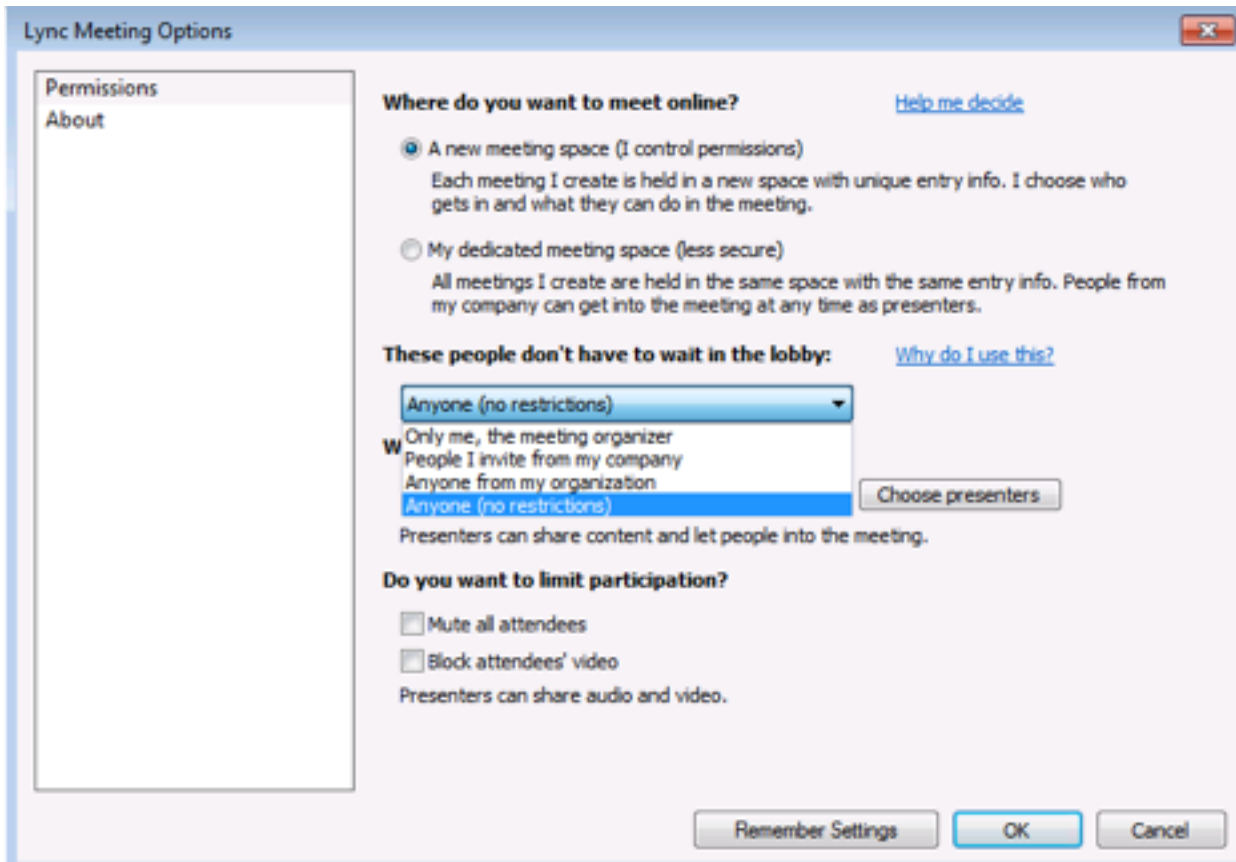
Commit Cancel

Scopes: Global

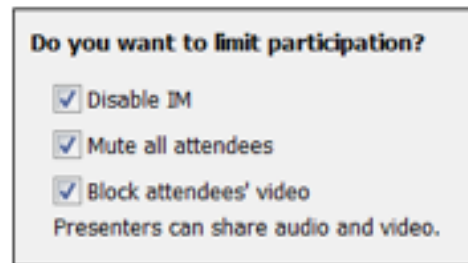
Name: Global

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	3.5.4907.123	Older than	Allow
OC	3.9995.9999.9999	Older than or same as	Allow
OC	4.0.7577.4000	Older than	Allow
OC	4.9995.9999.9999	Older than or same as	Allow
OC	15.0.4128.0	Older than	Allow
UCDP	2.0.5999.*	Older than or same as	Block



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



- 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:oW7iYHXiAOr19UH05ba07bMJ
```

```
a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:Gu  
+c81XctWoAHro7cJ9uN6WqW7QPJndjXfZsof18|2^31|1:1
```

- 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



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



MS Lync for Mac 2011
Client to be used for attacks



Viproxy 2.0



Windows 10
Skype for Business Clients



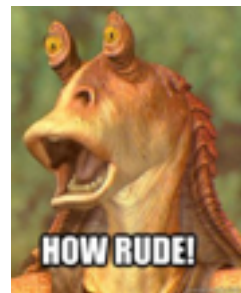
Windows 2012 R2
Skype for Business 2015 Server



- 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



- 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



to be shared later

to be shared later



Reverse browser visiting



Windows 10
Skype for Business Clients



MS Lync for Mac 2011
Client to be used for attacks

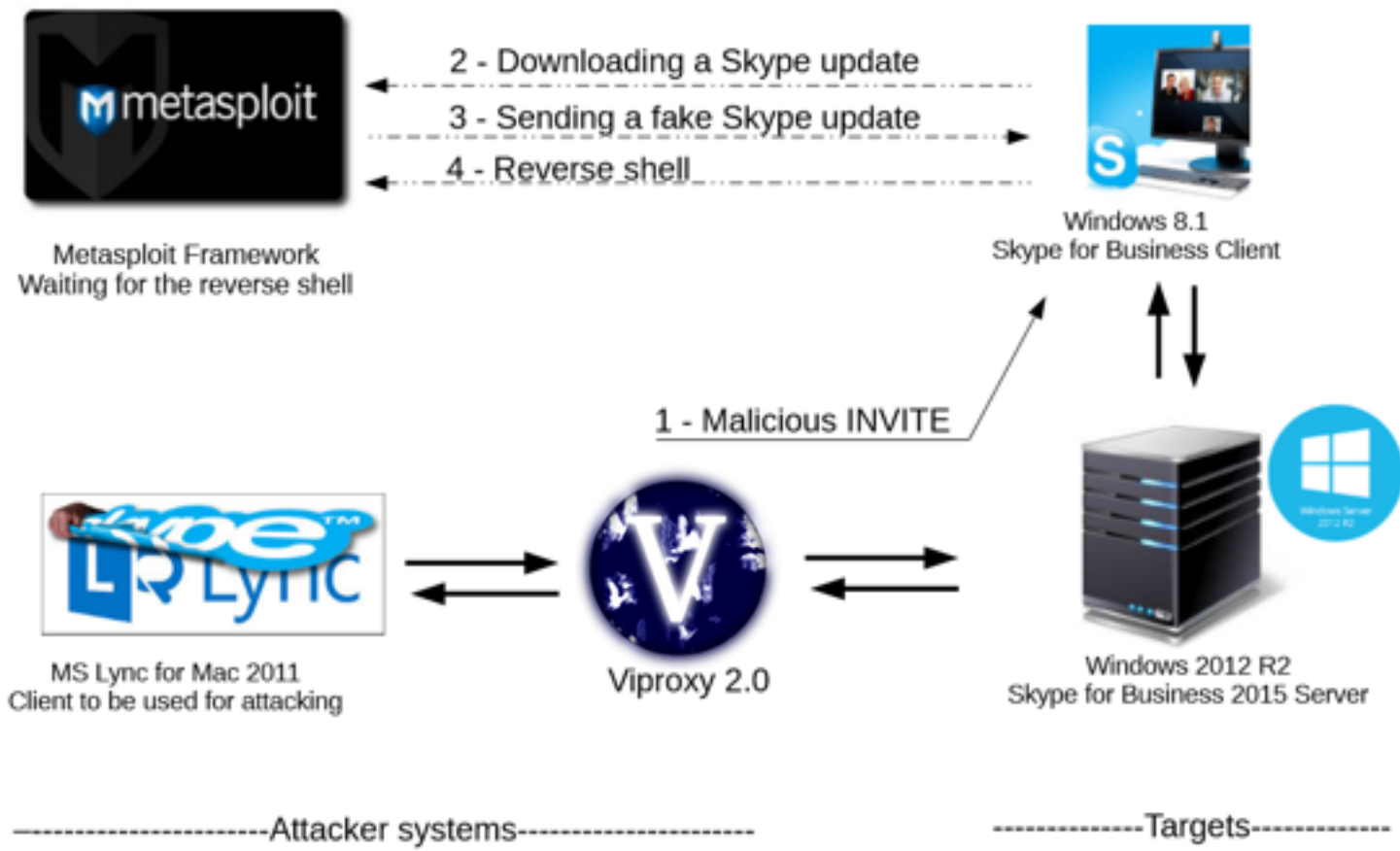


Viproxy 2.0



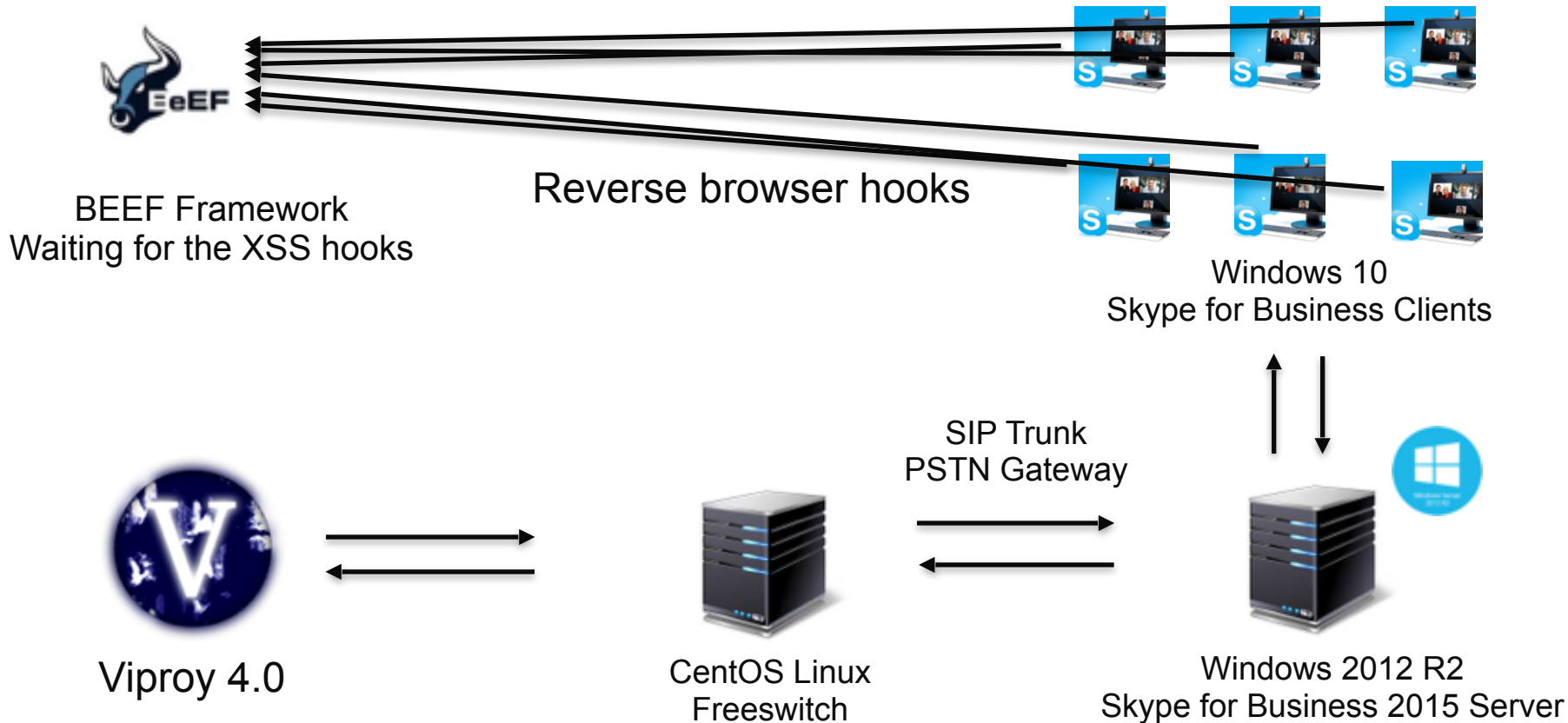
Windows 2012 R2
Skype for Business 2015 Server

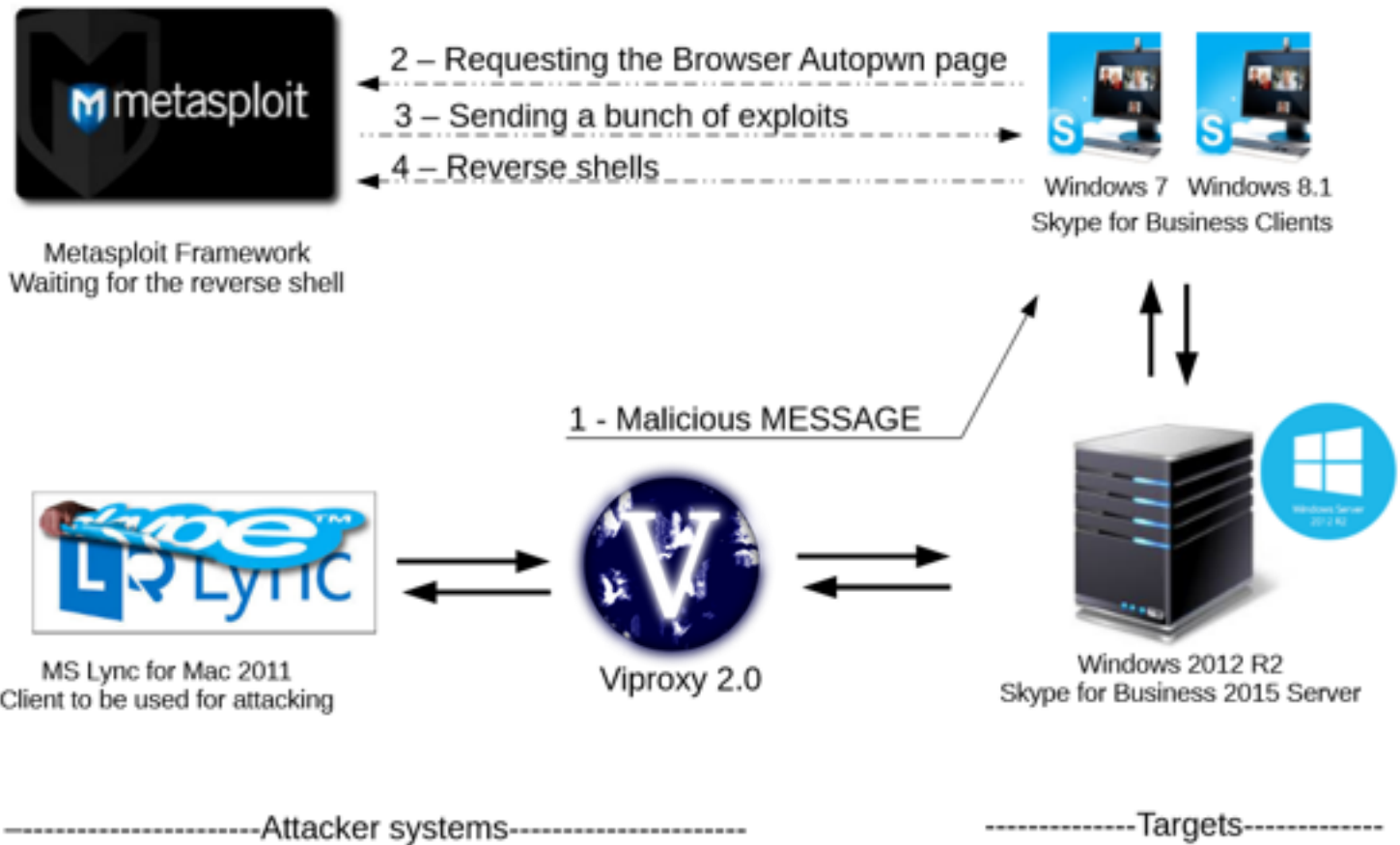
to be shared later



- 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

to be shared later





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

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

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>

Viproxy VoIP Penetration and Exploitation Kit

Author : <http://viproy.com/fozavci>

Homepage : <http://viproy.com>

Github : <http://www.github.com/fozavci/viproxy-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

Head office is level 8, 66 King Street, Sydney, NSW 2000, Australia.
Owner of trademark and all copyright is Sense of Security Pty Ltd.
Neither text or images can be reproduced without written permission.

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