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

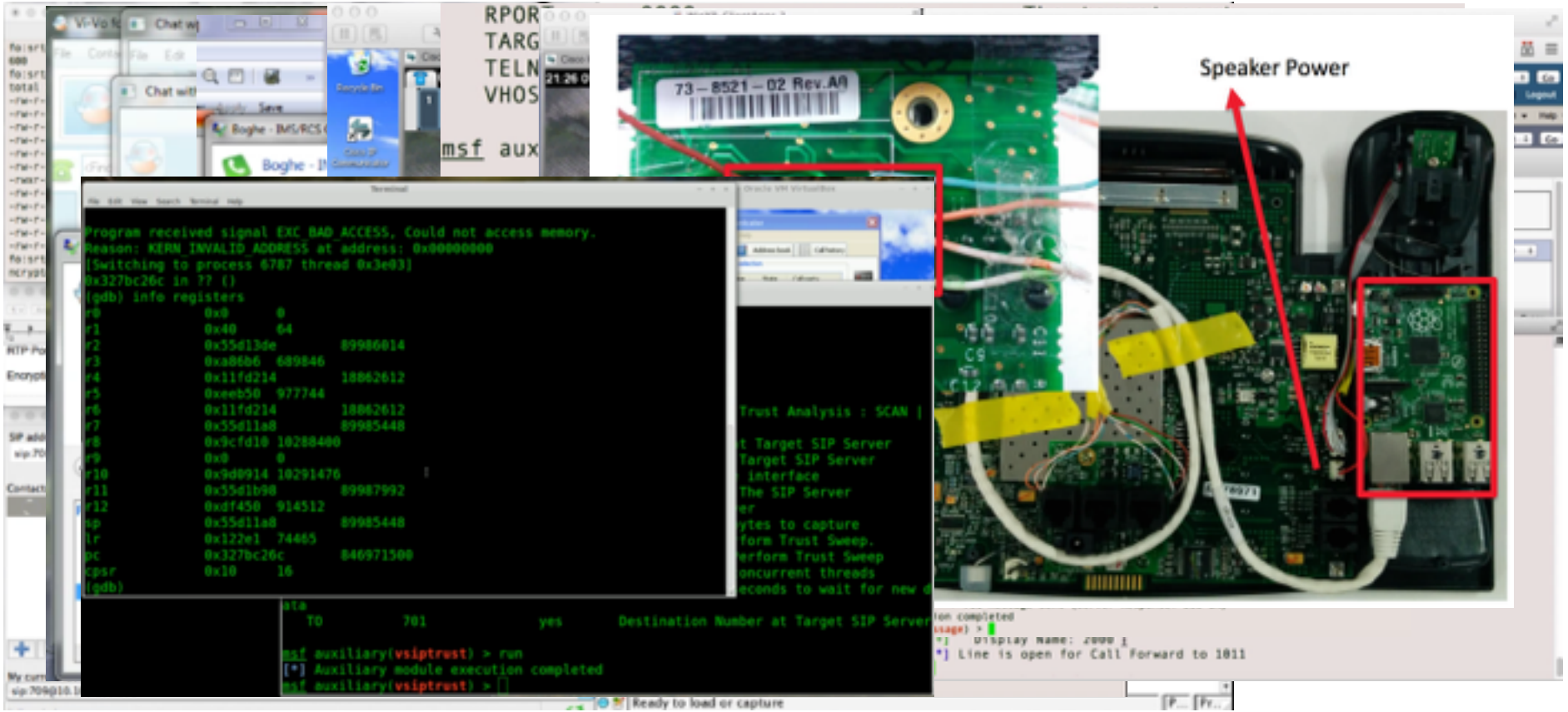
info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

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

Previously on VoIP Wars



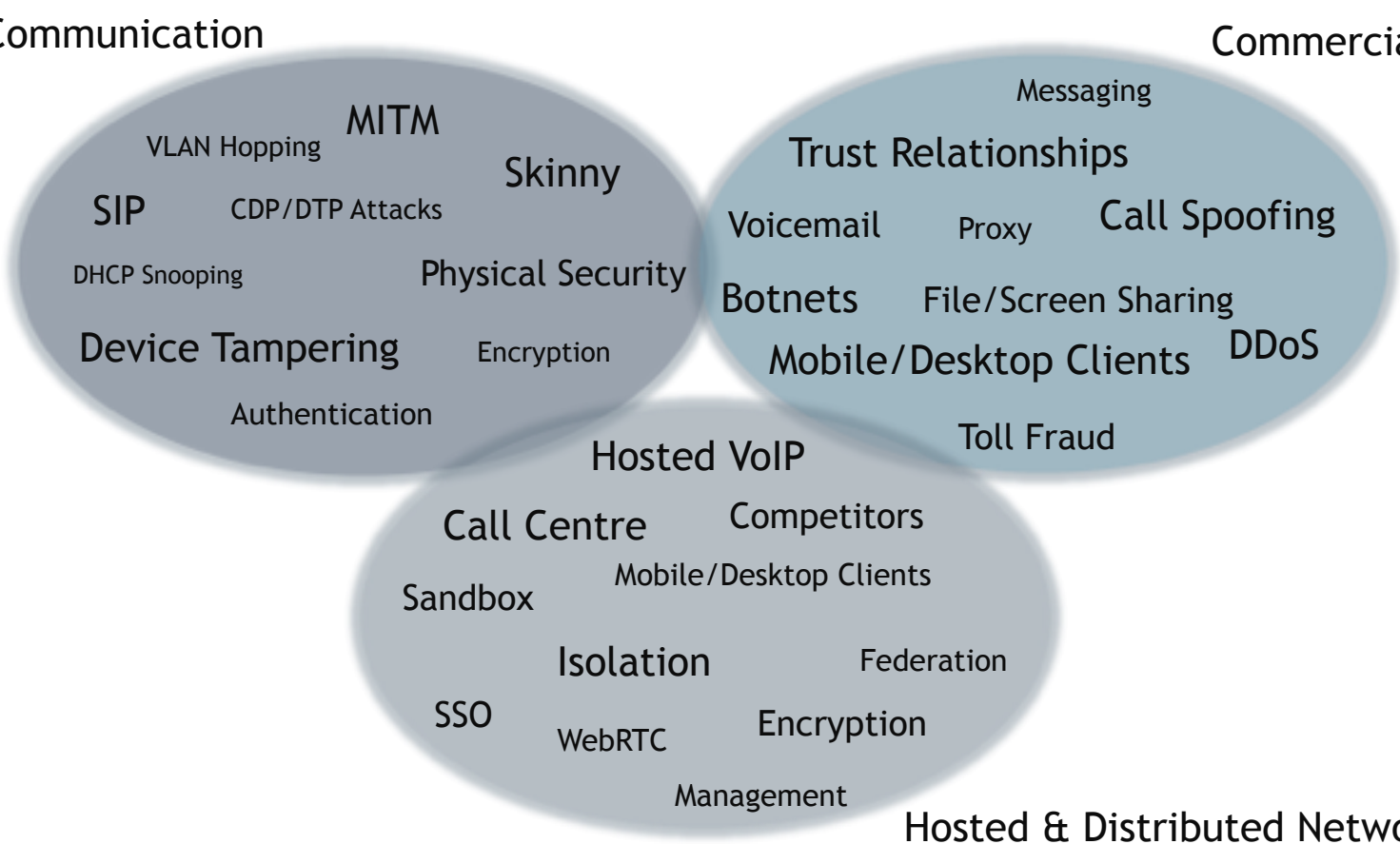
Current research status

- 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

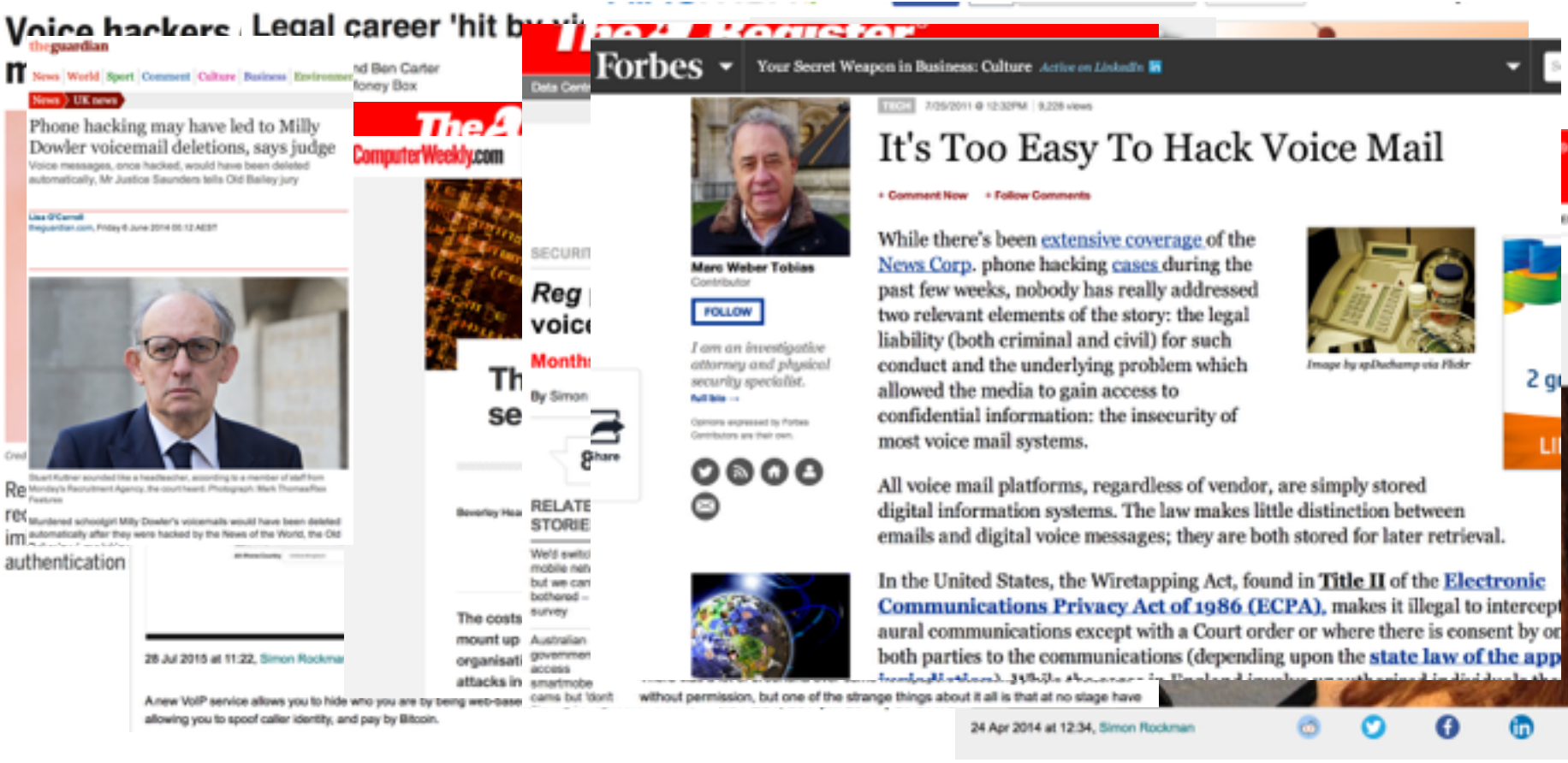
Agenda

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

Security requirements for UC



Modern threats targeting UC



Skype for Business

hotmail

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

Client A

1- REGISTER

1- 200 OK

2- INVITE

2- 100 Trying

4- 200 OK

4- ACK

SRTP (AES)

Skype for Business 2015

3- INVITE

3- 200 OK

RTP Proxy

SRTP (AES)

RTP Proxy

SRTP (AES)

Client B

Corporate communication

Mobile Devices

Laptops

Phones & Teleconference Systems

Skype for Business 2015

Windows 2012 R2
Domain Controller

Windows 2012 R2
Exchange & OWA

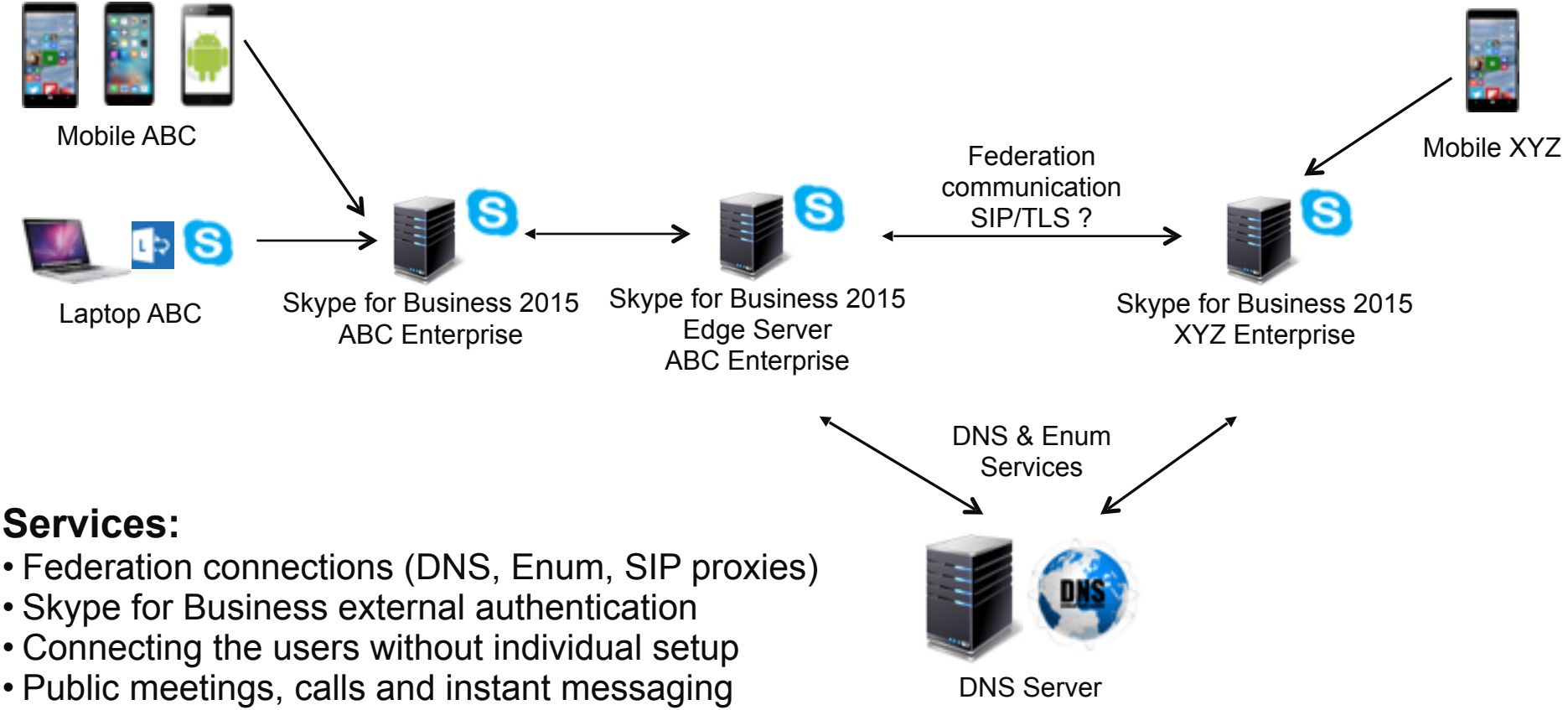
SIP/TLS ?

PSTN Gateway
SIP Trunk

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

Give control?

Give control?

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	•		•	•	•					•

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

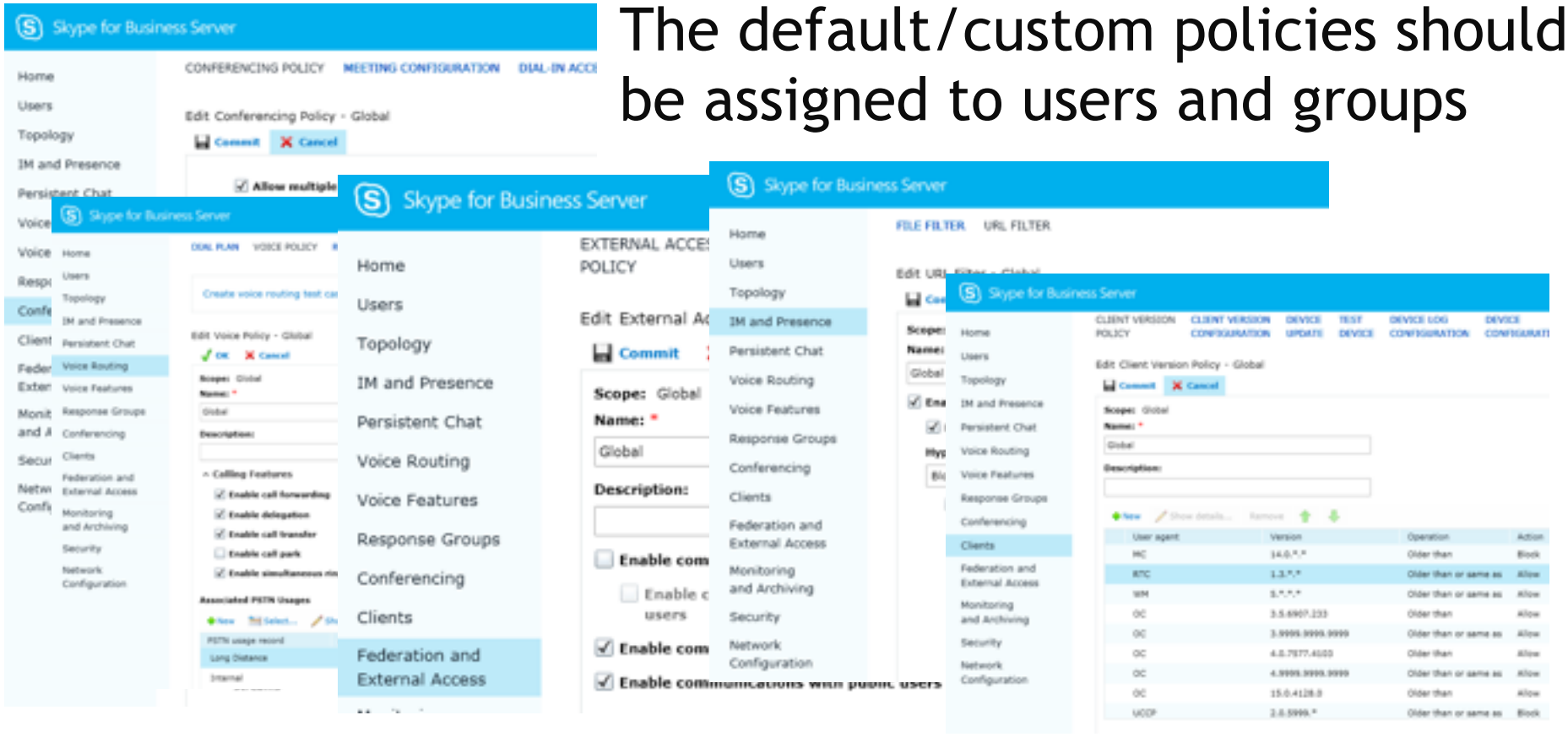
- Autodiscovery features
  - Autodiscovery web services
  - Subdomains and DNS records (SRV, NAPTR)
- Web services
  - Authentication, Webtickets and TLS web services
  - Meeting invitations and components
  - Skype for Business web application
- Active Directory integration
- Information gathering via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

Corporate communication policy

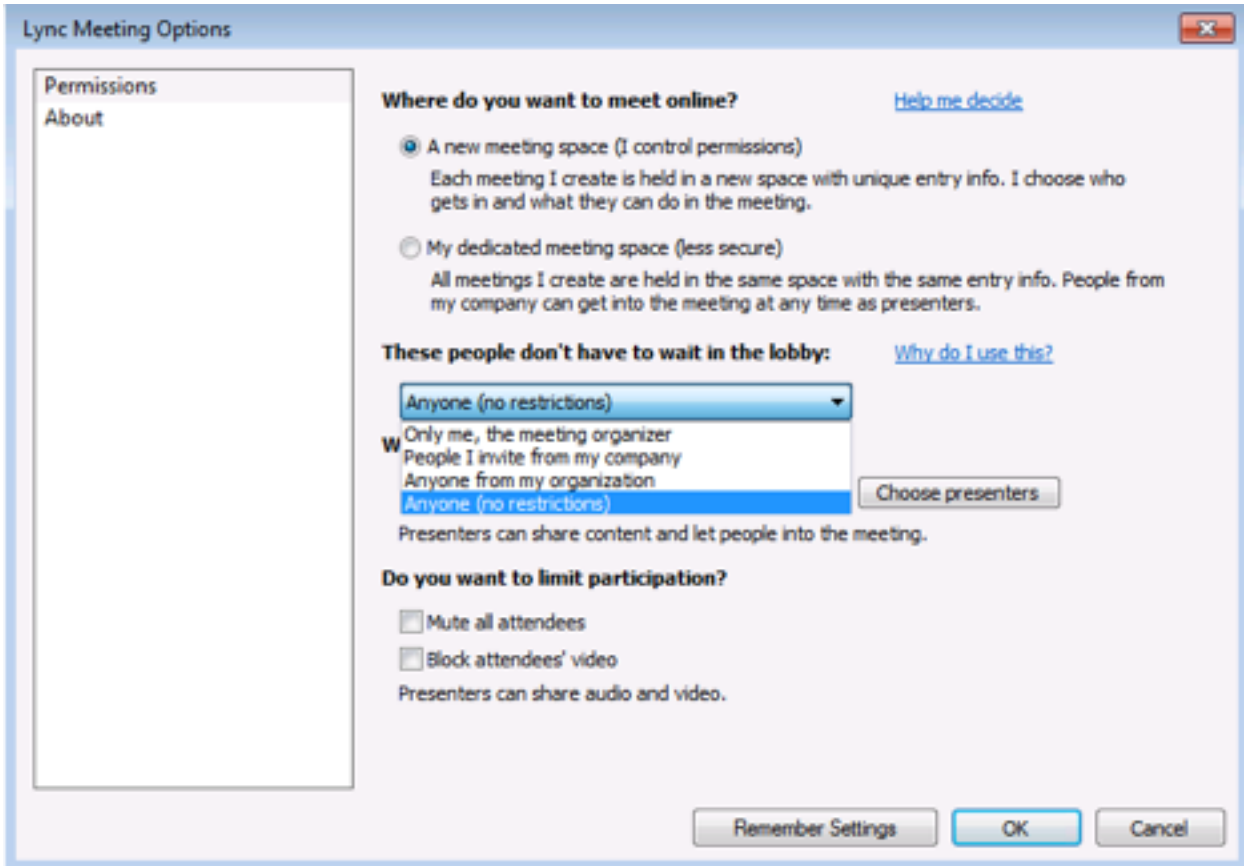
- Design of the communication infrastructure
  - Phone numbers, SIP URIs, domains, federations, gateways
- Client type, version and feature enforcements
  - Meeting codes, security, user rights to create meetings
  - Open components such as Skype for Business web app
  - Feature restrictions on clients
  - 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



Corporate communication policy



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

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

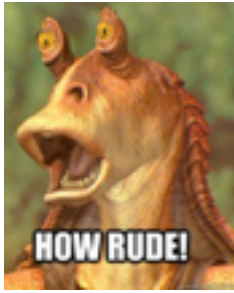
Windows 2012 R2
Skype for Business 2015 Server

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



Parsing errors and exceptions

to be shared later

Bypassing URL filter in IM

to be shared later

URL filter bypass

Reverse browser visiting

Windows 10
Skype for Business Clients

MS Lync for Mac 2011
Client to be used for attacks

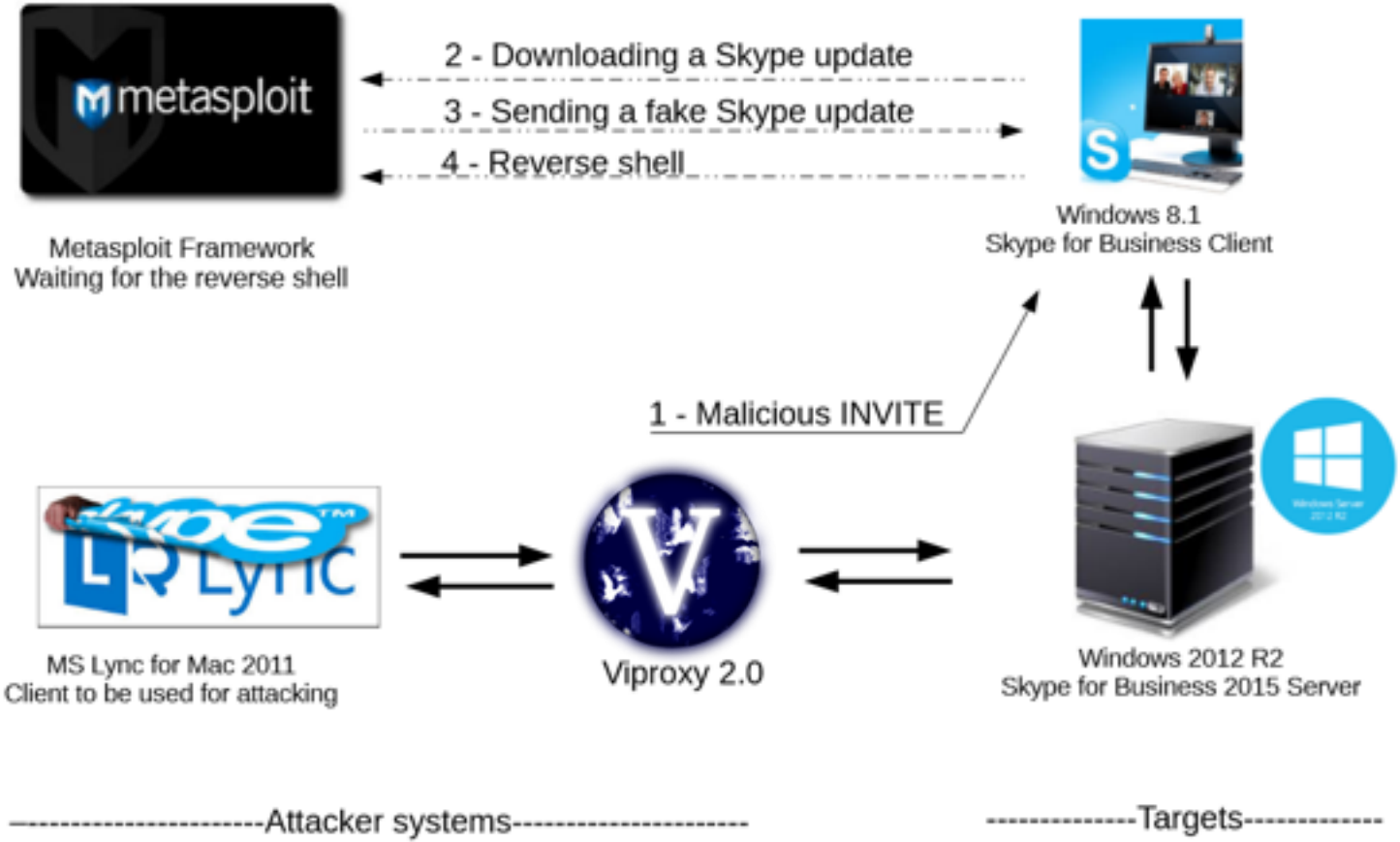
Viproxy 2.0

Windows 2012 R2
Skype for Business 2015 Server

Sending INVITEs w/ HTML/XSS

to be shared later

Fake Skype update via INVITE



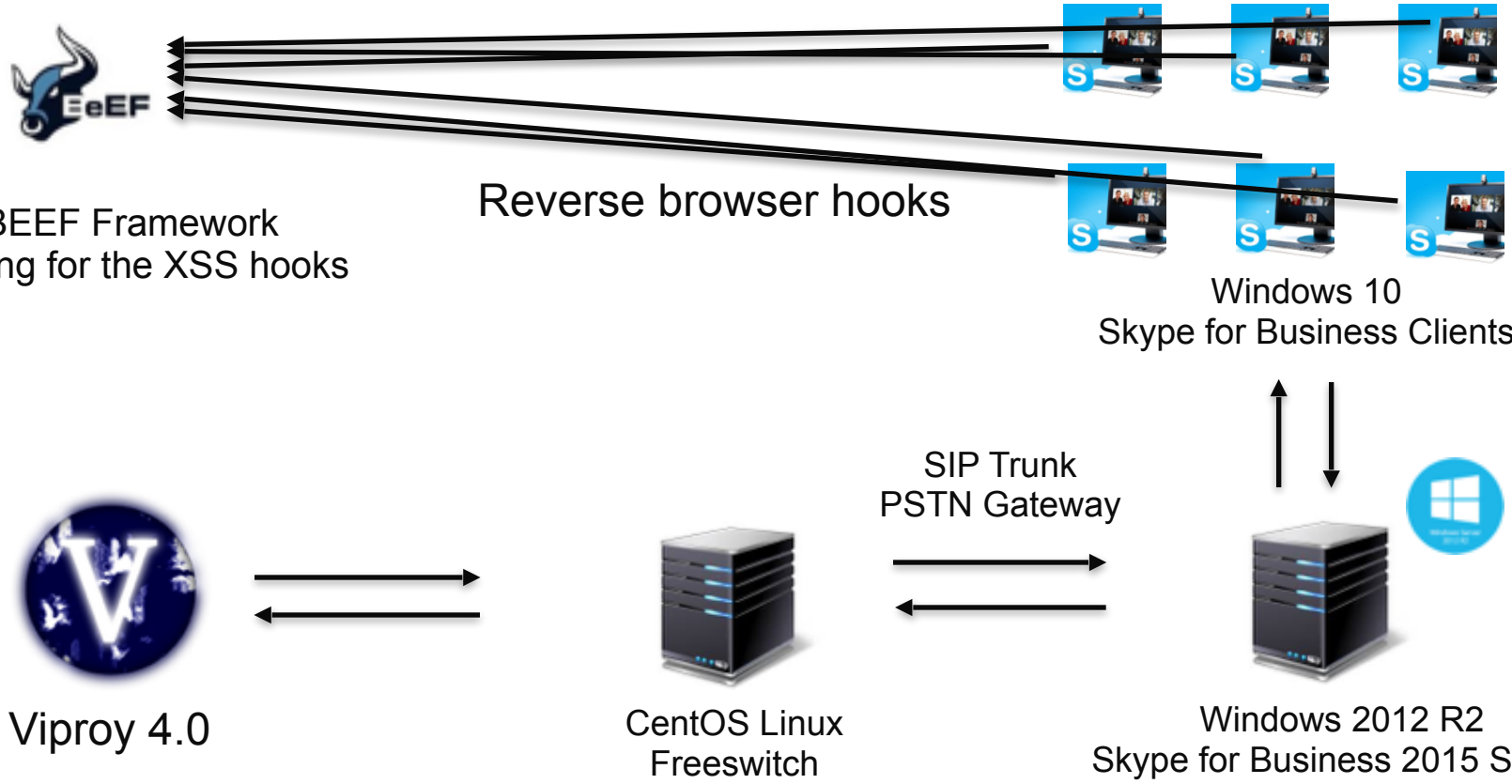
Multi endpoint communication

- 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

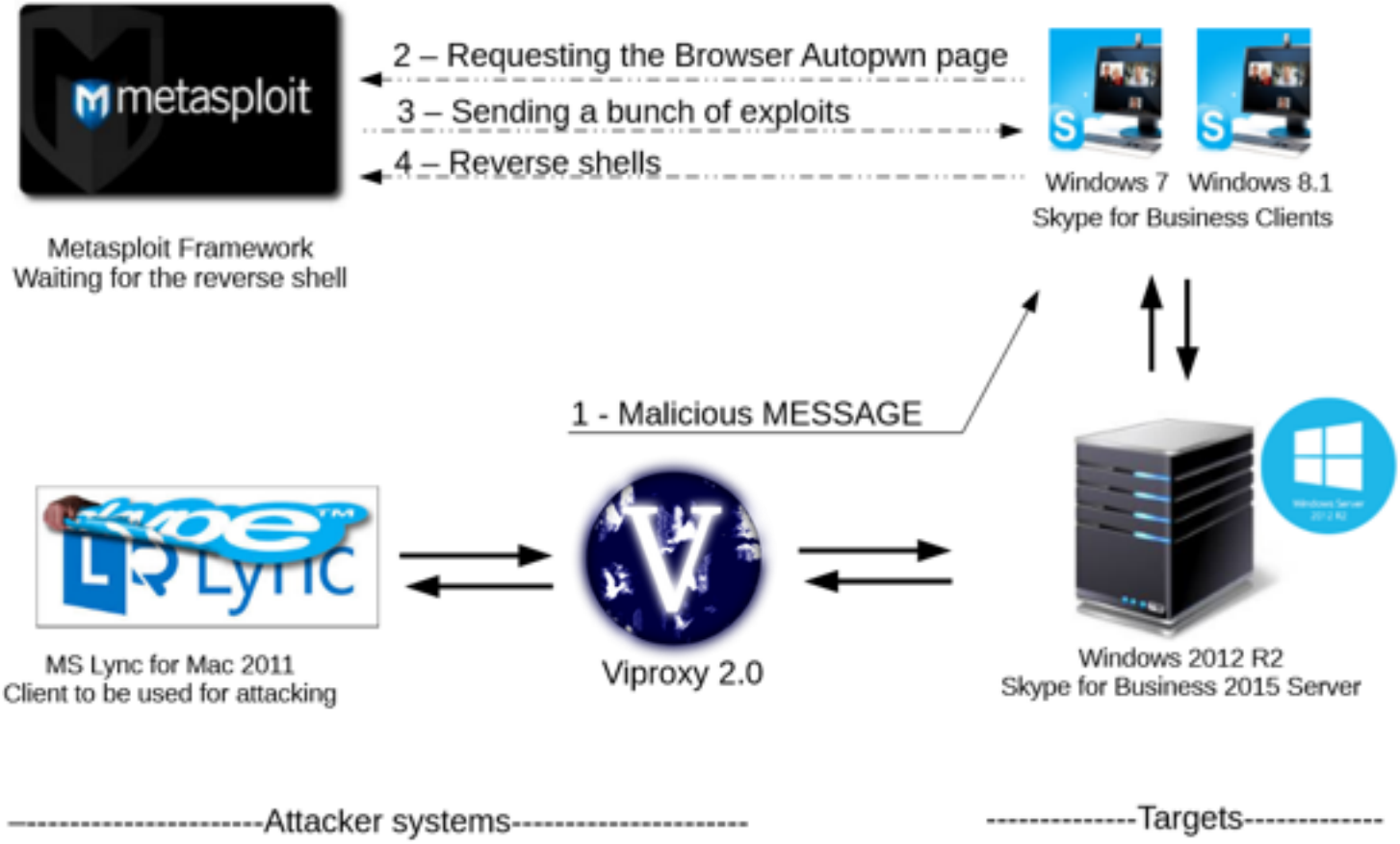
Sending messages w/ HTML/XSS

to be shared later

Mass compromise of clients



Mass compromise of clients



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

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