context

Departed Communications: Learn The Ways to Smash Them!

Fatih Ozavci (@fozavci)
Managing Consultant – Context Information Security

Speaker

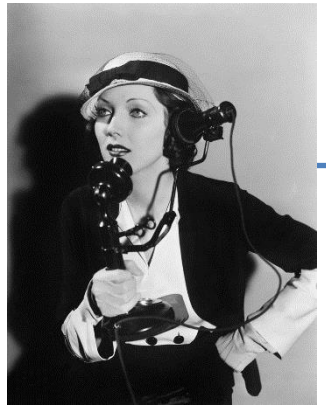
- Fatih Ozavci, Managing Consultant
  - VoIP & phreaking
  - Mobile applications and devices
  - Network infrastructure
  - CPE, hardware and IoT hacking
- Author of Viproy and VoIP Wars
- Public speaker and trainer
  - Blackhat, Defcon, HITB, AusCert, Troopers

Agenda

context

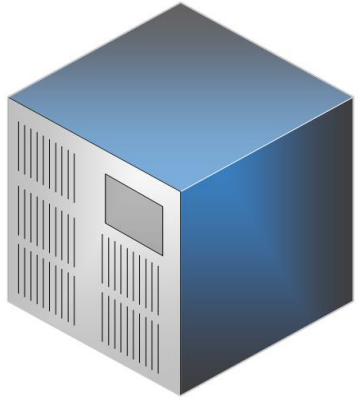
- VoIP, UC, IMS and more
- Security breaches
- Various implementations and issues
- Testing techniques
- Demonstrations

Traditional Phone Systems



Alice

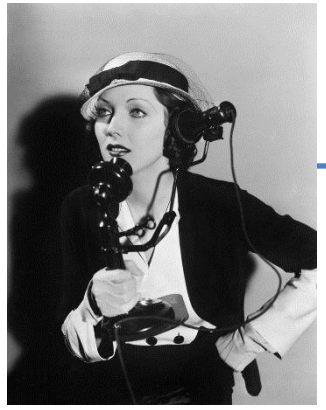
Audio Call



TDM

Bob

Unified Communications



Alice

Signalling

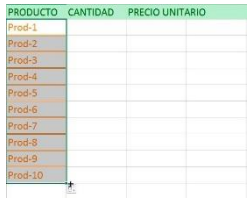
SIP Server

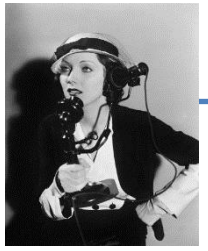
Bob

Media

RTP Proxy

Unified Collaboration





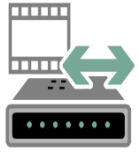
Alice

Signalling

SIP Server

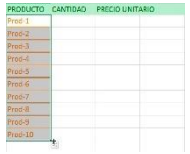
Bob

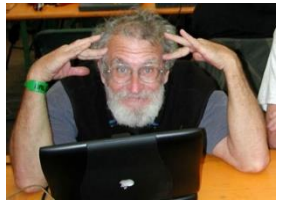
Media

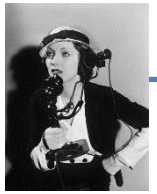


RTP Proxy

Unified Attack Surfaces







Signalling

SIP Server

Alice

Bob

Media

RTP Proxy

Security Concerns

- Toll Fraud
- Tenant Isolation
- Confidentiality

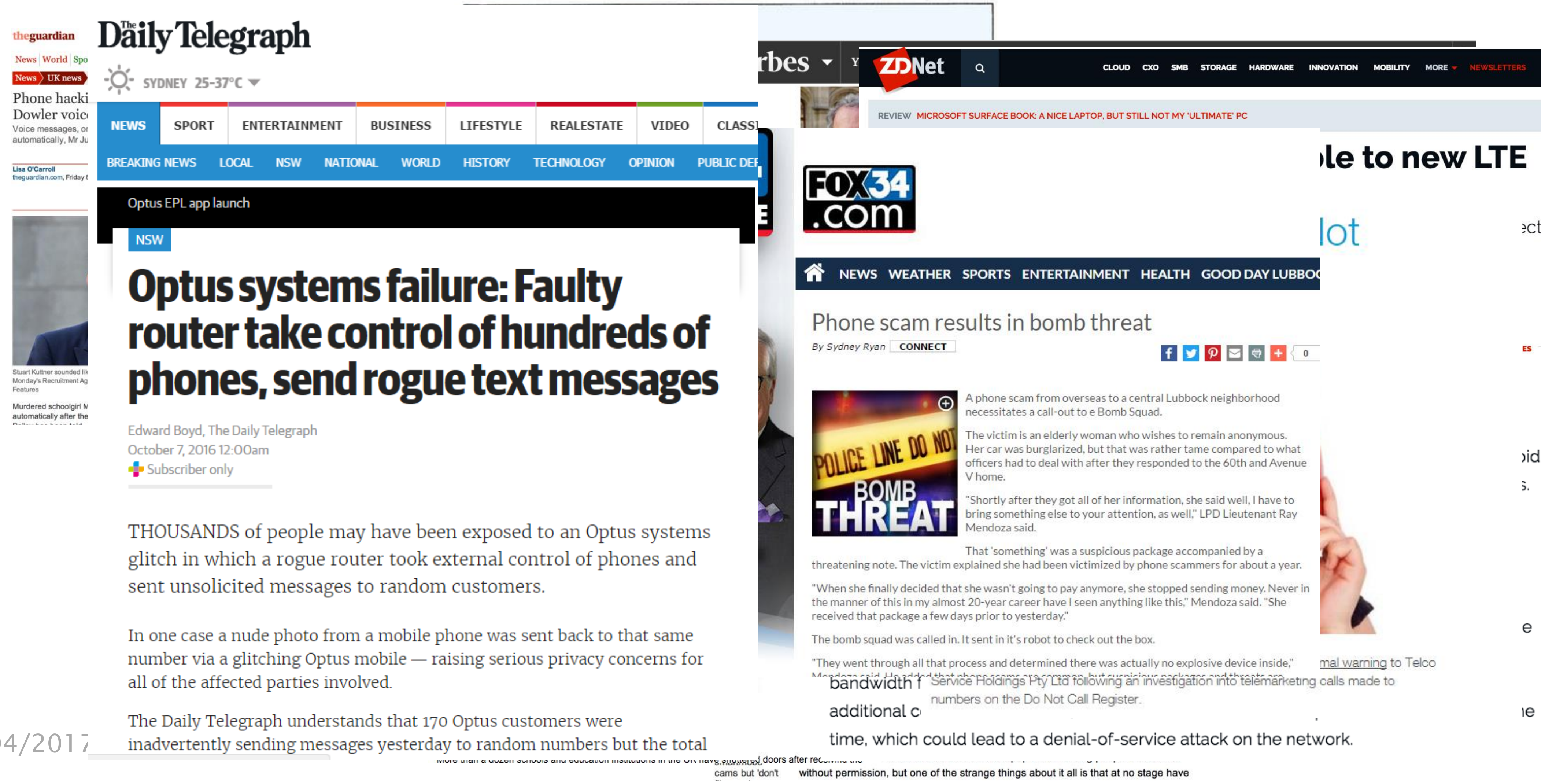
- Availability
- Privacy (eg PII)
- Regulations

- Call quality
- Infrastructure
- Endpoint Security

- Lawful / Illegal Interception
- Reputation Damage

Modern Challenges and Incidents

context



theguardian

Phone hacking: Dowler voice...

The Daily Telegraph

SYDNEY 25-37°C

NEWS | SPORT | ENTERTAINMENT | BUSINESS | LIFESTYLE | REALESTATE | VIDEO | CLASSI...

BREAKING NEWS | LOCAL | NSW | NATIONAL | WORLD | HISTORY | TECHNOLOGY | OPINION | PUBLIC DEF...

Optus EPL app launch

NSW

Optus systems failure: Faulty router take control of hundreds of phones, send rogue text messages

Edward Boyd, The Daily Telegraph
October 7, 2016 12:00am
Subscriber only

THOUSANDS of people may have been exposed to an Optus systems glitch in which a rogue router took external control of phones and sent unsolicited messages to random customers.

In one case a nude photo from a mobile phone was sent back to that same number via a glitching Optus mobile — raising serious privacy concerns for all of the affected parties involved.

The Daily Telegraph understands that 170 Optus customers were inadvertently sending messages yesterday to random numbers but the total

ZDNet

CLOUD | CXO | SMB | STORAGE | HARDWARE | INNOVATION | MOBILITY | MORE | NEWSLETTERS

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

...le to new LTE

FOX34.com

NEWS | WEATHER | SPORTS | ENTERTAINMENT | HEALTH | GOOD DAY LUBBO...

Phone scam results in bomb threat

By Sydney Ryan CONNECT

A phone scam from overseas to a central Lubbock neighborhood necessitates a call-out to e Bomb Squad.

The victim is an elderly woman who wishes to remain anonymous. Her car was burglarized, but that was rather tame compared to what officers had to deal with after they responded to the 60th and Avenue V home.

"Shortly after they got all of her information, she said well, I have to bring something else to your attention, as well," LPD Lieutenant Ray Mendoza said.

That 'something' was a suspicious package accompanied by a threatening note. The victim explained she had been victimized by phone scammers for about a year.

"When she finally decided that she wasn't going to pay anymore, she stopped sending money. Never in the manner of this in my almost 20-year career have I seen anything like this," Mendoza said. "She received that package a few days prior to yesterday."

The bomb squad was called in. It sent in it's robot to check out the box.

"They went through all that process and determined there was actually no explosive device inside,"

...mal warning to Telco Service Holdings Pty Ltd following an investigation into telemarketing calls made to numbers on the Do Not Call Register.

bandwidth f... additional c... time, which could lead to a denial-of-service attack on the network.

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

Summary of Security Breaches

- Legacy systems (15 years old)
- Insecure CPE deployment
- Lack of authentication
- Broken authorisation
- Too much trust
- No security patch whatsoever

VoIP in Real Life

Corporate/Federated Communications

Cloud Services

Service Providers

Mobile Operators

Warming Up

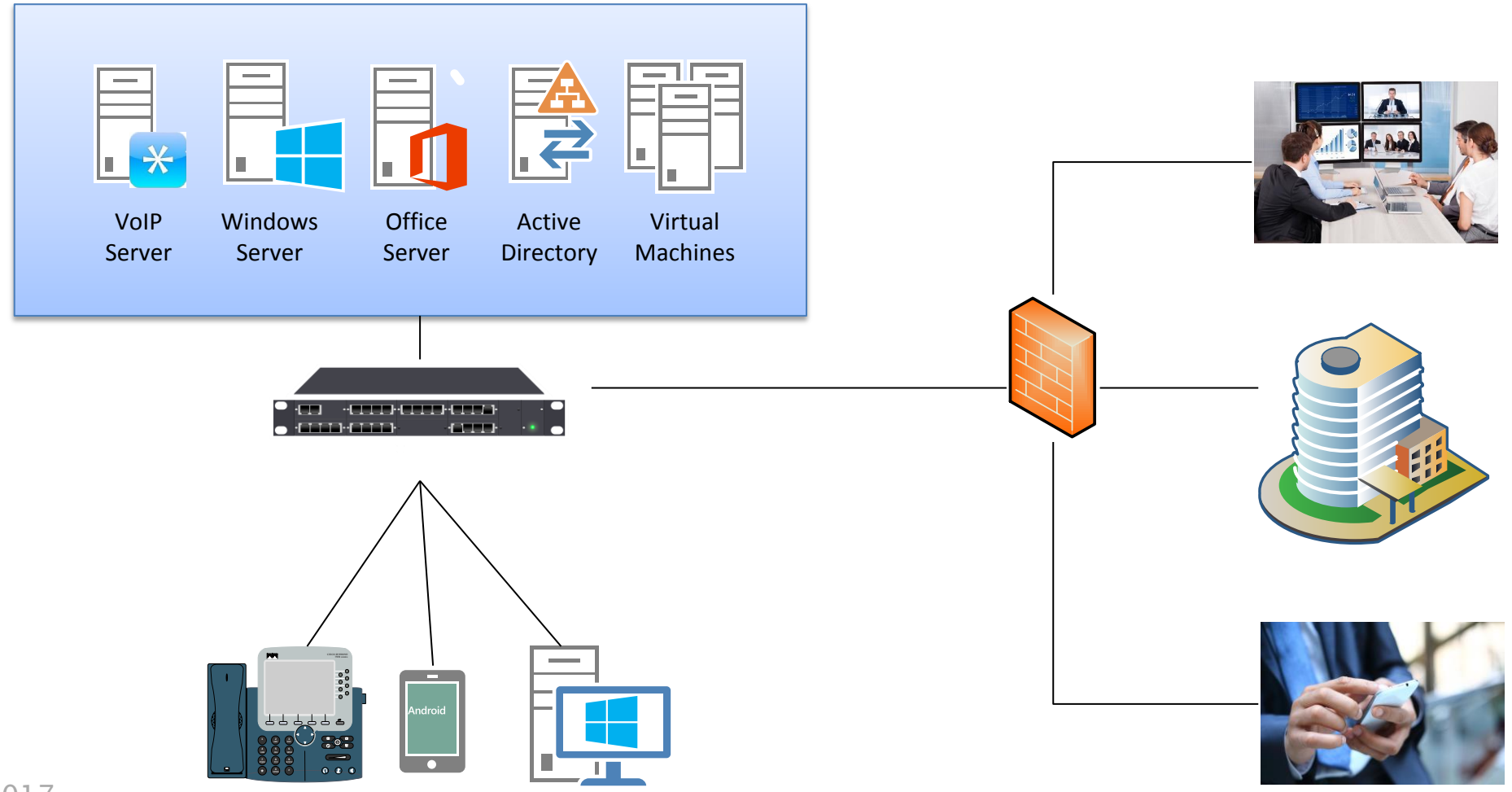
context

- VoIP Wars research series
  - Return of the SIP (Advanced SIP attacks)
  - Attack of the Cisco Phones (Cisco specific attacks)
  - Destroying Jar Jar Lync (SFB specific attacks)
  - The Phreakers Awaken (UC and IMS specific attacks)
- Tools
  - Viproy for sending signalling and cloud attacks
  - Viproxy for intercepting UC client/server traffic
- Viproy.com for videos and training videos

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)

Corporate Communications



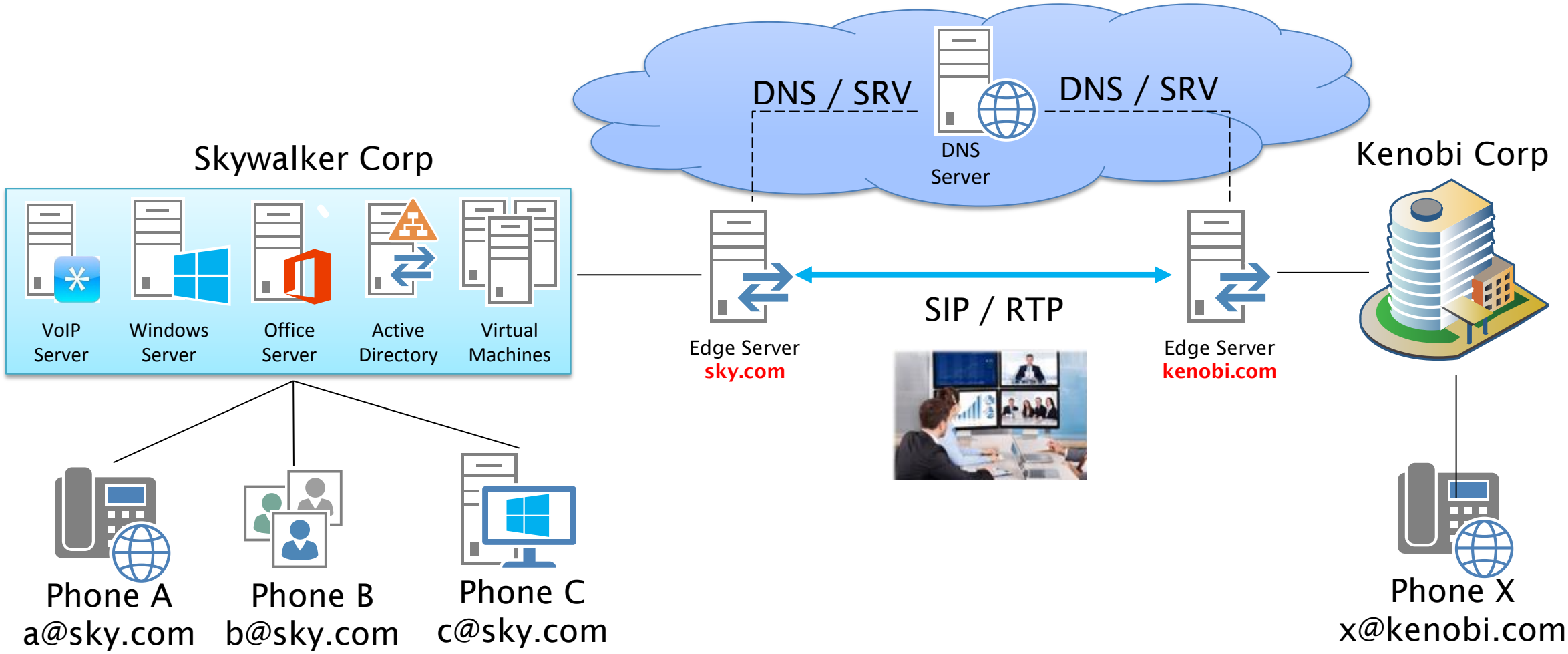
Analysing Corporate Communications

context

- Find a way to get in
  - Courtesy phones, meeting rooms, lobby
  - Replace or compromise it (e.g. raspberry pi)
- Analyse the network access
  - CDP discovery, VLAN hopping, ARP spoofing
- Compromise faster
  - Harvest conf and creds on TFTP/HTTP
  - Compromise conf files to deploy SSH keys
- Exploit service/server management
  - Legacy software, missing patches, default creds

Federated Communications

context



Attacking Through Signalling

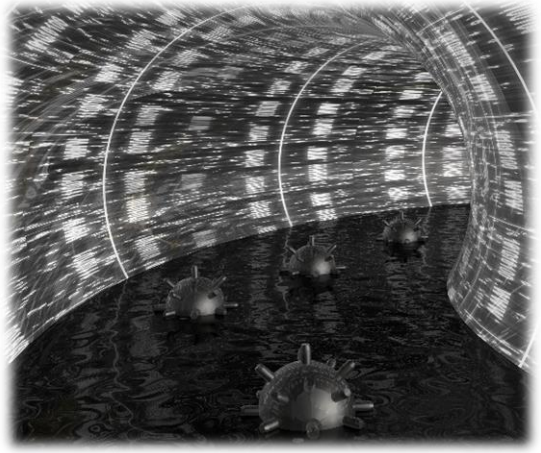
context

- Discover the protocols
  - SIP, Cisco Skinny/SCCP, Alcatel UA
- Discover the signalling gateways
  - Lack of authentication, insecure management
- Perform essential signalling attacks
  - Enumeration, brute force, call forwarding
- Inject custom headers to calls
  - Caller ID spoofing, billing or dial plan bypass
- Attack with a real client
  - Voicemail access, toll fraud, spread the attack to clients
- Combining other attacks

Attacking Through Messaging

context

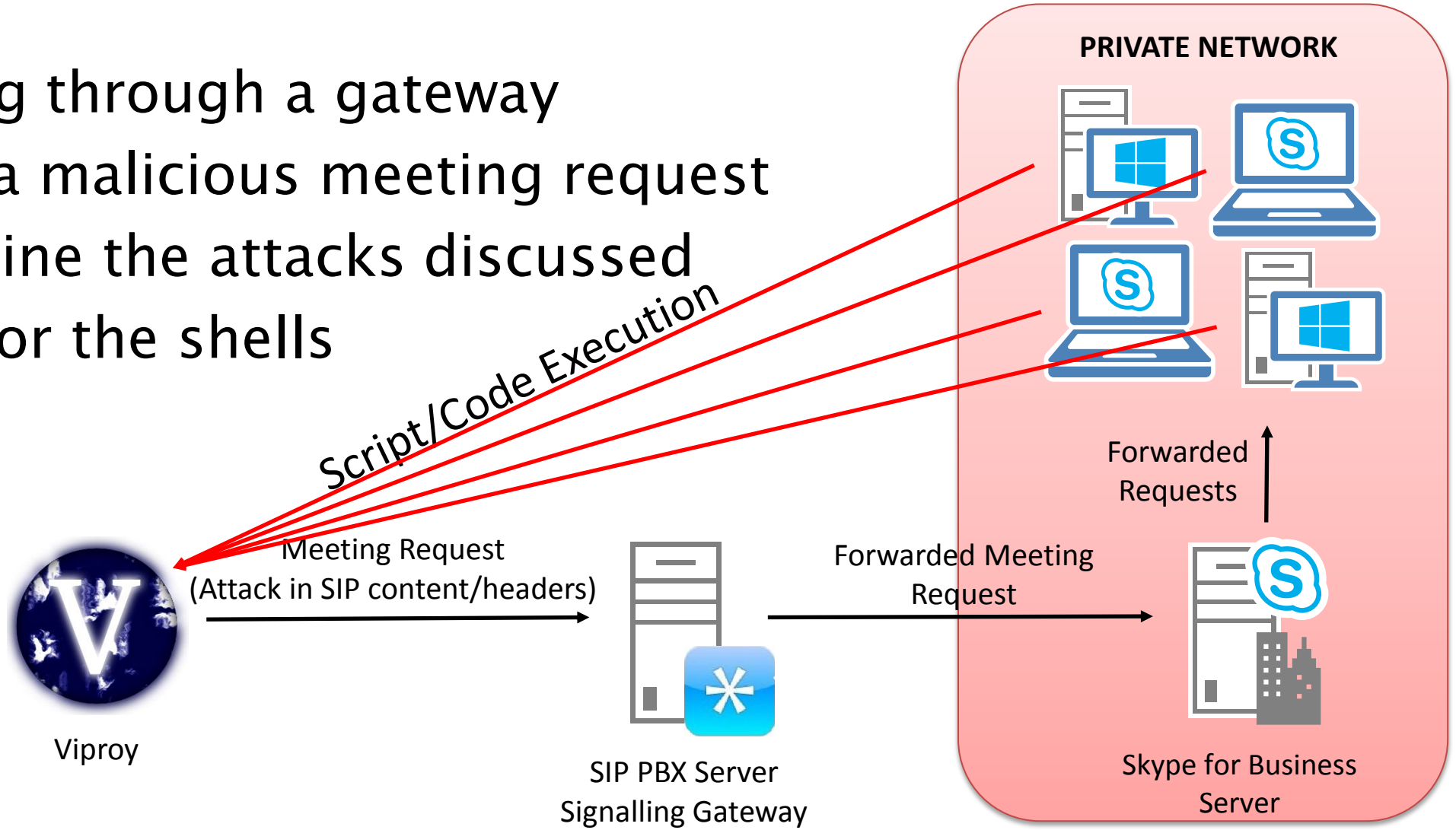
- Unified Messaging
  - Message types (e.g. rtf, html, images)
  - Message content (e.g. JavaScript)
  - File transfers and sharing features
  - Code or script execution (e.g. SFB)
  - Encoding (e.g. Base64, Charset)
- Various protocols
  - MSRP, XMPP, SIP/MESSAGE
- Combining other attacks



Mass Compromise

Attacking through a gateway

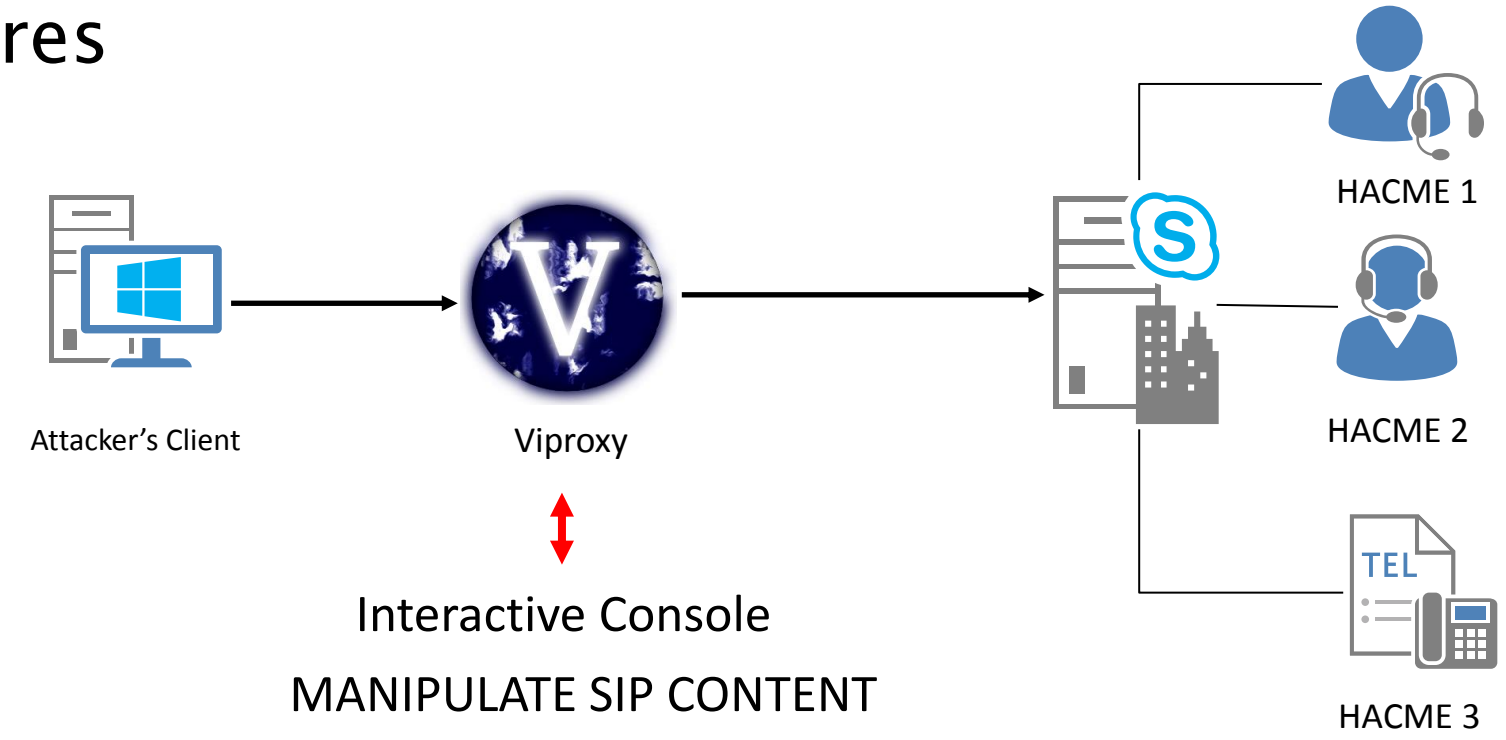
- Send a malicious meeting request
- Combine the attacks discussed
- Wait for the shells

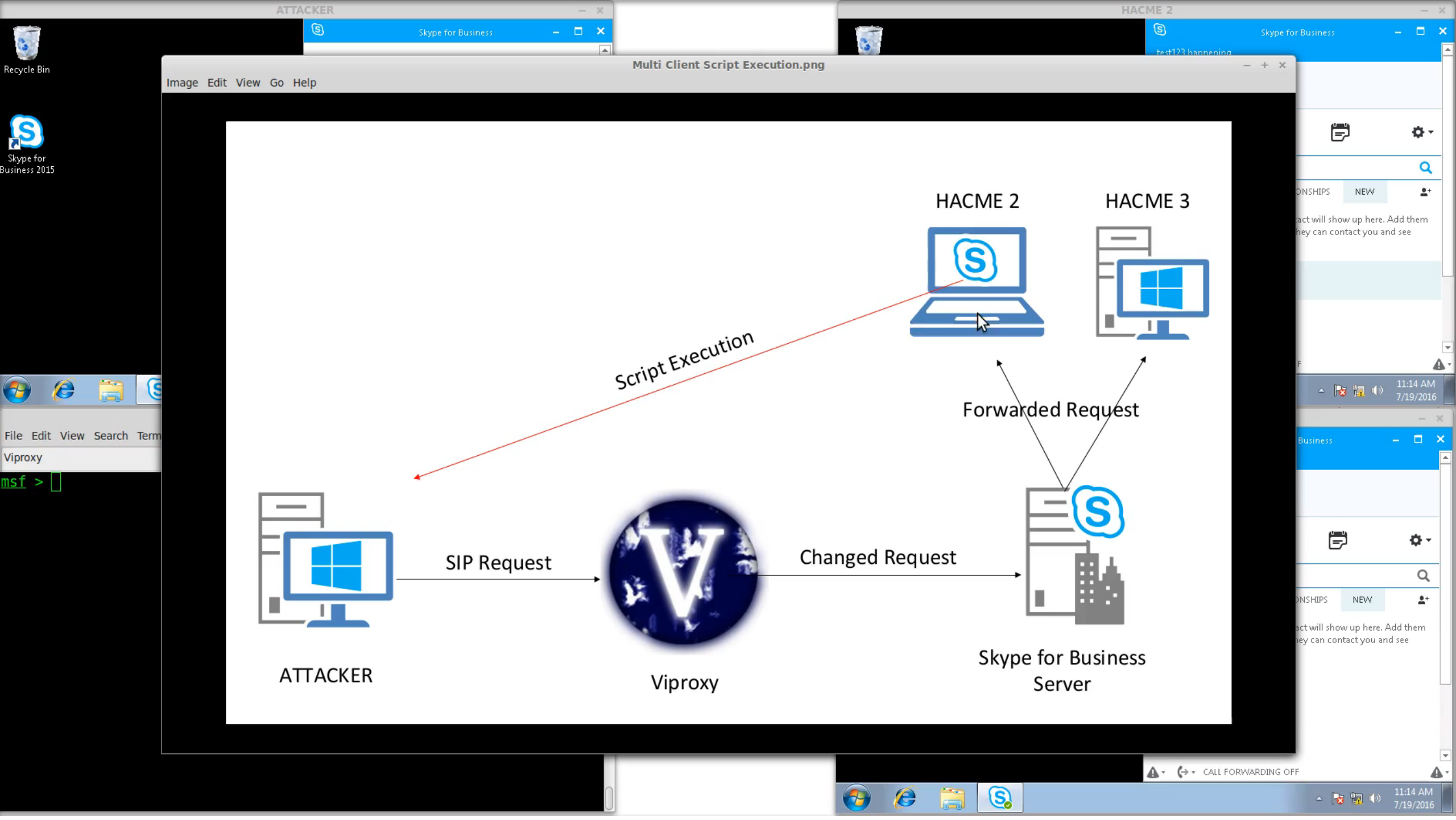


Attack Using Original Clients

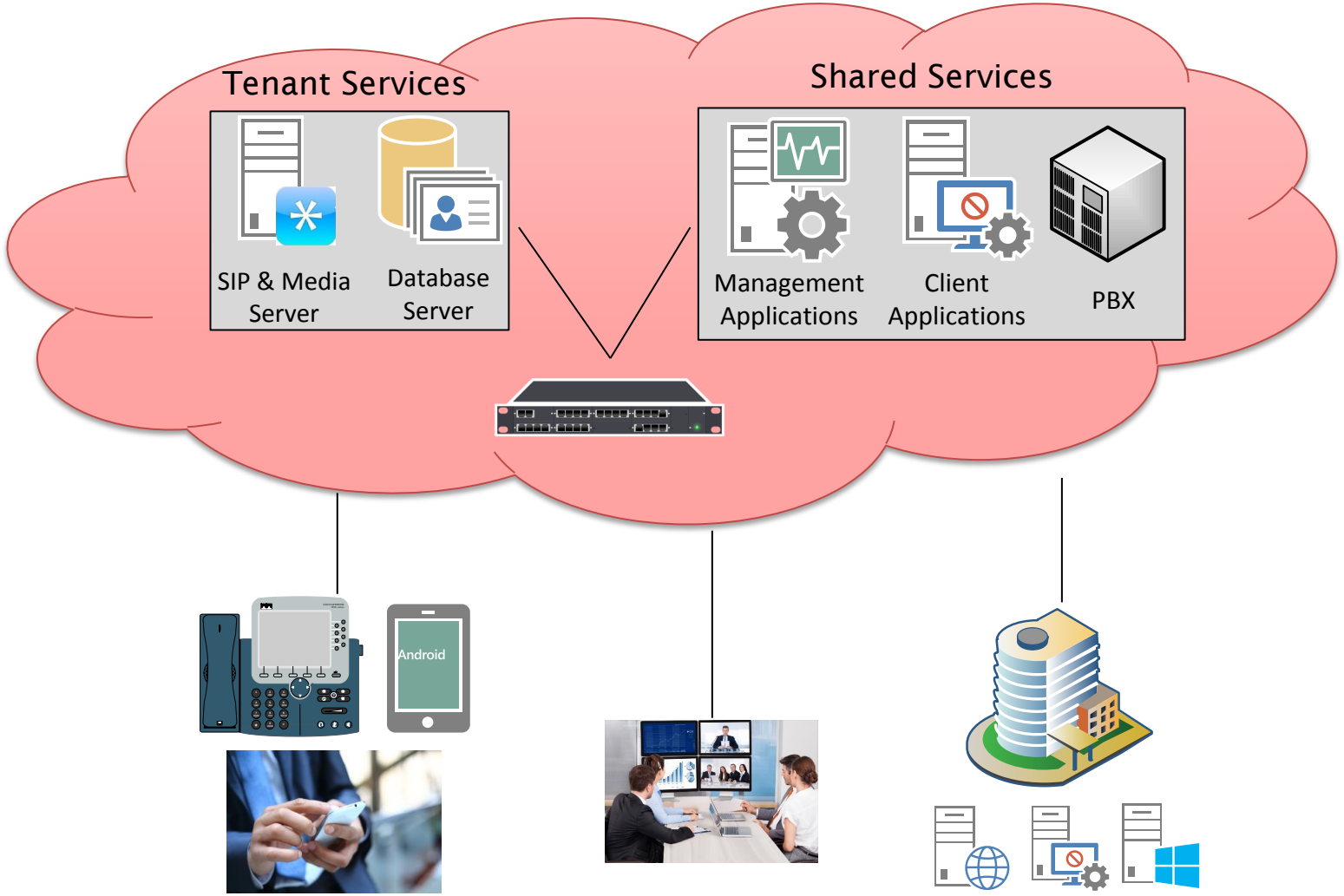
Reason: adding features

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




ATTACKER
Skype for Business
HACME 2
Skype for Business
Recycle Bin
Skype for Business 2015
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
File Edit View Search Term
Viproxy
msf >
CALL FORWARDING OFF
11:14 AM
7/19/2016

Cloud Communications



Targeting Tenants or Providers

- Persistent access
  - Raspberry PI with PoE, eavesdropping
- Shared services to jailbreak
  - Billing, PBX, recordings, client applications
- Unauthorised service access
  - Toll fraud, call forwarding, speed dial harvesting
  - Privilege escalation on shared management
  - SIP header manipulations for good
- Practical attacks w/ caller ID spoofing
  - Voicemail harvesting, robocalls

Targeting Clients

context

- 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 Through UC/IMS

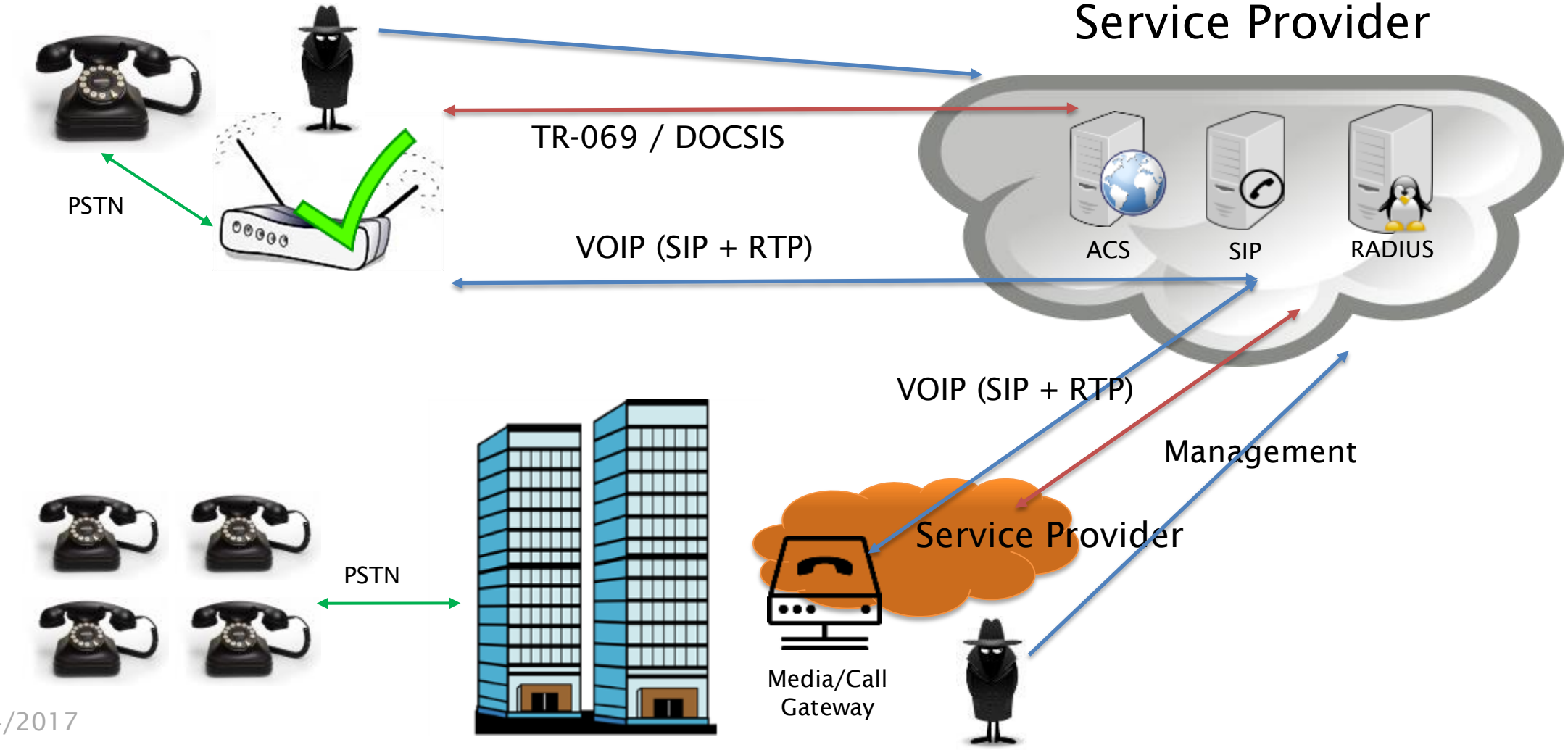
SIGNALLING / MESSAGING
- SDP / XML
- SIP Headers
- XMPP
- MSRP

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

UC/VoIP Subscriber Services



Subscriber Services Testing

context

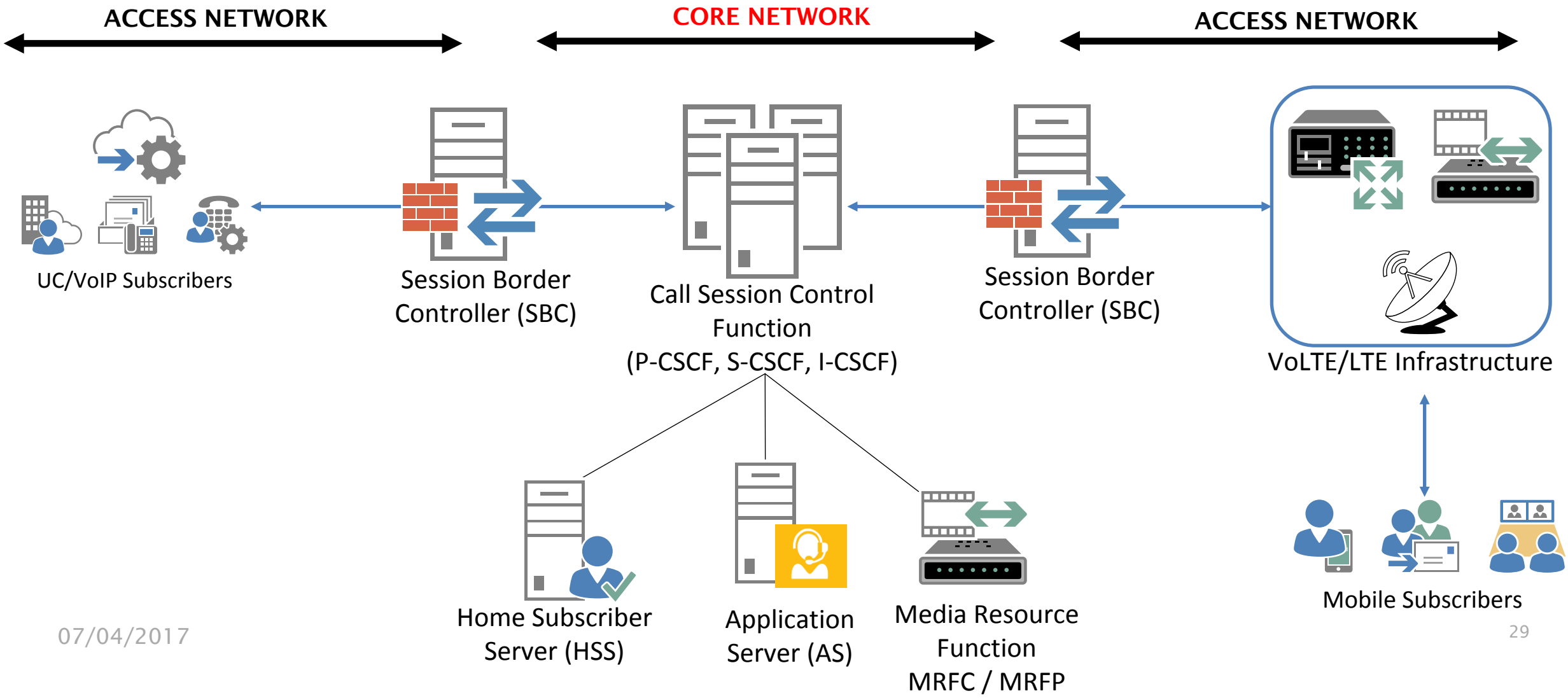
- Vulnerable CPE
  - Credential extraction
  - Attacking through embedded devices
- Insecurely located gateways
  - Hardware hacking, eavesdropping
  - Tampering gateways for persistent access
- SIP header manipulations
  - Toll Fraud
  - Attacking legacy systems (e.g. Nortel?)
  - Voicemail hijacking

Call Centre Security Testing

context

- 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

Mobile Networks (IMS / VoLTE)



Mobile Networks Testing

context

- Inter-vendor services design
- Accessing through mobile phones
  - Tampered phone/SIM/IMSI
  - IPSec interception for mobile phone – ENode-B traffic
- 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)

Security Testing Using Vipro(x)y

context

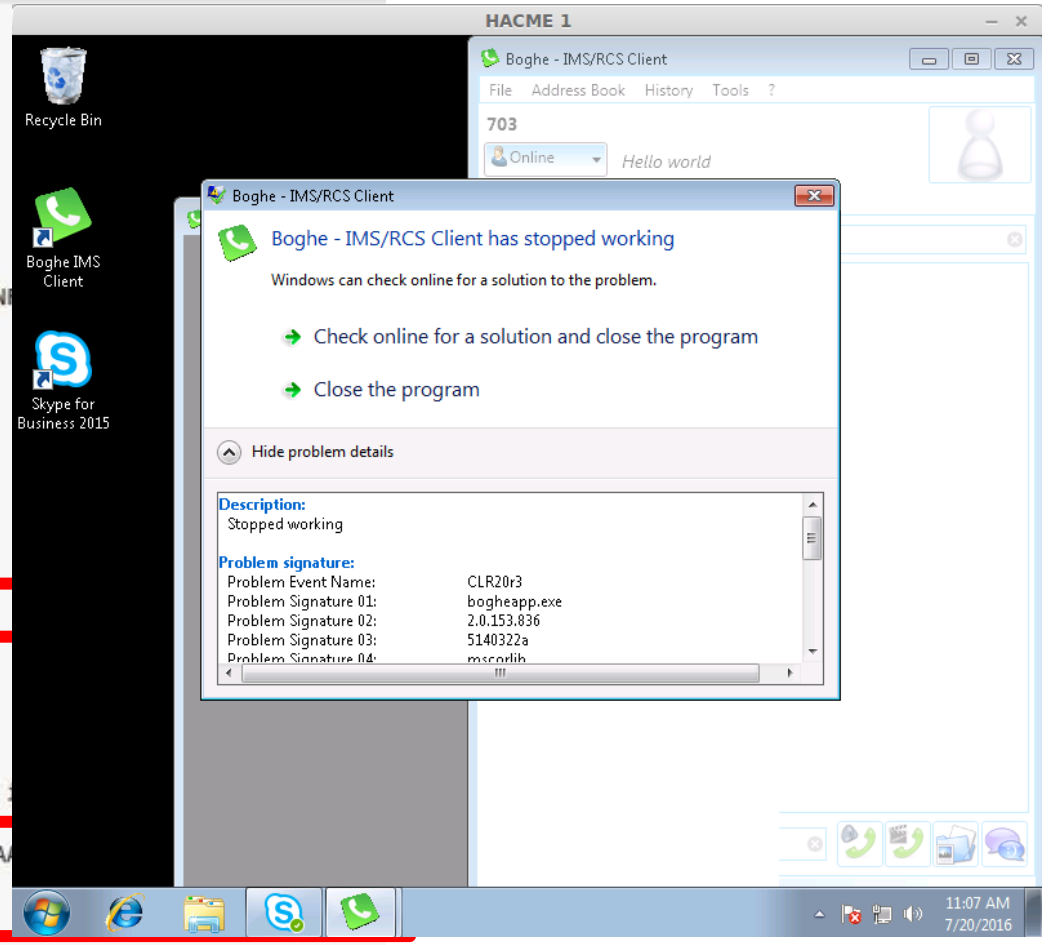
- Cloud communications
  - SIP header tests, caller ID spoofing,
  - Billing bypass, hijacking IP phones
- Signalling services
  - Attacking tools for SIP and Skinny
  - Advanced SIP attacks
    - **Proxy bounce, SIP trust hacking**
    - **Custom headers, custom message-types**
- UC tests w/ Viproxy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

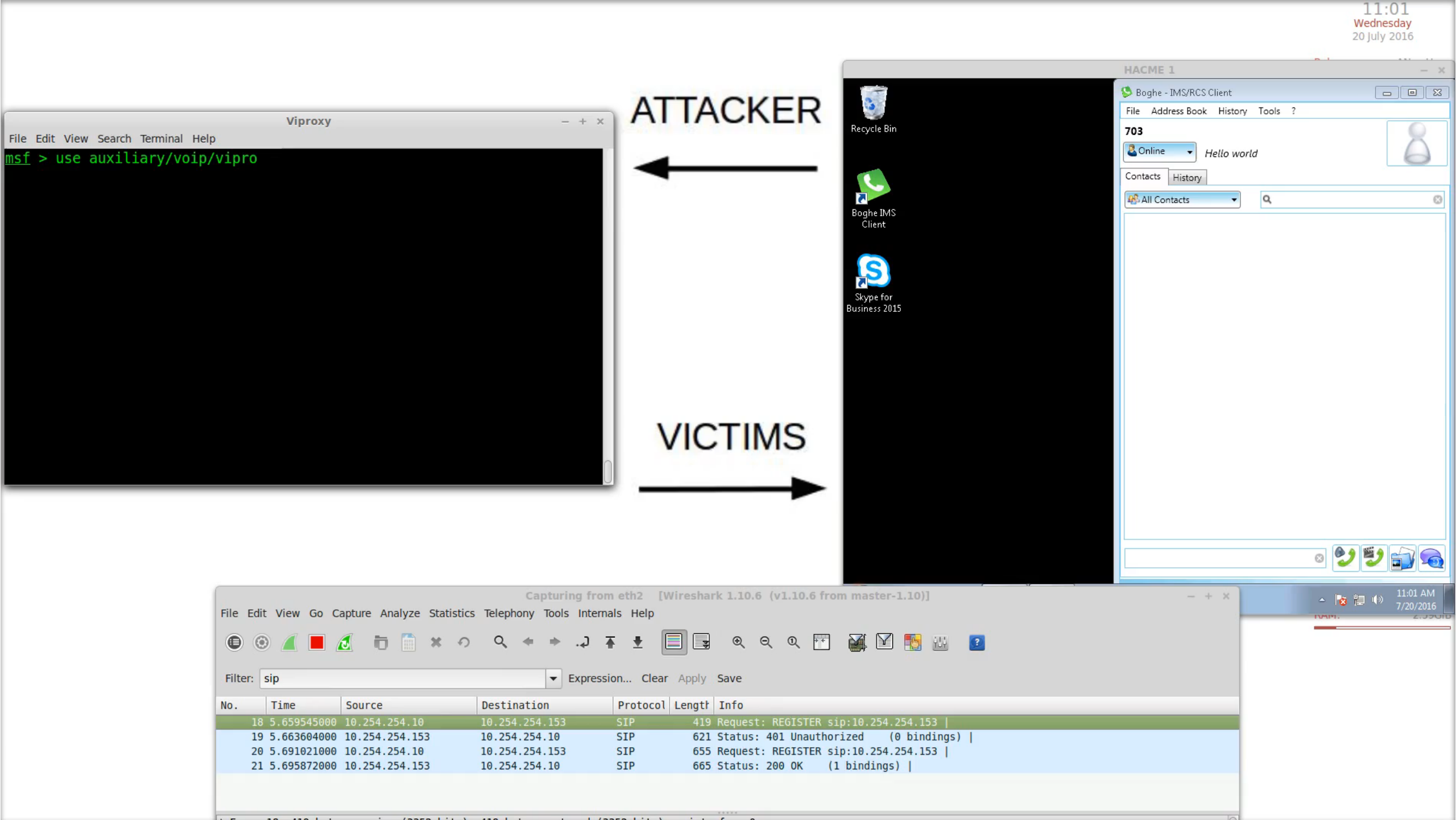
Sample SIP INVITE/SDP Exploit

context

```
▼ 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:"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    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) |

Viproyable PBX

context

Vulnerable VoIP server with exercises (hands-on during workshops)

- VoIP service discovery
- Enumeration using various responses
- Gathering unauthorised access to the extensions
- Hijacking voicemails
- Performing call spoofing attacks
- Discovering SIP trust relationships
- Harvesting information via IP phone configuration files
- Gaining unauthorised access to Asterisk Management
- Remote code execution through SIP services
- Remote code execution through FreePBX modules
- Decoding RTP sessions and Decrypting SRTP sessions for eavesdropping
- Exploiting Cisco CUCDM services

QumpIn Communications Analyser

context

- QumpIn: Communications Officer in Klingon
- Replaces Viproy and Viproxy
  - Lack of programming, lack of community support
  - Metasploit Framework, unstable communications
- What's On
  - Under development, pure Python 3.x code
  - Module structure like Empire and Metasploit Framework
- Phases
  1. Core functionalities of Viproy and Viproxy
  2. Advanced protocol and authentication support, fuzzers and exploits

Upcoming Features of QumpIn

context

Signalling Media

Cloud UC Assessment

Practical Exploits

IMS & VoLTE

IVR & CC Voicemail

Research Tools

Demonstrations

References

- Viproy VoIP Penetration Testing Kit
- QumpIn Communications Analyser
  http://www.viproy.com

- Context Information Security
  http://www.contextis.com

Any Questions

Context Information Security
https://www.contextis.com

Thanks

Context Information Security
https://www.contextis.com