



VOIP WARS: THE LIVE WORKSHOP

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

HEADLINES

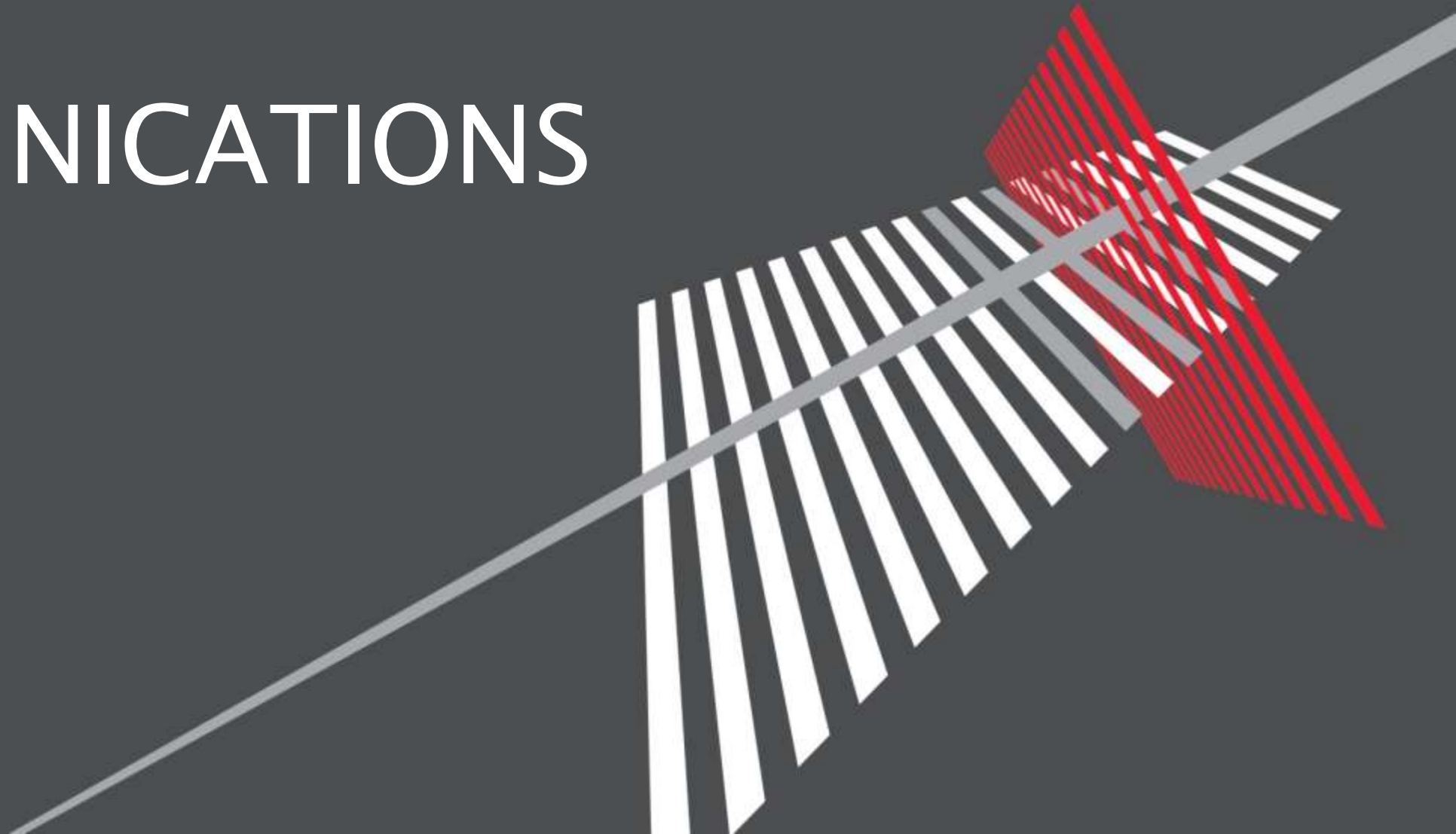
VOIP SERVER SECURITY

SIGNALLING SECURITY

**MEDIA TRANSPORT
SECURITY**

UC SUITES SECURITY

UNIFIED COMMUNICATIONS

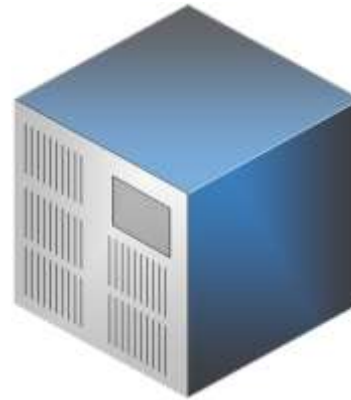


TRADITIONAL PHONE SYSTEMS



Alice

Audio Call

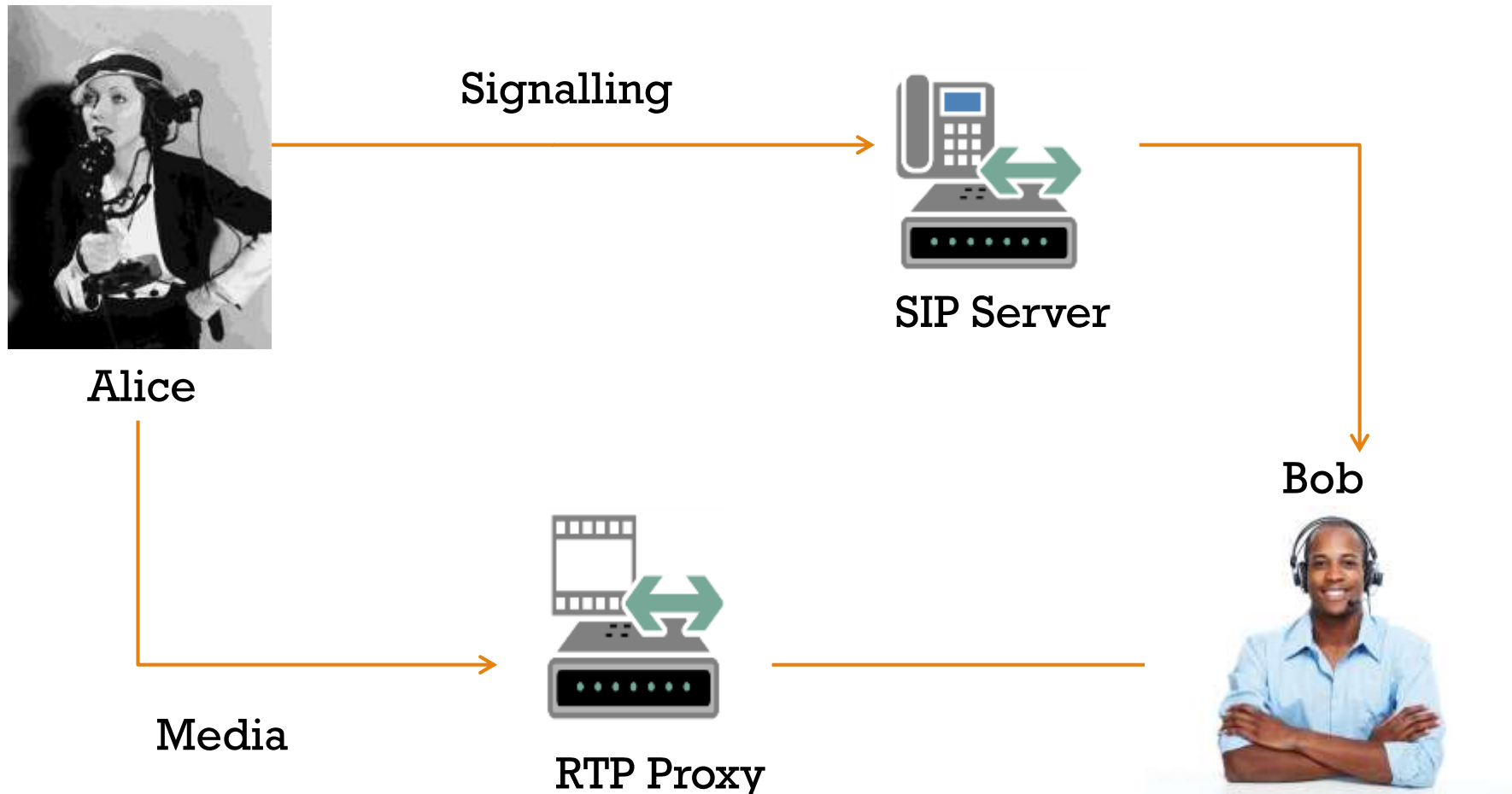


TDM

Bob



UNIFIED COMMUNICATIONS



UNIFIED COMMUNICATION SERVICES

- Audio and Video Calls
- Audio and Video Conferences
- Instant Messaging
- File or Content Sharing
- Screen Sharing



8

SECURITY CONCERNS



Cloud Communications

- Toll Fraud
- Tenant Isolation
- Confidentiality



Call Centre

- Availability
- Privacy (e.g. PII)
- Regulations



Subscriber Services

- Call quality
- Infrastructure
- Endpoint Security

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



USB CONTENT



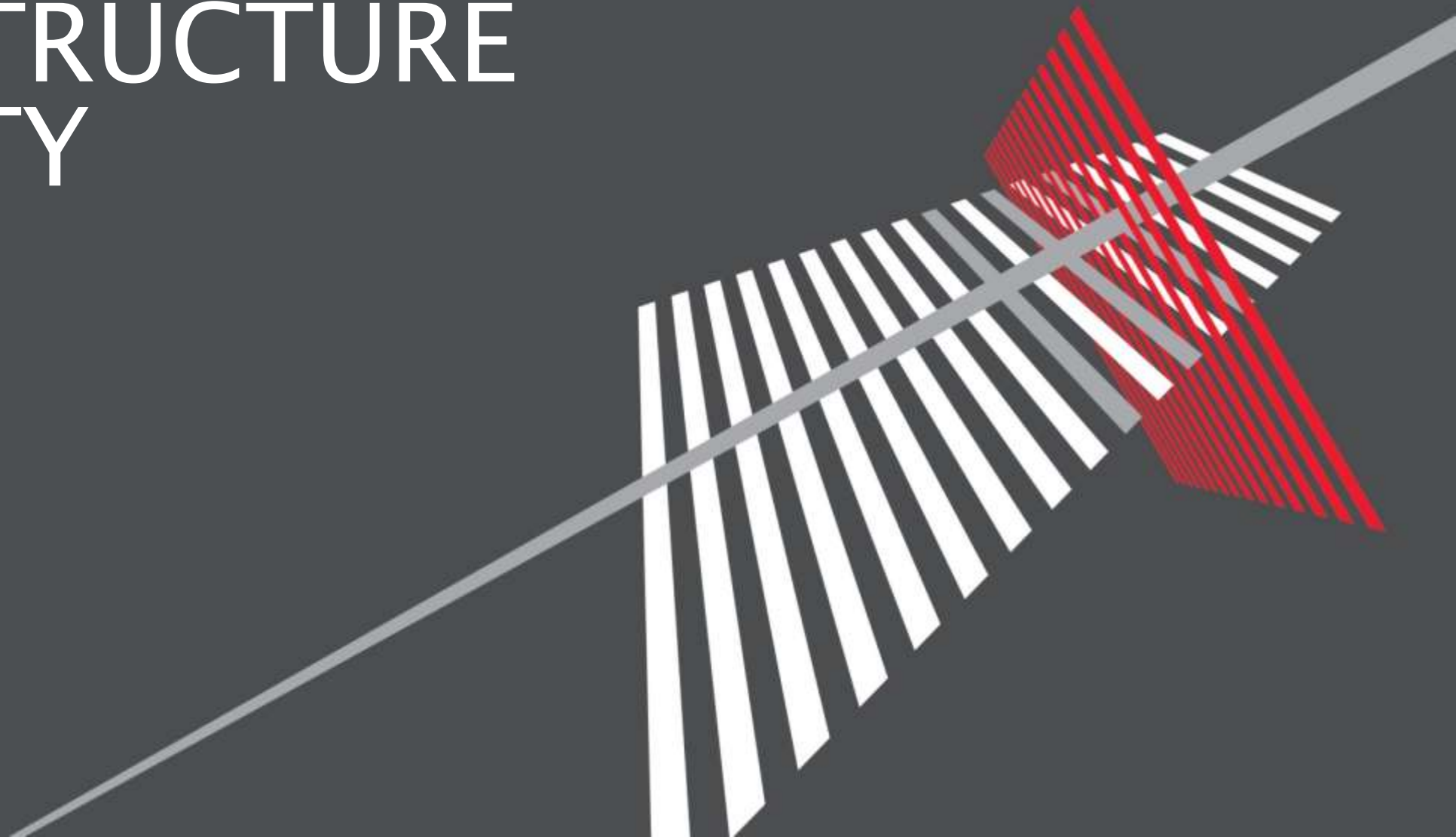
- Presentation in PDF
- Exercises booklet in PDF
- Virtual machines
 - Kali Linux with Viproy
 - Vulnerable SIP server
- Start VMs before exercises

EXERCISES LAB

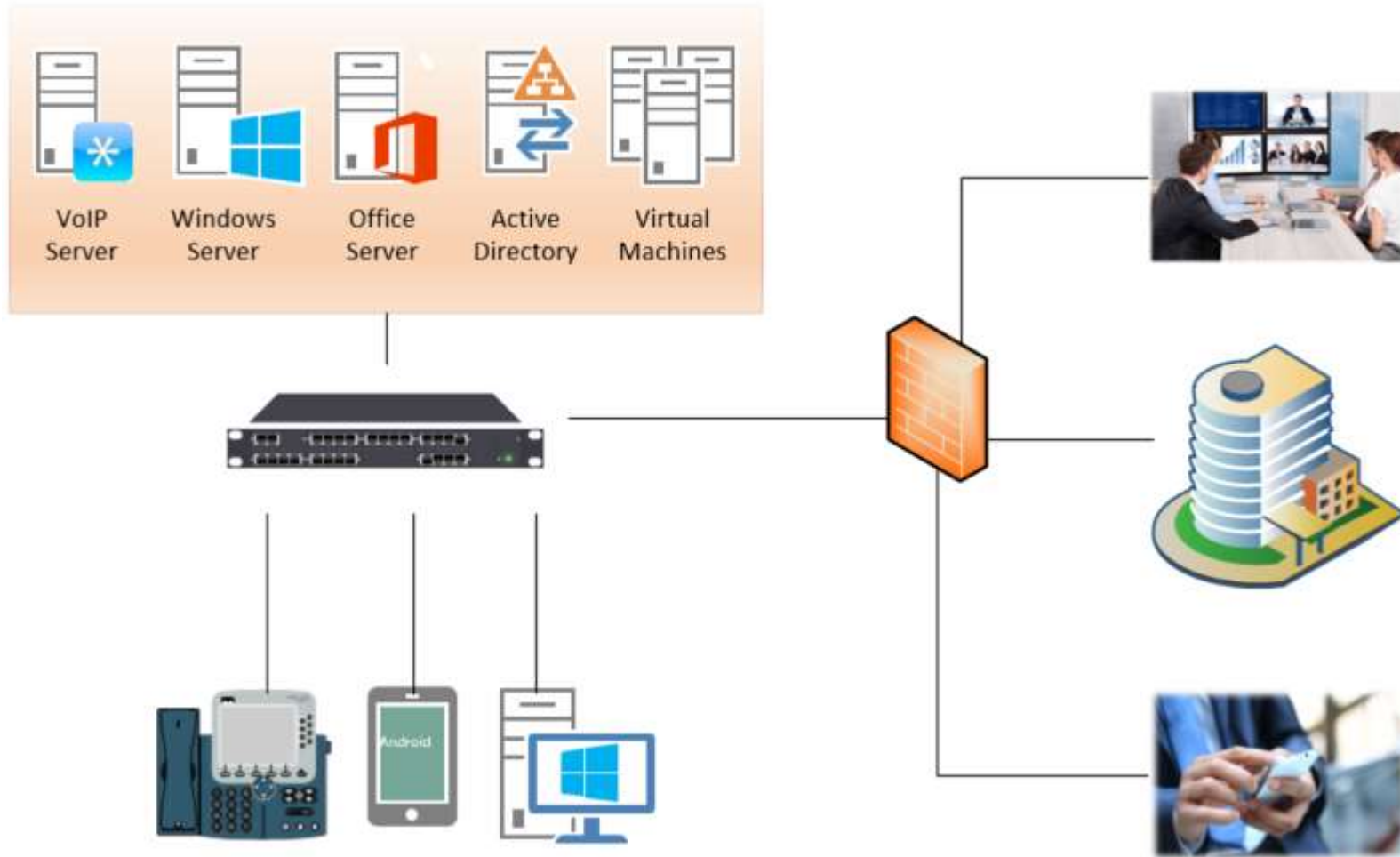


- Asterisk & FreePBX Server
 - VoIP Server Security
 - SIP and RTP Security
- Cisco CUCM
 - SIP and Skinny Security
- Microsoft Skype for Business
 - Analysing UC and Clients

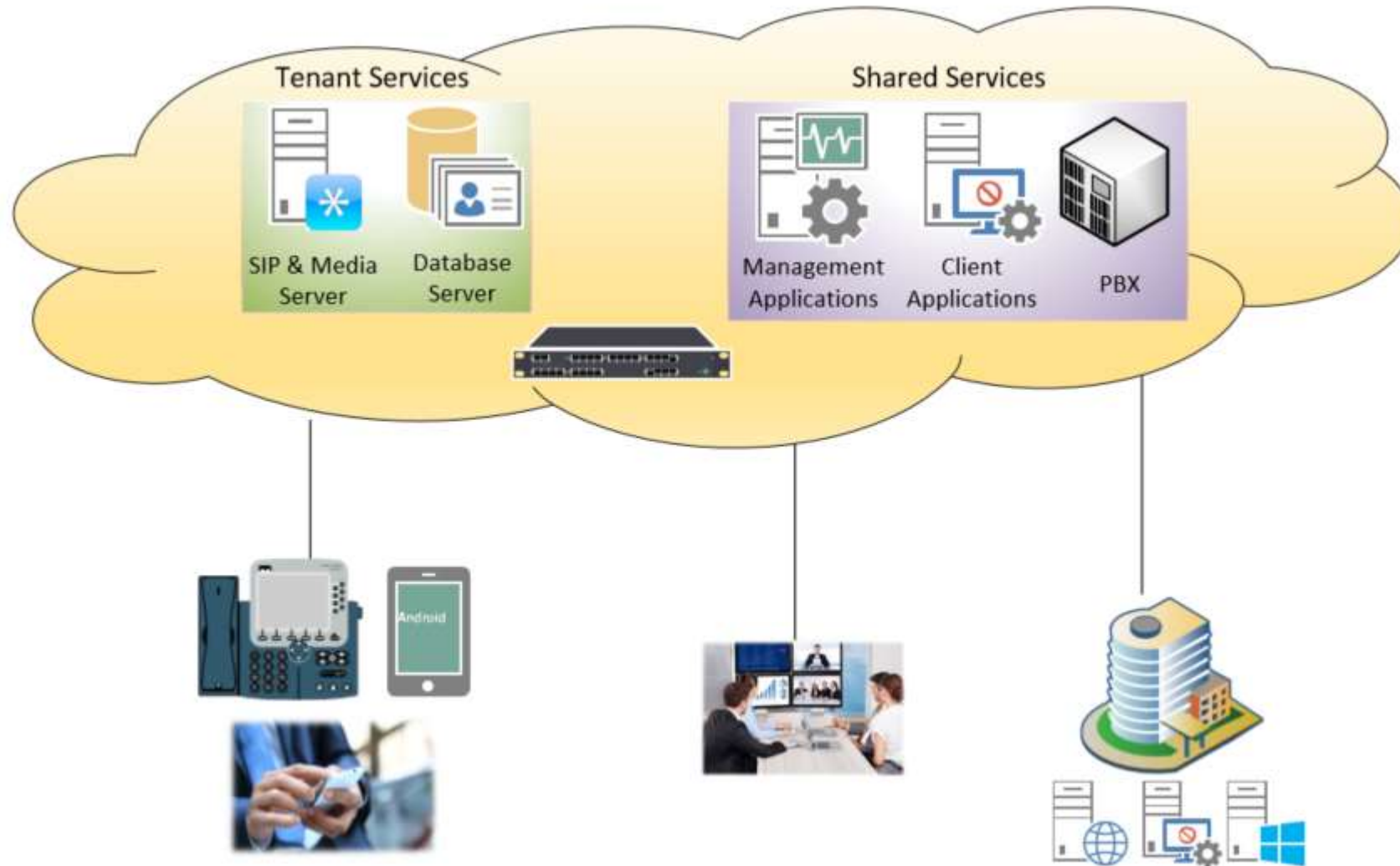
INFRASTRUCTURE SECURITY



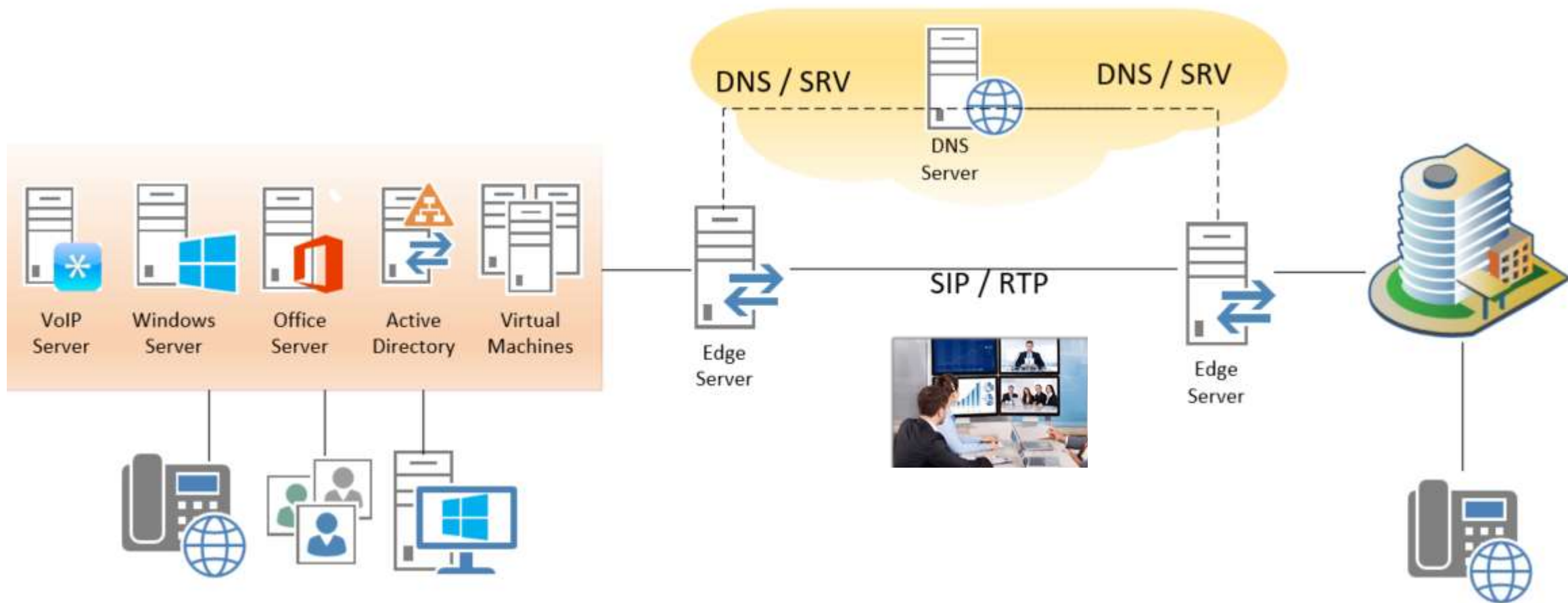
CORPORATE COMMUNICATIONS



CLOUD COMMUNICATIONS



FEDERATED COMMUNICATIONS



PHYSICAL ACCESS

- Service providers
 - Local distribution rooms and infrastructure
 - Network termination and endpoint facilities
- Larger organisations
 - Meeting room equipment
 - Public phones
 - Emergency or courtesy phones
- Persistent access via tampered devices
 - Tapberry Pi with PoE

ATTACKING INFRASTRUCTURE

- VLAN hopping
- DHCP sniffing and snooping
- ARP spoofing and MITM attacks
- Attacking TFTP servers
 - Collecting information (e.g. configuration, credentials)
 - Placing a rogue TFTP server (e.g. configuration upload)
- Attacking SNMP services

VOIP SERVER SECURITY



TO DO

- Discover servers and system services
- Vulnerability analysis of management services
 - Web applications and service APIs
 - Traditional services (Telnet, SSH, Asterisk console)
- Exploit the vulnerabilities for
 - Sensitive information (e.g. Voice or IVR recordings)
 - Persistent toll fraud
 - Persistent eavesdropping

SERVICES VS DEVICES

- Signalling servers
- Media and signalling gateways
- Session Border Controllers and Proxies
- IP phones
- Teleconference devices



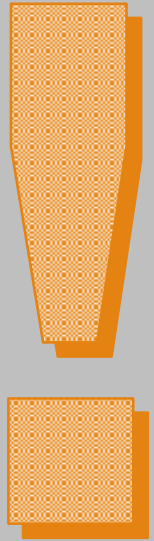
DISCOVERY

- Essential services
 - Signalling services
 - Media gateway or proxies
 - Management services
- Web services (Self-care portal, Logs, Billing)
- Looking for
 - Software information (e.g. type, version, patch level)
 - Weak credentials
 - Known vulnerabilities

SAMPLE VULNERABILITIES

- Shellshock (BASH) remote code execution
 - Heartbleed memory leak
 - FreePBX remote code execution
 - Harvesting credentials from IP phone config files
 - Weak credentials
 - Asterisk management console
 - FreePBX web interface
 - Cisco telnet/SSH interface
- *Numerous servers have missing security updates

EXERCISE



SIGNALLING SECURITY



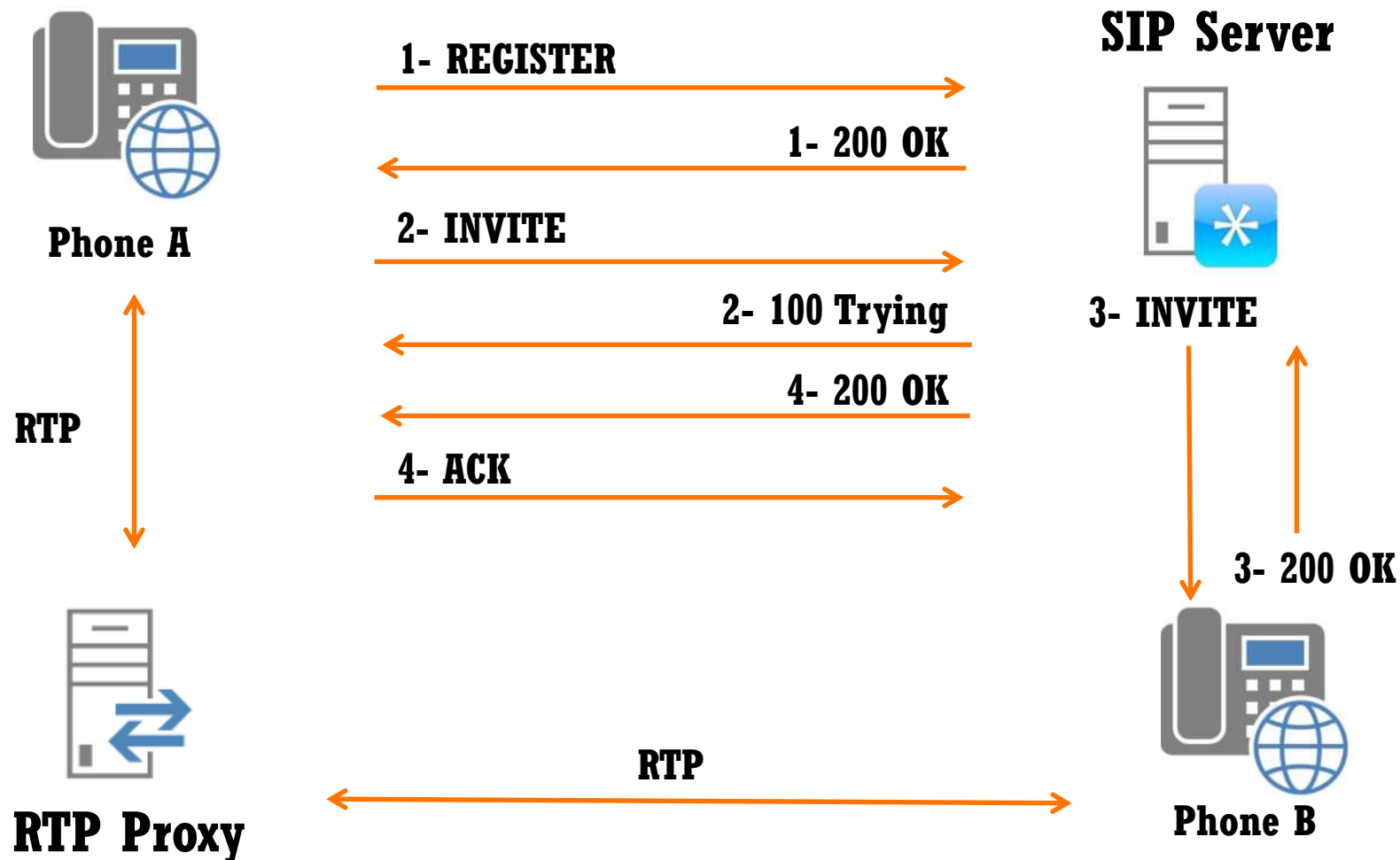
TO DO

- Collect information from signalling services
- Analyse authentication and authorisation
- Bypass call restrictions and billing
- Exploit the vulnerabilities and design issues for
 - Toll fraud
 - Billing and CDR bypass
 - TDoS and DDoS attacks

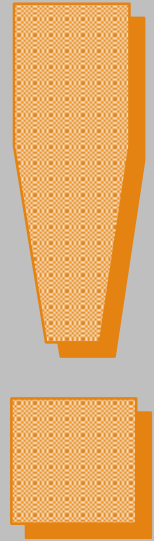
SESSION INITIATION PROTOCOL (SIP)

- It was developed in 1996, standardised in 2002
- SIP methods (e.g. Register, Invite, Message)
- Session Description Protocol (SDP)
- TLS / MTLS for encryption
- Authentication types
 - Digest
 - TLS-DSK
 - NTLM
 - Kerberos

BASIC SIP FLOW



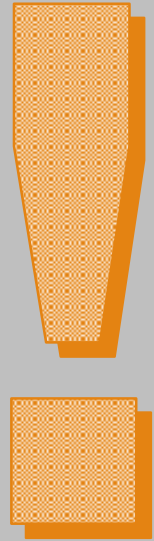
ANALYSIS



SIP SERVICE ANALYSIS

- Service tests
 - Information disclosure (e.g. software, methods)
 - Authentication (e.g. brute force, enumeration)
 - Authorisation (e.g. dial out, caller ID spoofing)
 - Discovery (e.g. trunk, gateway, proxy, voicemail)
- Advanced
 - SIP header injection (e.g. Remote-Party-ID, P-Charging-Vector, P-Asserted-Identity)
 - SIP trust hacking
 - SIP proxy bounce attack

DEMO



PRACTICAL CALLER ID SPOOFING

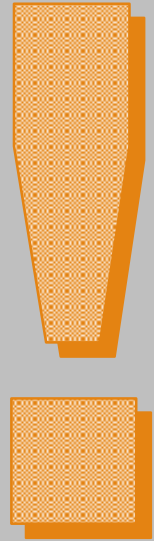
Header injection

Remote-Party-ID: <sip:31337@1.2.3.4>;party=called;screen=yes;privacy=off

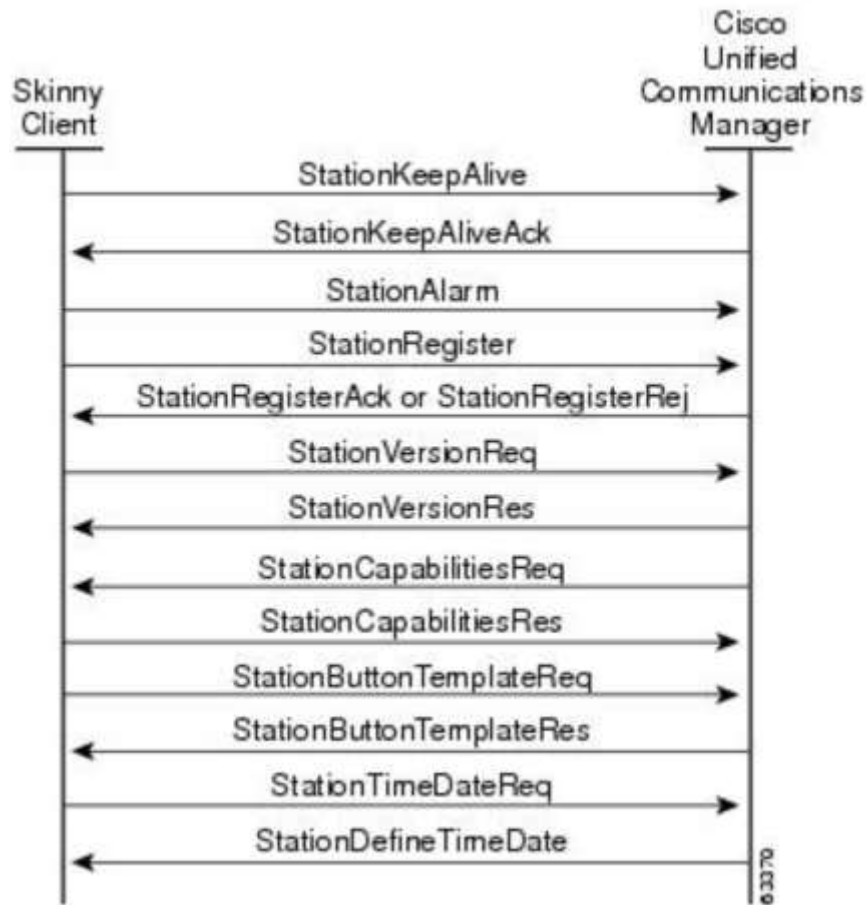
P-Asserted-Identity: <sip:31337@1.2.3.4>;party=called;screen=yes;privacy=off

- Voicemail, Call back systems, Social engineering
- Value added services via Ringing or Messages
 - Add a data package to my line
 - Subscribe me to a new mobile TV service
 - Reset my password/PIN/2FA
 - Group messages, celebrations

DEMO

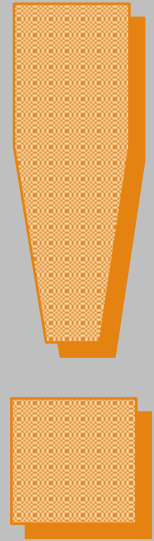


CISCO SCCP (SKINNY)



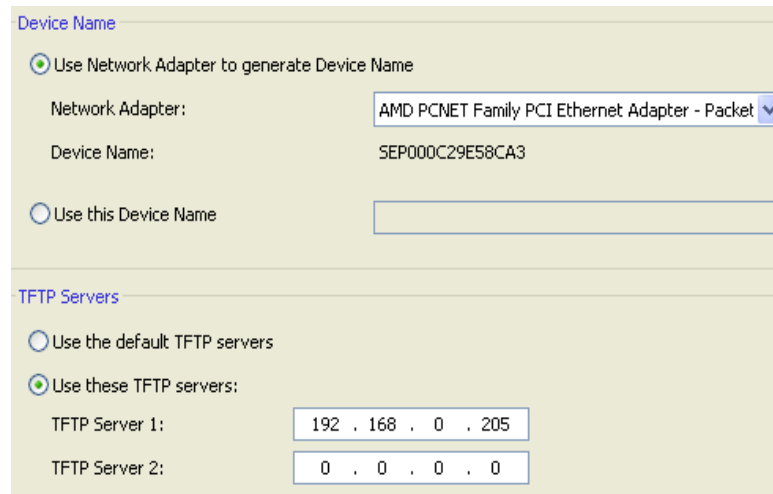
- Binary signalling
- Authentication
 - MAC + Phone model
 - Digital certificate
- Attack vectors
 - Impersonating an IP phone
 - Caller ID spoofing
 - Unauthorised calls
 - DoS attacks

ANALYSIS



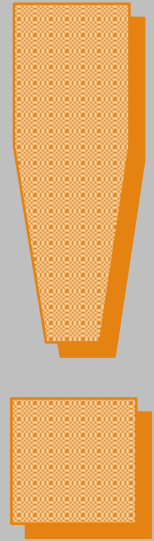
PREPARING A CLIENT FOR SKINNY

- Cisco IP Communicator (CIPC)
- Set the target device name (MAC address)
- Impersonate the target CIPC

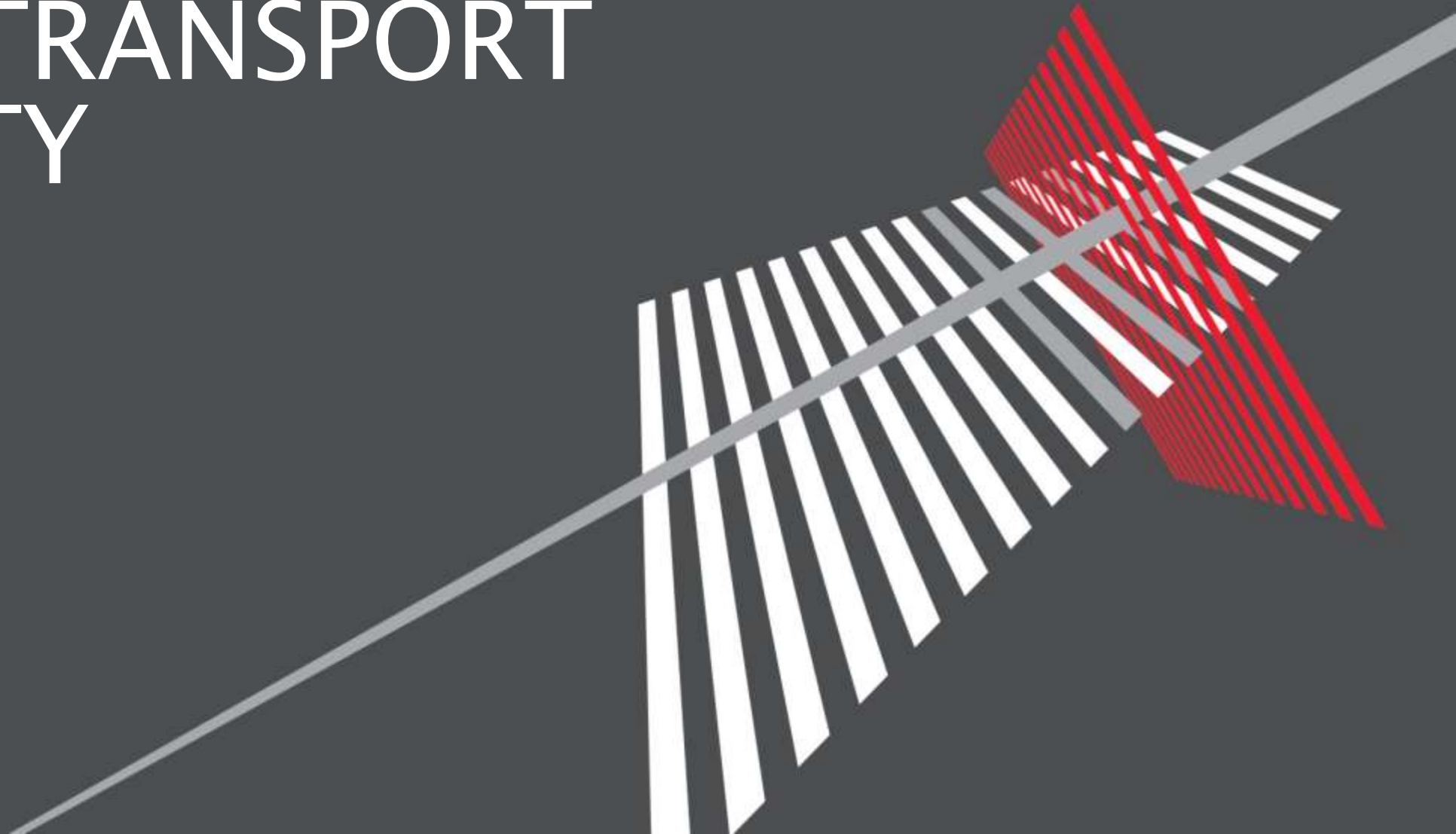


* Viproy supports multiple phone IDs for skinny

EXERCISE



MEDIA TRANSPORT SECURITY



TO DO

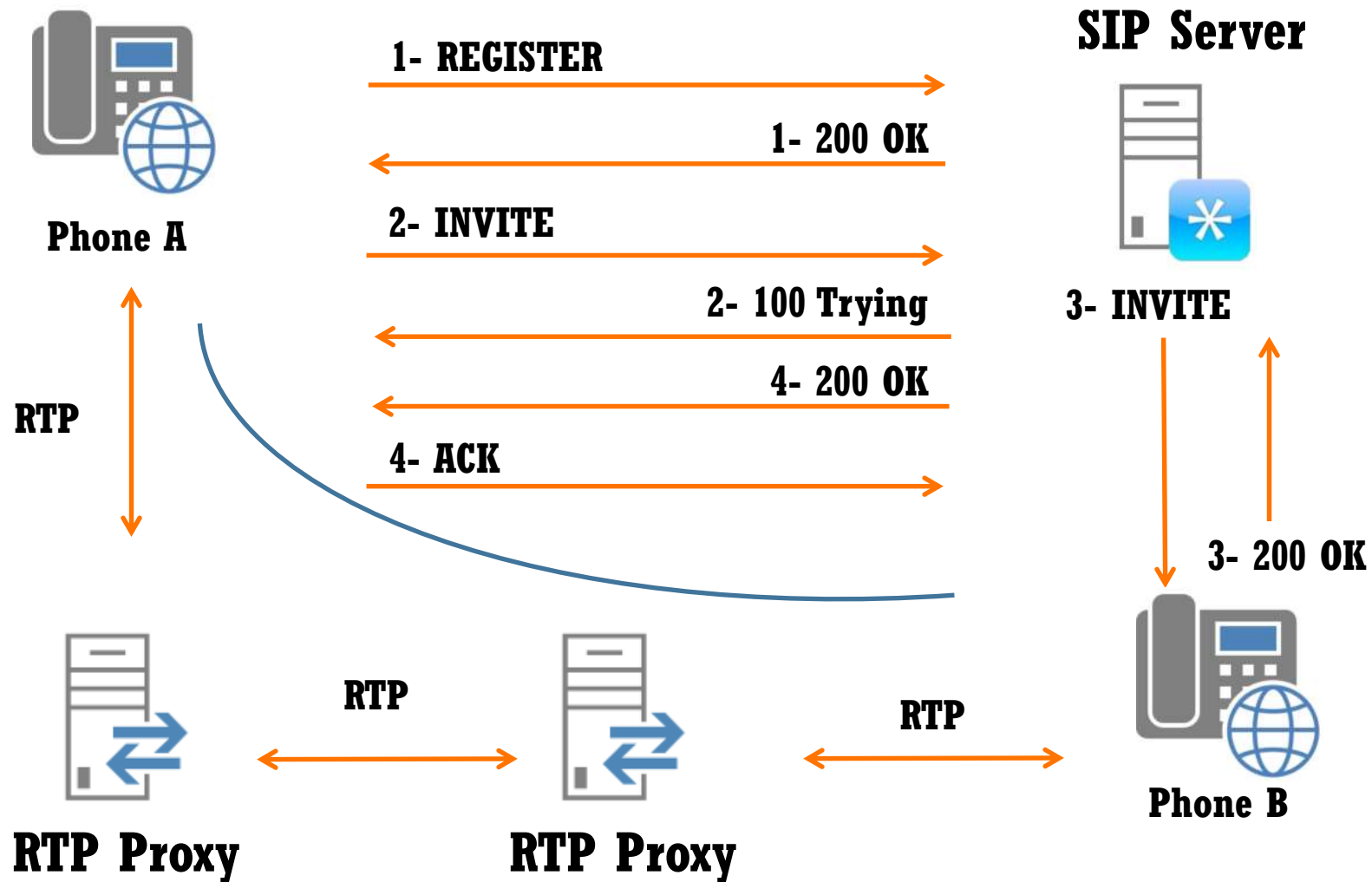
- Intercepting or capturing RTP/SRTP traffic
- Decrypting the SRTP traffic
- Converting the RTP content to raw media formats

- Performing attacks for
 - Eavesdropping
 - Content (audio/video) injection

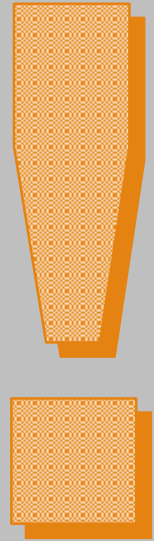
MEDIA TRANSPORT FUNDAMENTALS

- Real-time Transfer Protocol (RTP)
 - Vulnerable to MITM
 - Media is not encrypted
 - DMTF tones are transmitted as RTP events
- Secure Real-time Transfer Protocol (SRTP)
 - SDES (Symmetrical encryption w/ key exchange via SIP)
 - ZRTP (Asymmetrical encryption w/ Diffie-Hellman)
 - SRTP MIKEY (Symmetrical encryption w/ key management)

BASIC RTP FLOW



ANALYSIS



PRACTICAL ATTACKS

- Performing network interception for RTP
 - ARP spoofing, DHCP snooping, DNS spoofing
- Updating the SIP/SDP content for interception
 - IP addresses used for RTP proxies or endpoints
 - Updating the codecs
 - Updating or capturing the encryption keys
- Extracting the streams from RTP traffic
- Decrypting the SRTP traffic
- Decoding the streams to raw media formats

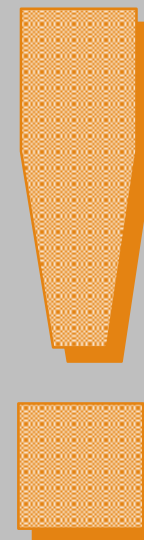
DECRYPTING SRTP

- Capture the traffic
- Find the key in the SIP/SDP content
- Dump the SRTP traffic from Wireshark
- Decrypt the content using srtp-decrypt
- Stream the unencrypted traffic to Wireshark back

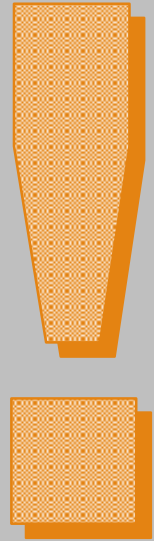
Hacking VoIP – Decrypting SDES Protected SRTP Phone Calls

<https://www.acritelli.com/hacking-voip-decrypting-sdes-protected-srtp-phone-calls>

DEMO



EXERCISE



SECURITY OF UNIFIED COMMUNICATION SUITES



TO DO

- Understanding the UC solution and design
- Attacking the cloud design (e.g. isolation, services)
- Identifying the vulnerabilities published
- Attacking client and server software used
- Exploit the vulnerabilities for
 - Jailbreaking the UC services tenant isolation
 - Compromising all clients and servers
 - Placing persistent toll fraud or backdoors

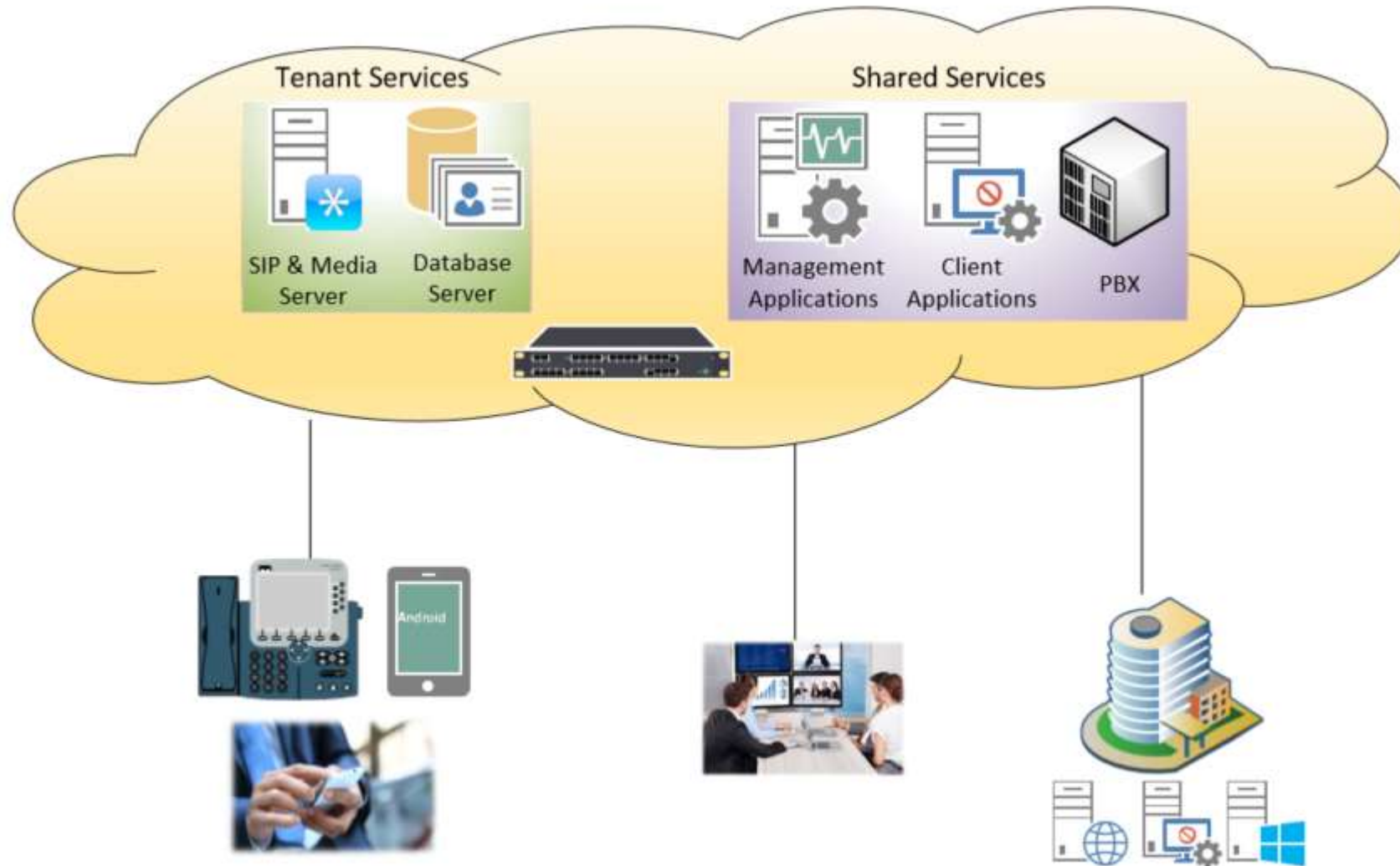
UC DESIGN AND ATTACKS

- Unified Communication Solutions
 - Cisco Hosted Collaboration Suite (CUCM, CUCDM, CUPS)
 - Microsoft Skype for Business (a.k.a MS Lync)
 - Open source solutions (Kamalio, Asterisk, FreeSwitch)
 - Other commercial solutions (Avaya, Alcatel, Huawei)
- Attacking through
 - Signalling services
 - Cloud management and billing services
 - Client services (e.g. self-care portals, IP phone services)
 - Trust relationships and authorisation scheme

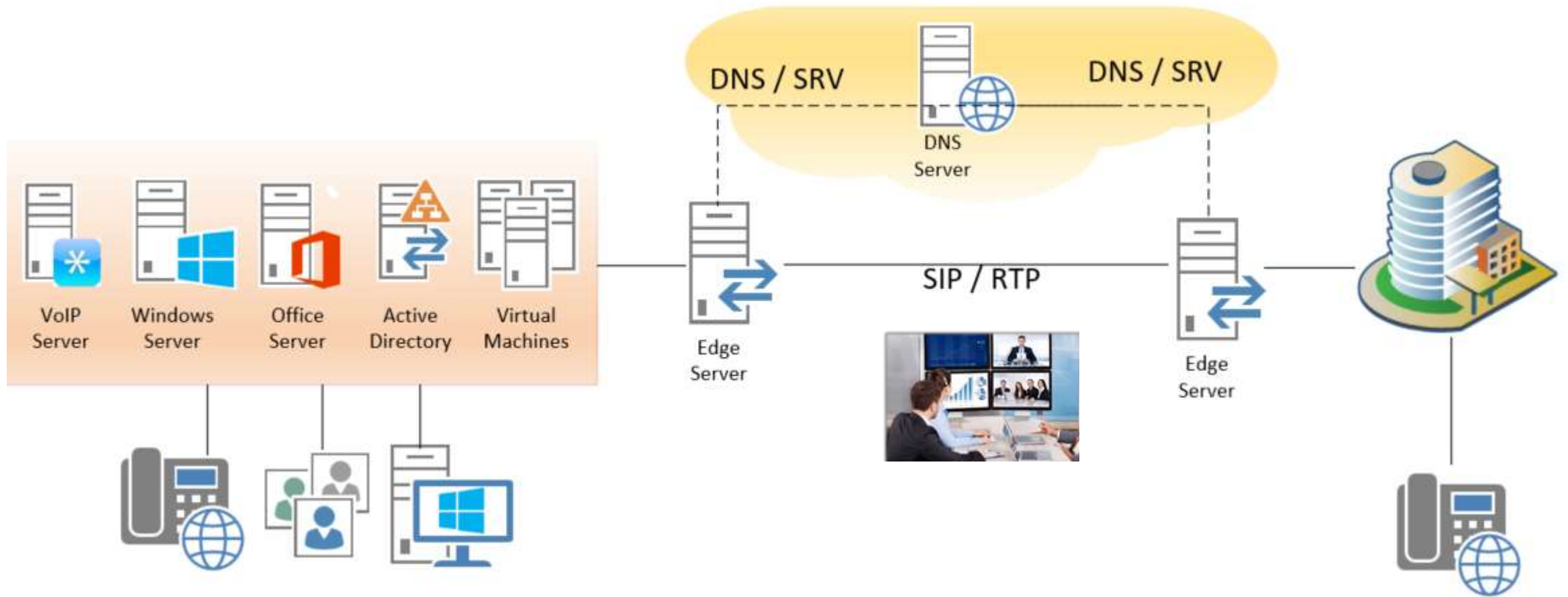
WARMING UP

- 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

CLOUD COMMUNICATIONS



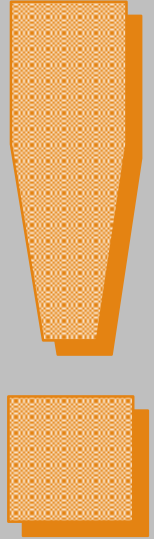
FEDERATED COMMUNICATIONS



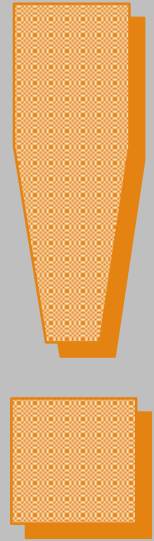
PRACTICAL ATTACKS FOR UC

- Exploiting business logic issues via Viproy
 - Caller ID spoofing, Billing bypass, Voicemail hijacking
- Exploiting cloud VoIP services
 - Using Viproy for CUCDM exploitation
 - Exploiting enumeration, XSS, SQL injection and privilege escalation issues of CUCDM
- Exploiting VoIP clients
 - Exploiting generic clients via Viproy (e.g. Boghe)
 - Exploiting commercial client via Viproxy (e.g. SFB, Jabber)

DEMO



EXERCISE



REFERENCES

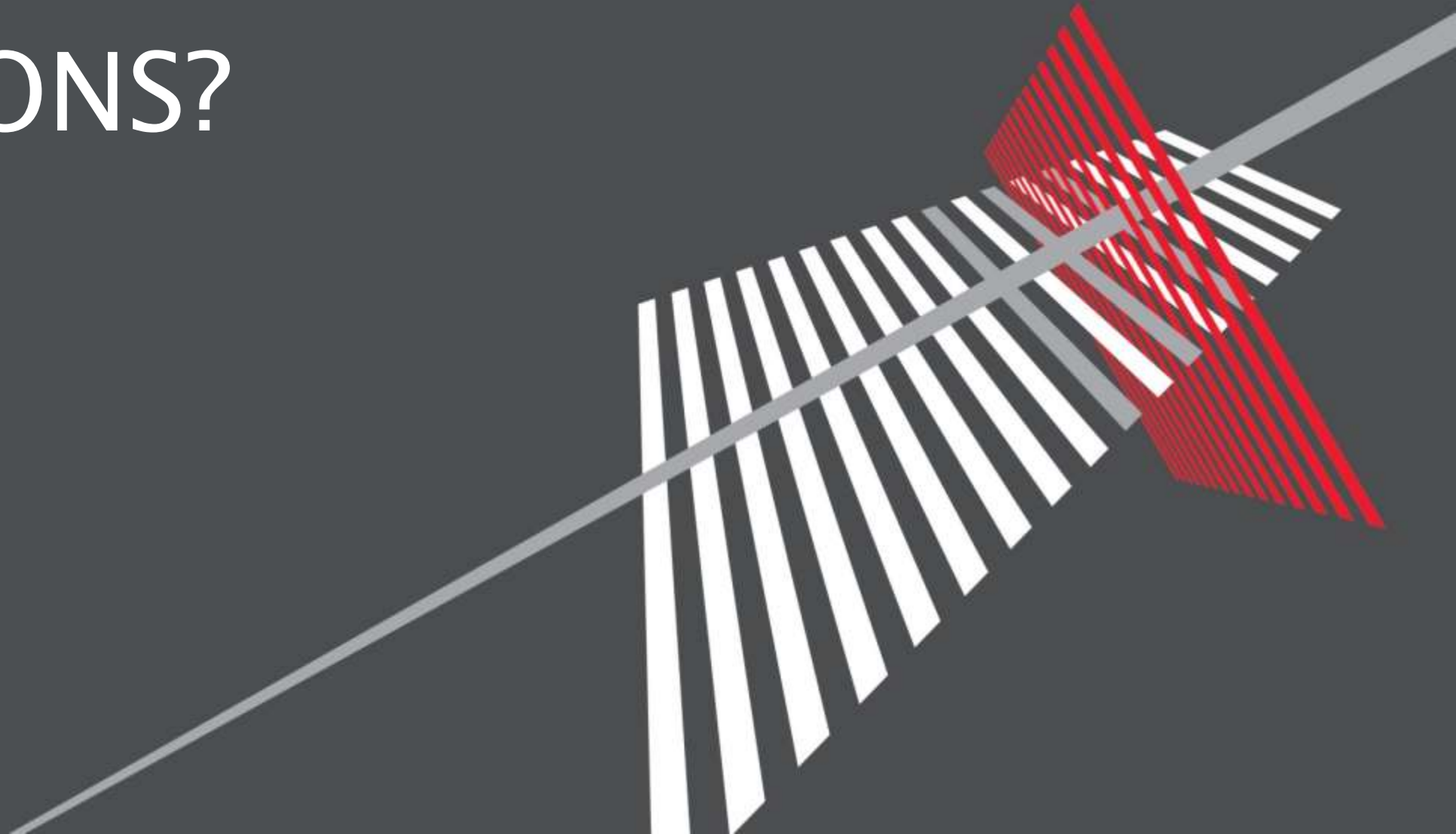
- Viproy VoIP Penetration Testing Kit

<http://www.viproxy.com>

- Context Information Security

<http://www.contextis.com>

QUESTIONS?



THANKS!

