RECITE
Revista Carioca de Ciência, Tecnologia e Educação

# INTERCEPTAÇÃO E ESCUTA DO FLUXO VoIP UTILIZANDO WIRESHARK

**Ismael Xavier Pinto**
Centro Universitário UniCarioca
https://orcid.org/0000-0002-1947-4770

Data de Submissão: 27/09/2022
Data de Aprovação: 30/12/2022

## RESUMO

O artigo apresenta, dentre muitas, ao menos uma fragilidade na implementação de configurações padrões que vem de fábrica ou são mal feitas nos *softwares* das centrais privadas de comunicações por ramais (PBX) em ambientes de produção, que tratam a interceptação das conversas por agentes não autorizados através da exploração e mineração das Redes nos elementos que constituem a estrutura de comunicação *VoIP*, como o protocolo *SIP* e *RTP*. A metodologia utilizada é simples, porém exige um certo grau de conhecimento na utilização de *sniffer* de rede, como por exemplo o *Wireshark*, para fazer a identificação e separação do tráfego, análise, decodificação e extração da conversa audível. Em síntese, além de demonstrar a vulnerabilidade, o artigo que teve o desenvolvimento da demonstração da fragilidade em ambiente controlado para fins de conhecimento e caráter científico, apresenta alternativa de configuração e utilização de elementos tecnológicos que contribuem na proteção da conversa em ambiente de Rede.
**Palavras-chave**: segurança cibernética; voip; wireshark; escuta telefônica; codec.

## *INTERCEPTION AND LISTENING OF THE VOIP FLOW USING WIRESHARK*

## *ABSTRACT*

*The article presents, among many, at least one fragility in the implementation of standard configurations that come from the factory or are poorly made in the software of private branch exchanges by extensions (PBX) in production environments, which deals with the interception of conversations by unauthorized agents through the exploitation and mining of Networks in the elements that constitute the VoIP communication structure, such as the SIP and RTP protocol. The methodology used is simple, but requires a certain degree of knowledge in the use of network sniffers, such as Wireshark, to identify and separate the traffic, analyze, decode and extract the audible conversation. In summary, in addition to demonstrating the vulnerability, the article that had the development of the demonstration of protection in a controlled environment and for purposes of knowledge and scientific character, presents alternative for configuration and use of technological elements that they created in the protection of the conversation in a Network environment.*
***Keywords**: cyber security; voip; wireshark; wiretapping; codec.*

## *INTERPRETACIÓN Y ESCUCHA VoIP CON WIRESHARK*

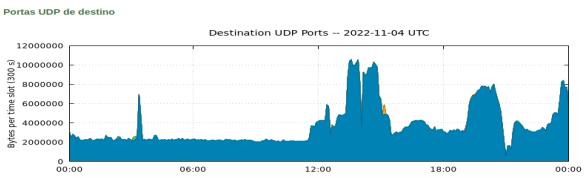
## *RESUMEN*

*El artículo presenta, entre muchos, al menos una debilidad en la implementación de configuraciones estándar que vienen de fábrica o están mal hechas en el software de las centrales telefónicas privadas (PBX) en entornos de producción, que trata de la interceptación de conversaciones por agentes no autorizados a través de la exploración y minería de redes en los elementos que constituyen la estructura de la comunicación VoIP, como los protocolos SIP y RTP. La metodología utilizada es sencilla, pero requiere un cierto grado de conocimiento en el uso de sniffer de red, como Wireshark, para realizar la identificación y separación del tráfico, análisis, decodificación y extracción de la conversación audible. En resumen, además de demostrar la vulnerabilidad, el artículo que tuvo el desarrollo de la demostración de la fragilidad en un ambiente controlado para fines de conocimiento y científicos, presenta alternativas de configuración y utilización de elementos tecnológicos que contribuyen en la protección de la conversación en un ambiente de Red.*
***Palabras clave:*** *ciberseguridad; voip; wireshark; escuchas; códec.*

## 1 - INTRODUÇÃO

O serviço de ***Voice over Internet Protocol* – VoIP**, é uma realidade em todo o mundo desde 1995. Sua operação é transformar a voz, sinais analógicos, em pacotes digitais capazes de serem transportados por modernos sistemas de comutação digitais. A explosão de aplicativos de chamadas audiovisuais, denominado *streaming*, são efetuados entre dispositivos com algum tipo de aplicativo *softphone*, porém muitos desconhecem a tecnologia existente por trás deste serviço que hoje traz comodidade, além de possibilitar um custo menor em chamadas de curta e de longa distância apenas utilizando a Rede local e a *Internet* sem a necessidade de intervenção da operadora de telefonia.
Sob o prisma de Ross, o VoIP é uma tecnologia convergente porque pode interoperar em diferentes plataformas e fabricantes, além de ser capaz de transportar áudio, vídeo e dados pela internet e se manter em plena evolução nos dias atuais. VoIP – Voz sobre IP
A tecnologia VoIP, difundida nas corporações de todos os portes e no cotidiano das pessoas, é implementada em aparelhos telefônicos IP, *smartphones*, *tablets* e computadores através de inúmeros *softwares* proprietários e *open source*, como o MicroSIP, PortSip, Zoiper, Whatsapp, Skype *etc*, sendo a principal forma de comunicação a utilização da voz, deixando a escrita em segundo plano. Por isso, segundo apuração de dados estatísticos, nos últimos 5 (cinco) anos, de 2018 a 2022, o protocolo mais explorado é o SIP, sendo nas últimas 24h com 97,77% dos ataques cibernéticos, como mostra a Figura 1.

Figura 1: Estatística de ataque ao protocolo SIP




| # | Chave | Porta | Nome | Total | | Máx. | Média |
|---|---|---|---|---|---|---|---|
| 01 | | 5060 | SIP (Protocolo de Iniciação de Sessão) | 1,06 GB | 97,77% | 35,25 KB/s | 12,28 KB/s |
| 02 | | 123 | NTP (protocolo de tempo de rede) | 1,49 MB | 0,14% | 596,47 B/s | 17,28 B/s |
| 03 | | 161 | SNMP (Protocolo de Gerenciamento de Rede Simples) | 1,31 MB | 0,12% | 607,50 B/s | 15,15 B/s |
| 04 | | 500 | ISAKMP | 1,20 MB | 0,11% | 1,17 KB/s | 13,84 B/s |
| 05 | | 6500 | N / D | 1,03 MB | 0,10% | 3,29 KB/s | 11,96 B/s |
| 06 | | 1900 | SSDP | 899,77 KB | 0,08% | 77,33 B/s | 10,41 B/s |
| 07 | | 53 | DNS (Sistema de Nomes de Domínio) | 803,85KB | 0,07% | 894,20 B/s | 9,30 B/s |
| 08 | | 389 | LDAP (Lightweight Directory Access) | 783,24 KB | 0,07% | 526,50 B/s | 9,07 B/s |
| 09 | | 443 | N / D | 636,78 KB | 0,06% | 721,97 B/s | 7,37 B/s |
| 10 | | 1434 | Monitor do Microsoft SQL | 506,52 KB | 0,05% | 667,63 B/s | 5,86 B/s |

Fonte: cert (2022).

Neste contexto, o problema do artigo é a interceptação não autorizada de conversas em centrais *VoIP* particulares por agentes não autorizados e a apresentação de ao menos um método que contribui para mitigar as escutas clandestinas.
Desta forma, o objetivo geral proposto nesta pesquisa constituiu-se em apresentar a interceptação de um fluxo *SIP* em andamento com a sinalização criptografada com *TLSv1.2* e ouvir a conversa, cujo o sistema esteja sem nenhuma ou pouca segurança. Para tal, teve-se como objetivos específicos a utilização do *software sniffer*, conhecido como *Wireshark*, amplamente utilizado para análise de Rede por equipes *Red Team* e *Blue Team* para a identificação e separação do fluxo *streaming*, análise do fluxo separado, decodificação e escuta do fluxo VoIP.

### 1.1 - Abordagem

Neste artigo foi adotado uma abordagem prática que estão descritas as várias etapas de desenvolvimento do experimento até a sua conclusão final e para isto, faz-se a utilização de figuras ilustrativas, gráficos para o melhor entendimento e aprendizado. Importante observar que estas orientações aqui descritas estão baseadas nas atuais tecnologias vigentes e que deverão passar por atualizações sempre que disponibilizadas e se fizer necessária.

## 2 - FUNDAMENTAÇÕES

Entender um pouco mais sobre como acontece a comunicação entre dois terminais *SIP* é muito importante para assimilar o conhecimento e conceber o conceito da tecnologia *VoIP*. Por outro lado, deve-se levar em consideração as leis vigentes do país e as consequências em não observá-las.

### 2.1 - Teórica

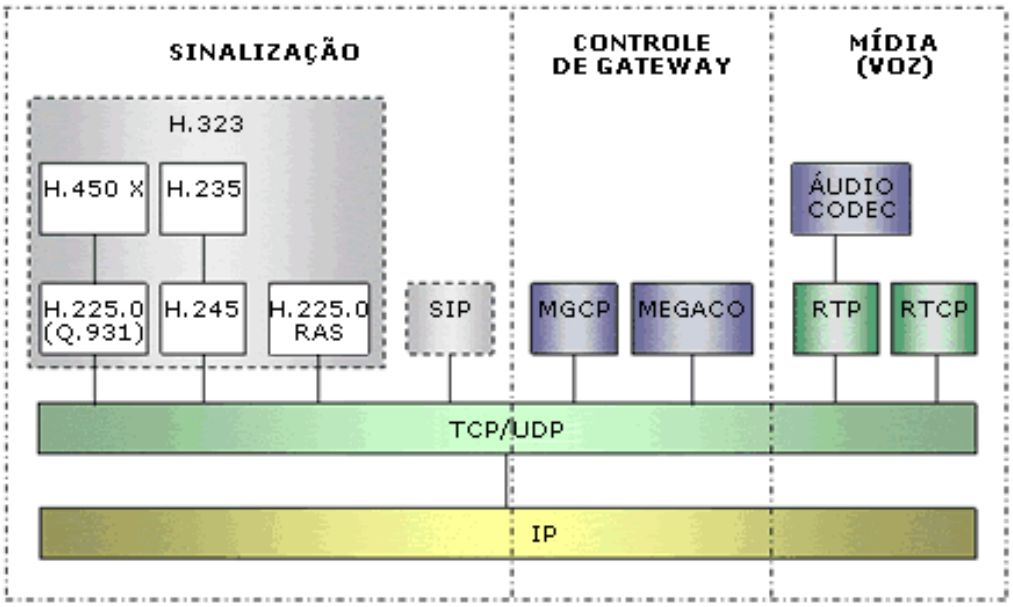
Neste tópico, buscou-se, na doutrina literária, dentre diversos autores independentes e instituições renomadas, uma abordagem resumida dos principais protocolos de segurança envolvidos no processo da comunicação VoIP. Vejamos.
O *National Institute of Standards and Tecnology* – NIST, define que “Voice over Internet Protocol (VOIP) refere-se à transmissão de fala através de um estilo de rede de dados. Essa forma de transmissão é conceitualmente superior à comunicação comutada por circuito convencional em muitos aspectos”. Security Considerations for Voice Over IP Systems.
Segundo Ross, “Dentre as muitas tecnologias convergentes, capazes de transportar voz e dados pela internet, uma das que mais se destaca atualmente é a chamada Voz sobre IP ou simplesmente VoIP”. VoIP – Voz sobre IP
Kurose, afirma que “áudio interativo em tempo real pela internet é frequentemente denominado **telefone por internet**, já que, da perspectiva do usuário, é semelhante ao tradicional serviço telefônico por comutação de circuitos. Também é chamado comumente por **Voice-over-IP (VoIP)**”. Redes de Computadores e a Internet.
O sistema VoIP foi desenvolvido sobre o modelo de Rede *TCP/IP*. O protocolo H.323, desenvolvido pelo *International Telecommunications Union* - , foi o primeiro a ser utilizado e sob o seu guarda-chuva abriga uma pilha de outros protocolos para transmissão de áudio e vídeo, além de prover interoperabilidade em diferentes plataformas e fabricantes. Logo depois o *Internet Engineering Task Force* - Session Initiation Protocol (sip)

desenvolveu o SIP, sendo este, muito mais utilizado nos dias atuais pela sua eficácia para Redes IP.

O *Session Initiation Protocol* – SIP, pertence a Camada de Aplicação, assim como o HTTP e outros para *web*, inclusive a semelhança entre os dois é muito grande em suas arquiteturas porque o SIP foi criado com base no http, é utilizado para sinalização e sua função é negociar, estabelecer e encerrar sessões multimídia. Porém, ao contrário do HTTP, que pode carregar grandes capacidades de mensagens, o SIP tem limitação reduzida para mensagens.

O desenvolvimento do SIP foi moldado no método do triplo *handshake*, implementado no protocolo TCP, como pode ser observado na Figura 4, é totalmente voltado, não apenas para a transmissão de texto, mas principalmente para áudio e vídeo. Na Camada de Transporte pode ser transportado tanto pelo TCP, quanto pelo UDP, sendo o TCP utilizado para sinalizar e negociar as sessões e o UDP para o transporte da mídia.

*Figura 2: Pilha de protocolos para VoIP*




Fonte: retirado do site *Segurança em Voz sobre IP*

Os protocolos MGCP Media Gateway Control Protocol (MGCP) v1.0e MEGACO Megaco Protocol v1.0, estão presentes para modernizar e interoperar o sistema VoIP com gerenciadores do serviço de telefonia convencional (*Gateways*), fornecendo endereçamento e controle de mídias em Redes que ainda utilizam centrais analógicas PABX[1]. Sendo o MEGACO uma atualização do MGCP desenvolvido através do esforço em conjunto entre o ITU-T e IETF, que para esse modelo de comunicação por voz, recomendam o protocolo H.248.

**Co**dificadores e **Dec**odificadores – CODECs, são responsáveis por tratar o áudio analógico em pacotes digitalizados, ou seja, são capazes de comprimir, descomprimir, retirar ruídos e suprimir espaços, como o silêncio muito longo.Redes de computadores Na

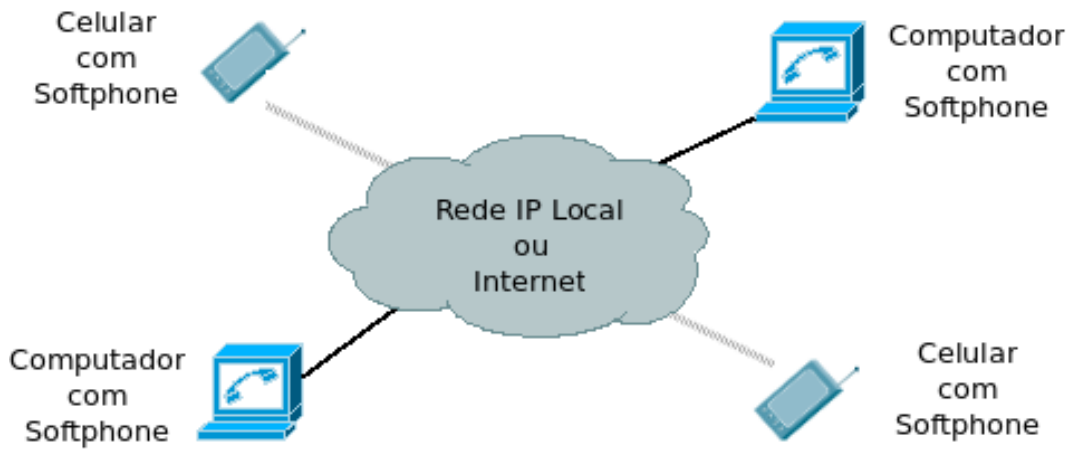
[1] Private Automatic Branch Exchange – PABX é um dispositivo eletrônico físico, também conhecido por central telefônica interna nas empresas, interligando os ambientes por cabos chamados de ramais, e esta central pode ser conectado a uma operadora telefônica externa por uma linha telefônica da operadora. Sua função é facilitar a comunicação na rotina de trabalho.

arquitetura H.323, tudo que inicializa com "*H.3xx*" é codec multimídia, já na arquitetura SIP os codecs são separados sob o protocolo RTP e são identificados com "*G.7xx*". O codec escolhido na aplicação VoIP determina a qualidade e o desempenho na comunicação e na Rede. Um exemplo de codec de áudio é *G.711*, gratuito e amplamente usado em comunicação no sistema VoIP.Introdução à Voz sobreIP e Asterisk

O ***R**eal **T**ime **P**rotocol* – RTP, definido na RTP: A Transport Protocol for Real-Time Applications pelo IETF, é o protocolo mais importante no sistema VoIP. Em sua forma mais simples encapsula os codecs, não garante qualidade de serviço em tempo real, além de sofrer todo os intempéries como o protocolo UDP na camada de transporte por não terem controle de fluxo, de confirmação, de erro e de retransmissão. Por isso, o ***R**eal-Time **T**ransport **C**ontrol **P**rotocol* – RTCP, definido pela mesma RFC 3550, agrega tais controle em tempo real e a identificação dos pacotes na transmissão e recepção da mídia, fazendo com que a experiência possa ser agradável aos usuários. Isto só é possível porque na camada de transporte existem processos sendo executados fim a fim nos terminais. Redes de computadores.

Os avanços tecnológicos permitem inúmeras formas de realizar uma chamada VoIP e um dos métodos de implementação mais simples atualmente se dá entre dois *softphones* instalados e configurados, seja em *smartphones* ou computadores conectados na Rede IP local e a Internet. Voz sobre IP I: A Convergência de Dados e Voz.

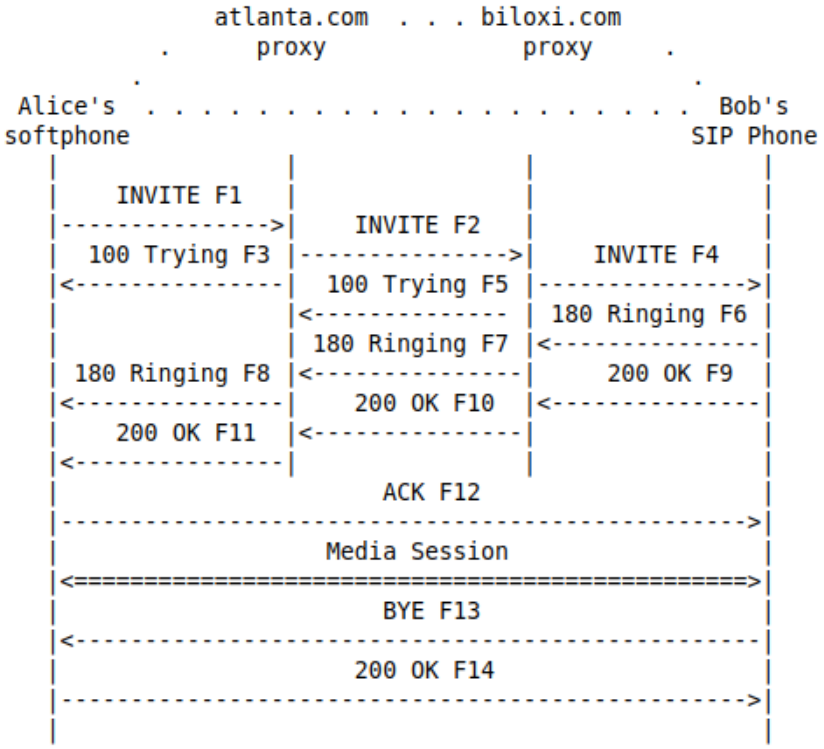
*Figura 3: Softphones instalados em dispositivos*




Fonte: o autor (2022).

Na , o autor RFC 3261 - SIP: Session Initiation Protocol e outros, retratam a Figura 4 no estado da arte do que é a comunicação SIP entre dois terminais. Já a Figura 5, afere, através do *Wireshark*, a comunicação acontecendo verdadeiramente. Contudo, a ausência de segurança, tanto na sinalização quanto na mídia é imperativa.

*Figura 4: Setup de uma sessão SIP*




Fonte: Retirado da RFC 3261

*Figura 5: Comunicação SIP capturada no Wireshark*

| Dst Port | Protocol | Length | Info |
|---|---|---|---|
| 60665 | SIP/SDP | 937 | Request: INVITE sip:200@192.168.15.105:60665;ob \| |
| 5060 | SIP | 352 | Status: 100 Trying \| |
| 5060 | SIP | 551 | Status: 180 Ringing \| |
| 5060 | SIP/SDP | 949 | Status: 200 OK (INVITE) \| |
| 60665 | SIP | 479 | Request: ACK sip:200@192.168.15.105:60665;ob \| |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6142, Time=160, Mark |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6143, Time=320 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6144, Time=480 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6145, Time=640 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6146, Time=800 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6147, Time=960 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6148, Time=1120 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6149, Time=1280 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6150, Time=1440 |
| 13230 | RTP | 214 | PT=ITU-T G.711 PCMU, SSRC=0xCE14FC0, Seq=6151, Time=1600 |

Fonte: o autor (2022).

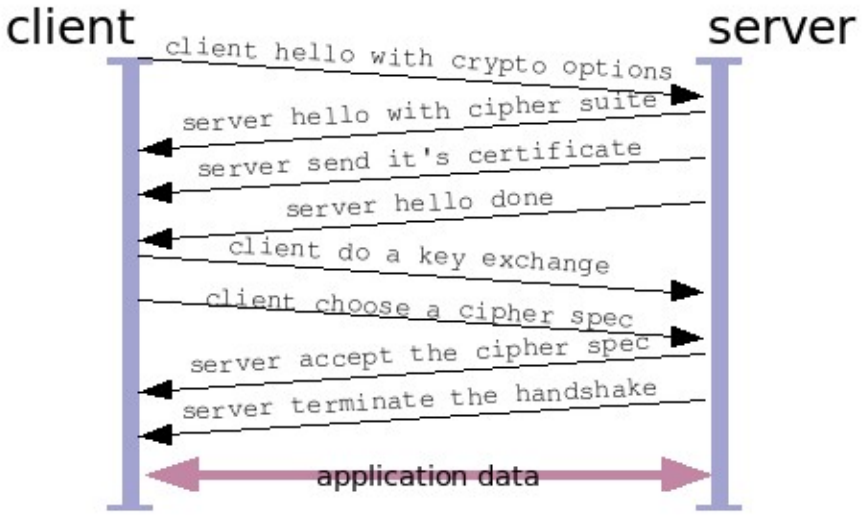
Como observa-se na Figura 4, o chamado com origem no terminal de Alice que inicializa a negociação de uma sessão por meio de uma pequena mensagem de requisição "*Invite*", no próprio protocolo SIP. O recebedor Bob sinaliza que recebeu a requisição e responde com "*100 Trying*". Após o recebedor atender, novamente, uma mensagem com status "*180 Ringing*" é enviada ao originador e o "*200 OK invite*" confirma que a requisição para o

estabelecimento do inicio da sessão foi aceito e imediatamente a requisição é respondida com um "*ACK*" enviado do originador (Alice) ao recebedor (Bob) e a sessão é estabelecida. A partir desse ponto outro protocolo entra em ação bidirecionalmente, o RTP na Sessão de Mídia, responsável na transmissão dos *codecs*, contendo os pacotes de voz digitalizados. O término "*Bye*" é enviado do recebedor para o originador, porém pode ser usado por qualquer um na chamada e confirmado em seguida com um "*200 OK*".

O uso exponencial desta tecnologia para fins comerciais e por organizações impactou diretamente na confidencialidade e integridade das sessões SIP, levando os fabricantes de hardware e softwares ao amadurecimento em tecnologias que pudessem dar algum tipo de segurança aos usuários para mitigar fraudes, como acontece em aplicações *web*. Pensando assim, alguns protocolos de segurança foram incorporados e outros desenvolvidos para o sistema VoIP, como o TLS e o SRTP. Neste artigo foram abordados apenas estes protocolos para mitigar a vulnerabilidade.

O Security Considerations for Voice Over IP Systems, coloca que no cabeçalho do protocolo SIP existem três campos de registro voltados para negociar a segurança entre um cliente e o servidor SIP. Segundo o IETF, na Security Mechanism Agreement for the Session Initiation Protocol (SIP) são 5 (cinco) os mecanismos suportados para os três campos e um dele é o *TLS*.

*Figura 6: Handshake TLS*




Fonte: retirado do site *Mecanismos de Segurança para Ambientes VoIP*

O ***T**ransport **L**ayer **S**ecurity* - TLS, está tipificado na RFC 2246 The TLS Protocol v1.0, e desde janeiro de 2018 encontra-se na versão 1.3 conforme a Session Initiation Protocol (sip), e sua função é prover uma camada de segurança em conjunto com o TCP. Determina que os detalhes da conexão serão cifrados através de algorítimos, como o *SHA*, não permitindo serem identificados durante a sessão. Com a utilização do TLS para fazer sinalização cifrada, passou-se a utilizar as chaves e os certificados criptográficos através das Autoridades Certificadoras – Cas. Com estas incorporações, mitiga-se ataques de toda sorte como a falsificação de mensagens no cabeçalho, ataques *Man in the middle* – MITM, SIP Redirect, ataque por quebra de senha, ataques de sequestro de chamadas, negação de serviço *Dos* através do SIP Bombing e a escuta telefônica.

O ***Secure Real-Time Transport Protocol*** – SRTP, está descrito e tipificado pelo The Secure Real-time Transport Protocol (SRTP), diz que é um protocolo desenvolvido para fornecer confidencialidade, autenticação de mensagem e segurança na reprodução contra reenvio de mensagens em repetição, evitando fraudes. Sua função é proteger o tráfego RTP e o tráfego de controle do RTP/RTCP. No tópico 5 - RESULTADOS E DISCUSSÕES, observa-se, na pratica, a implementação deste protocolo no sistema VoIP com a finalidade de mitigar os ataques de escuta ao protocolo RTP e de adulteração dos CODECs.

As centrais ***Private Branch Exchange Internet Protocol*** – PBX IP, são as versões atualizadas dos PABX, porém totalmente virtualizadas e dedicadas para Rede Local ou a internet e que podem ser conectadas às centrais das operadoras telefônicas por *Gateways*. Hoje, existem muitos softwares que fazem esse trabalho das centrais e os terminais também são programas, com isto deixa-se de ocupar espaço físico, além de eliminar cabos. Neste artigo utilizaremos os FreePBX, sobre o Asterisk.

Nos dias atuais, o sistema VoIP precisa estar protegido para a conversação por voz, afim de manter a privacidade e confidencialidade nas conversas. Recomenda-se a aplicação de criptografia por segmento, dispositivo ou usuário. Contudo, alerta-se que criptografar indiscriminadamente é prejudicial na qualidade do serviço, podendo ocasionar atrasos, *jitter*, latência, sobrecarregando a Rede. Neste artigo, enfatizou-se a implementação de segurança oriundas no próprio sistema, porém não ativadas, ou seja, criptografar a sinalização da Sessão SIP com o TLS e principalmente criptografar as mídias – CODECs no protocolo RTP com o protocolo SRTP.

## 2.2 - Legislativa

Os profissionais de segurança cibernética precisam estar atentos as questões legais para desempenharem suas atividades dentro do mais restrito cumprimento das leis. Pensando assim, cabe mostrar aos agentes de seguranças cibernética como os *pentests*, equipes *Red Teams* e os *Blue Teams* que todos estão enquadrados nas leis brasileiras e internacionais.

Segundo a Constituição Federativa do Brasil, em seu Artigo 5º, inciso X, “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. O art. 5º, X

De acordo com o Código Penal, no Artigo 151 - “Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena - detenção, de um a seis meses, ou multa.” Ainda no mesmo Artigo em seu Inciso 1º:

> “na mesma pena incorre:
> I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;
> Violação de comunicação telegráfica, radioelétrica ou telefônica (grifei)
> II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;
> IV - quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.” **(CP, 1940).**

O Código de Processo Civil deixa bem claro que as escutas telefônicas clandestinas constituem crime como diz a Lei Nº 9.296 em seu Artigo 10:

"Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei". (CCivil, 1996)

Segundo a Lei Geral de Proteção de Dados – LGDP, há responsabilidades para os profissionais de segurança e equipes *Blue Teams* no sentido de agirem proativamente no quesito de proteção as comunicações e aos dados, vejamos o Artigo 46:

"Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

Observa-se que a violação da privacidade, de dados e telefônica encontra amplo abrigo no âmbito jurídico brasileiro e se violados, sem a devida autorização legal, os agentes envolvidos estão sujeitos às sansões previstas em lei.

## 3 - METODOLOGIA

Neste experimento, em ambiente controlado para testes, para fins de conhecimento e de caráter científico, foram utilizados alguns dispositivos e *softwares* descritos nos itens 4.1, 4.2 e 4.3 para fazer a interceptação e a escuta da conversa da seguinte maneira: com a central PBX e os ramais configurados para o transporte criptografado com TLSv1.2; a dinâmica é simples, com tudo devidamente configurado e em funcionamento, abrimos o *Wireshark* para capturar o tráfego da Rede de testes; em seguida inicializou-se uma ligação do ramal 4011 para o ramal 4010; analisar o tráfego identificado; forçar o *Wireshark* a decodificar o fluxo UDP para RTP; ouvir o conteúdo audível.

### 3.1 - Ambiente controlado – Rede interna

- Roteador com 4 portas LAN, uma WAN e Wi-Fi – DHCP de classe "C" para LAN com o *range* 192.168.15.0/24;
- switch 16 portas 10/100/1000Mbps.

### 3.2 - Softwares

- FrePBX - versão 16.0.21.9 - virtualizado com dois ramais (4010 e 4011), sobre o Asterisk (PBX IP) - versão 16.27.0 – IP: 192.168.15.113;
- Wireshark - versão 4.0.1;
- Windows 10 – *desktop* virtualizado, abrigando o Microsip – IP: 192.168.15.107;
- Microsip – versão 3.21.3 - com o Ramal 4011;
- PortSIP UC – versão 11.0.1 – Ramal 4010.

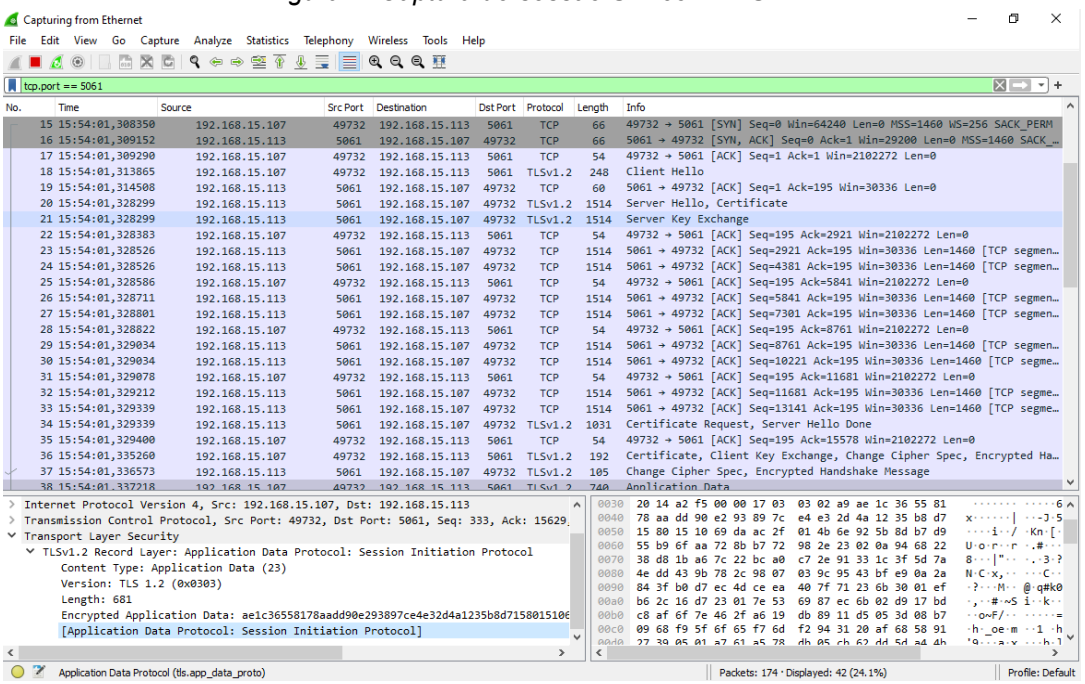
### 3.3 – Dispositivos hardware

- Celular Xiomi - Redmi 7A - Android na versão 10 – conectado ao Wi-Fi e recebendo o IP:192.168.15.110 - abrigando o PortSip;
- servidor XCP-NG - versão 8.2.1 - para virtualização;
- computador *desktop* físico com linux.

## 4 - RESULTADOS E DISCUSSÕES

A partir deste ponto passa a ser feito a descrição dos passos efetuados para a realização do experimento de forma sucinta e objetiva, ou seja, desenvolver um ataque em ambientes de Rede com aplicação *VoIP*. Inicializando o ambiente de teste controlado, central FreePBX, *Wireshark* e os terminais com o cliente *SIP*, ao iniciar a captura do tráfego na Rede com o *sniffer Wireshark*, podemos observar diversas comunicações sendo efetuadas entre os dispositivos conectados na Rede.

*Figura 7: Captura de sessão SIP com TLSv1.2*

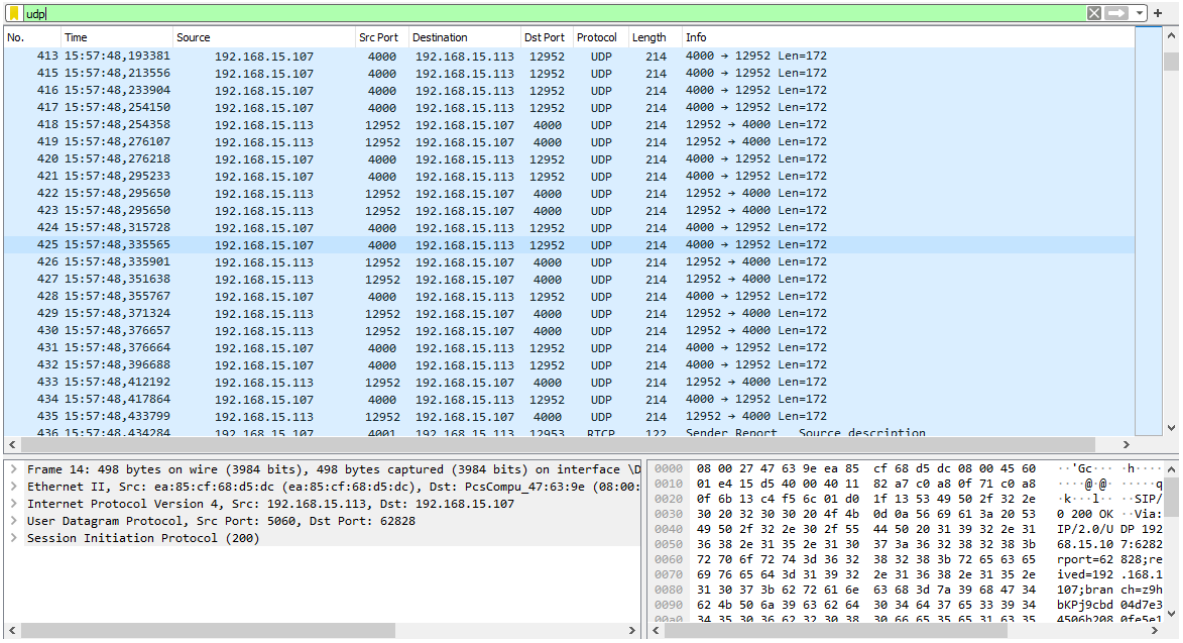



Fonte: o autor (2022).

Antes de inicializar a chamada entre os terminais, separando o tráfego com o filtro "*tcp.port == 5061*", fica evidenciado o flagrante na o "*invit*", podemos entender, na prática, um pouco mais sobre a captura em andamento, ou seja, identificamos o instante em que o terminal *SIP* passa ter o registro de transporte criptografado. Na comunicação entre o terminal *SIP* com o *IP* 192.168.15.107, na porta de origem 49732, para a central *VoIP* com *IP* 192.168.15.113, na porta de destino 5061 (*TLS*), o protocolo utilizado é o *TCP*, fazendo o *handshake* triplo para iniciar a troca dos certificados. Em seguida o cliente envia uma sinalização "*Client Hello*" e o servidor responde já com o certificado "*Server Hello*". A partir desse momento toda a sinalização do protocolo *SIP* está criptografada sob o protocolo *TLSv1.2*, como podemos verificar na Camada de Transporte Segura, não sendo mais possível identificá-lo pelo *Wireshark.*

Feito essa observação, inicializa-se a chamada entre os terminais, que neste caso foi efetuada a partir do ramal 4011 com o *softphone* MicroSIP para o ramal 4010 no celular com *softphone* PortSIP e mantêm-se um diálogo por aproximadamente 2 minutos. Neste ponto, a captura do tráfego na Rede ainda está em andamento e se substituir o filtro, aplicado anteriormente, pelo filtro *"rtp"* também não será possível identificar o protocolo. Se retirado todo o filtro o que se observa são muitas trocas de todo o tráfego da Rede. Porém, se usar o filtro "*udp*", é exibido não apenas todo o fluxo "*UDP*" da Rede, mas principalmente um grande intervalo de trocas de pacotes efetuadas entre o terminal e a central *sip* utilizando o protocolo *UDP* e é justamente nele que se concentra os esforços para a decodificação.

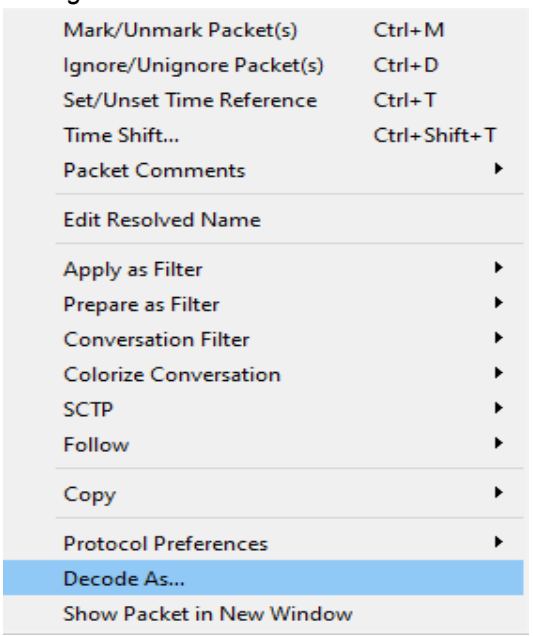
*Figura 8: Fluxo UDP entre o terminal e a central SIP*




Fonte: o autor (2022).

O protocolo *SIP*, assim como o *HTTP,* pertencem a Camada de Aplicação e são transmitidos em texto aberto. Quando é implementado uma camada de segurança, utilizando o *TLS* por exemplo, apenas protege-se o cabeçalho de interpretações no transporte, ou seja, neste caso o *Wireshark* não identifica os protocolos *SIP* e *RTP* em texto plano, porém todos os dados do pacote, no caso o *streaming payload*, continua aberto e utiliza o protocolo *UDP* da Camada de Transporte para fazer a entrega fim a fim e é neste ponto que se força o *sniffer Wireshark* para efetuar a leitura dos pacotes. Uma vez que o tráfego está separado, pode-se fazer a decodificação, forçando o *Wireshark* a ler o protocolo *UDP* como *RTP*. Para isso, clica-se com o botão da direita do *mouse* sobre o tráfego separado e clica-se em "*Decode As…*".

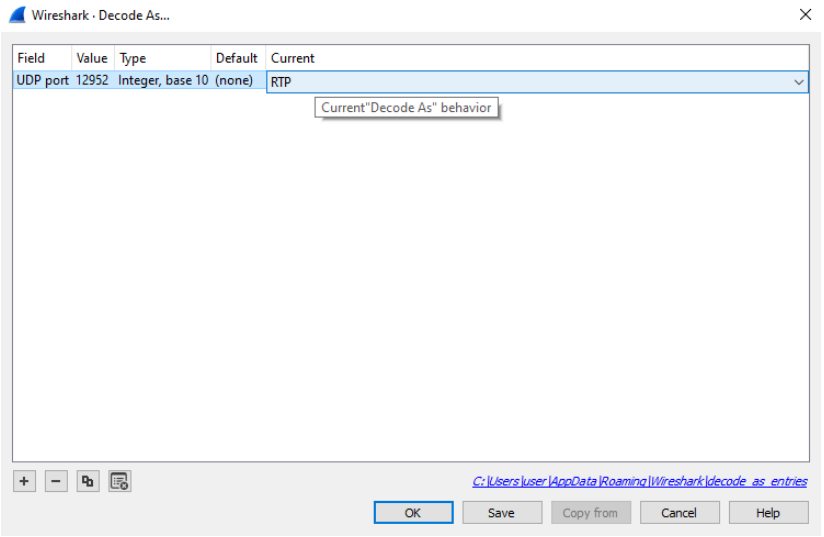
*Figura 9: Menu de atalho Decode As*




Fonte: o autor (2022).

Na janela "*Decode As...*", como mostra a Figura 10, no campo "*Current*", altera-se o registro de *UDP* para *RTP* e em seguida clica-se no "*OK*". Com esta simples operação, reorienta-se o *sniffer Wireshark* a ler o fluxo udp como rtp. User Specified Decodes.

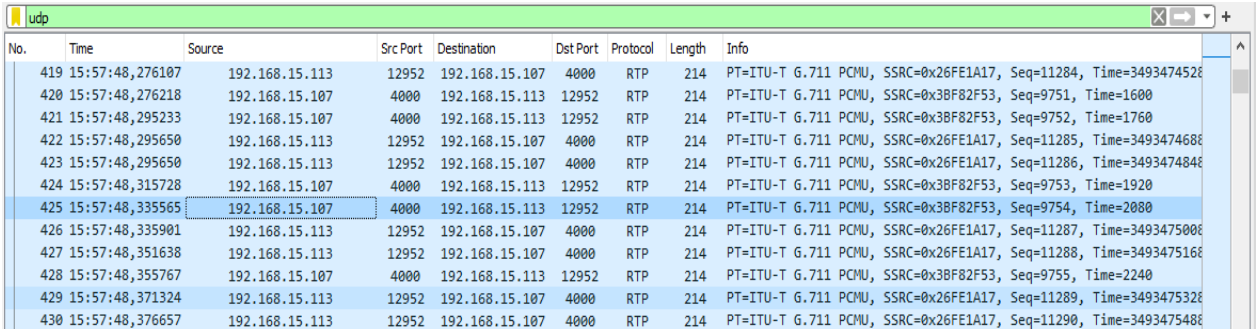
*Figura 10: Forçando decodificação UDP/RTP*




Fonte: o autor (2022).

Observa-se na Figura 11, que após a aplicação do filtro, todo o fluxo é reapresentado forçosamente como *RTP*, ou seja, o *Wireshark* consegue ler este fluxo sem maiores problemas, inclusive a carga útil, além de outras informações.

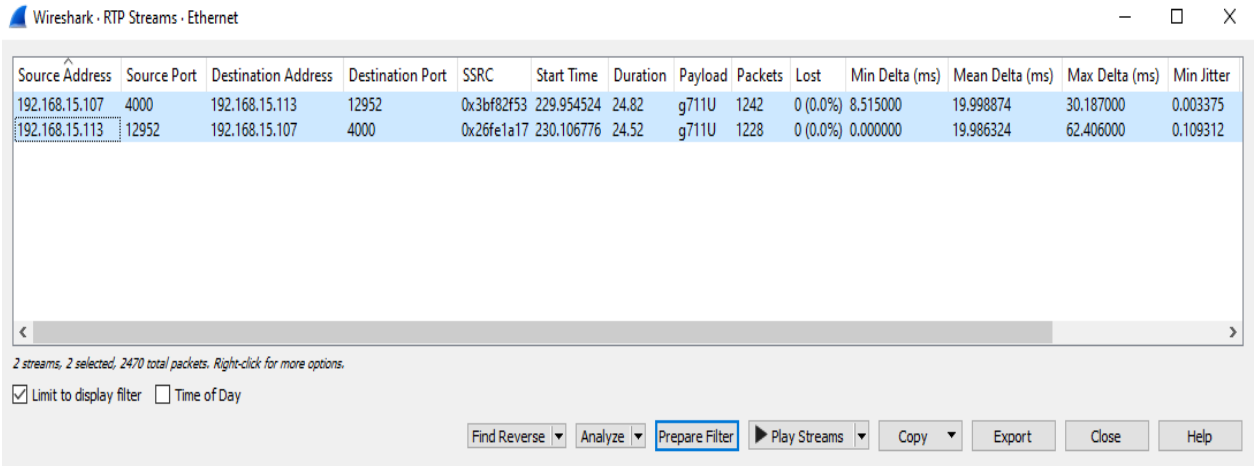
*Figura 11: Fluxo UDP decodificado para RTP*




Fonte: o autor

Para realizar a escuta clicamos no menu "*Telephony*", deslisa-se o *mouse* até "*RTP"* e clica-se em "*RTP Streams"*, visualiza-se a captura de todo o fluxo da conversa com informações adicionais como no campo "*Payload*", o *codec* utilizado é o "*g711*", a quantidade de pacotes e outros dados estatísticos, conforme a Figura 12.

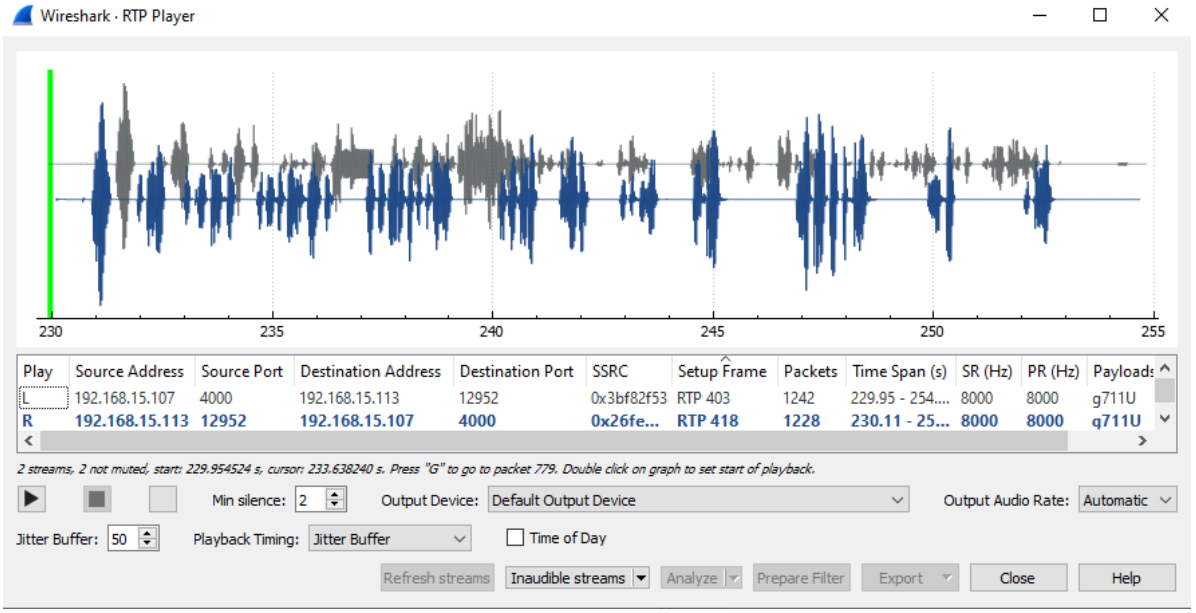
*Figura 12: Fluxo VoIP mais dados estatísticos*




Fonte: o autor (2022).

Ainda na Figura 12, clica-se no botão "*Play Streams*" para abrir propriamente o *stream*. Abre-se uma nova janela contendo um gráfico representativo e finalmente, clicando no "*play*", de forma audível, escuta-se a conversa, conforme mostra a Figura 13.

*Figura 13: Representação gráfica do áudio audível.*




Fonte: o autor (2022).

De forma alternativa à configuração padrão no *software* FreePBX, que no campo "*Criptografia de Mídia*" mostra o registro como "*nenhum*", para mitigar essa vulnerabilidade de ataque ao RTP, a recomendação é adicionar mais uma camada de criptografia, não apenas na sinalização do *SIP* com a incorporação do TLS, como foi mostrador até então, mas também criptografar a mídia com o protocolo *SRTP*, conforme Figura 14.

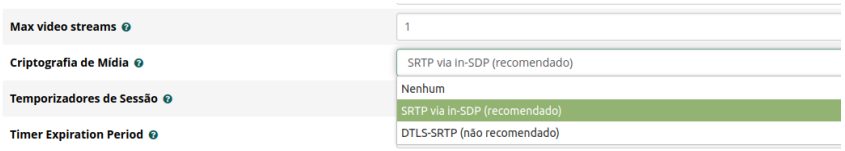


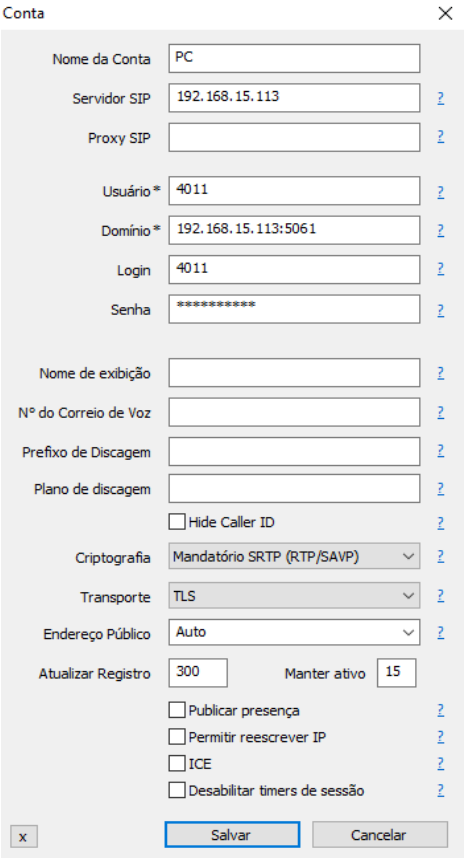

*Figura 14: Inserção de criptografia para mídia*
Fonte: o autor

Os terminais SIP também precisam passar por ajustes de configuração, como mostra a Figura 15 e a Figura 16, ou seja, no campo "*criptografia*", habilitar o transporte de mídia como mandatório *SRTP*.

*Figura 15: Habilitando SRTP no terminal celular.*


Fonte: o autor (2022).

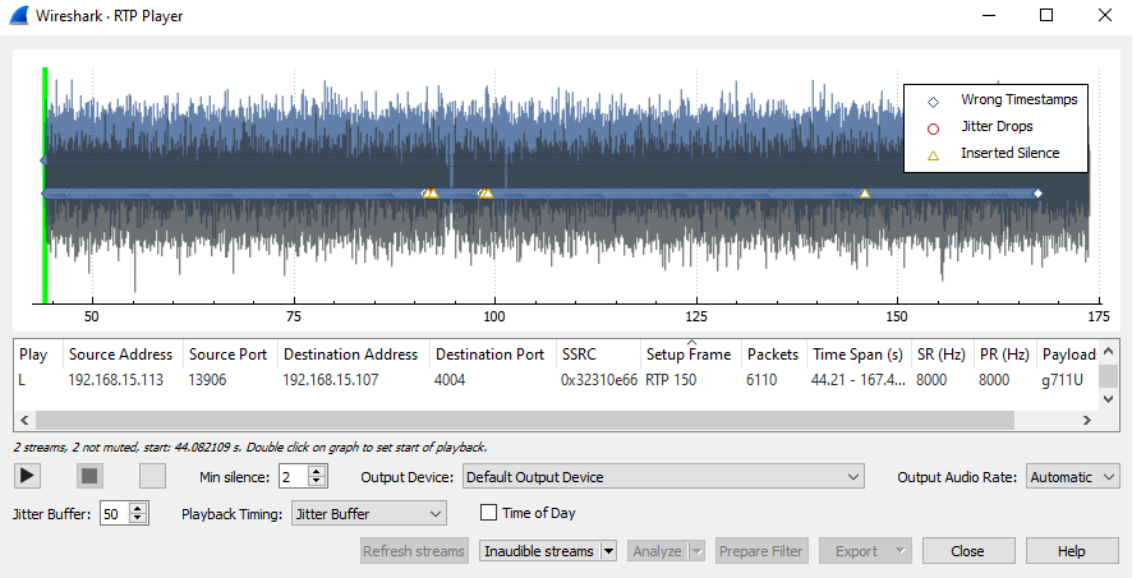
*Figura 16: Habilitando SRTP no terminal PC*




Fonte: o autor (2022).

Efetuados todos os procedimentos de configuração no servidor VoIP e nos terminais, pode-se refazer todo o procedimento de captura demonstrados na etapa anterior e o resultado para audição do fluxo será apenas um ruído – chiado, como se vê na Figura 17.

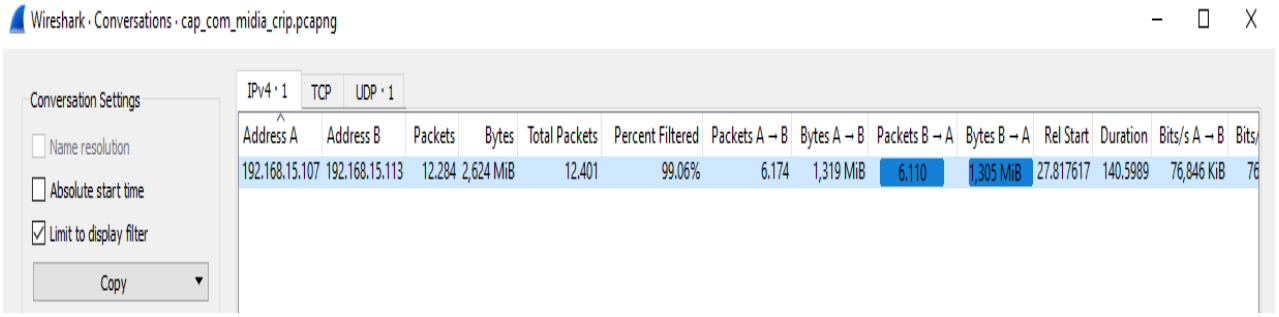
*Figura 17: Representação gráfica do áudio, inaudível.*




Fonte: o autor (2022).

Nos casos de forense computacional, aonde se procura provas técnicas entre o investigado "*A*" e o investigado "*B*", por mais que não se alcance o objetivo de escutar a conversa, ainda é possível dissecar o fluxo com a finalidade de acostar à investigação mais elementos probatórios como o tempo de duração da conversa, que neste caso durou 140.5989 segundos - 2:34 min (dois minutos e 34 segundos), quantidade de pacotes etc, como mostra a Figura 18. Prova técnica irrefutável de que os terminais de "A" e "B" conversaram.

*Figura 18: Dados estatísticos para prova técnica.*




Fonte: o autor (2022).

## 5 - CONCLUSÃO

O artigo trata em mitigar a vulnerabilidade no protocolo SIP e RTP, caso haja invasão ou acesso indevido a Rede com o objetivo de fazer escutas telefônicas no sistema VoIP.
Comparando-se o início da tecnologia VoIP com as inovações, mesmo com os avanços em segurança, como a incorporação de novos algoritimos, protocolos e certificados, existem muitos perigos para os empreendimentos de todos os portes e para as pessoas quando deixam de contratar profissionais para a implementação e apenas utilizam

configurações padrões advindas de fábrica ou configurações realizadas de forma pífia, permitindo a possibilidade de escutar as conversas. Observa-se, inclusive, a possibilidade de inúmeros tipos de fraudes como o sequestro de identidade através da técnica *main in the middle*, já que os certificados e as chaves podem ser facilmente identificados e usados, fraudando a central e ou o terminal SIP.

Tratar a segurança responsavelmente é indispensável e primordial nos dias atuais. A vulnerabilidade apresentada neste artigo e resolvida é apenas uma, ou seja, existem outras inúmeras ações de segurança envolvidas neste sistema que os profissionais de tecnologia e proficientes de segurança cibernética precisam estar atentos e agregá-las para garantir aos usuários confidencialidade e integridade em sua utilização, além de estar sempre disponível para usuários devidamente autorizados.

Assim como na maioria das aplicações em informática, conclui-se que, no quesito segurança, apesar de haver uma área específica para este serviço, a responsabilidade fica a cargo de quem o implementa, seja para ativá-la no próprio sistema ou adicioná-la em camadas, demandando conhecimento de outras tecnologias em segurança, como *firewall*, IDS/IPS, separação do tráfego de voz do tráfego de dados por *VLANs*, monitoramento de tráfego de Rede *etc*. A implementação da segurança no serviço VoIP, invariavelmente, impacta no seu próprio funcionamento e consumo de recursos, além de impactar na segurança da Rede local. Por esta razão, que os fabricantes abordam de maneira rasa e ou superficial este quesito, tratando apenas da aplicação disponibilizada.

## REFERÊNCIAS

BORDIM, Jacir L. **Introdução à Voz sobre IP e Asterisk**. Escola Superior de Redes - RNP, 2010. 260 págs

BRASIL **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988. O art. 5º, X**. Disponível em: <https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: nov - 2022.

BRASIL **Código Penal**. 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: nov 2022.

BRASIL **Código Civil.** 1996. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: nov 2022.

BRAS**IL LEI Nº 13.709, DE 14 DE AGOSTO DE 2018.** Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: nov 2022.

CERT. **Projeto Honeypots Distribuídos**. 2022. Disponível em: <https://honeytarg.cert.br/honeypots/stats/flows/current/>. Acesso em: 4 nov. 2022.

CISCO. Disponível em: <https://www.cisco.com/c/pt_br/solutions/small-business/resource-center/security/tips-ip-phone-security.html>. Acesso em: jan 2023.

D. Richard; Walsh Thomas J.; Fries Steffen. **Security Considerations for Voice Over IP Systems**. 2005. Disponível em: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-58.pdf>. Acesso em: nov 2022.

IETF. **Session Initiation Protocol (sip).** Disponível em: <https://datatracker.ietf.org/wg/sip/about/>. Acesso em: dez 2022.

IETF. **The Secure Real-time Transport Protocol (SRTP)**. Disponível em: <https://datatracker.ietf.org/doc/html/rfc3711>. Acesso em: jan 2023.

IETF. **Media Gateway Control Protocol (MGCP) v1.0.** Disponível em: <https://www.rfc-editor.org/rfc/rfc2705>. Acesso em: dez 2022.

IETF, Arkko, et. al. **Security Mechanism Agreement for the Session Initiation Protocol (SIP)**. Disponível em: <https://www.rfc-editor.org/rfc/rfc3329.txt>. Acesso em: jan 2003.

IETF, Cuervo F.; et al. **Megaco Protocol v1.0.** Disponível em: <https://www.rfc-editor.org/rfc/rfc3015>. Acesso em: dez 2022.

IETF, T. DIERKS; c. ALLEN. **The TLS Protocol v1.0**. Disponível em: <https://www.rfc-editor.org/info/rfc2246>. Acesso em: dez 2022.

ITU. **A recomendação ITU-T H.323.** Disponível em: <https://www.itu.int/dms_pubrec/itu-t/rec/h/T-REC-H.323-202203-I!!SUM-HTM-E.htm>. Acesso em: nov 2022.

TANENBAUM Andrew S. **Redes de computadores**. 4: Campus, 2003. 632 págs. .

IETF. RTP: **A Transport Protocol for Real-Time Applications**. Disponível em: <https://www.rfc-editor.org/rfc/rfc3550>. Acesso em: dez 2022.

DA SILVA, Glaucia. **Voz sobre IP I:** A Convergência de Dados e Voz. Disponível em: <https://www.teleco.com.br/tutoriais/tutorialvoipconv/pagina_4.asp>. Acesso em: dez 2022.

KUROSE, Jim F.; Ross, Keith W. **Redes de Computadores e a Internet**. 6 ed. São Paulo - SP: Pearson Education do Brasil, 2014. 658 p.

NIST, D. Richard; Walsh Thomas J.; Fries Steffen. **Security Considerations for Voice Over IP Systems**. Disponível em: <https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-58.pdf>. Acesso em: jan 2023.

OLCHIK, Alejandro. **Segurança em Voz sobre IP.** Disponível em: <https://www.teleco.com.br/tutoriais/tutorialsegvoip/pagina_2.asp>. Acesso em: dez 2022.

ROSS, Julio. **VoIP – Voz sobre IP**. Rio de Janeiro: Antenna Edições Técnicas, 2007. 52 págs.

ROSENBERG J.; et. al. **RFC**. Disponível em: <https://www.rfc-editor.org/rfc/rfc3261.html>. Acesso em: jan 2023.

ROSENBERG. RFC 3261 - SIP: Session Initiation Protocol. Disponivel em: <https://www.rfc-editor.org/rfc/rfc3261#page-86>. Acesso em: nov 2022.

VERAS, ROBSON. **Mecanismos de Segurança para Ambientes VoIP**. Disponivel em: <https://biblioteca.inatel.br/cict/acervo%20publico/sumarios/Artigos%20de%20TCC/TCC_Pos%20Gradua%C3%A7%C3%A3o/SRST-%20Engenharia%20de%20Redes%20e%20Sistemas%20de%20Telecomunica%C3%A7%C3%B5es/2015/TCC_Mecanismos%20de%20seguran%C3%A7a%20para%20ambientes%20VoIP.pdf>. Acesso em: dez 2022.

WIRESHARK. **User Specified Decodes.** Disponivel em: <https://www.wireshark.org/docs/wsug_html_chunked/ChCustProtocolDissectionSection.html#ChAdvDecodeAsFig>. Acesso em: nov 2022.