PROTEÇÃO DA COMUNICAÇÃO VoIP NA IMPLEMENTAÇÃO DO ASTERISK COM USO DE CRIPTOGRAFIA NOS PROTOCOLOS DE SINALIZAÇÃO E MÍDIA

Breno Francisco Rafael Pombo[1], Rogério Antônio Casagrande [2]

Resumo: A segurança em uma rede VoIP é um dos pontos críticos, visto que os protocolos padrões utilizados na comunicação VoIP foram desenhados não visando à segurança. Com isso, têm surgido ataques na rede VoIP como espionagem, violação de mensagens e entre outros. O objetivo deste trabalho é analisar recursos disponíveis no Asterisk capazes de melhorar a camada de segurança da comunicação VoIP. Para alcançar esse feito, foi instalado o Asterisk, funcionando como um PABX IP, configurado os protocolos SRTP e TLS para criptografar o fluxo de sinalização e a mídia entre dois usuários SIP. Os resultados mostram que, com o uso de criptografia, torna-se difícil de verificar o fluxo de sinalização e também ter acesso a conversa ou ao stream de áudio entre os participantes da ligação. Chegando à conclusão que aplicando as camadas de segurança do Asterisk em redes VoIP, tem-se uma comunicação VoIP mais segura.

Palavras-chave: VoIP; Asterisk; Segurança, TLS, SRTP, SIP, RTP.

ABSTRACT: Security in a VoIP network is one of the critical points since the standard protocols used in VoIP communication were designed not with security in mind. As a result, attacks have emerged on the VoIP network, such as spying, message tampering, and others. The objective of this work is to analyze resources available in Asterisk capable of improving the security layer of VoIP communication. To achieve this feat, Asterisk was installed, working as an IP PBX, configured the SRTP and TLS protocols to encrypt the signaling flow and the media between two SIP users. The results show that, with the use of cryptography, it becomes difficult to verify the signaling flow and also to access the conversation or the audio stream between the callers. Concluding that by applying Asterisk security layers in VoIP networks, you have a more secure VoIP communication.

[1] Breno Francisco Rafael Pombo, graduando de Ciência da Computação na Universidade do Extremo Sul Catarinense- UNESC. Emal:brenopombobp@hotmail.com.

[2] Rogério Antônio Casagrande, Doutor em Engenharia de Automação e Sistemas pela UFSC, professor do Curso de Ciência da Computação na UNESC. Email:roc@unesc.net.

Keywords:VoIP; Asterisk; Security, TLS, SRTP, SIP, RTP.

1 INTRODUÇÃO

A tecnologia Voz sobre Internet Protocol (VoIP) surgiu como um método alternativo da tradicional comunicação de voz usando Rede Telefônica Pública Comutada (RTPC). O crescimento da Internet possibilitou a realização de chamadas internacionais com tarifas muito baixas. Desde a primeira implementação até hoje, a tecnologia tem melhorado significativamente (CIOPEA; BUCICOIU; ROSNER, 2013, nossa tradução).

Geralmente o tráfego VoIP consiste em sinalização e mídia. Diferentes abordagens de comunicação VoIP usam vários protocolos, nomeadamente protocolos de sinalização e de mídia. Os protocolos de mídia são usados para transmitir mídia como áudio e vídeo em redes IP. Os protocolos de sinalização são responsáveis pelo estabelecimento, preservação e desativação das sessões de chamada. Eles também são responsáveis pela negociação de parâmetros de sessão, como codecs, tons, recursos de largura de banda, etc. (SINAM et al., 2014, nossa tradução).

As chamadas VoIP podem ser facilmente rastreadas/ouvidas, podendo o invasor editar sua comunicação ou alguma conversa confidencial, pode vazar ou ser usada indevidamente enquanto é usada a Internet, pois é um sistema aberto (HASSAN; HUSSEIN, 2017, nossa tradução).

No entanto, esses serviços usam a Internet como meio de comunicação, o que a torna mais vulnerável a ameaças de segurança porque as vulnerabilidades da Internet também são herdadas na tecnologia VoIP. A segurança VoIP também é importante porque as conversas nos telefones são transmitidas em texto simples pela Internet, o que ajuda o invasor a obter acesso ao canal de comunicação devido à autenticação fraca do SIP. a principal causa de ataques à tecnologia VoIP é devido às vulnerabilidades do SIP. Como o SIP foi projetado sem nenhuma preocupação de segurança, ele é vulnerável a vários ataques como sequestro de registro, personificação, violação de mensagem, espionagem e ataques man-in-the-middle (REHMAN; ABBASI, 2014, nossa tradução).

Visto em conta as vulnerabilidades encontradas nas redes VoIP relatadas acima, a pesquisa em questão tem como objetivo analisar recursos disponíveis no Asterisk capazes de melhorar a camada de segurança da comunicação VoIP. De forma específica, a pesquisa tem como objetivos de compreender as principais vulnerabilidades já relatadas da comunicação VoIP; identificar os recursos de segurança do Asterisk; compreender o funcionamento de cada recurso de segurança do Asterisk; aplicar técnicas capazes de tornar mais robusta a camada de segurança da comunicação VoIP.

Desta feita, o presente trabalho está dividido em seções, na segunda seção é apresentado como foi desenvolvido a pesquisa, criação do cenário e realização dos testes. Na seção 3, é feita a discussão dos resultados obtidos mediante aos testes elaborados. E no final, apresentado à conclusão junto com trabalhos futuros.

2. TRABALHO CORRELATOS

O trabalho de Dakur, Aditya e Dakur, Shruthi (2014, nossa tradução) teve como objetivo analisar a arquitetura e os padrões da tecnologia VoIP focado na implementação das metodologias de segurança. os autores explicaram os protocolos usados na tecnologia e como é feito o ganho ilegal de acesso de uma conversa. No final, os autores listaram soluções de algumas falhas de segurança a serem superadas. Para interceptação a solução foi segurança física da rede local (*LAN*), criptografia para os serviços VoIP, segurança na rede wireless.

Oche et al. (2013, nossa tradução) explanou de forma resumida sobre as configurações necessárias para a segurança dos sistemas VoIP, com o objetivo de empoderar o usuário VoIP público com estratégias de atenuar ameaças. Os autores consideraram como métodos para segurar a rede VoIP a utilização de firewall e *VPN*, separando VoIP e dados segmentados com *VLANs* separadas logicamente e tornar robustos os *Endpoints* de voz e serviços de aplicação.

Neacşu, Eugen e Şchiopu, Paul (2020, nossa tradução), apresentam VoIP como uma das tecnologias mais implementadas atualmente na indústria de comunicação. No entanto, os autores apresentaram uma imersão optimizada da implementação das políticas de segurança no nível das redes de comunicação para garantir a proteção e confidencialidade dos dados. No ponto de vista de segurança, a

rede VoIP deve ser analisada em todos os aspectos (dispositivos, software e protocolos). Auditoria de rede VoIP em uma perspectiva VoIP é um ponto inicial para entender os riscos da infraestrutura da rede e seus componentes, no entanto, auditoria de rede VoIP, identificação de violações de segurança e então implementação de solução de redução de risco é o melhor procedimento . Os autores ainda acreditam que a segurança é um aspecto geral a ser analisada nos sistemas de comunicação em grande escala, sendo essa análise baseada na percepção de riscos e perigos.

3 MATERIAIS E MÉTODOS

A presente pesquisa, segurança na comunicação VoIP usando o Asterisk, é uma pesquisa aplicada de base tecnológica, descritiva e bibliográfica. Para concretização da pesquisa, foi desenvolvido um PABX Asterisk com capacidade de realizar controle de encaminhamento de chamadas intraterminais entre dois usuários SIP, com a sinalização e mídia criptografada. Abaixo a apresentação da arquitetura geral da pesquisa (figura 1).

Figura 1. Arquitetura geral da pesquisa

O desenvolvimento desta pesquisa se estabeleceu em etapas, nomeadamente, configuração do Asterisk com a possibilidade de habilitar a criptografia de sinalização e mídia, criação e configuração dos usuários SIP e no final o resultado de uma comunicação dentro de uma rede VoIP com a mídia e sinalização criptografada.

3.1. Asterisk

O Asterisk é um tipo de software de código aberto executado no Linux para implementar o sistema IP-PBX e suportar vários protocolos VoIP como SIP, H.323, MGCP, SCCP. Pode ser conectado com rede IP e pode ser conectado com as redes

telefônicas existentes via interfaces analógicas/digitais (ISEKI; SATO; KIM, 2011, nossa tradução).

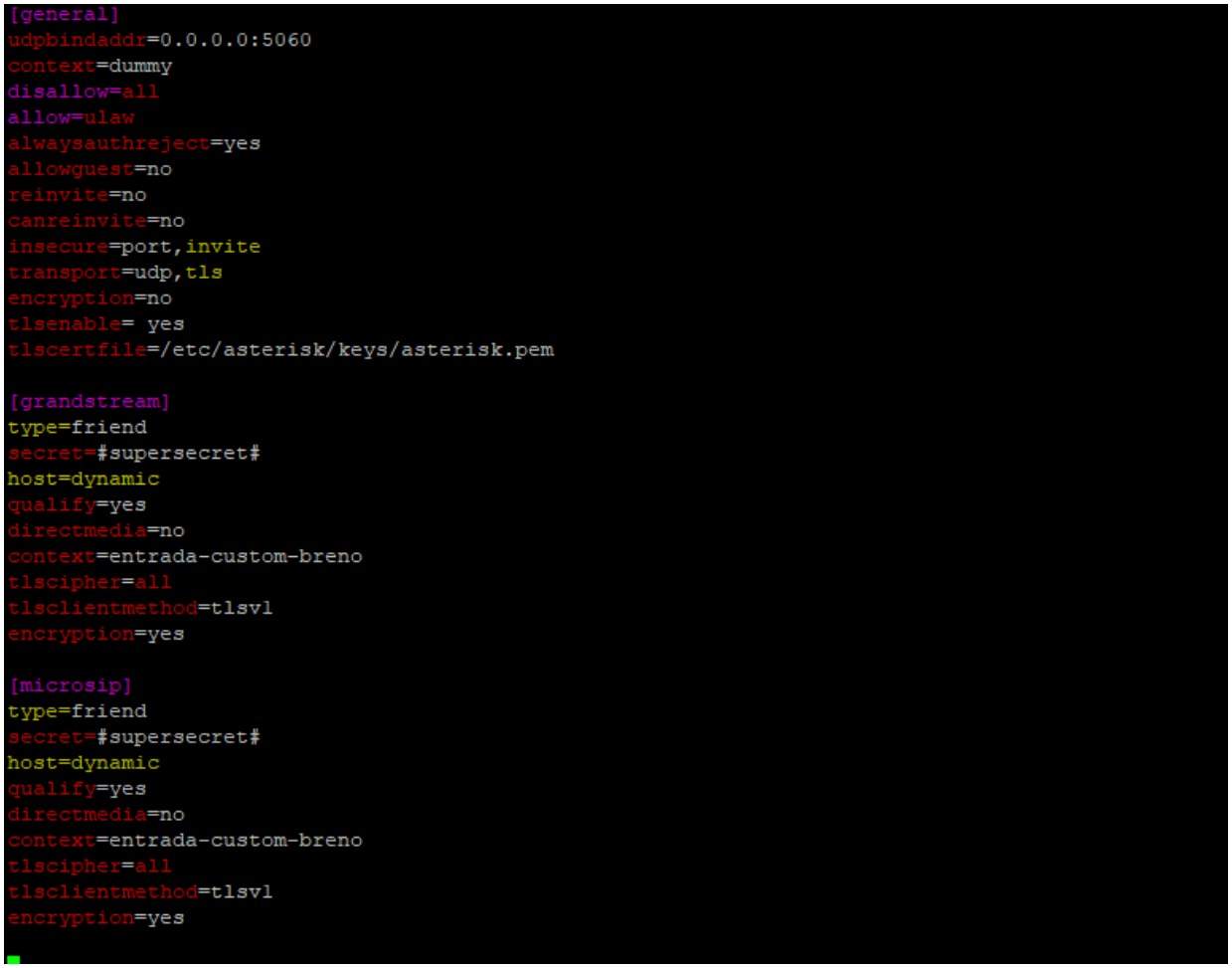
Asterisk é um sistema telefônico completo em software. Ele substitui sistemas telefônicos complexos e caros que alimentam milhares de ramais e ajuda os usuários a economizar dinheiro no uso de longas chamadas internacionais.

Depois de implementar o software, ele se torna extremamente versátil, fácil de customizar e fácil de estender (GUPTA; AGRAWAL; QADEER, 2013, nossa tradução).

3.1.1. Configuração do Asterisk

Inicialmente, para realizar a instalação do Asterisk foi necessário uma máquina virtual com um servidor. No entanto, utilizou-se como virtualizador o VMWare Workstation Player em sua versão 16.2.1, que se encontra disponível gratuitamente para Windows e para Linux. O virtualizador em questão foi escolhido pela sua disponibilidade, fácil acesso, licença de uso gratuita. Em seguida, criou-se uma VM com o Ubuntu server na versão 20.04.2, essa versão encontra-se disponível gratuitamente. A escolha do sistema operacional, deu-se pela disponibilidade, fácil acesso e licença gratuita. E, para acessar o servidor criado, utilizou-se o PuTTY, um programa que serve para se conectar com servidores remotos através de protocolos de rede como telnet e SSH, para a pesquisa acessou-se o servidor via SSH.

Tendo a primeira fase do cenário criado, fez-se a instalação da versão 18.8.0 do Asterisk no Ubuntu server, em seguida fez-se a configuração dos usuários SIP, essas configurações são feitas no arquivo /etc/asterisk/sip.conf, como apresentado na figura 2. Esse arquivo está dividido em duas partes, a seção geral e a parte destinada a cada peer/usuário SIP.



```
[general]
udpbindaddr=0.0.0.0:5060
context=dummy
disallow=all
allow=ulaw
alwaysauthreject=yes
allowguest=no
reinvite=no
canreinvite=no
insecure=port,invite
transport=udp,tls
encryption=no
tlsenable= yes
tlscertfile=/etc/asterisk/keys/asterisk.pem

[grandstream]
type=friend
secret=#supersecret#
host=dynamic
qualify=yes
directmedia=no
context=entrada-custom-breno
tlscipher=all
tlsclientmethod=tlsv1
encryption=yes

[microsip]
type=friend
secret=#supersecret#
host=dynamic
qualify=yes
directmedia=no
context=entrada-custom-breno
tlscipher=all
tlsclientmethod=tlsv1
encryption=yes
```

Figura 2. Configuração do arquivo /etc/asterisk/sip.conf

A seção geral contém as opções de configurações gerais e nele podem ser utilizados para definir os parâmetros padrão. Na segunda seção onde se encontram as configurações de cada peer, granstream e microsip.

Até o momento, haviam sido somente criados os peers, no entanto seria necessário realizar o plano de discagem para o Asterisk entender o que fazer quando um peer realizar uma discagem para o outro. Nesta senda, foi criado o plano de discagem, esse plano é feito no arquivo /etc/asterisk/extensions.conf figura 3.

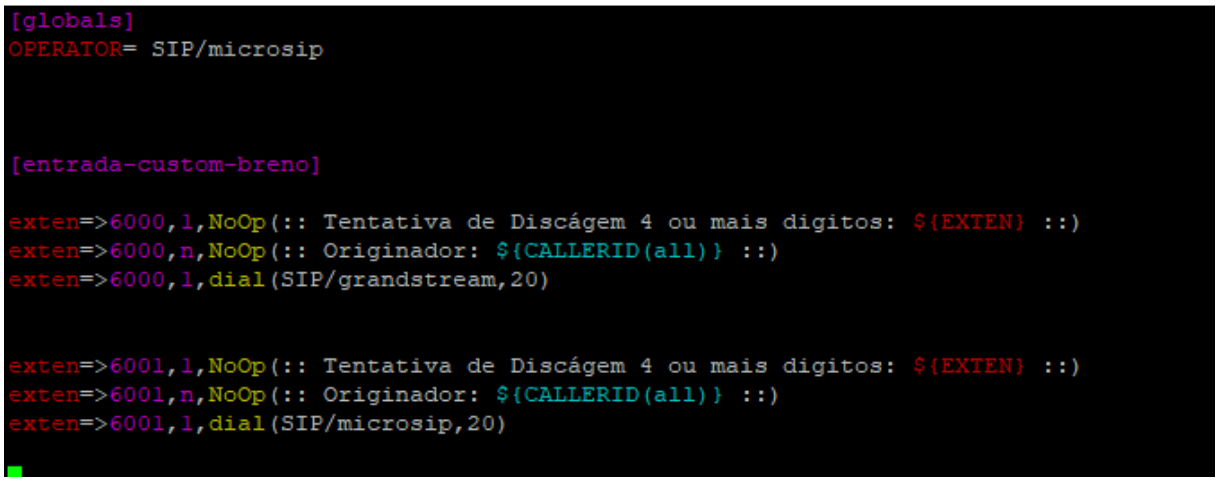


Figura 3. configuração do arquivo /etc/asterisk/extensions.conf

3.2. Softphone

Finalizado a configuração do Asterisk com os respectivos peers, foi feita a instalação dos usuários SIP em softphones, um dos softphones foi instalado em um notebook (figura 4) e outro em um celular . O softphone instalado no notebook foi microsip em sua versão 3.20.7, que se encontra atualmente disponível somente para Windows de forma gratuita. Foi escolhido pela disponibilidade, fácil acesso e permitir o uso de criptografia na versão gratuita. No celular, foi instalado o GrandStream Wave lite na versão 1.2.14.1, diferente do microSIP, ele encontra-se disponível somente para celular, tanto para Android como para IOS, ambos disponíveis gratuitamente. Foi escolhido o GrandStream Wave lite por permitir criptografia na versão utilizada, fácil acesso e disponibilidade.

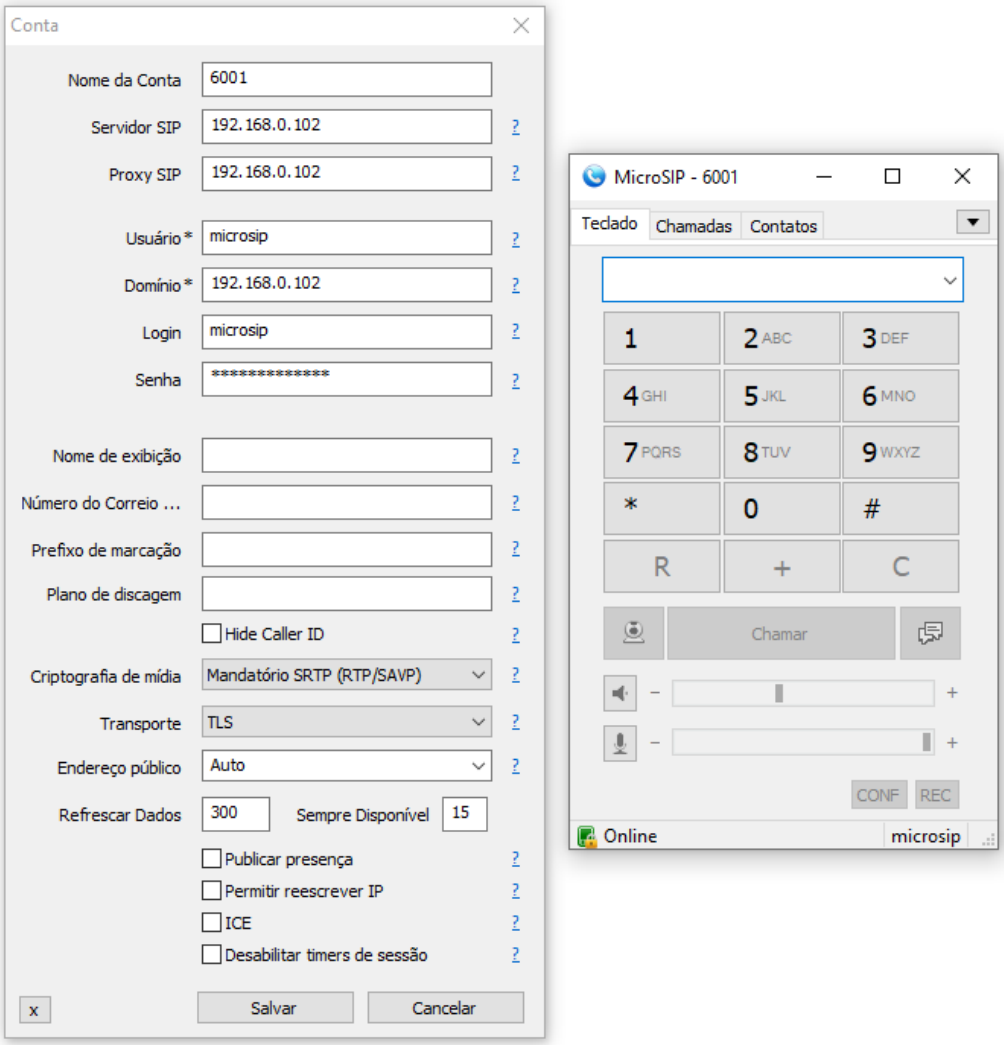


Figura 4. instalação do peer microsip

Finalizado a instalação de cada usuário SIP nos softphones, foram feitos os testes de ligação de um usuário SIP para outro, as ligações completaram perfeitamente como apresentado na figura 5, o cli do Asterisk.

```
  == Using SIP RTP CoS mark 5
     > 0x7fe05c01e120 -- Strict RTP learning after remote address set to: 192.168.0.101:49196
    -- Executing [6001@entrada-custom-breno:1] NoOp("SIP/grandstream-0000001c", ":: Tentativa de Discágem 4 ou mais digitos: 6001 ::") in new stack
    -- Executing [6001@entrada-custom-breno:2] NoOp("SIP/grandstream-0000001c", ":: Originador: "" <grandstream> ::") in new stack
    -- Executing [6001@entrada-custom-breno:3] Dial("SIP/grandstream-0000001c", "SIP/microsip,20") in new stack
  == Using SIP RTP CoS mark 5
    -- Called SIP/microsip
    -- SIP/microsip-0000001d is ringing
     > 0x7fe064008810 -- Strict RTP learning after remote address set to: 192.168.0.103:4012
    -- SIP/microsip-0000001d answered SIP/grandstream-0000001c
    -- Channel SIP/microsip-0000001d joined 'simple_bridge' basic-bridge <c0bd4bba-5f8a-4b80-9c0e-a9e60463a22c>
    -- Channel SIP/grandstream-0000001c joined 'simple_bridge' basic-bridge <c0bd4bba-5f8a-4b80-9c0e-a9e60463a22c>
     > 0x7fe064008810 -- Strict RTP switching to RTP target address 192.168.0.103:4012 as source
  == SRTCP unprotect failed on SSRC 169907759 because of unsupported parameter
     > 0x7fe05c01e120 -- Strict RTP switching to RTP target address 192.168.0.101:49196 as source
     > 0x7fe05c01e120 -- Strict RTP learning complete - Locking on source address 192.168.0.101:49196
    -- Channel SIP/microsip-0000001d left 'simple_bridge' basic-bridge <c0bd4bba-5f8a-4b80-9c0e-a9e60463a22c>
    -- Channel SIP/grandstream-0000001c left 'simple_bridge' basic-bridge <c0bd4bba-5f8a-4b80-9c0e-a9e60463a22c>
  == Spawn extension (entrada-custom-breno, 6001, 3) exited non-zero on 'SIP/grandstream-0000001c'
astserver*CLI>
```

Figura 5. cli no Asterisk

4 RESULTADOS E DISCUSSÃO

Analisando os dois ambientes, sem criptografia e com criptografia, com o wireshark. Não há qualquer segurança nos protocolos SIP e RTP, por essa razão no primeiro ambiente, qualquer usuário que estiver na rede VoIP consegui ver o fluxo de sinalização (figura 7) entre os usuários que estiverem em comunicação e também poderá ter acesso a conversa, e com isso consegue ouvir a mensagem trocada pelos usuários.

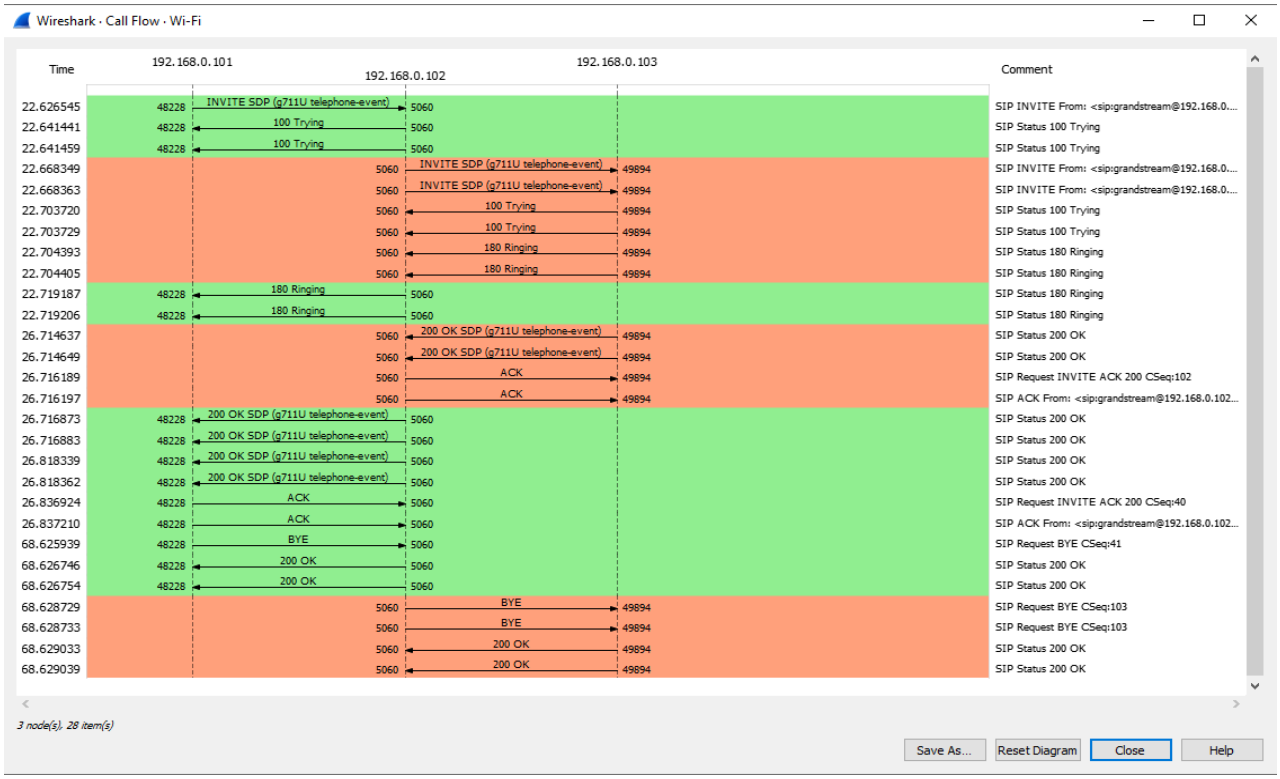


Figura 6. Fluxo de sinalização

No ambiente criptografado, fez-se a configuração dos protocolos SRTP e TLS, para criptografar a mídia e o fluxo de sinalização respectivamente. Configurado o protocolo SRTP utilizando o protocolo SRTP para criptografia da mídia, ainda assim

consegue-se ver o fluxo de sinalização entre os usuários SIP, porém a grande diferença de ativação do SRTP para o RTP é que a mídia é completamente criptografada. Desta forma, mesmo tendo acesso ao stream de áudio, não seria possível compreender na íntegra a mensagem que está a ser transmitida de um ponto para o outro, pois ouve-se somente o áudio deformado com ruídos. A figura 7 apresenta o stream de áudio criptografado.

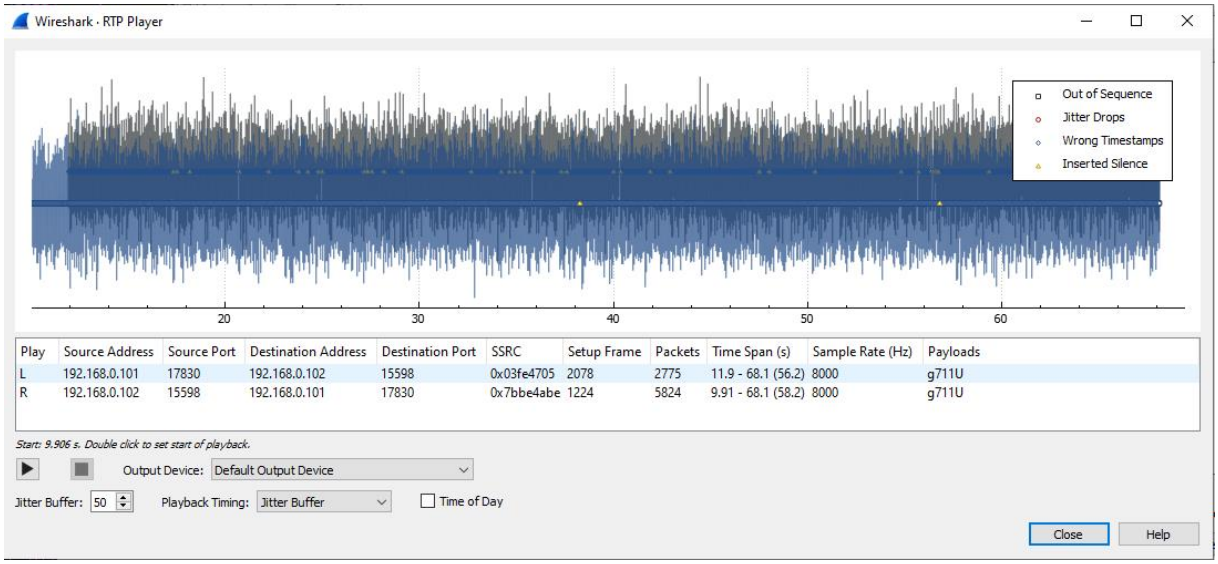


Figura 7. Stream de áudio criptografado.

E finalizando a última parte, a instalação do protocolo TLS fez com que estivesse indisponível o fluxo de sinalização na rede, impossibilitando de igual modo o acesso ao stream de áudio. Resultando em uma comunicação criptografada, tornando a rede mais difícil de ser invadida por um invasor.

5 CONCLUSÃO

Com base no que foi apresentado no presente trabalho, notou-se que utilizar o Asterisk como um mediador entre os usuários da rede VoIP, aplicando os recursos de segurança disponíveis (para o presente trabalho, criptografia) no Asterisk, tem-se uma rede com maior resistência a ataques de maliciosos, consequentemente os usuários estarão mais seguros e menos preocupados com extravío de informações confidenciais.

O objetivo da pesquisa foi analisar recursos disponíveis no Asterisk capazes de melhorar a camada de segurança da comunicação VoIP, no entanto, ao habilitar os protocolos TLS e SRTP, conseguiu-se chegar ao objetivo, aumentando a camada de segurança rede.

Para trabalhos futuros, pode ser estendido a pesquisa para realizar a análise para as PSTN, em um ambiente idêntico, com um acréscimo de um SIP Trunk para realizar e receber as ligações entre VoIP e PSTN.

REFERÊNCIAS

CIOPONEA, Cătălin; BUCICOIU, Mihai; ROSNER, Daniel. **Analysis of VoIP encryption performance using dedicated hardware. 2013**. Disponível em:<https://ieeexplore-ieee-org.ez318.periodicos.capes.gov.br/document/6511751 > Acesso em 15 Nov 2021.

DAKUR, Aditya; DAKUR, Shruthi. **Eavesdropping and interception security hole and its solution over VoIP service**. 2014. Disponível em: <https://ieeexplore-ieee-org.ez318.periodicos.capes.gov.br/document/7030837 > Acesso em 15 Nov 2021.

GUPTA, Priyanka; AGRAWAL, Neha; QADEER, Mohammed Abdul. **GSM and PSTN gateway for asterisk EPBX. 2013**. Disponível em:<https://ieeexplore.ieee.org/document/6616225 > Acesso em 15 Nov 2021.

HASAN, Muhammad Zulkifl; HUSSAIN, Muhammad Zunnurain. **Collective Study On Security Threats In VOIP Networks**. 2017. Disponível em:<https://www.researchgate.net/profile/Muhammad-Zulkifl-Hasan-3/publication/344737338_Collective_Study_On_Security_Threats_In_VOIP_Networks/links/5f8d1c3392851c14bcd2a109/Collective-Study-On-Security-Threats-In-VOIP-Networks.pdf > Acesso em 15 Nov 2021.

ISEKI, Fumikazu; SATO, Yuki; KIM, Moo Wan. **VoIP system based on Asterisk for enterprise network**. 2011. Disponível em: <https://ieeexplore-ieee-org.ez318.periodicos.capes.gov.br/document/5746040 > Acesso em 12 Nov 2021.

NEACŞU, Eugen ; ŞCHIOPU, Paul. **An Analysis of Security Threats in VoIP Communication Systems**. 2020. Disponível em: <https://ieeexplore.ieee.org/document/9223162 > Acesso em 12 Nov 2021.

OCHE, Michael et al. **Securing VoIP network: An overview of applied approaches and analysis**. 2013. Disponível em <https://ieeexplore-ieee-org.ez318.periodicos.capes.gov.br/document/7055097 > Acesso em 13 Nov 2021.

SINAM et al. **A technique for classification of VoIP flows in UDP media streams using VoIP signalling traffic**. 2014. Disponível em: <https://ieeexplore-ieee-org.ez318.periodicos.capes.gov.br/document/6779348 > Acesso em 15 Nov 2021.