CENTRO DE INSTRUÇÃO DE GUERRA ELETRÔNICA

Cap QCO/Infor EVALDO GALVÃO MENDONÇA

TELEFONE SEGURO: UM ESTUDO DE CASO COM FOCO NO ATAQUE

Brasília
2017

Cap EVALDO GALVÃO MENDONÇA

TELEFONE SEGURO: UM ESTUDO DE CASO COM FOCO NO ATAQUE

Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais apresentado ao Centro de Instrução de Guerra Eletrônica como requisito para obtenção do Grau de Pós-Graduação *Lato Sensu*, nível de especialização em Guerra Cibernética.

Orientador: 1° Ten Com VINÍCIUS LUIS PALUDETO
Co-orientador: 2° Ten OTT/Biblio THAIS RIBEIRO MORAES MARQUES

Brasília
2017

Ficha Catalográfica Elaborada pela Biblioteca
do Centro de instrução de Guerra Eletrônica (CIGE)
Bibliotecária Responsável: 2° Ten Thais Moraes CRB1/1922

M539t
Mendonça, Evaldo Galvão
Telefone seguro: um estudo de caso com foco no ataque. / Evaldo Galvão Mendonça – Brasília: Centro de Instrução de Guerra Eletrônica, 2017.
64f.; il.

Trabalho de conclusão apresentado ao Curso de Guerra Cibernética para Oficiais – Centro de Instrução de Guerra Eletrônica, Brasília, 2017.

Bibliografia: f. 64.

1. Telefonia, segurança. 2. Ataque, telefonia. 3. Voip. 4. Criptografia. I Marcelino, Mendonça, Evaldo Galvão. II. Centro de Instrução de Guerra Eletrônica. III. Título.

CDD 621.385

Cap EVALDO GALVÃO MENDONÇA

TELEFONE SEGURO: UM ESTUDO DE CASO COM FOCO NO ATAQUE

Trabalho de Conclusão do Curso de Guerra Cibernética para Oficiais apresentado ao Centro de Instrução de Guerra Eletrônica como requisito para obtenção do Grau de Pós-Graduação *Lato Sensu*, nível de especialização em Guerra Cibernética.

Aprovado em: ___ de novembro de 2017

_____
Vinícius Luis Paludeto – 1° Ten Com
Orientador

_____
Thais Ribeiro Moraes Marques – 2° Ten OTT/Biblio
Coorientador

_____
Adão dos Santos – 1º Sgt Com
membro da comissão de avaliação

_____
Anderson Lellis Alves Moura – Maj Com
membro da comissão de avaliação

Brasília
2017

Aos meus queridos pais, por todo amor, carinho, compreensão, fé e estímulo.

AGRADECIMENTOS

Agradeço a minha esposa Silvana Schirmer Mendonça que sempre me apoiou em todas as fases da minha carreira e, que em especial, para a realização deste Curso de Especialização, em que permaneci distante de nosso lar, cuidando da educação e saúde de nosso Filho.

Ao meu filho Arthur Schirmer Mendonça, pela compreensão do tempo distante em prol da viabilização de todo o processo de estudo para a conclusão deste Curso, que é coroado pelo trabalho ora apresentado.

A todos os militares do Curso que direta ou indiretamente contribuíram para a elaboração do presente trabalho, que encerra mais um degrau na contínua busca do aperfeiçoamento para melhor desempenhar as funções atinentes aos Oficiais do Exército Brasileiro.

Temos o destino que merecemos. O nosso destino está de acordo com nossos méritos.

Albert Einstein.

RESUMO

Referencia**:** MENDONÇA, Evaldo Galvão. **Telefone Seguro: Um estudo de caso com foco no ataque**. 2017. 61 folhas. Monografia (Curso de Guerra Cibernética para Oficiais)- Centro de Instrução de Guerra Eletrônica, Brasília, 2017.

O Projeto **Telefone Seguro** do Sistema de Inteligência de Defesa (SINDE), foi proposto por meio da tecnologia de Voz sobre *Internet Protocol* (VoIP) para a comunicação telefônica segura entre os assinantes da Rede de Inteligência de Defesa (RINDE). Tal iniciativa veio da necessidade de padronização de meios, possível com a utilização do Protocolo de Internet (IP), desenvolvido para proporcionar a interoperabilidade entre os diversos sistemas que integram a Internet. O serviço implementado permite efetuar chamadas de voz e vídeo, enviar mensagens, compartilhar arquivos, realizar videoconferências, entre outros. A partir deste serviço, com todas as funcionalidades citadas, foi necessário implementar camadas de segurança adicionais às existentes para uma maior profundidade na defesa do sistema, preservando a máxima Disponibilidade, Integridade ,Confidencialidade e Autenticidade (DICA), pilares da Segurança da Informação e Comunicações. As camadas de segurança adicionais foram implementadas com a utilização de Certificados Digitais SSL/TLS para a autenticação dos ramais *Session Initiation Protocol* (SIP), Criptografia Simétrica AES 256 para o fluxo *Real Time Protocol* (RTP) e *Virtual Private Network* (VPN) para os equipamentos instalados fora do Ministério da Defesa. O presente trabalho pretende, numa primeira fase, apresentar a metodologia de ataque a uma arquitetura padrão de sistemas VoIP, descrita por Regueira (2015). Em uma segunda fase, realizar o estudo das tecnologias de segurança que implementam as camadas de defesa em profundidade do presente estudo de caso, simulando os mesmos ataques com a finalidade de verificar a eficácia dos mecanismos implementados. Tendo em conta os resultados obtidos no presente trabalho, pode-se concluir que é viável a utilização da tecnologia VoIP, utilizando-se da Internet, desde que sejam implementados mecanismos de segurança para a defesa em profundidade computacionalmente seguros, principalmente visto que países como os Estados Unidos possuem a *Communications Assistance for Law Enforcement Act* (CALEA), uma Lei que autoriza o grampo nas comunicações públicas.

Palavras-chave: Telefone Seguro. Criptografia. Certificados Digitais. VPN. TLS/SSL. SIP. SRTPS. Ataque. Cibernética.

ABSTRACT

The project Secure Telephone of the Defense Intelligence System (SINDE) was proposed through Voice Internet Protocol (VoIP) technology for secure telephone communication between subscribers of the Defense Intelligence Network (RINDE). This initiative came from the need for standardization of means, possible with the use of Internet Protocol (IP), developed to provide interoperability between the various systems that integrate the Internet. The implemented service allows you to make voice and video calls, send messages, share files, hold videoconferences, and more. From this service, with all the mentioned functionalities, it was necessary to implement additional layers of security to the existing ones for a greater depth in the defense of the system, preserving the maximum Availability, Integrity, Confidentiality and Authenticity (DICA), pillars of Information Security and Communications. Additional security layers were implemented using SSL / TLS Digital Certificates for Session Initiation Protocol (SIP), AES 256 Symmetric Encryption for Real Time Protocol (RTP) and Virtual Private Network (VPN) streams for equipment installed outside the Ministry of Defense. The present work intends, in a first phase, to present the methodology of attack to a standard architecture of VoIP systems, described by Regueira (2015). In a second phase, carry out the study of security technologies that implement the in-depth defense layers of the present case study, simulating the same attacks in order to verify the effectiveness of the mechanisms implemented. Considering the results obtained in the present work, it is possible to conclude that it is viable to use VoIP technology, using the Internet, provided that security mechanisms for defense in computer security are implemented, especially since countries such as The United States has the Communications Assistance for Law Enforcement Act (CALEA), a law that authorizes the clampdown in public communications.

Keywords: Secure Telephone. Intelligence. VoIP. Encryption. Digital Certificates. VPN. TLS / SSL. SIPS. SRTP.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
SISBIN	Sistema Brasileiro de Inteligência
SINDE	Sistema de Inteligência de Defesa
RINDE	Rede de Inteligência de Defesa
SIDE	Subchefia de Inteligência de Defesa
CALEA	*Communications Assistance for Law Enforcement Act*
LBDN	Livro Brando de Defesa Nacional
AdiDef	Adidos de Defesa
RBJID	Representação Brasileira na Junta Interamericana de Defesa
TSG	Telefone Seguro Governamental
ITU-T	*International Telecommunications Union*
IETF	*Internet Engineering Task Force*
RPTC	Rede Pública de Telefonia Comutada
PSTN	*Public Switched Telephone Network*
TDM	*Timedivision Multiplexing*
PBX	*Private Branch eXchange*
VoIP	Voz sobre Internet Protocolo
SIP	*Session Initialization Protocol*
RTP	*Real-Time Transport Protocol*
SDP	*Session Descriptor Protocol*
RFC	*Request for Comments*
DHCP	*Dynamic Host ConFiguration Protocol*
DNS	*Domain Name System*
HTTP	*Hypertext Transfer Protocol*
MIME	*Multipurpose Internet Mail Extensions*
DoS	*Deny of Service*

MITM	*Man-in-the-middle*
PKI	*Public Key Infrastructure*
EAP	*Extensible Autentication Protocol*
VPN	*Virtual Private Network*
TLS	*Transport Layer Security*

SUMÁRIO

1 INTRODUÇÃO

O presente estudo demonstra a importância da prospecção de soluções em tecnologia da informação e comunicações para suportar os novos processos finalísticos que ora se apresentam na sociedade da informação, que segundo Clark (2015), depende do setor privado que detém a maioria das infraestruturas críticas por onde a informação trafega, elevando o potencial destrutivo da Guerra da Informação. Neste contexto, foi desenvolvido o Projeto Telefone Seguro no âmbito do MD para atender o SINDE sob a coordenação da SIDE.

O SINDE foi instituído no âmbito do Ministério da Defesa (MD) e das Forças Armadas (FA), em 2002, a fim de integrar as ações de planejamento e execução da atividade de inteligência de defesa, sendo um dos componentes do Sistema Brasileiro de Inteligência (SISBIN). As atividades de Inteligência exigem a utilização de meios sigilosos para preservar suas comunicações, uma vez que podem se antecipar a ameaças tais como o terrorismo, sendo composto por membros no Brasil e em outros países, o que torna inviável a manutenção de mecanismos de segurança específicos para cada tecnologia de telefonia local.

Como assegura-Brasil (2012), pode-se dizer que a atividade de inteligência de defesa é caracterizada por ser técnico-militar desenvolvida com a finalidade de salvaguardar os conhecimentos de interesse da Defesa, estando divididos em duas áreas de atuação:

> - inteligência estratégica de defesa: voltada para a produção dos conhecimentos necessários ao processo decisório, bem como à formulação e condução, no mais alto nível, do planejamento estratégico militar, de politicas e de planos, no âmbito nacional ou internacional, de interesse da Defesa Nacional; e
> - inteligência operacional de defesa: voltada para a produção e salvaguarda dos conhecimentos necessários ao planejamento, condução e sustentação de campanhas e operações militares, visando atingir objetivos estratégicos abrangidos nas áreas de operações. (Brasil, 2012, p. 77).

Neste contexto, Gonçalves (2011) deixa claro que a atividade de inteligência de defesa está descentralizada com a finalidade de atender a três percepções. A primeira refere-se à inteligência em si, o tratamento analítico da informação formada de dados brutos até a produção do conhecimento. A segunda é o manuseio do dado sigiloso, das técnicas de obtenção do dado negado, que alimentarão a primeira. A terceira é o ato de assessorar, reportando em tempo hábil, mesmo que a informação não esteja completa. O mais preocupante, contudo, é realizar as duas primeiras

fases de forma sigilosa e comprometer o processo decisório por uma falha de segurança no meio de comunicação utilizado.

Não é exagero afirmar que a evolução das redes sociais possibilitou essa comunicação em tempo real, e, que, muitas vezes são utilizadas por não haver outro meio disponível com a mesma facilidade de uso. Diante do exposto, este trabalho apresenta um estudo de caso sobre as camadas de **Segurança da Informação e Comunicações (SIC)** utilizadas para compor a **Solução Telefone Seguro** da RINDE, uma solução capaz de prover a efetividade das comunicações a quem tem à necessidade de conhecer.

Para demonstrar a eficácia da solução, foi utilizada como referência a metodologia de ataque a sistemas VoIP proposto por Regueira (2015), de forma que aplicado contra um cenário do estudo de caso, possa comprovar que os princípios da Segurança da Informação foram preservados. Essa comprovação pode demonstrar que a solução, implementada com Softwares Livres e Algoritmos Criptográficos de conhecimento público, porém, computacionalmente seguros, podem prover uma infraestrutura racional de comunicação segura, sem a dependência de grandes empresas, ou soluções do tipo caixa-preta desenvolvidas por Órgãos do Estado**.**

Por outro lado, de acordo com o Decreto 7.845, de 14 de novembro de 2012, deve-se utilizar Algoritmo de Estado, que é a função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal. Diz ainda que a cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.

Porém, segundo Tanembaum (2011), é de extrema importância o caráter não sigiloso do algoritmo de encriptação a ser utilizado. Ao tornar o algoritmo público, inúmeros criptólogos podem tentar decodificar o sistema e caso muitos tenham tentado isso durante cinco anos após a sua publicação e nenhum tenha conseguido, há uma grande probabilidade de que o algoritmo seja sólido.

1.1 PROBLEMA

O Órgão central da RINDE fica localizado na Subchefia de Inteligência de Defesa (SIDE) do MD, compartilhando os mesmos ativos de telefonia e de redes usadas pela Administração Central do MD, que podem estar sendo mantidos por empresas privadas contratadas ou servidores públicos de outros Órgãos.

Existem membros da RINDE fisicamente localizados em outros países tais como os Adidos de Defesa (AdiDef) e a Representação Brasileira na Junta Interamericana de Defesa (RBJID), que possuem sistemas de telefonia distintos e não padronizados.

Há uma solução de criptografia (algoritmo de Estado) para telefonia fixa desenvolvida pela Agência Brasileira de Inteligência (ABIN) chamada de Telefone Seguro Governamental (TSG) que necessita estar conectado às duas extremidades da ligação para funcionamento, dependendo da Rede Pública de Telefonia Comutada (RPTC).

1.2 JUSTIFICATIVA

Existe a necessidade latente de minimizar os Riscos, mantendo domínio de toda a infraestrutura crítica necessária para manter a segurança do serviço VoIP em perfeito funcionamento

Há demanda de acesso em tempo real de informes de inteligência disponibilizados pela SIDE.

A situação atual da segurança da informação requer providências tecnológicas urgentes para assegurar que nenhuma informação seja desviada do seu destino certo. As atualizações e manutenções para acompanhar a evolução da tecnologia fazem-se necessárias para que a segurança da informação seja efetiva.

Sendo assim, é de suma importância que tal assunto seja alvo de debates e estudos, com enfoque na solução de tal problema, pois caso contrário poderá ficar refém de uma falsa sensação de segurança da informação apenas seguindo aquilo que é exigido pelos normativos vigentes.

1.3 DELIMITAÇÃO DO TEMA

O presente trabalho se restringe a apresentar de forma geral a arquitetura ostensiva do Telefone Seguro implementado no estudo de caso, focando o detalhe nos mecanismos de segurança conhecidos publicamente, utilizados para mitigar as vulnerabilidades inerentes do protocolo SIP que ficaram evidenciadas na exploração e ataques realizados por Regueira (2015). Serão apresentados os resultados dos ataques realizados no ambiente simulado segundo a metodologia de referência.

1.4 OBJETIVOS

Seguem os objetivos geral e específicos.

1.4.1 Objetivo Geral

O objetivo geral deste trabalho é comparar os aspectos de vulnerabilidade e de segurança que podem ser utilizados tanto para o ataque quanto para defesa de sistemas que utilizam o serviço VoIP.

1.4.2 Objetivos Específicos

A fim de atingir o objetivo geral, os seguintes objetivos específicos serão buscados:

a) identificar as ameaças e vulnerabilidades do serviço VoIP;

b) aplicar uma metodologia de ataque a serviço VoIP;

c) empregar as técnicas de segurança em profundidade;

d) apresentar os resultados comparativos de ataque ao ambiente simulado do estudo de caso.

1.5 METODO DE PESQUISA

A metodologia segue os preceitos do estudo exploratório, realizando pesquisa

bibliográfica, que segundo Gil (2008), é desenvolvida a partir de material já elaborado, constituído de livros e artigos científicos. A partir das fontes selecionadas e de um estudo de caso, será realizando um laboratório simulado, onde serão abordadas as técnicas de ataque a sistemas voip segundo a metodologia proposta por Regueira (2008). Ao final a resposta ao problema de pesquisa será analisada e interpretada.

1.6 ESTRUTURA DO TRABALHO

Inicialmente serão estudados os serviços necessários para a montagem de um sistema VoIP, fase de extrema importância para que um atacante possa familiarizar com as vulnerabilidades inerentes a cada serviço.

Por conseguinte, serão identificadas as vulnerabilidades no sistema através da metodologia de ataque proposta por Regueira (2015), sendo responsável por enumerar os diversos vetores de ataques, bem como as ferramentas que podem explorá-las.

Logo após, a implementação de técnicas de segurança para a defesa em profundidade com a finalidade de mitigar as vulnerabilidades exploradas na fase anterior, estas medidas também servirão para mitigar outros Riscos não explorados, colocando o leitor do outro lado da Guerra Cibernética.

Finalizando, serão apresentados os resultados do ataque no ambiente simulado tomando-se como referência o modelo do estudo de caso.

2 REVISÃO BIBLIOGRÁFICA

No contexto do ataque, para ser efetivo em suas ações, um atacante necessita realizar o reconhecimento do sistema alvo, fase que depende do conhecimento prévio das tecnologias utilizadas para a implementação dos serviços. Por outro lado, o agente defensor, além de disponibilizar o serviço, precisa conhecer as técnicas de ataque para preservar a Segurança da Informação ao maior nível possível, tudo isso levando-se em conta o valor do serviço para a Organização.

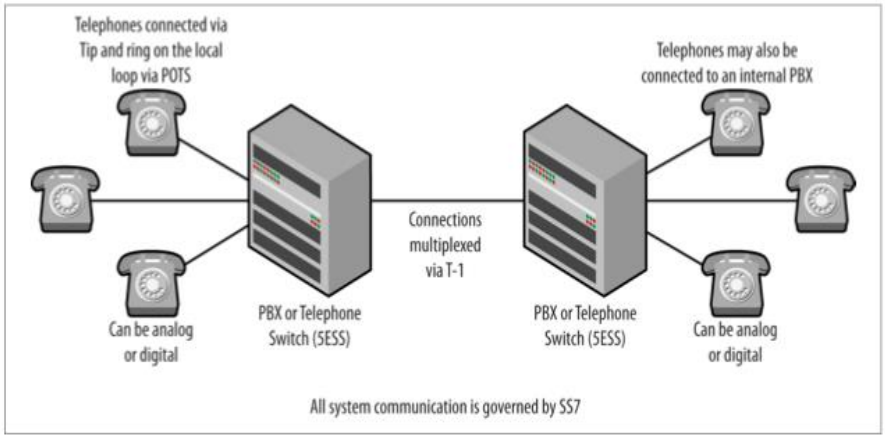
Neste contexto, serão apresentados os aspectos da tecnologia VoIP, bem como as suas vulnerabilidades exploradas segundo a metodologia proposta por Regueira (2015).

2.1 EVOLUÇÃO DO SISTEMA TELEFÔNICO

De acordo com HARTPENCE (2013), os serviços tradicionais de telefonia geralmente são descritos por termos com sistemas de sinalização, *Public Switched Telephone Network* (PSTN), conexões de discagem, loops locais, troca de circuitos e qualquer coisa proveniente das normas e protocolos estabelecidos pela *International Telecommunications Union* (ITU-T) e *Internet Engineering Task Force* (IETF). A Figura 1 mostra um exemplo da topologia desse sistema, que foi usado há décadas para oferecer chamadas telefônicas confiáveis, de baixa largura de banda com alto nível de qualidade.

Na telefonia comutada, onde a multiplexação é feita pela divisão de tempo (TDM), cada canal ou circuito fica alocado para uma chamada, com uma velocidade máxima de 64 Kbits/seg. Caso ocorra uma ociosidade do canal durante a chamada, ele não poderá ser compartilhado com outra chamada. A voz tem uma via expressa, sem congestionamentos.

Figura 1- Topologia de telefonia tradicional



FONTE: Hartpence (2013)

2.2 INTRODUÇÃO A VOZ SOBRE IP

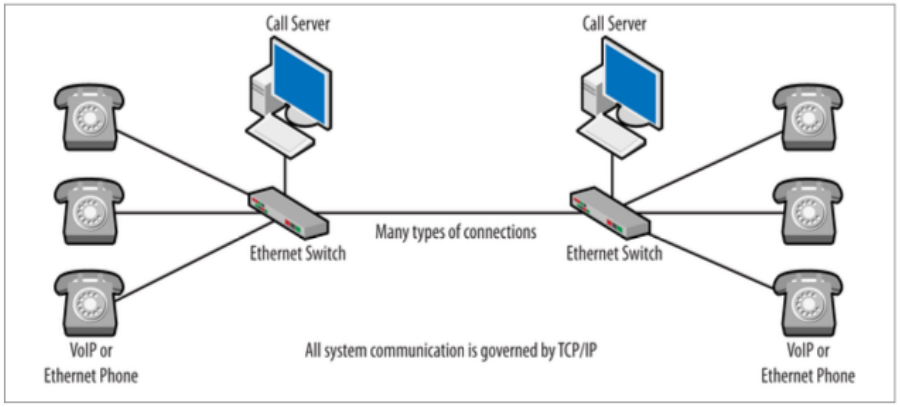
Os sistemas VoIP nativos eliminam muito do que é considerado na telefonia tradicional. Um sistema como o ilustrado na Figura 1 envolve muita sinalização de controle para realizar as várias tarefas necessárias. Por exemplo, os números de telefone são discados e esses números têm significado. Sons ou tons como ocupado e desligado também são mensagens de um tipo. As pesquisas de banco de dados para números 190 ou 0800 requerem mensagens adicionais, como serviços como identificador de chamadas, recursos avançados e roteamento de chamadas. Esses sinais são enviados entre os dispositivos como o *Private Branch eXchange* (PBX) antes que qualquer comunicação humana possa ocorrer.

VoIP leva todas essas mensagens de sinalização dentro dos pacotes IP. Após a implementação de um projeto VoIP, os *endpoints* não são mais conhecidos como telefones, mas telefones VoIP ou Ethernet. O nome PABX é retido, embora agora seja chamado de PBX IP, o que realmente significa que é um servidor executado em um computador. Redesenhando a topologia, pode-se ver algo como a Figura 2. Os protocolos utilizando pelos dois sistemas são completamente diferentes, com sistemas tradicionais usando o Sistema de Sinalização e as redes VoIP usando o TCP/IP.

Na telefonia VoIP, não existem os conceito de canal e circuito de transporte de pacote. Sua velocidade não está limitada a 64 Kibts/seg, onde a velocidade permitida pela tecnologia pode chegar a 10 Gbits/seg se for uma rede Ethernet. Em

VoIP, a voz vai disputar espaço com todas as outras aplicações que trafegam na rede, como outros pacotes de voz, de dados, de gerência de rede etc. Se não houver um tratamento adequado para os pacotes de voz, eles poderão ser perdidos ou chegar com atrasos ou fora de ordem.

Figura 2- Topologia de telefonia VoIP

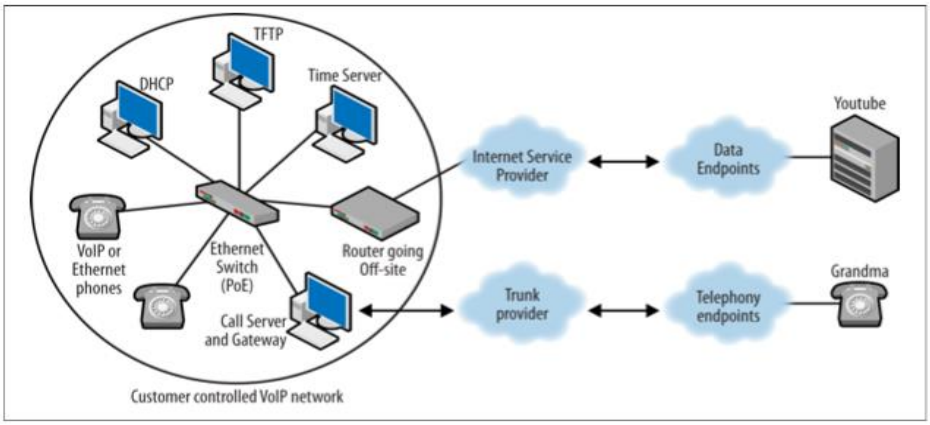


FONTE: Hartpence (2013)

Segundo Bates (2015), VoIP é um meio de amostragem e empacotamento de voz em tempo real para que possa ser enviado através de uma rede de dados (ou voz) em forma de pacote. O que isso significa é que a voz é amostrada, um pacote é criado e transportado em uma rede, podendo estar sob o domínio da organização ou passando pela Internet.

Se houver uma integração entre a rede VoIP e a PSTN, haverá a necessidade de um *Gateway* de mídia, com a finalidade de realizar a conversão da voz em um fluxo de dados para ser enviada por uma rede IP e vice-versa, conforme mostra a Figura 3, com uma topologia básica dos sistemas que compõem a solução VoIP dentro de uma empresa.

Figura 3- Integração VoIP TDM



FONTE: Hartpence (2013)

Já a telefonia IP inclui os itens acima e todos os recursos e funcionalidades das Centrais Telefônicas PBX tais como reencaminhamento de chamadas, atendimento automático de chamadas, conferência, etc. No mundo da telefonia IP, são usados sistemas como IP-PBXs, enquanto que no serviço anterior chamado VoIP tudo o que é necessário é um meio para converter a voz em pacotes.

À medida que a tecnologia se tornou mais confiável nos últimos anos, as organizações e clientes residenciais estão mudando para VoIP pelas seguintes razões:

a) a consolidação de voz e dados em uma rede reduz custos e resulta em um Custo Total de Propriedade (TCO) de rede menor;

b) a economia de despesas operacionais inclui menores custos de longa distância, custos de suporte reduzidos e economias via virtualização de força de trabalho;

c) as funcionalidades mais recentes implementadas, roteamento especificamente automático de chamadas para o conjunto de telefones VoIP, não importa onde possa estar;

d) as empresas também usam a migração para a VoIP como uma oportunidade para substituir equipamentos de telefonia em antigos por equipamentos ricos em tecnologia, como tele conferência e colaboração, aplicações multimidia;

e) VoIP suporta maior mobilidade, uma vez que os colaboradores remotos têm o mesmo acesso a recursos de voz que funcionários corporativos, etc.

A Figura 4 mostra uma relação de *endpoints* que podem ser utilizados como dispositivos VoIP, que vão desde *softwares* específicos instalados em computadores desktop (*Softfones*) até dispositivos físicos que podem realizar chamadas de videoconferência.

Esses dispositivos VoIP possibilitam uma série de funcionalidades para os usuários, mas, por outro lado, passam a ser alvos de ataques, pois possuem suas próprias vulnerabilidades elevando o risco de ameaças. Geralmente eles implementam uma série de protocolos como HTTP, FTP, TFTP, etc, herdando também as vulnerabilidades típicas de uma rede de dados.

Figura 4- *Endpoints* VoIP

FONTE: Bates (2015)

2.2.1 Protocolo de Sinalização SIP

A concorrência sempre foi parte de protocolos de rede, tais como o Appletalk e TCP/IP, 802.11g e 802.11a, Token Ring e Ethernet. Normalmente, a competição vai até que um se torne o padrão de fato. VoIP não foi diferente, existem vários protocolos de sinalização, todos manipulando o mesmo conjunto de funções.

Conforme descreve Hartpence (2013), o *Session Initialization Protocol* (SIP) foi a escolha do mercado, ele é padronizado na RFC 3261, embora existam várias outras RFCs complementares. É um protocolo de sinalização suportado por quase todos os fornecedores da indústria de VoIP. Embora haja uma base instalada significativa de sistemas que funcionem com outros tais como Skinny e H.323. Como os outros protocolos de sinalização, o SIP depende do *Real-Time Transport Protocol* (RTP) para transportar pacotes de voz entre a origem e o destino. Além disso, a RFC 3261 indica que outros protocolos de suporte, como MEGACO para controlar as funções do *Gateway* para a PSTN.

O SIP opera na camada de aplicação com o objetivo de iniciar sessões de usuários para transmissões multimídia, como voz, vídeo, bate-papo, etc. Essas sessões podem ser *unicast* ou *multicast* e podem operar com ou sem um servidor de chamadas ou *Gateway*. De acordo com a RFC, uma sessão é uma troca de dados

entre os participantes, onde é utilizado outro protocolo para negociar os parâmetros chamado *Session Descriptor Protocol* (SDP). Em uma arquitetura SIP são comuns os seguintes componentes:

a) User Agent (UA): Porção lógica que inicia ou responde às transações SIP, podendo ser um cliente ou servidor dependendo do estado, portanto, mantém a sessão;

b) User Agent Client (UAC): Inicia pedidos e aceita respostas. Normalmente, é o telefone SIP que inicia a chamada;

c) User Agent Server (UAS): Aceita pedidos e envia respostas;

d) Proxy: Componente intermediário que encaminha solicitações de um UA para outro UA ou outro proxy. Isso é feito principalmente para o roteamento, mas pode impor políticas como a autenticação, e provê maior segurança, onde os clientes nunca se comunicam realmente com o servidor;

e) Redirect Server: envia pedidos de um UAC para um conjunto alternativo de IDs de recursos uniformes ou URIs;

f) Registrar Server: UAS que aceita mensagens de REGISTO e atualiza a localização.

A Figura 5 mostra a arquitetura geral do SIP com os componentes descritos, para que possa lidar com sessões multimedias através do IP.

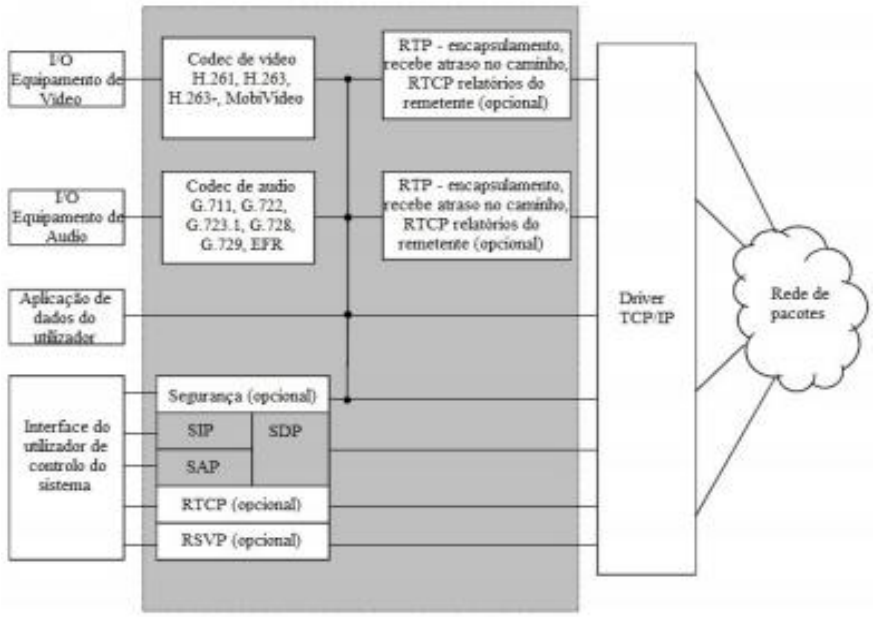
Figura 5- Componentes SIP

FONTE: Jorge (2017)

Conforme descreve Jorge (2017), o SIP utiliza facilidades de outros protocolos, incluindo ainda o *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. A organização dos protocolos pode ser observada na Figura 6.

Figura 6- Organização dos Protocolos



FONTE: Jorge (2017)

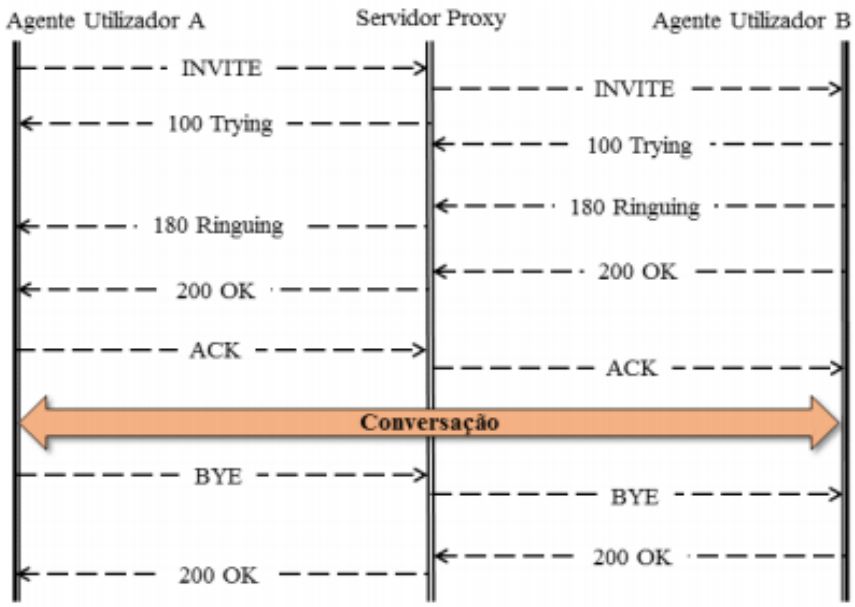
Para efetuar o registo no servidor existe uma primeira fase, onde é enviado um pedido de registo sem credenciais. Como é negado pelo servidor, é posteriormente enviado um desafio (*nounce*). De seguida, é efetuado um novo pedido de registo com credenciais e com a resposta ao desafio. Este processo pode ser observado na Figura 7.

Figura 7- Cenário de Registro

FONTE: Jorge (2017)

Após a realização do registo, quando se pretende efetuar uma chamada, o cenário de sinalização segue o processo representado na Figura 8.

Figura 8- Sinalização de uma chamada



FONTE: Jorge (2017)

2.3 TÉCNICAS DE ATAQUE A SISTEMAS VOIP BASEADOS EM SIP

Regueira (2015) apresenta uma metodologia de ataque onde são explorados os princípios básicos da Segurança da Informação: Confidencialidade, Integridade e Disponibilidade (CID), expondo os passos de um ataque, desde as técnicas iniciais como o *Footprinting,* até finais como o DoS, passando pelo *Eavesdropping, Registration Hijacking* e *Message Tampering.* Ainda, de acordo com Regueira (2015), o Laboratório foi conduzido no Centro de Instrução de Guerra Eletrônica do Exército Brasileiro (CIGE) e na residência do autor no período de agosto a outubro de 2015. A seguir serão apresentadas as ferramentas utilizadas em cada tentativa de ataque, bem como as técnicas e o princípio explorado.

2.3.1 Ataque à Confidencialidade

Segundo a metodologia descrita por Regueira (2015), inicialmente deve ser adotada a técnica de *FootPrinting*, onde se busca a identificação da infraestrutura do sistema VoIP, identificando serviços e vulnerabilidades inerentes. Para tanto, foi

escolhido o *framework SIPVICIOUS*, caracterizado por ser um conjunto de ferramentas *open source* constituído por: *Svmap* (efetua um *scan* na rede tentando identificar um PBX-IP), *Svwar* (enumera extensões a partir do servidor encontrado) e Svcrak (quebra de senhas das extensões através de um dicionário).

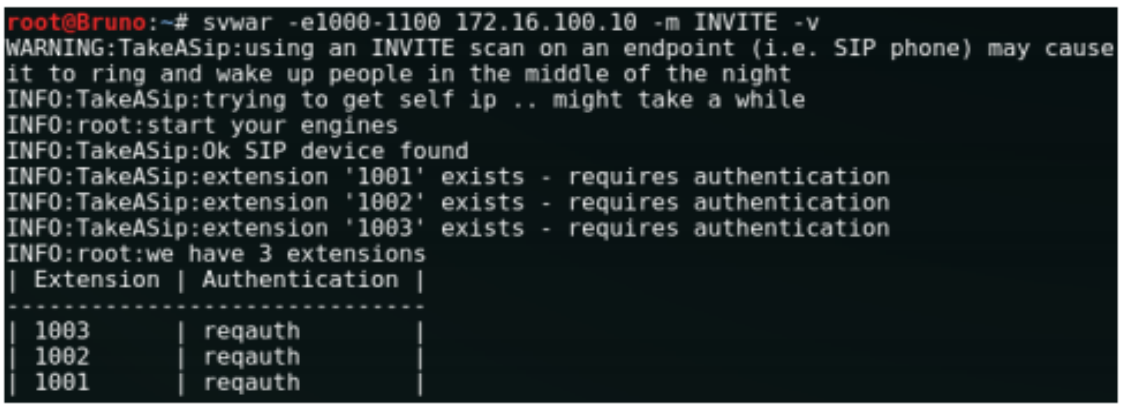
De acordo com a Figura 9, foi possível identificar cada servidor com a versão do *User Agent*, de forma que pode ser analisada a vulnerabilidade inerente. Em complemento pode ser utilizado o *Nmap* com as opções -sS e -sV.

Figura 9- Saída do *Svmap*

FONTE: Regueira (2015)

Após identificar a versão de cada sistema, é necessário enumerar as extensões, porém, no Laboratório proposto pelo autor não foi possível, pois as distribuições utilizadas não seguiam a RFC de referência. Por outro lado, Jorge (2017) consegue realizar a enumeração das extensões realizando o comando mais completo, dispondo das opções "*INVITE"*, "*REGISTER"* e "*OPTIONS"* do protocolo SIP, conforme Figura 10.

Figura 10- Saída do *Svwar*

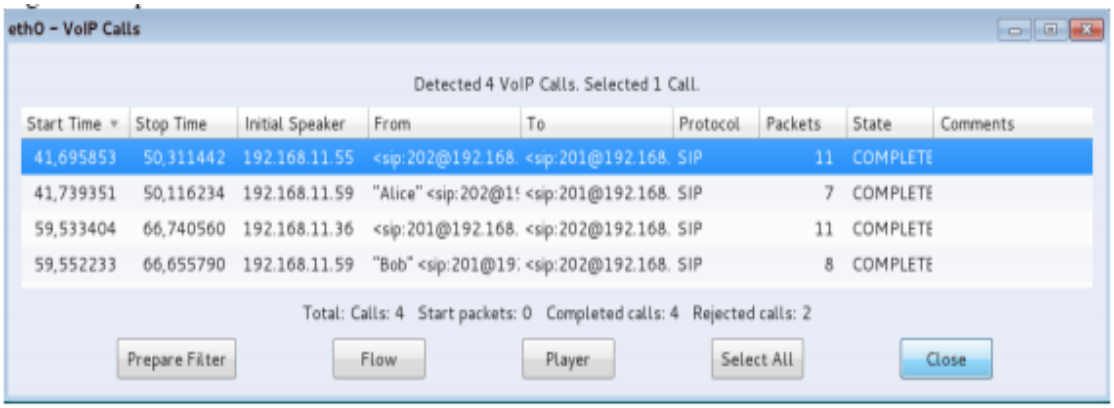


FONTE: Jorge (2017)

Outra forma de enumerar as extensões apresentada por Regueira (2015) foi a utilização da técnica de *MAC Flooding*, fazendo com que o *switch* se

transformasse em um *HUB* e o atacante pudesse capturar todo o tráfego do meio, conforme mostra a Figura 11 do *Wireshark.* Neste caso foi identificada uma ligação entre Alice e Bob, sendo possível capturar os ramais 202 e 201.

Figura 11- Saída do *Wireshark*

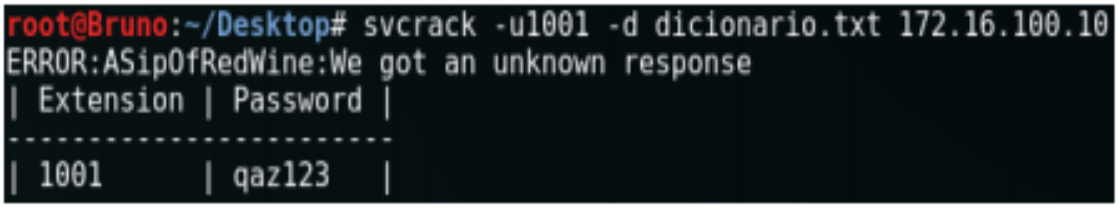


FONTE: Regueira (2015)

Após a identificação dos ramais, é necessária a descoberta de autenticação, porém, no caso em tela, a distribuição implementava uma política de senhas e bloqueios que inviabilizava o ataque por força bruta, mesmo possuindo dicionário direcionado, dito isso, o foco do ataque passou a ser na aplicação WEB que gerencia a configuração do UAC, o que resultou na descoberta da senha padrão “000000”. Para automatizar este ataque podem-se utilizar ferramentas como o Hydra ou o Medusa.

Com a finalidade de complementar Regueira (2015), a Figura 12 apresenta a utilização do *Svcrack* com um dicionário criado, que pode ser testado com a velocidade de até 80 palavras-frase por segundo. Cabe ressaltar que o servidor pode bloquear o IP do atacante, o que pode ser contornado spoofando-se o IP.

Figura 12- Saída do *Svcrack*

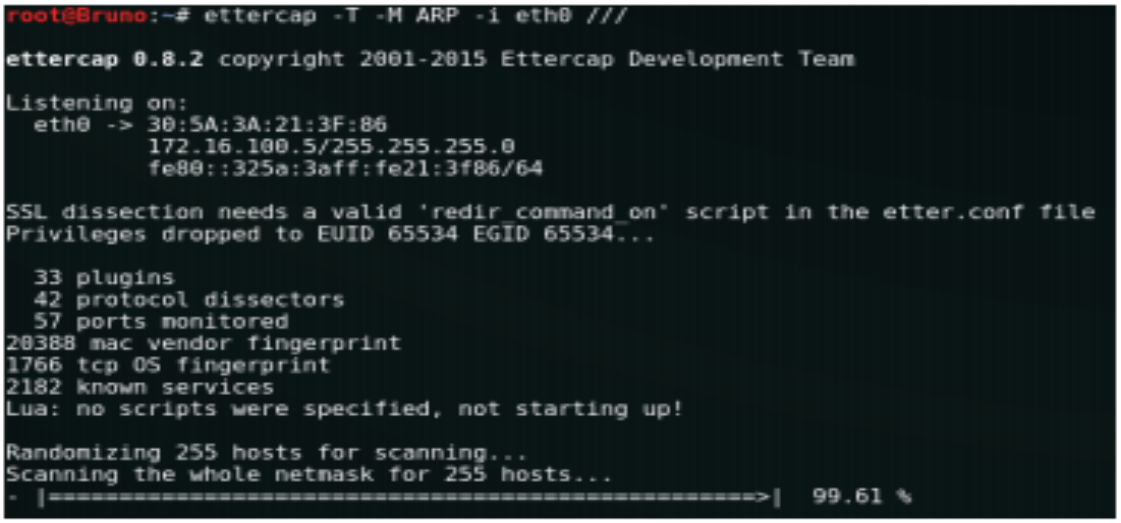


FONTE: Jorge (2017)

A técnica de *Man-in-the-middle* (MITM) não foi explorada por Regueira (2015), porém, pela sua relevância no ataque à Confidencialidade, cabe destacar que consiste em fazer com que todo o tráfego da(s) vitma(s) passe pelo atacante, de

forma que possa ser feita a escuta. De acordo com Jorge (2017) para realizar a escuta de todo o tráfego na presente VLAN, pode-se utilizar ferramentas como o *Ettercap* e o *Wireshark.* Primeiramente se inicia a escuta com o *Ettercap* conforme a Figura 13, passando a registrar todo o tráfego por meio do Wireshark.

Figura 13- Saída do *Ettercap*



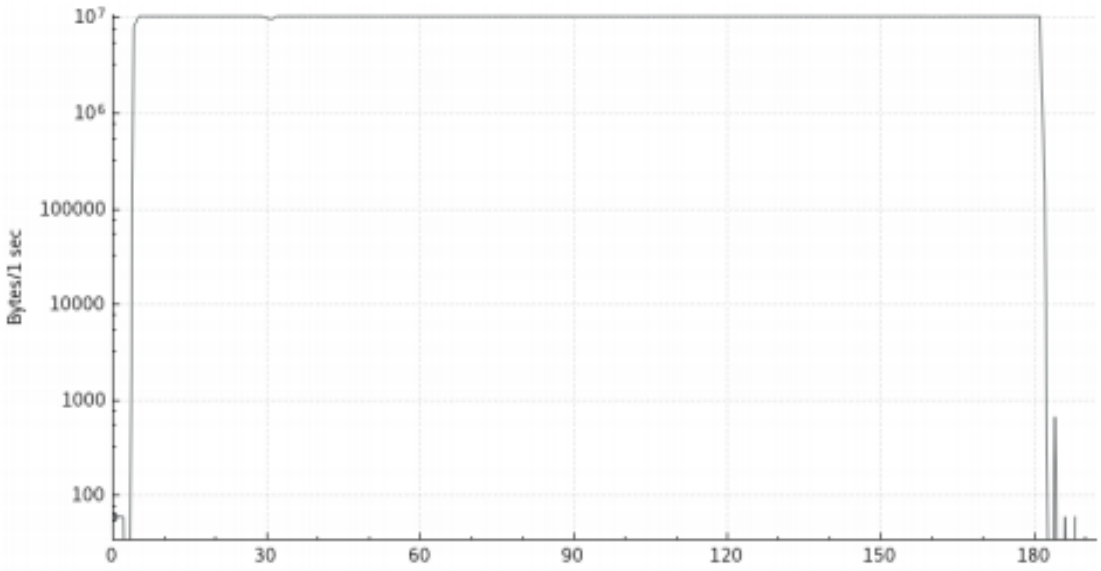
FONTE: Jorge (2017)

2.3.2 Ataque à Disponibilidade

Com a finalidade de impedir a utilização dos sistemas pelos usuários válidos, Regueira (2015) apresenta a técnica *INVITE FLOOD*, onde é feita uma inundação de pacotes de requisições de chamadas para o servidor, esgotando os recursos de rede e processamento. Todas as distribuições testadas estavam vulneráveis a esta técnica, que pode ser acionada com o seguinte comando: ***"inviteflood eth0 203 192.168.11.X 192.168.11.X 1000000"***, onde 203 é um ramal válido do servidor de final X e 10000000 é o número de requisições.

Destaca-se que a técnica de inundação de rede pode-se valer de outras ferramentas que não são específicas para VoIP, tais como: ***"atk6-flood-router6 eth0"***, que inunda a rede local com *router advertisements,* conforme mostra o gráfico de consumo de largura de banda da Figura 14.

Figura 14- Saída do *atk6-flood-router6*



FONTE: Jorge (2017)

2.3.3 Ataque à Integridade

Para manipular as sessões ou as mensagens, é necessária a descoberta da senha de acesso de um ramal válido, por meio dos passos anteriores. Diante dessas informações, Regueira (2015) realizou a técnica de *Registration Hijacking,* ou seja, realizou uma ligação se fazendo passar por uma extensão válida através do *framework Metasploit* com o módulo auxiliar *VIPROY..* A extensão 201 aceitou a ligação como mostra a Figura 15.

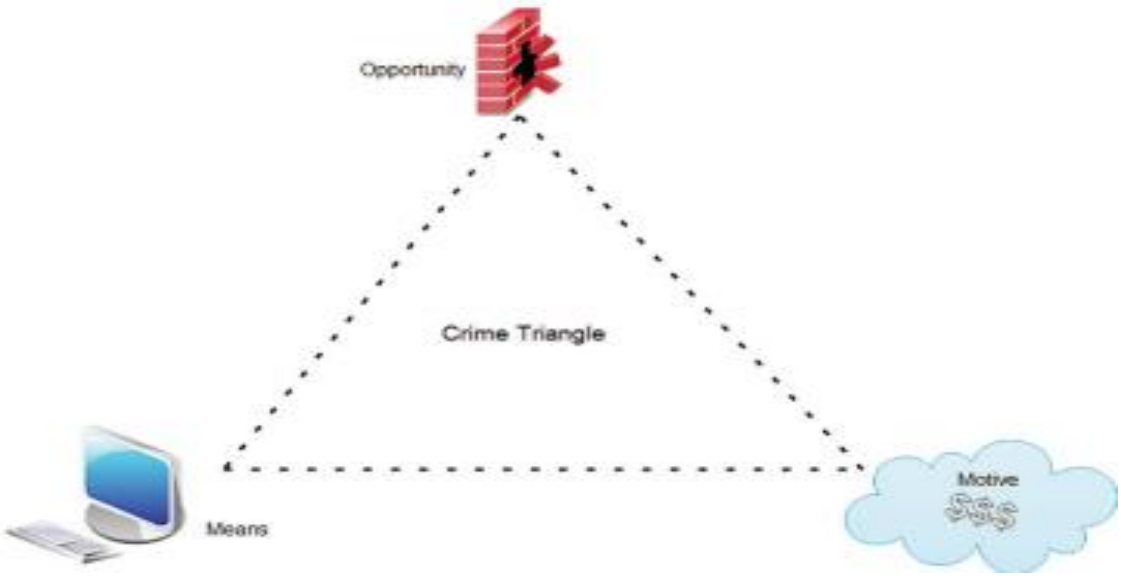
Figura 15- Saída do *Viproy*

FONTE: Regueira (2015)

2.4 SEGURANÇA VOIP

Algumas preocupações adicionais devem ser consideradas nas implementações VoIP, que segundo Bates (2015) há pouco esforço colocado na segurança do sistema. Muitas vezes a pessoa responsável pelo sistema VoIP não é tecnicamente capacitada para os novos desafios que a rede IP oferece. Como pode ser visto na Figura 16, para o crime ocorrer, há a necessidade da ocorrência de três componentes: meios, motivo e oportunidade, que formam o Triângulo do Crime. Se faltar qualquer um dos três componentes, então um crime não será confirmado.

Figura 16- Triângulo do crime



FONTE: Bates (2015)

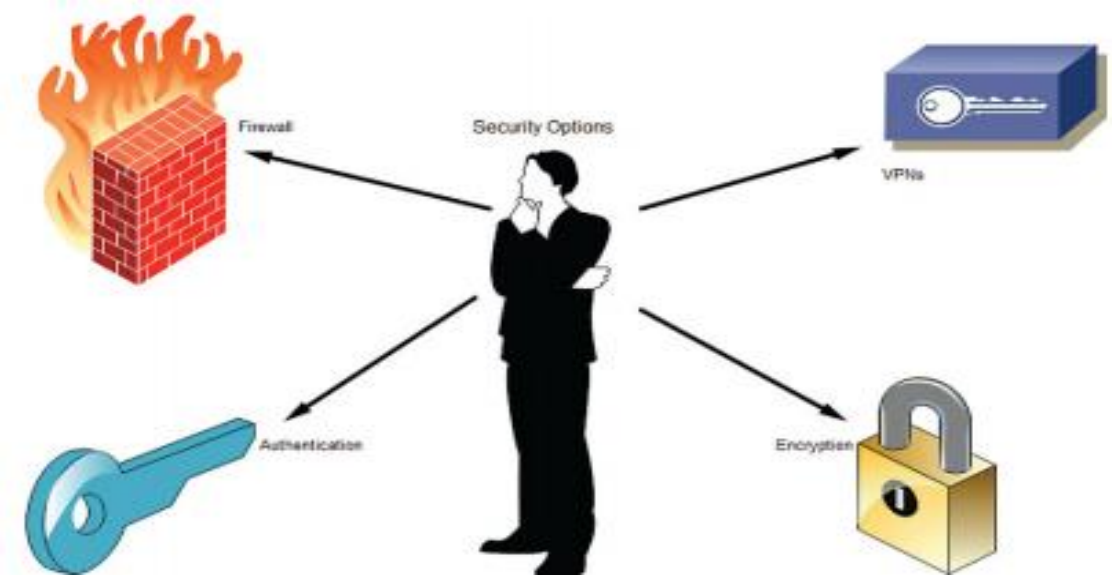
a) Se tiver um meio e uma oportunidade, mas não se sabe o motivo, então não deve haver nenhum incentivo para um atacante de tentativa de violação do sistema VoIP.

b) Se tiver os meios e o motivo, mas não a oportunidade, então, não deve haver nenhum vetor de ataque para o sucesso na violação sistema VoIP.

c) Se tiver a oportunidade e o motivo, mas não os meios, então, a ameação não se concretizará, e, assim, o crime não será cometido.

Avaliar as três hipóteses acima ajuda a entender que impedindo a criação do triângulo pode-se garantir a segurança do sistema VoIP. O desafio consiste em manter um ou mais componentes da pirâmide indisponíveis ao atacante. Bates (2015) apresenta na Figura 17 uma lista de possibilidades para ajudar a proteger o sistema VoIP.

Figura 17- Opções de Segurança VoIP



FONTE: Bates (2015)

2.4.1 Firewalls

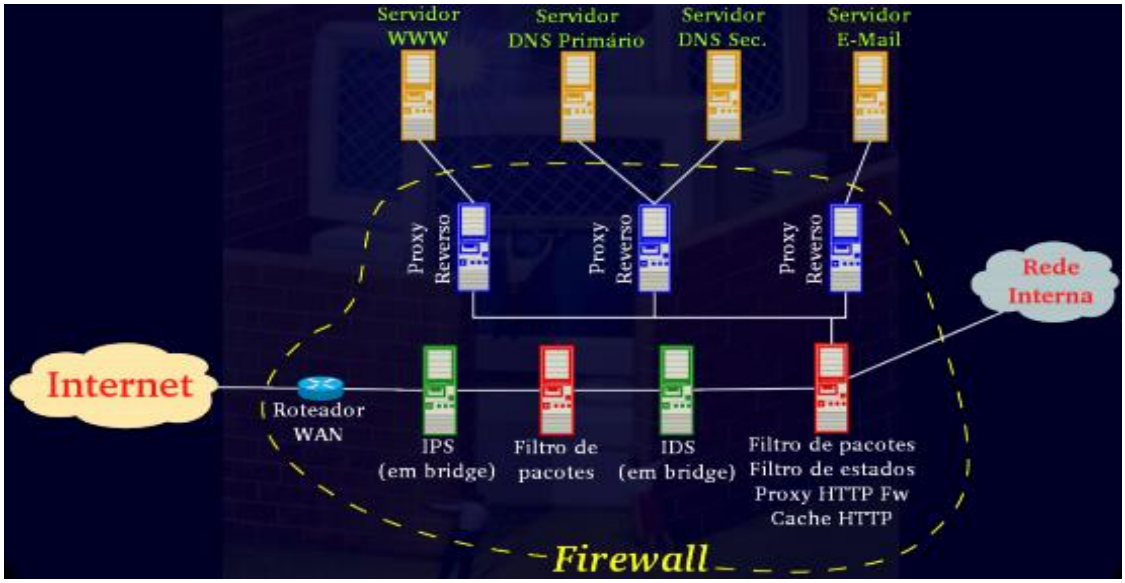
Esses componentes normalmente são os primeiros alvos tanto de redes internas quanto externas. O reconhecimento do tráfego VoIP pelos Firewalls são um requisito para que eles não impeçam a passagem desses pacotes. Isto também inclui a necessidade de realizar NAT de redes privadas. A Sessão Transversal de UDP sobre NAT, chamada de STUN, permite o uso dos protocolos VoIP com toda a combinação de NAT e Firewalls.

De acordo com Mota (2017), Firewall é um Sistema. É todo o esforço físico e

lógico voltado para a segurança da rede. Os sistemas de firewall podem ser compostos por diversos elementos tais como: filtros de frames, filtros de pacotes, filtros de estados, proxies, IDS, IPD, etc. A segurança em profundidade é fundamental em sistemas de firewall como a teoria da cebola. Apenas uma máquina não pode ser considerada um sistema de firewall.

A Figura 18 mostra um exemplo de um sistema de firewall com alguns elementos que podem compor a solução, não se limitando a estes.

Figura 18- Sistema de Firewall



FONTE: Mota (2017)

Outra importante decisão a ser tomada é quanto à utilização de criptografia com firewalls, pois ela CEGA o sistema de firewall. Uma solução descrita por Mota (2017) é utilizar proxies reversos para fechar o túnel criptografado, e elementos de firewall entre os reversos e os servidores efetivos, neste caso utilizar um *proxy* SIP.

2.4.2 Autenticação

É imperativo que os usuários que acessam os serviços de VoIP são quem eles dizem ser. A autenticação do aparelho (ou *softphone*) e o usuário real é uma forma sólida de segurança da rede, chamado de duplo fator. Infelizmente, nem todos os procedimentos de autenticação são os mesmos. O método preferido é a autenticação baseada em porta para o aparelho e autenticação baseada em identidade para o indivíduo. Rede baseada em identidade pode ser construída com

Certificados e *Public Key Infrastructure* (PKI). Muitos dos fabricantes de sistema VoIP, inclusive *endpoints,* estão disponibilizando a instalação de certificados em seus dispositivos.

Conforme Bates (2015), quando surge o tema de autenticação, é natural falar do 802.1X, que é o padrão de autenticação usando um formulário do *Extensible Autentication Protocol* (EAP). 802.1X são usados para liberar ou negar o acesso à rede. Além disso, é um protocolo de segurança que também funciona com redes sem fio 802.11 (a/b/g/b/ac). Uma empresa com maturidade em segurança não utiliza solução de rede sem fio sem alguma forma de autenticação baseada no protocolo 802.1X EAP.

Como mostra a Figura 18, as principais partes do 802.1 X na autenticação são as seguintes:

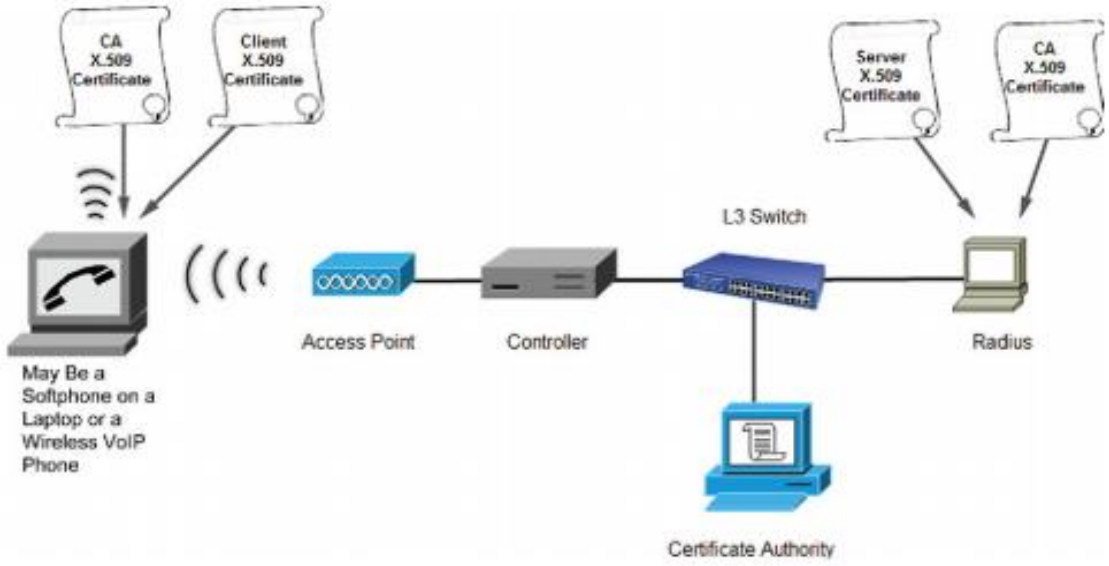
a) **Um suplicante:** um usuário final, que quer ser autenticado. Este é geralmente um computador sem fio, *tablet*, smartphone ou telefone VoIP, podendo ser com ou sem fio.

b) **Um autenticador:** um ponto de acesso sem fio ou um *switch* de camada 2/3. O autenticador atua como um intermediário para o dispositivo do usuário final, é o primeiro nível de conexão do suplicante.

c) **Um servidor de autenticação:** o dispositivo de autenticação normalmente é um Servidor de autenticação remoto (Radius Server) mas pode se integrar com AD Server, LDAP Server, etc). O Radius que verifica quem é o usuário e se tem o acesso liberado ou negado dependendo do sucesso na troca de credenciais (username a password ou certificados digitais).

O EAP oferece vários métodos de autenticação: EAP-MD5, LEAP, EAP-TTLS, PEAP e o EAP-LTS, que utiliza uma PKI, conforme mostra a Figura 19, onde dois certificados são utilizados, um certificado de servidor e um de cliente, para a autenticar o suplicante (cliente), e o servidor de autenticação. Neste caso é realizada uma autenticação mútua.

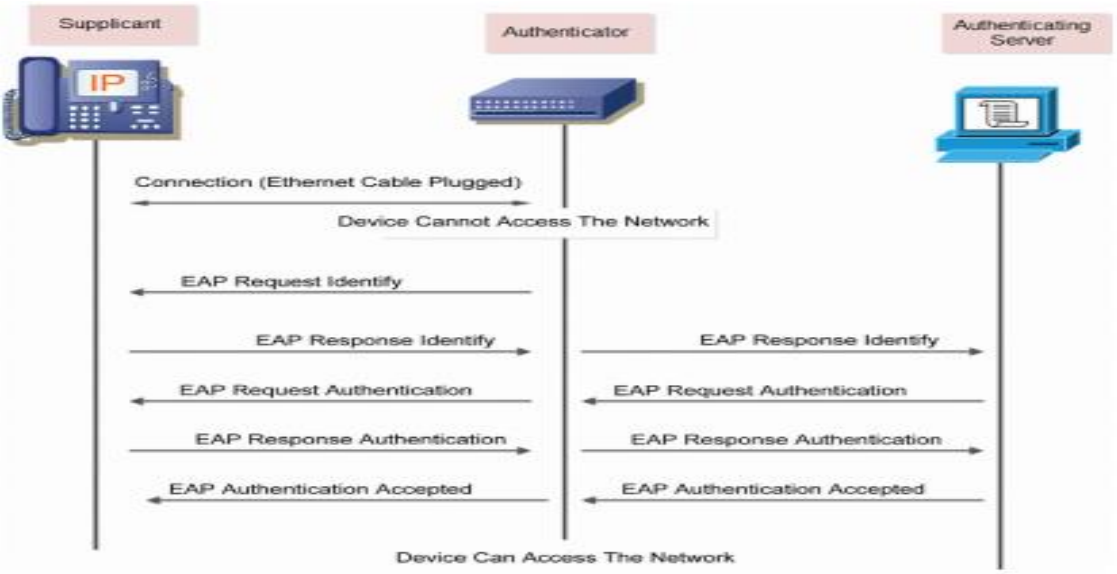
Figura 19- Autenticação EAP-TLS



FONTE: Bates (2015)

Neste processo, qualquer porta livre em um switch Ethernet estará bloqueada até que o processo de autenticação 802.1X esteja completo. Quando um dispositivo se conecta e é detectado, a porta do switch é definida como “não autorizado” e somente o tráfego de autenticação é liberado. Somente após a conclusão do processo de autenticação com sucesso que a porta é liberada ao dispositivo para acesso à rede (Figura 20).

Figura 20- Processo 802.1X



FONTE: Bates (2015)

2.4.3 Criptografia

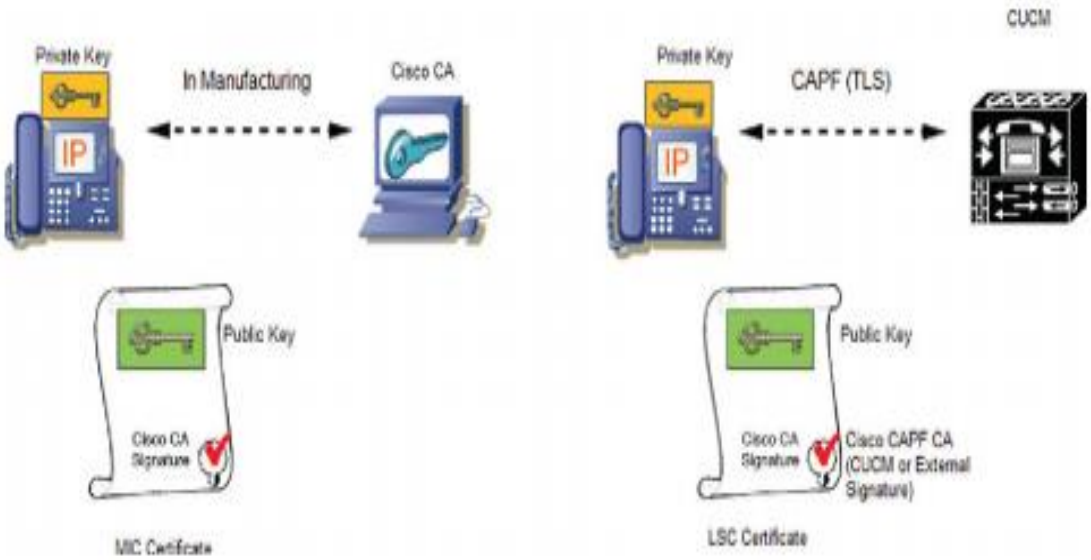
Independentemente da sobrecarga, que pode ser significativa, habilitar protocolos seguros para os sistemas VoIP são uma obrigação. Para evitar escutas, manipulação e inserção bem como repetição, os protocolos seguros como o SRTP, SIPS, e outros sistemas criptografados são necessários. De acordo com Stallings (2015), há quatro características desejáveis que podem ser fornecidas por várias funções criptográficas: Confidencialidade, Integridade, Autenticação e Não-repúdio.

Como já visto nas discussões anteriores, é possível o tráfego VoIP ser capturado e manipulado, assim, mudar totalmente os significados em uma conversa, quebrando sua integridade. Um meio de autenticar o chamador e a mensagem enviada é usar uma criptografia de chave pública (PKI).

Se for realizada uma combinação de verificação de integridade e autenticação, dá-se o que pode-se considerar não-repúdio. Um combinado de chave pública de criptografia e *hash* unidirecional podem ser usados para gerar uma assinatura digital. A assinatura digital pode unir uma parte chamadora com as informações de voz que garantirão quase que estamos falando com o partido a quem achamos que estamos falando e que a voz não foi manipulada.

Stallings (2015) descreve os tipos e modos de operação dos algoritmos criptográficos, diferenciados pela chave utilizada para criptografar e decriptografar o texto em claro, sendo simétricos caso seja utilizada a mesma chave nos dois processos, e assimétricos quando as chaves são diferentes, porém, geradas no mesmo instante. Na criptografia de chave simétrica, os atores envolvidos na comunicação precisam manter uma chave compartilhada para os processos de criptografia e decriptografia, enquanto que na criptografia de chave assimétrica, uma das chaves é utilizada para a criptografia (chave pública) e a outra para a decriptografia (chave privada). Alguns exemplos de algoritmos de chave simétrica incluem o 3DES, IDEIA, RC4 e AES. Enquanto os de chave assimétrica incluem o ELGamal, Curvas Elípticas e RSA.

Figura 21- Uso de Certificados em telefones



FONTE: Bates (2015)

A Figura 21 mostra um exemplo do uso de criptografia no sistema VoIP, onde é utilizada uma forma mais fácil de gerenciar as chaves, são utilizados Certificados Digitais PKI x.509 emitidos por uma Autoridade Certificadora, que valida as Chaves Públicas dos telefones IP, dessa maneira, as chaves privadas não necessitam ser trocadas e expostas à captura.

Conforme Bates (2015), quase todos os fabricantes reconhecem que um sistema baseado no certificado é necessário nos telefones IP, PBXs e equipamento periférico. Muitos dos fabricantes oferecem suporte a clientes VPN SSL, IPSec clientes e clientes TLS em uma mistura e combinam conforme necessário. Isto permite maior suporte para os dispositivos de usuário final e dá ao usuário muito mais flexibilidade na definição das estratégias de segurança para sua organização.

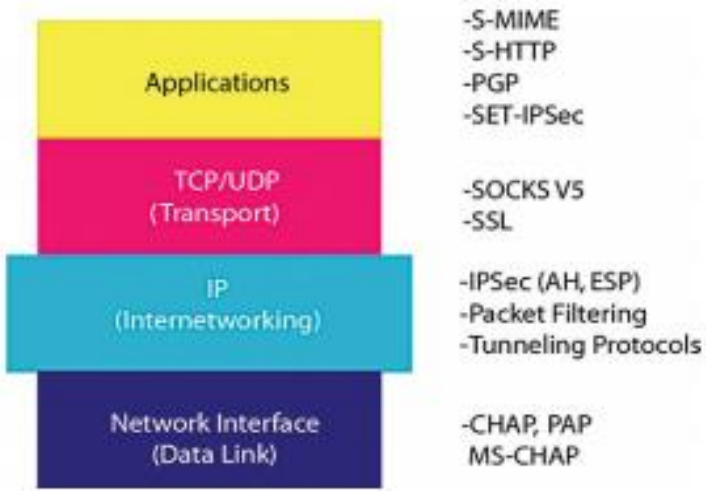
2.4.4 *Virtual Private Network* (VPN)

A VPN também é uma boa medida quando existem conexões remotas, tanto entre PBX-IP quanto entre estes e os *endpoints,* sendo utilizados por funcionários remotos, *Home Offices,* etc. A VPN permite a mistura e combinação de criptografia, autenticação e os dispositivos de hardware necessário para proteger o VoIP, bem como dados atravessando a Internet ou redes não confiáveis.

A Figura 22 mostra as várias soluções de VPN que podem ser empregadas

de acordo com a necessidade de segurança da solução. Para este estudo de caso, o foco fica no SSL, um dos protocolos de encapsulamento mais comumente usados por ser robusto de de múltiplos propósitos. Trabalhando na camada 4 (Transporte), o protocolo SSL foi renomeado como para *Transport Layer Security* (TLS). Uma VPN SSL é um dos três tipos de VPN mais usados, juntamente com o PPTP e IPSec.

Figura 22- Soluções VPN



FONTE: Bates (2015)

O que diferencia VPNs SSL de outras soluções é que SSL pode ser usada com o navegador web padrão, sem a necessidade de clientes instalados nos usuários. Isso facilita a utilização com aplicativos do tipo *softphones,* e, também, já estão vindo habilitados em vários modelos de telefones IP.

A VPN, especialmente a SSL pode fornecer:

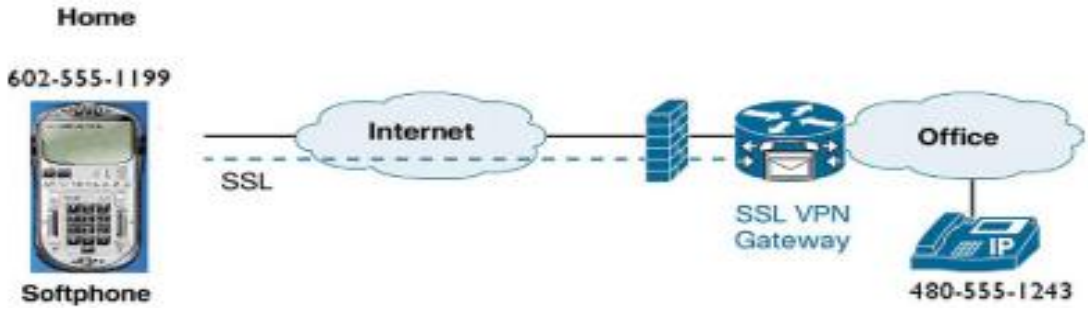
a) Criptografia que irá oferecer comunicações seguras. Normalmente uma VPN irá usar criptografia de 128 ou 256 bits usando AES.

b) Autenticação para que os sistemas só permitam que usuários se conectem e usem a rede uma vez autorizados.

c) Túneis que escondem os dados, criptografam os dados, autenticam o usuário e esconder o endereço das partes.

A figura 23 mostra um exemplo de um *softphone* em casa sendo usado para chamar outro telefone IP do escritório por meio da Internet usando a VPN SSL. Este cenário é um bom exemplo do uso da telefonia em locais públicos, tais como: aeroportos, *ciber* café, shoppings, locais que ofereçam internet Wi-Fi abertas. Finalmente um dos pontos de maior interesse da segurança, é que as portas específicas dos serviços VoIP podem permanecer bloqueadas no *Firewall*, estando no estado *accept* apenas para a Vlan de Voz.

Figura 23- VPN SSL



FONTE: Regueira (2015)

3 TELEFONE SEGURO: ESTUDO DE CASO ADAPTADO

Entende-se por Telefone Seguro um sistema que possibilita as comunicações telefônicas criptografadas, que oferecem segurança no tráfego de voz e dados, e preservem os princípios da segurança da informação e comunicações. De acordo com a ABIN, existe uma solução de criptografia desenvolvida pelo Centro de Pesquisa em Criptografia (CEPESC), órgão daquela agência, que acoplada a um telefone fixo viabiliza o Telefone Seguro Governamental (TSG). Tal solução é composta por uma caixa do tipo "***black-box***" com duas interfaces de rede, sendo uma para conexão ao telefone IP e outra para conexão à rede local.

De acordo com o Decreto 7.845, o Algoritmo de Estado é a função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal. Diz ainda que a cifração e a decifração de informação classificada em qualquer grau de sigilo deverão utilizar recurso criptográfico baseado em algoritmo de Estado.

Durante o laboratório de ataque realizado nesta observação, não foram utilizados algoritmos de estado tendo em vista a restrição de acesso e divulgação de informação e material classificado, entretanto, todas as camadas de segurança reconhecidas foram recriadas.

Neste sentido, a informação classificada é toda a informação sigilosa em poder dos órgãos e entidades públicas, classificada como ultrassecreta, secreta ou reservada, que deve ser armazenada ou tramitada utilizando-se os tamanhos mínimos de chaves de acordo com os quadros 1 e 2.

Quadro 1- Criptografia assimétrica

Nível de Segurança da Informação	RSA/LD	Curvas Elípticas
Reservado	2048	224
Secreto	3248	256
Ultrassecreto	Não recomendado	Não recomendado

FONTE: GSI (2013)

Quadro 2- Criptografia simétrica

Classificação	Algoritmo	
	Chave	Bloco
Reservado	192	128
Secreto	256	128
Ultrassecreto	Não recomendado	

FONTE: GSI (2013)

3.1 ARQUITETURA VOIP IMPLEMENTADA

A arquitetura implementada para a realização do laboratório de ataque ao telefone seguro, segundo o estudo de caso adaptado, segue a seguinte descrição de equipamentos utilizados:

Quadro 3- Equipamentos e Softwares

Hardware/ Software	Quantidade	Equipamentos	Modelo
Hardware	2	Notebook	Core I5, 04 GB RAM, HD 200 GB
	3	Videofone IP	GXV-3275 Grandstream
	1	Switch Gerenciável	D-Link DSG-3100-24SFP
	1	Access Point	Ruckus R600
Software	1	PBX-IP	Issabel 4.0 PBX 64-bit
	1	Kali Linux	Kali Linux 2012.2 64-bit;
	2	PFSense	PFSense 2.4.1 64-bit

FONTE: Do autor

3.1.2 Descrição dos Equipamentos utilizados

O Notebook foi utilizado para levantar as 03 (três) máquinas virtuais que fazem parte deste laboratório, sendo utilizado para isto o *Hypervisor* do Tipo 2 *Vmware Workstation 12 Player.*

Como forma de replicar a primeira camada de segurança de redes implementada para o serviço, foi utilizado o Switch do quadro 3. Como forma de evitar ataques como os de ***ARP Poisoning*** , foi separando o tráfego de voz e de dados em Vlans segregadas.

Os videofones IP foram utilizados por se tratar de equipamentos simulares aos utilizados no projeto, possui um **SO Android versão 4.2.2,** sendo assim, possuem capacidade de oferecer recursos tais como troca de mensagens, acesso a navegadores, e instalação de aplicativos.

3.1.2 Descrição dos Aplicativos utilizados

A solução foi implementada com a Plataforma IP-PBX **ASTERISK**, um software livre de PBX completo. Ele roda em Sistema Operacional Linux e provê todas as funcionalidades esperadas de um PABX. Para o laboratório foi utilizada a distribuição **ISSABEL 4.0 64-bit**, uma solução open source completa para comunicações unificadas, implementando o Asterisk 11.25.0. Com forma de evitar ataques como os de ***Eavesdropping****,* foi habilitada a biblioteca libSRTP no Asterisk para prover criptografia AES 256 mandatória em todas as chamadas SIP.

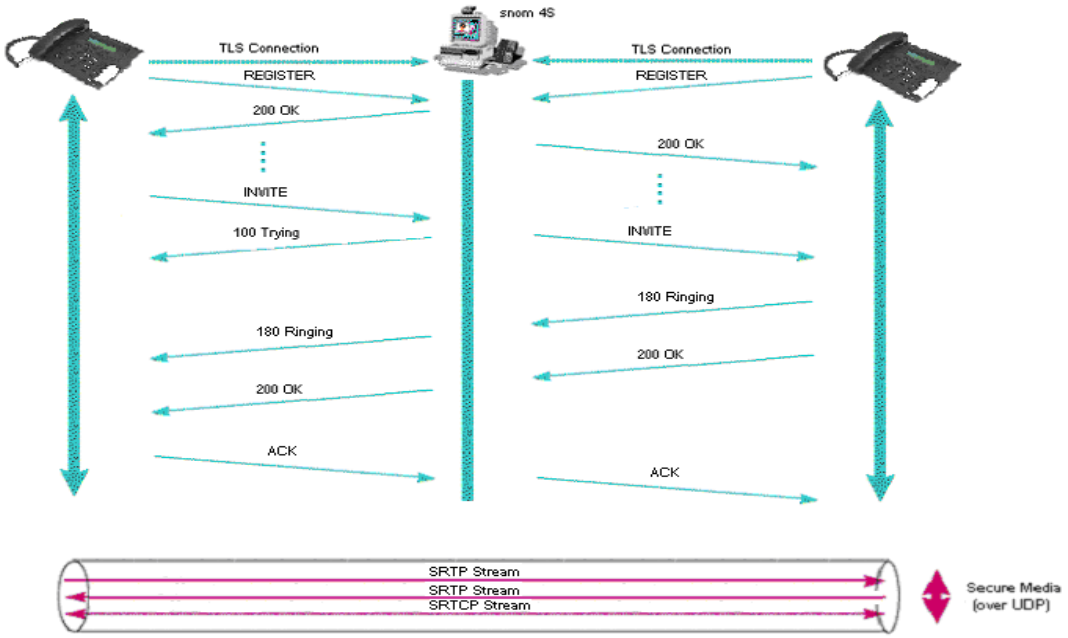
Para evitar ataques como os de ***Registration Hijacking*****,** foi criada uma Autoridade Certificadora para a emitir Certificados Digitais padrão X.509 [1] para a autenticação de duplo fator dos telefones IP. Para o laboratório foi utilizada a distribuição **PFSense 2.4.1 64-bit,** uma solução *open source* completa para segurança de redes de computadores.

O Protocolo de sinalização SIP, chamado SIPs quando implementado com Segurança na Camada de Transporte (TLS), sendo responsável pela inicialização das sessões dos ramais e Criptografia sobre o Protocolo RTP, chamado de SRTP responsável pela transmissão dos pacotes de voz e vídeo. O objetivo foi prover confidencialidade nas ligações e autenticidade dos clientes, conforme é apresentada na representação de uma chamada segura na figura 24.

---

1 Padrão para infraestrutura de chaves públicas, utilizado na ICP-Brasil.

Figura 24- VoIP Criptografado

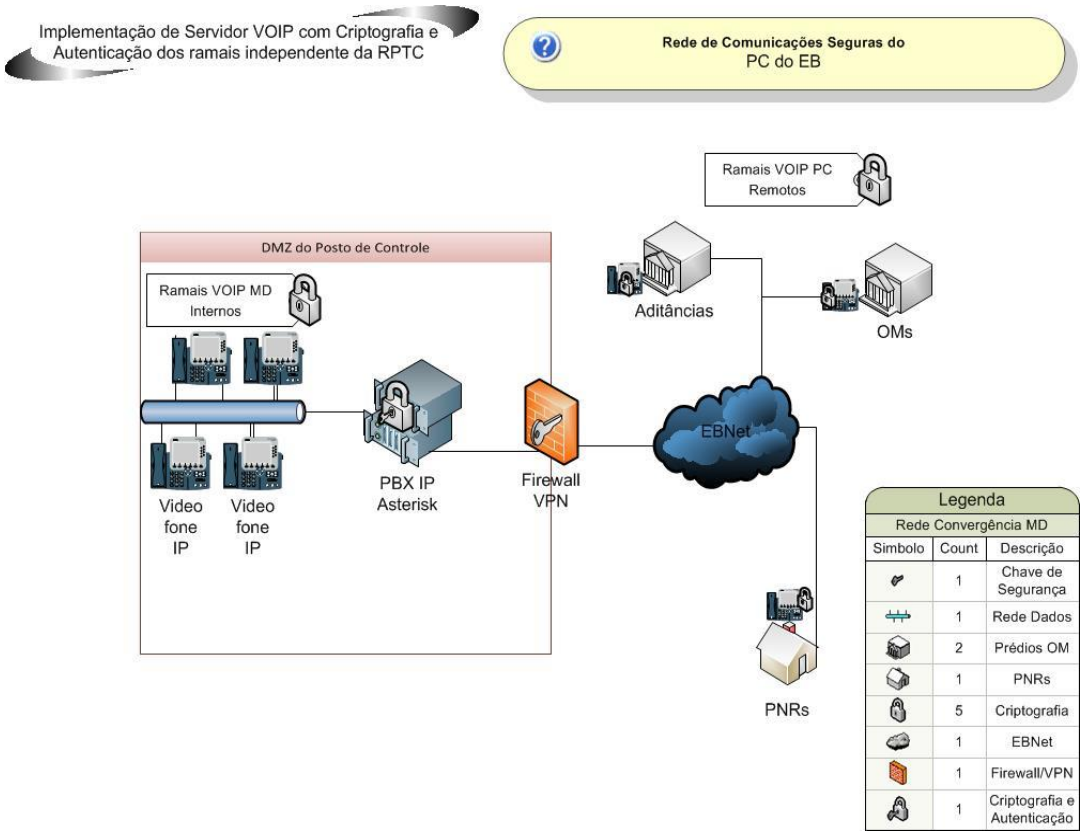


FONTE: Bates (2015)

Com a finalidade de restringir as ameaças ao serviço implementado, os equipamentos telefônicos IP do projeto possuem um cliente VPN [2]embarcado, de forma que o servidor Asterisk não esteja disponível em redes não confiáveis, mas apenas aos clientes conectados com sucesso no servidor VPN, conforme exemplo da figura 25.

2 Rede Privada Virtual

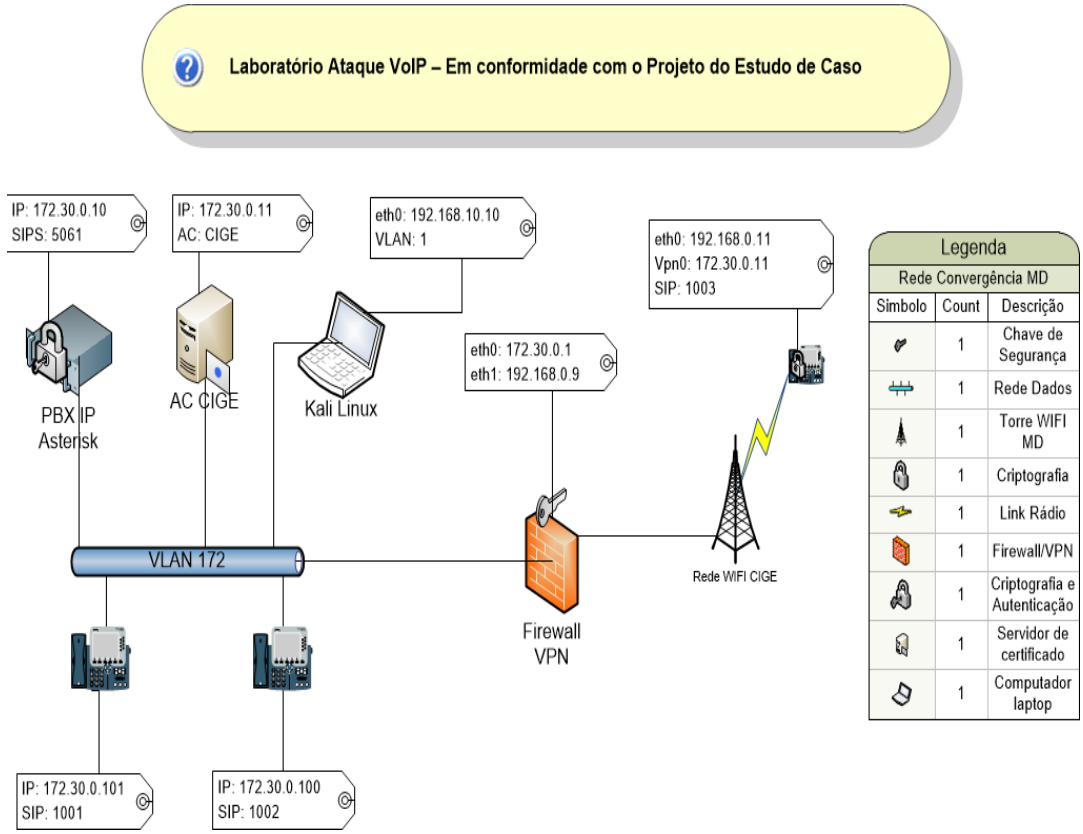
Figura 25- VoIP com VPN



FONTE: Do autor

Completando o laboratório, foi instalado o Kali Linux 2012.2 como sendo a máquina do atacante que já está presente na rede da organização, esta distribuição disponibiliza diversas ferramentas úteis para testes de segurança e de penetração em redes e serviços. O Diagrama do laboratório pode ser mais bem entendido na figura 26, onde se pode notar a VLAN 172 segregada da rede de dados, apenas para trêfego de voz. A máquina do atacante, Kali Linux, conseguiu acesso à VLAN 1, default da rede de dados, onde precisará utilizar ferramentas como VoIP Hopper para descobrir a rede correta. Este acesso não é escopo deste estudo de caso. Existe uma máquina (AC CIGE) responsável pela emissão dos Certificados que autenticam os ramais na rede VoIP. O iPBX Asterisk está implementado com autenticação TLS no protocolo SIP (SIPS) e com Criptografia no protocolo RTP (SRTP), tudo de forma mandatória para garantir maior segurança. O Firewall/VPN é a única porta de entrada de dispositivos de fora da rede, sendo necessário o estabelecimento de uma conexão *OpenVPN* entre o telefone e o Firewall para que o equipamento receba um IP da VLAN 172.

Figura 26- Diagrama do laboratório



FONTE: Do autor

3.2 ATAQUES CONTRA OS PRINCÍPIOS DA DICA

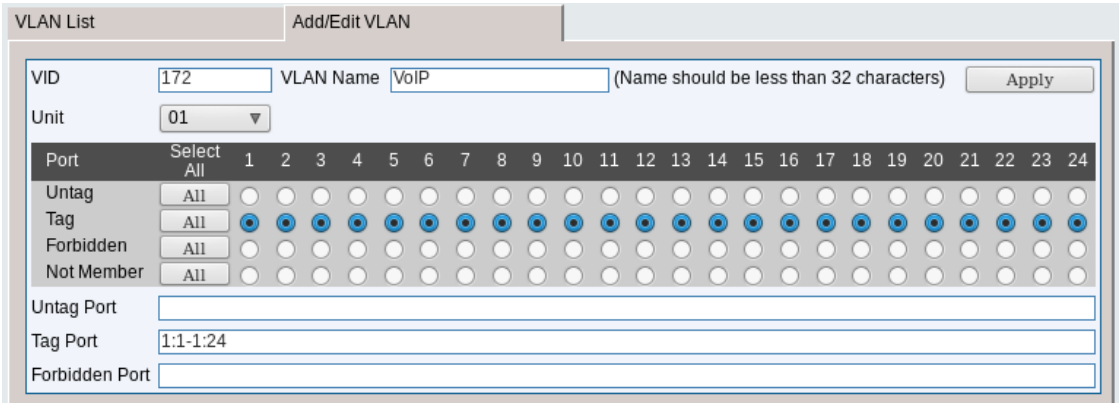
Seguindo a metodologia de referência, serão reproduzidos os ataques explorados por Regueira (2015) e apresentados na seção 2.3 deste trabalho. Caso alguma ferramenta não apresente resultados devido à segurança implementada, outra ferramenta será apresentada com a finalidade de aplicar a mesma técnica de ataque. Este laboratório foi conduzido no CIGE, no período de outubro e novembro de 2017, sendo os resultados nas subseções abaixo.

3.2.1 Confidencialidade: Escuta do Meio (*Eavesdropping)*

Uma vez que o atacante é *insider* ou já comprometeu alguma máquina da rede alvo e ganhou o acesso, é necessário procurar por equipamentos de telefonia IP na rede. Uma rede bem estruturada possui o tráfego VoIP segregado do tráfego de dados, como forma de garantir a qualidade do serviço (QoS) e mesmo a confidencialidade.

Conforme é apresentado no diagrama do laboratório e na figura 27, a Vlan de Voz está taggeada com o ID 172, com range de endereços 172.30.0.0/24 e o atacante tem uma máquina na Vlan *default* do *switch*, com range de endereços 192.168.10.0/24

Figura 27- Confoguração do *Switch*



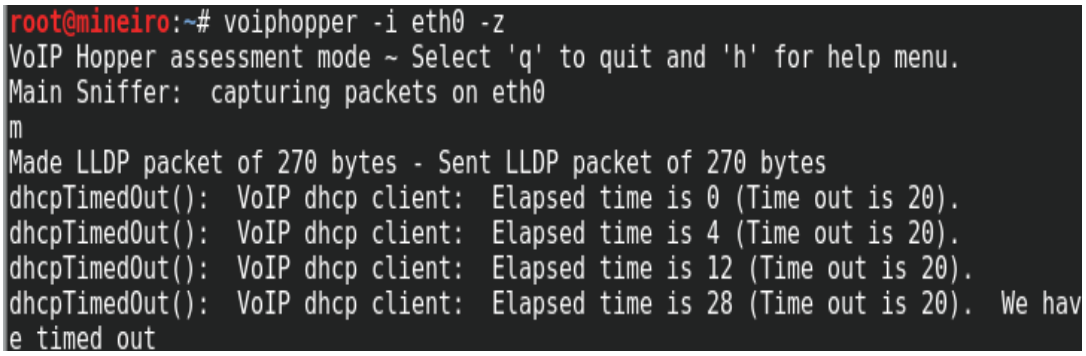
FONTE: Do autor

A execução do comando ***svmap*** apresentado na figura 9 não teve resultados, assim, o atacante precisa ter a certeza que está na Vlan correta, para isso, existe a técnica de *Hopper* VoIP, usada para entrar na Vlan de voz, comportando-se como

um telefone IP. A ferramenta ***voiphopper***, que implementa a técnica, possui recursos de DHCP *Client*, CDP/LLDP *Generator, MAC Address Spoofing* e VLAN *hopping*.

A figura 28 mostra o uso da ferramenta para escutar o tráfego dos Protocolos *Link-Layer Discovery* (LLDP) e criar automaticamente a interface de rede na Vlan 172. Este protocolo é configurado no *Switch* e no Servidor DHCP para a configuração automática de Vlan de voz. A partir desse ponto, a máquina do atacante já está dentro da Vlan de voz 172, possuindo acesso direto aos equipamentos.

Figura 28- Uso do Voiphopper



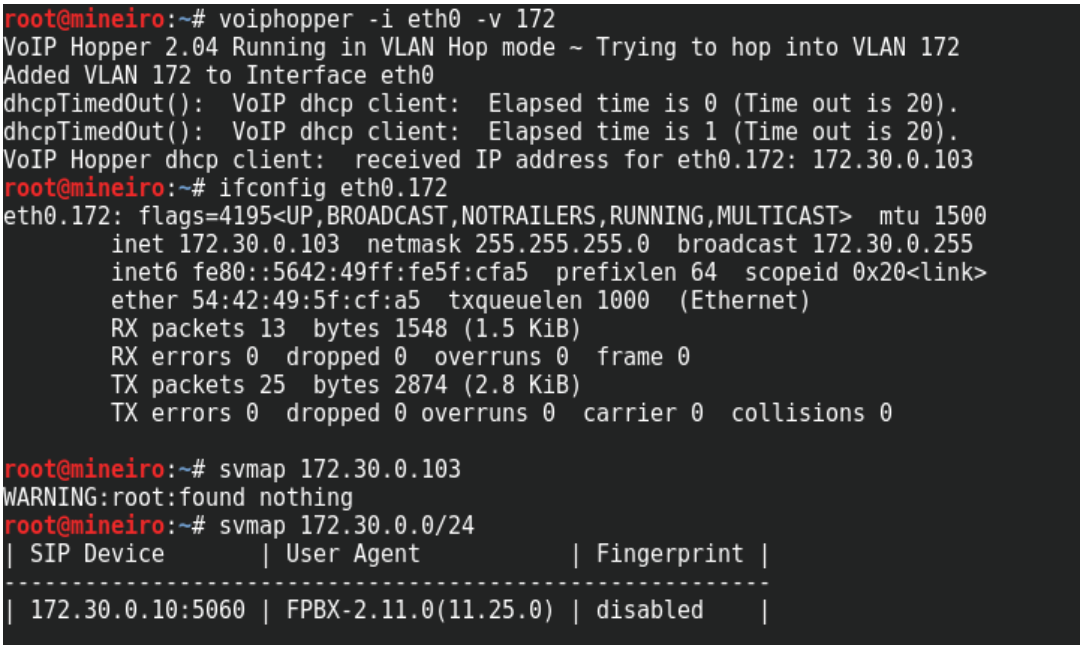
FONTE: Do autor

Caso a rede não possua esta implementação, será necessária uma ação de Engenharia Social para descobrir TAG-ID da Vlan de voz, e após receber as configurações de rede, começar o scanner para descobrir os dispositivos SIP, conforme pode ser visto na figura 29.

O comando apresentado com *voiphopper* adiciona uma interface virtual na máquina com o ID passado no parâmetro -v, ele já possui um cliente DHCP que faz uma requisição para receber as configurações da rede, como pode ser visto na saída do comando ***ifconfig eth0.172.***

A ferramenta de *scan svmap* apresentou apenas um dispositivo SIP com o UA FPBX-2.11.0, que é o Servidor Asterisk 11.25.0, pois os telefones não estão na configuração padrão para a autenticação SIP na porta 5060 do protocolo UDP. Dessa forma, foi necessário executar o *Nmap* com as opções de scannear as portas TCP abertas e trazer a versão dos serviços instalados: "***nmap -sS -sV 172.30.0.0/24***", conforme pode ser visto o resultado na figura 30.

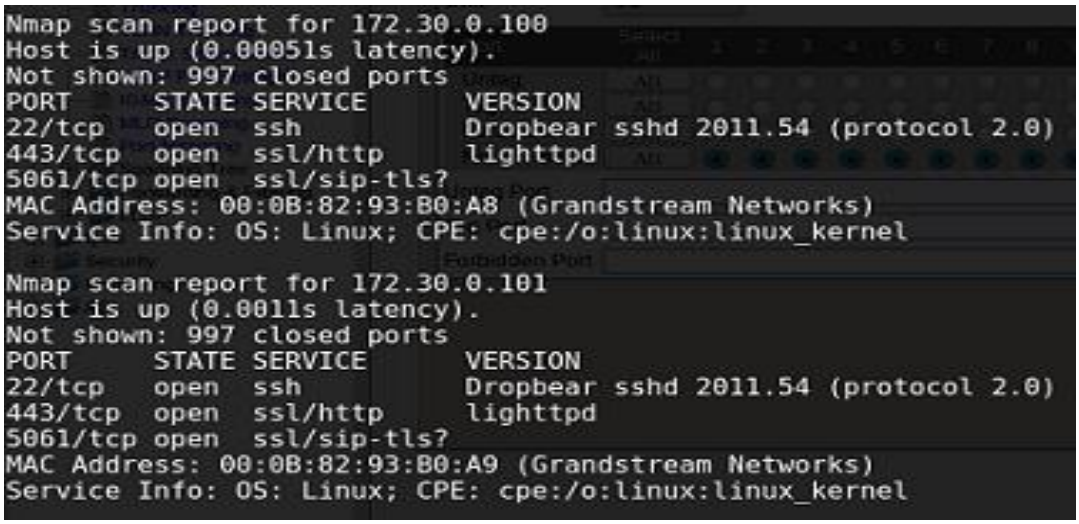
Figura 29- Voiphopper e Svmap



FONTE: Do autor

O resultado mostra a porta TCP 5061 aberta com o serviço SIP sob TLS, e o MAC *Address* apresenta como fabricante a *Grandstream Networks*, uma companhia especializada em soluções VoIP. Finalizada a fase inicial de escaneamento da rede em busca dos dispositivos SIP, foram realizadas as tentativas de enumerar as extensões, conforme apresentado na subseção 2.3.1 deste trabalho, porém, todas foram fracassadas tendo em vista a implementação da camada adicional de segurança TLS antes da autenticação SIP dos clientes.

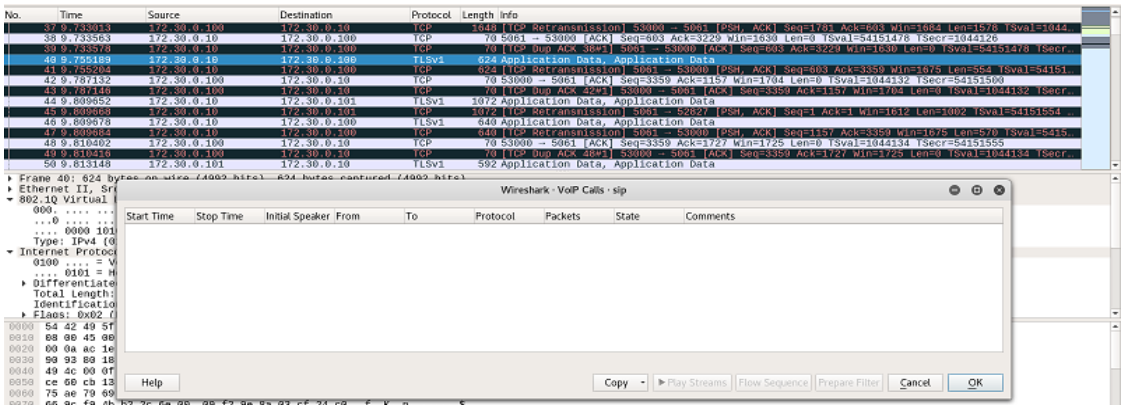
Figura 30- Nmap na rede VoIP



FONTE: Do autor

Outra técnica que pode ser utilizada para enumerar as extensões é a de *spoofing* da rede VoIP, fazendo com que o atacante se torne MiTM, porém, não foi possível recuperar as chamadas VoIP que poderiam identificar as extensões, e mesmo as conversas. Para o resultado mostrado na figura 31, foram utilizadas as ferramentas ***arpspoof*** com os endereços do servidor e dos clientes, o ***tcpdump*** para capturar e salvar todo o tráfego em um arquivo, que foi lido pelo ***wireshark*.** Para o teste foram realizadas duas chamadas completas entre cada extensão.

Figura 31- Tráfego SIP com TLS



FONTE: Do autor

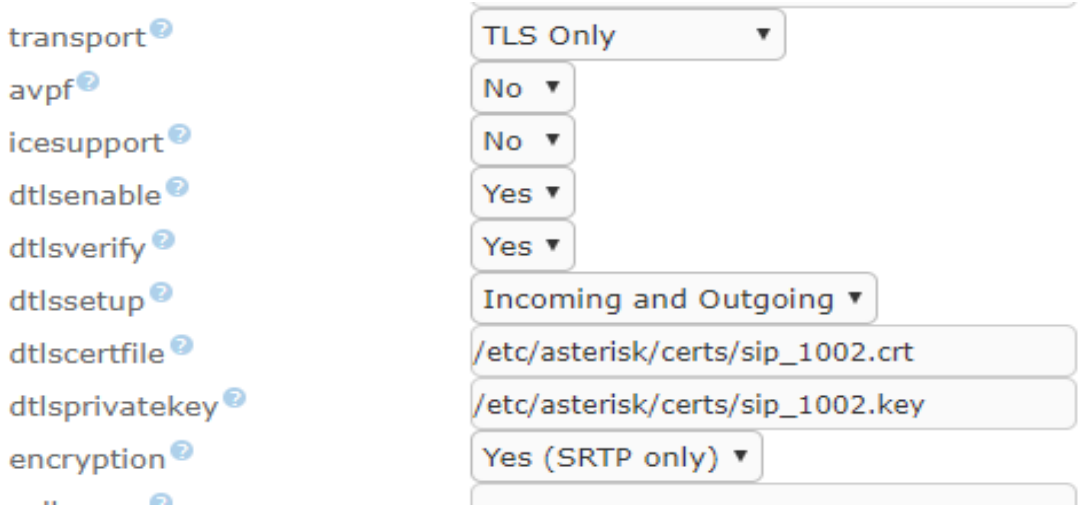
Todos os ataques contra a Confidencialidade foram frustrados tendo em vista a utilização do protocolo TLS na camada de transporte para encapsular o protocolo SIP, cabe destacar que os clientes possuem uma autenticação realizada por meio de certificados digitais X.509 emitidos pela autoridade certificadora com algoritmo RSA 4096 bits, e não apenas senhas, inviabilizando a técnicas de quebra de senhas por Força bruta ou Dicionário, conforme pode ser visto na figura 32.

Figura 32- Autenticação SIP X.509 no telefone

FONTE: Do autor

A figura 33 mostra a configuração para requerer autenticação via certificado do lado do servidor para a extensão criada, onde é mandatório para inicar as trocas de mensagens SDP de controle do protocolo, note também que o tráfego de voz RTP, que ocorre após o estabelecimento da chamada também é criptografado de forma mandatória com algoritmo **AES 256 bits**, que irá trafegar encapsulado pelo TLS, ou seja, criptografia dentro de criptografia.

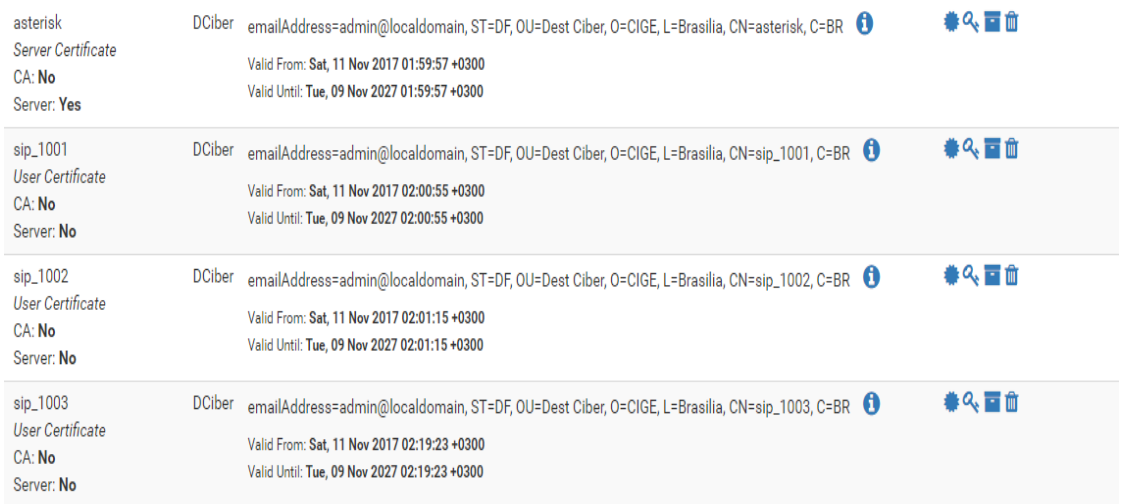
Figura 33- Autenticação SIP X.509 no servidor



FONTE: Do autor

Essa cadeia de confiança foi criada no ***PFSense*** conforme a figura 34, onde existe uma AC-Raíz DCiber, que emite os certificados de serviço, como do Asterisk, VPN, e de usuário, como as extensões SIP.

Figura 34- Autoridade Certificadora DCiber



FONTE: Do autor

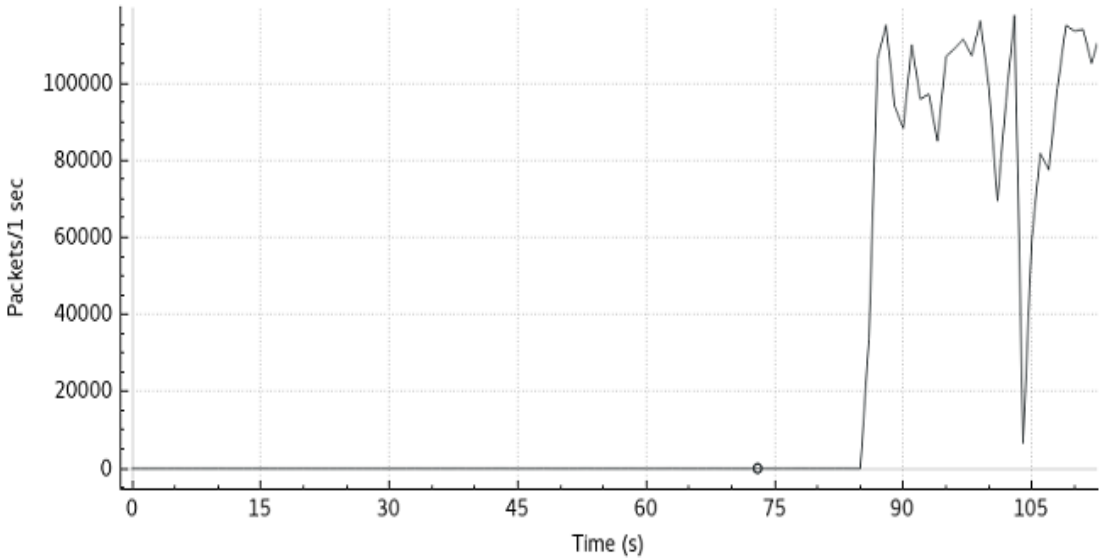
3.2.2 Disponibilidade: Negação de Serviço (*Denial of Service)*

O ataque de negação de serviço DoS em redes VoIP, conforme apresentado na subseção 2.3.2, pode ser realizado sobre a rede padrão ou específicos em serviços VoIP. No caso de êxito na quebra da confidencialidade, uma das utilidades é disponibilizar uma determinada extensão para se autenticar no servidor.

A técnica realizada sobre a rede padrão, de *flood* de requisições SIP do tipo INVITE e *stream* RTP não tiveram êxito, conforme já esperado, pois esses protocolos não estão abertos na rede, para estas técnicas foram utilizadas as ferramentas ***inviteflood*** e ***rtpflood*.**

Para a rede comum, foram utilizadas as ferramentas ***atk6-flood-route6*** na interface eth0.172, **T50** e **Hping3**, todas tiveram o resultado esperado, indiposnibilizando a rede toda ou dispositivo específico do IP alvo. A figura 35 mostra o gráfico de consumo de largura de banda gerado, o que tornou indisponível todos os hosts da Vlan 172 no momento que o gráfico bateu os 100000 pacotes por segundo.

Figura 35- Saída do *atk6-flood-router6 na Vlan 172*



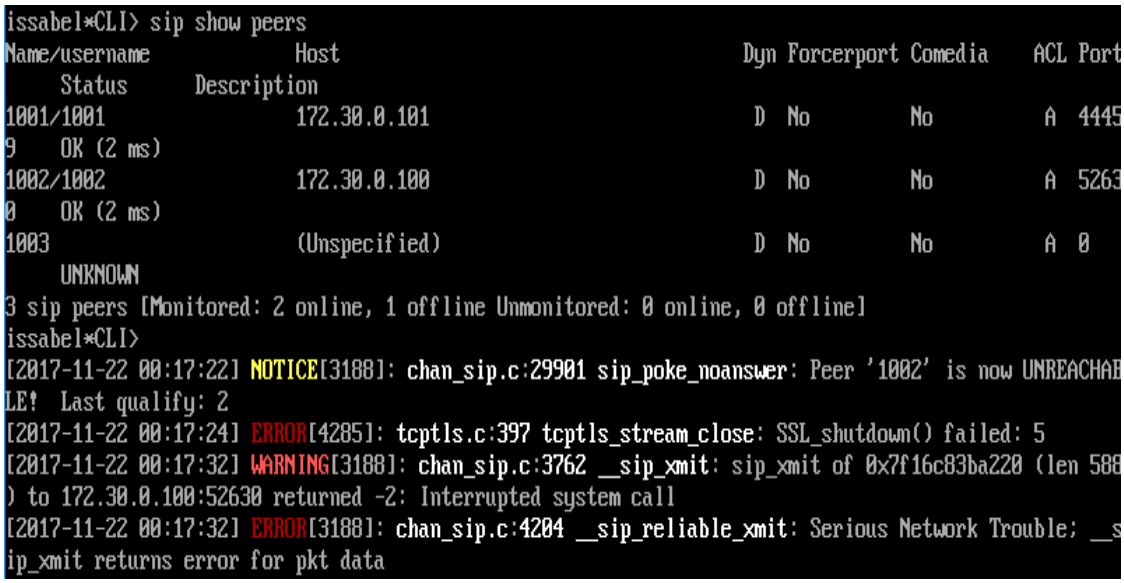
FONTE: Do autor

Esta ferramenta 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 rede fica também praticamente inutilizado. Para ser possível executar o ataque, introduziu-se o

comando ***"atk6-flood_router6 eth0.172"*** , outra alternativa seria o **Ataque *Smurff,*** cuja sintaxe é ***smurf6 interface alvo-ip [multicast-network-address]***

Os ataques direcionados a portas de serviços no servidor Asterisk foram rejeitados por existir na distribuição utilizada o serviço ***Fail2Ban***, onde os IPs maliciosos são colocados em uma *black list* e impedidos de chegarem à aplicação por um determinado tempo reconfigurado. Já nos telefones IP, todos os ataques de DoS tiveram sucesso, como pode ser visto na figura 36, onde a extensão 1002 estava online e após um curto período de tempo o Asterisk começou a informar que estava indisponível, que o SSL com a extensão tinha caído e que haviam sérios problemas de rede. O comando executado foi ***"t50 172.30.0.100 –flood -S –turbo –protocol T50"***.

Figura 36- Ataque T50 ao telefone IP

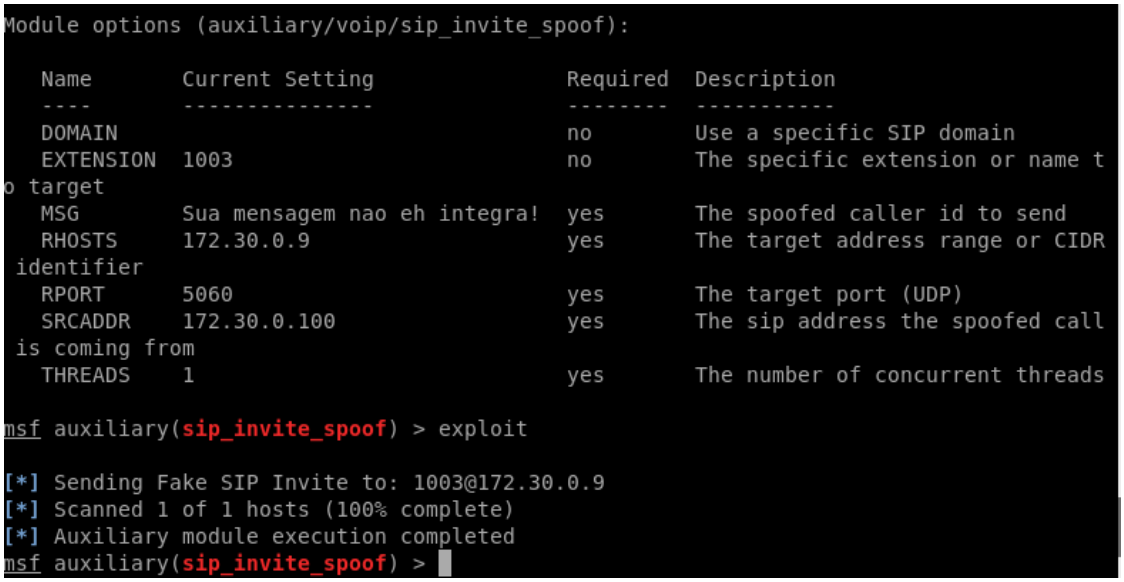


FONTE: Do autor

3.2.3 Integridade: Adulteração de mensagem (Message *Tampering)*

Como técnica para falsificar uma mensagem e enviar ao destinatário, foi utilizado um módulo auxiliar do *Metasploit-Framework* chamado ***sip_invite_spoof***, que cria uma mensagem falsa e envia para a extensão do alvo, não foram obtidos satisfatórios, conforme figura 37, pois o servidor somente aceita chamadas autenticadas com certificado digital conforme já apresentado. A ferramenta ***inviteflood*** também pode ser utilizada para aplicar esta técnica.

Figura 37- Ataque sip_invite_spoof



FONTE: Do autor

3.2.4 Autenticidade: Sequestro de Registro (*Registration Hijacking*)

Ao mesmo passo que a integridade não pôde ser comprometida pelos ataques efetuados, a quebra de autenticidade também ficou prejudicada por existir duplo fator de segurança implementado com o Certificado Digital e a senha de cada extensão utilizada, dessa forma, todo o sistema VoIP se manteve capaz de garantir o não-repúdio das informações trocadas na rede.

Por outro lado, Bates (2015) afirma que a grande maioria dos serviços VoIP ainda trabalham com uma autenticação básica, onde podem ser utilizadas outras técnicas para passar com facilidade, já, quando é utilizado algo que se sabe como a senha e algo que se tem como o certificado, o risco de quebra de autenticidade diminui consideravelmente.

Diante do exposto, nessa seção, o atacante que encontrar uma rede como esta, deve partir para outras técnicas direcionadas às pessoal, que envolvam Engenharia Social para tentar por exemplo, utilizar um dos equipamentos que fazem parte dessa rede, como os telefones IP, PBX-IP, Autoridade Certificadora.

3.3 DISCUSSÕES E ANÁLISE DOS RESULTADOS

Diante das questões de estudo, verificou-se a necessidade de implementar medidas de segurança após a instalação de um Sistema VoIP, pois a metodologia proposta no estudo realizado por Regueira (2015) não teve sucesso neste estudo de caso, visto as técnicas de segurança em profundidade incorporadas ao projeto. Por outro lado, cresce a preocupação com o vetor Humano na Segurança da Informação, por ser o elo mais fraco dessa corrente e mais exposto a ameaças, assim, mesmo adotando procedimentos implementados por uma solução que envolve as mais avançadas tecnologias, são necessárias normas e políticas bem definidas de forma a mapear e definir os processos envolvidos, base para o Ciclo do Sistema de Gestão da Segurança da Informação (SGSI) apresentado na figura 27.

Figura 38- Cliclo SGSI - PDCA

FONTE: Coelho (2013)

Foi bem definido também o que é criptografia de Estado, qual órgão tem a maior expertise para seu desenvolvimento em apoio à Administração Pública Federal (APF), bem como a incorporação de uma dessas tecnologias (PCAD) à solução proposta. Cabe ressaltar, conforme figura 28, que os algoritmos utilizados neste trabalho, AES 256 e ESA 4096, são de domínio público e implementam uma Criptografia computacionalmente segura, porém, em atenção à legislação estudada, ainda assim, é necessário o uso de algoritmo de Estado.

Figura 39- Segurança em algoritmos públicos

Method	Date	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
[1] Lenstra / Verheul	2014	81	1562 1216	143	1562	152	162
[2] Lenstra Updated	2014	78	1218 1309	155	1218	155	155
[3] ECRYPT II	2011 - 2015	80	1248	160	1248	160	160
[4] NIST	2011 - 2030	112	2048	224	2048	224	224
[5] ANSSI	2014 - 2020	100	2048	200	2048	200	200
[6] NSA	-	-	-	-	-	-	-
[7] RFC3766	-	-	-	-	-	-	-
[8] BSI (signature only)	2014 - 2015	-	1976	224	2048	224	224

All key sizes are provided in bits. These are the minimal sizes for security.

FONTE: Keylenght (2014)

Por fim, a partir da análise das questões de estudo apresentadas e discutidas dentro do trabalho, podemos responder à situação problema que existe uma Solução de Tecnologia da Informação e Comunicações para proteger as comunicações telefônicas da Rede de Inteligência de Defesa, independente do local onde os integrantes estão instalados. A solução viabiliza ainda a troca de informação classificada com a utilização da PCAD, em conformidade com a Lei n° 12.527 e os Decretos 7.724 e 7.845, o que é viável para a utilização em Órgãos/Agências de Inteligência do EB utilizando a infraestrutura da **EBNet**, mantendo ainda os sistemas existentes.

Apenas ataques contra a disponibilidade tiveram êxito neste laboratório, pois o atacante conseguiu acesso à Vlan de voz utilizando de uma facilidade implementada por padrão em ***Switches***, principalmente aqueles que implementam o protocolo CDP/LLDP. Como sugestão deve-se desativar esses protocolos e utilizar a configuração manual da Vlan de voz com a utilização de ***Port Security*** nos ativos de rede, ou, sendo mais paranoico com a segurança, segregar fisicamente toda a rede com ativos dedicados.

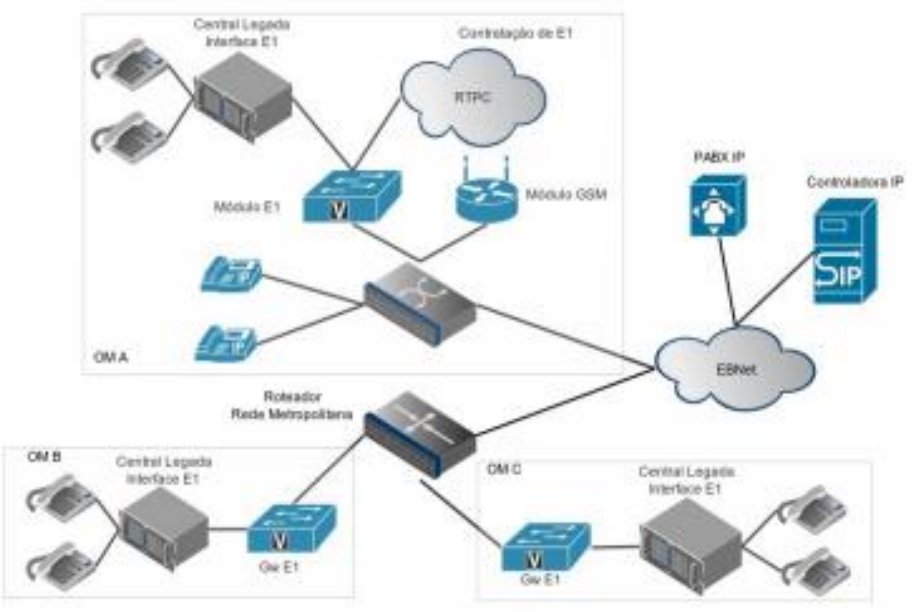
4 PROPOSTA PARA O EBVoIP

De acordo com o CITEx, o Projeto EBVoIP tem por objetivo implantar uma solução completa, escalável e segura de telefonia utilizando a tecnologia Voz sobre *IP* (*Voice over Internet Protocol – VoIP*), baseada em *software* para atender às demandas da Rede Integrada de Telefonia do Exército (RITEx) nas diversas Organizações Militares (OM) do Exército Brasileiro (EB).

.A solução VoIP proposta para o EB também segue o padrão SIP e está sendo realizada através das redes locais das diversas OM contempladas pela solução, principalmente para ligações internas (entre ramais), das redes metropolitanas, para os casos de chamadas locais, e da EBNet (MPLS Contratada), por onde trafegarão os pacotes de voz durante as ligações de longa distância nacional.

A função de interconexão e interoperabilidade será provida através de gateways IP com interfaces E1, FXO, FXS e GSM. Esses equipamentos permitem a comunicação entre a rede VoIP, a rede de telefonia convencional da OM, a Rede Telefônica Pública Comutada (RTPC), a rede de telefonia celular e o *backbone* da RITEx (EBNet), conforme a figura 29.

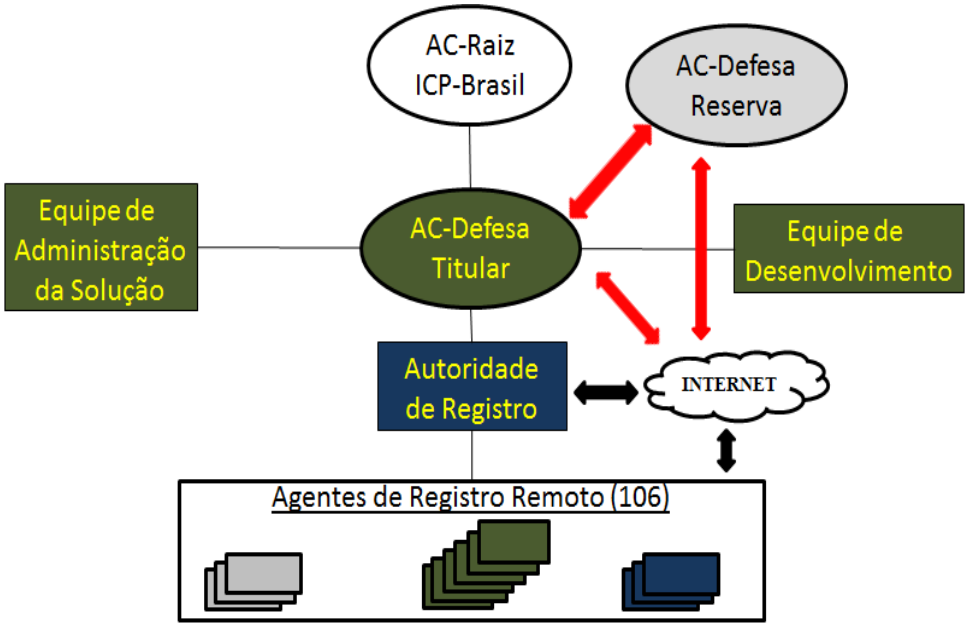
Figura 40- Cenário EBVoIP



FONTE: CITEx (2015)

De acordo com a figura 30, o MD resolveu implantar uma Autoridade Certificadora de Defesa (AC-Defesa), aderente à ICP-Brasil, designando o EB como coordenador das atividades, com a finalidade de conferir autenticidade, confidencialidade e integridade na troca de informações em forma eletrônica no âmbito do Ministério da Defesa e das Forças Armadas, designando o EB como coordenador das atividades, em consonância com a Diretriz Ministerial nº 0014/2009, de 9 NOV 2009, que atribui ao EB a responsabilidade pela coordenação e integração da estruturação do **Setor Cibernético do MD**.

Figura 41- Arquitetura AC-Defesa



FONTE: Brasil (2013)

Conforme a arquitetura definida para a operação conjunta das FA, a AC-Raiz ficou instalada no EB, a AC-Reserva na MB e a AR na FAB, sendo que as três forças possuem Agentes de Registro Remotos implantados nos respectivos Órgãos de Identificação, prestando serviço de emissão, renovação e revogação de certificados digitais no âmbito do Ministério da Defesa , considerando a Administração Central, os órgãos vinculados e os comandos da Marinha, do Exército e da Aeronáutica, atendendo aos padrões estabelecidos pela infraestrutura de Chaves Públicas do Brasil (ICP-BRASIL).

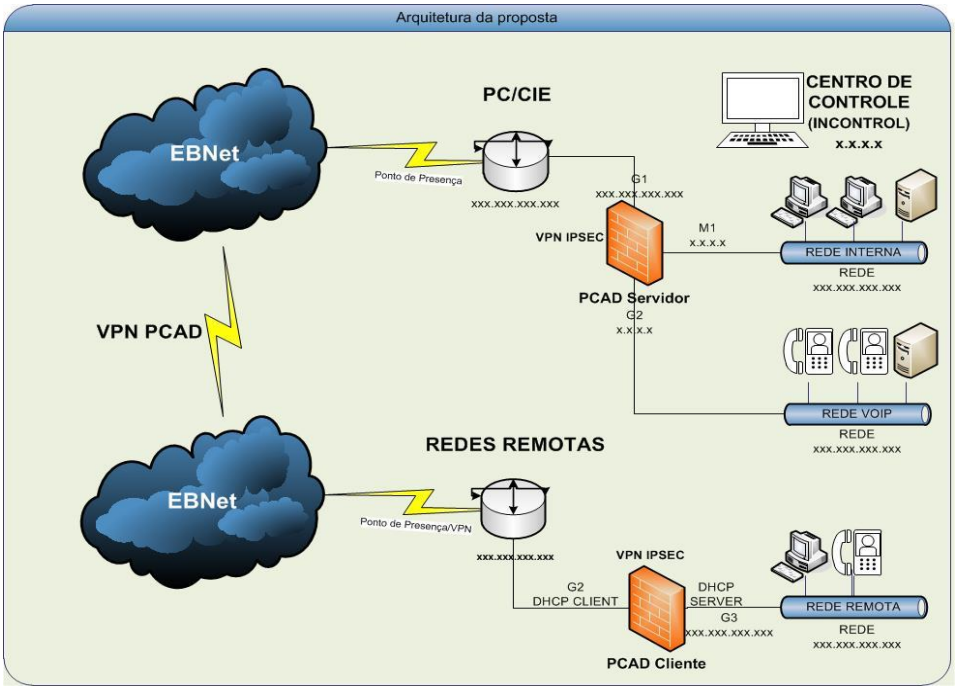
Diante do exposto, e pelas características semelhantes ao estudo de caso, o presente trabalho pode contribuir para o aumento do nível de segurança do EBVoIP, propondo a emissão de Certificados Digitais padrão X.509 pela AC-Defesa para a

instalação nos dispositivos e sistemas do EBVoIP, tais como: telefones IP, iPBX, Gateway E1, etc. Essa camada de segurança garante a autenticidade dos dispositivos integrantes do sistema, tanto aqueles ramais locais em cada OM, quanto nas ligações remotas onde será necessária a utilização de VPN.

Em complemento às medidas de segurança já mencionadas no presente trabalho, aqueles telefones IP que são utilizados para a transmissão de informações classificadas devem utilizar uma camada adicional de segurança com criptografia gerada por Algoritmo de Estado, em conformidade com a legislação de referência. Para esta medida, sugere-se a utilização da Placa Criptográfica de Auto Desempenho (PCAD), desenvolvida pela ABIN para o TSG. Esse recurso é instalado entre o telefone IP e a rede de dados da OM, criando um túnel VPN, que pode ser *Site-to-Site* ou *Client-to-Site*.

A arquitetura proposta pode ser visualizada na figura 31, onde existe uma camada adicional de segurança implementada com algoritmo de Estado e de fácil gestão pelos Centros de Telemática (CT/CTA), conforme diretriz do Centro de Inteligência do Exército (CIE).

Figura 42- Diagrama de segurança do EBVoIP



FONTE: Do autor

5 CONCLUSÃO E TRABALHO FUTURO

O presente trabalho teve como objetivos principais comparar os aspectos de vulnerabilidade e de segurança que podem ser utilizados tanto para o ataque quanto para a defesa de sistemas que utilizam o serviço VoIP. As ferramentas utilizadas na metodologia proposta para o laboratório não obtiveram os mesmos resultados, o que já era esperado a partir da **hardenização** dos sistemas com a utilização de mecanismos de segurança em camadas e de criptografia.

Através da literatura, foi elaborado um levantamento das falhas de segurança já referenciadas por Regueira (2015). Foi verificado que, além do protocolo SIP, as fragilidades da infraestrutura de rede e as vulnerabilidades inerentes ao protocolo IP tornam o sistema menos seguro. Isto se deve ao fato de que, se um atacante conseguir acesso à rede VoIP, pode realizar diversos tipos de ataque, tais como *Eavesdropping*, *SIP Port Scan*, *ARP Poisoning* e DoS.

A implementação de um sistema de Firewall, conforme a figura 17 são requisitos essenciais para minimizar tais vulnerabilidades, visto que a medida que os serviços convergem para esta arquitetura, cresce o risco de um ataque que pode comprometer todos os sistemas e serviços da organização a partir do serviço menos seguro, conforme a teoria do elo mais fraco da corrente.

De modo a comprovar a eficácia das mediadas de segurança implementada no projeto do estudo de caso, foi configurado um cenário controlado, onde foi possível realizar diversos tipos de teste de intrusão. Mesmo com o atacante dentro da rede, diversas tentativas foram frustradas, dessa forma, verifica-se a necessidade de prospecção de novas ferramentas para a condução dos testes, e novas técnicas, onde o alvo passa a serem outras aplicações que dão suporte aos sistemas, tais como servidores HTTP, TFTP, SSH, presentes em todos os telefones IP.

Do lado do servidor pode-se explorar o ***Asterisk Call Manager,*** a própria administração do ***FreePBX*** que é toda Web, verificando a possibilidade de enviar um ***webshell.php*** que pode ser utilizado para realizar o *upload* de um ***payload*** para abrir um *shell* reverso no servidor, realizar a escalada de privilégio para a conta de ***root*** do sistema, e dessa forma, realizar todos os ataques que foram barrados pelas camadas de defesa em profundidade implementados. Estas propostas são

apresentadas como trabalho futuro para contribuir com a evolução da maturidade do sistema VoIP tendo como resultado final manter o **Telefone Seguro no EBVoIP**.

Com o atacante fora da rede, não há neste estudo de caso conectividade para o iPBX, fato que foi considerado para iniciar uma análise de vulnerabilidade nos telefones IP remotos que se conectam pela VPN, resultando na desativação de diversos serviços desnecessários, tais como servidor Web para configuração do equipamento. Foi instalado ainda, um aplicativo para bloqueio de tela com senha, de modo que apenas o proprietário do ramal possa manipular suas configurações.

Apesar do *overhead* de processamento, o desempenho não ficou prejudicado, não causando impactos para o usuário.

Através dos resultados obtidos, foi realizada uma proposta para o EBVoIP com o objetivo de implementar mecanismos adicionais de segurança ao sistema em implantação no EB, tendo em conta que foi efetuada uma análise aprofundada das falhas de segurança e privacidade neste tipo de infraestrutura, potencializado pela descentralização de iPBX necessária dentro da EBNet.

REFERÊNCIAS BIBLIOGRÁFICAS

BATES, Regis J. (Bud). ***Securing VoIP:*** *keeping your voip network safe*. Waltham, MA, USA: Syngress, 2015.

BRASIL. **Decreto nº 7.845 de de 14 de novembro de 2012.** Tratamento da informação classificada**.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-014/2012/Decreto/D7724.htm>. Acesso em: 10 nov. 2017.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional LBDN.** Disponível em: <http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf> Acesso em: 17 set. 2017.

CLARK, Richard A.; KNAKE, Robert K. **Guerra Cibernética:** a próxima ameaça à segurança e o que fazer a respeito. Rio de Janeiro: Brasport, 2015.

GIL, A.C. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008.

GONÇALVES, Joanisval Brito. **Atividade de inteligência e legislação correlata**. 2. ed. Niterói, RJ: Impetus, 2011.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Indrodução à Segurança de Computadores**. Porto Alegre: Bookman, 2013.

HARTPENCE, Bruce. **Packet Guide to Voice over IP.** Sebastopol, CA: O'Reilly Media, Inc., 2013

JORGE, Bruno Tiago Correia. **Segurança e Privacidade numa Infraestrutura VoIP**. 2017. 89 f. Dissertação (Mestrado Integrado em Engenharia Eletrotécnica e de Computação) – Faculdade de Engenharia da Universidade do Porto, Porto-PT.

MOTA FILHO, João Eriberto. **Sistemas de Firewall**. 2017. Disponível em <http://eriberto.pro.br/wiki/index.php?title=Minhas_palestras#Sistemas_de_firewall>. Acesso em: 8 ago. 2017

REGUEIRA, Flávio Augusto Coelho. **Ataques a sistemas de voz sobre IP**. 2015. 18 f. Artigo Científico (Pós-graduação em Perícia Digital) – Universidade Católica de Brasília, Brasília-DF.

STALLINGS, William. **Criptografia e Segurança de Redes:** princípios e práticas. 6. ed. São Paulo: Pearson Prentice Hall, 2015.

TANENBAUM, Andrew S.; WETHERALL, David. **Redes de Computadores.** São Paulo: Pearson Prentice Hall, 2011.

KEYLENGHT. **Recomendação de tamanho de chaves criptográficas.** Disponível em: <http://www.keylength.com/> Acesso em: 10 de novembro de 2017.

COELHO, F. E. S.; ARAÚJO, L. G. **S. de. Gestão da Segurança da Informação: NBR 27001 e 27002**. Rio de Janeiro: Escola Superior de Redes, 2013.