

**UNIVERSIDADE FEDERAL DE SANTA CATARINA  
DEPARTAMENTO DE INFORMÁTICA E ESTATÍSTICA**

Vitor Augusto Schweitzer

**PROPOSTAS DE SEGURANÇA PARA O AMBIENTE DE TELEFONIA  
IP DA UNIVERSIDADE FEDERAL DE SANTA CATARINA**

Florianópolis - SC  
2017

Vitor Augusto Schweitzer

**PROPOSTAS DE SEGURANÇA PARA O AMBIENTE DE TELEFONIA  
IP DA UNIVERSIDADE FEDERAL DE SANTA CATARINA**

Trabalho de Conclusão de Curso apresentado  
como requisito para obtenção do título de  
Bacharel em Sistemas de Informação na  
Universidade Federal de Santa Catarina.

Orientadora: Profa. Dra. Carla Merkle Westphall

Florianópolis - SC

2017

Vitor Augusto Schweitzer

**PROPOSTAS DE SEGURANÇA PARA O AMBIENTE DE TELEFONIA  
IP DA UNIVERSIDADE FEDERAL DE SANTA CATARINA**

Este Trabalho de Conclusão de Curso foi julgado adequado para a obtenção do Título de Bacharel em Sistemas de Informação, e aprovado em sua forma final pelo Curso de Sistemas de Informação.

Florianópolis, \_\_\_\_ de \_\_\_\_\_ de \_\_\_\_\_.

Banca examinadora:

---

Profa Dra Carla Merkle Westphall  
Orientadora

---

Prof. Dr. Carlos Becker Westphall  
Membro da banca

---

Bel. Estefania Borm  
Membro da banca

Dedico este trabalho a minha família,  
amigos, e todos que estiveram presentes  
neste momento da minha vida.

## **AGRADECIMENTOS**

Agradeço a Universidade Federal de Santa Catarina, instituição onde dedico dois terços do meu dia, como aluno e servidor, buscando crescimento profissional e pessoal. A Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação, por disponibilizar o ambiente e condições necessárias para execução deste trabalho, e aos colegas da Coordenadoria de Gestão de Redes e Serviços, que participaram de tantas discussões sobre o tema e auxiliaram no que foi necessário.

A minha orientadora, Profa. Dra. Carla Merkle Westphall, que além de contribuir com o seu conhecimento, aceitou a proposta e confiou neste trabalho desde o início. Também a Estefania Borm, que me auxiliou por estes três anos e mais uma vez disponibilizou seu tempo e experiência para o apoio neste projeto.

A minha família, por proporcionar condições pessoais, incentivo e acima de tudo o exemplo de dedicação e perseverança sob os mais diversos obstáculos.

Por fim a todos os amigos que ajudaram a transformar tantos dias difíceis em risadas e esperança.

## RESUMO

Este trabalho apresenta um estudo sobre a aplicação de segurança da informação em ambientes de telefonia IP, objetivando a elaboração e validação de propostas que contribuem para a segurança do serviço de telefonia da Universidade Federal de Santa Catarina. Com a constante substituição da telefonia convencional da universidade pelo VoIP, identificou-se a necessidade de melhorias nos seus quesitos de Confidencialidade, Integridade e Disponibilidade, fatores de segurança essenciais para manutenção de serviços prestados sobre a rede IP. O trabalho resultou na aplicação de três propostas em pontos específicos do sistema. Certificados digitais foram utilizados para implementação de autenticação e criptografia para acesso e transferência de dados centralizados em um servidor de provisionamento, distribuindo de forma segura as configurações de terminais telefônicos. O tráfego de voz foi criptografado através da habilitação do protocolo SRTP nos dispositivos VoIP, aumentando a confidencialidade das chamadas. O isolamento da rede VoIP foi planejado através da implementação de Voice VLAN sobre os switches, possibilitando a restrição de tráfego e reduzindo riscos de invasões e ataques de negação de serviço. Todas as propostas foram testadas no atual ambiente de telefonia da instituição, concluindo-se que todas são aplicáveis e poderão contribuir para a segurança do serviço prestado.

**Palavras-chave:** Telefonia IP. VoIP. Segurança da Informação. Criptografia.  
Certificado Digital

## **ABSTRACT**

This work presents a study on the application of information security in IP telephony environments, aiming at the elaboration and validation of proposals that contribute to the security of the telephony service at Universidade Federal de Santa Catarina. With the constant replacement of the university's conventional telephony by VoIP, it was identified the need for improvements in its Confidentiality, Integrity and Availability requirements, essential security factors for the maintenance of services provided over the IP network. This work resulted in the application of three proposals at specific points in the system. Digital certificates were used to implement authentication and encryption for centralized data access and transfer on a provisioning server, securely distributing endpoint configurations. Voice traffic was encrypted by enabling the SRTP protocol on VoIP devices, increasing the confidentiality of calls. VoIP network isolation was planned by implementing Voice VLAN over switches, enabling traffic restriction and reducing the risk of intrusion and denial of service attacks. All the proposals were tested in the current telephony environment of the institution, concluding that all are applicable and may contribute to the security of the service provided.

**Keywords:** IP Telephony. VoIP. Information Security. Encryption. Digital Certificate

## LISTA DE FIGURAS

Figura 1 - Fluxo de mídia entre agentes SIP .....	20
Figura 2 - Sinalização SIP para registro de usuário .....	22
Figura 3 - Sinalização SIP para estabelecimento de sessão .....	22
Figura 4 - Modelo simplificado de criptografia simétrica.....	27
Figura 5 - Criptossistema de chave assimétrica: autenticação e sigilo .....	29
Figura 6 - Esquema simplificado de assinatura digital .....	30
Figura 7 - Assinatura e validação de um certificado digital .....	31
Figura 8 - Certificado digital formato X.509 .....	33
Figura 9 - Handshake TLS mútuo .....	36
Figura 10 - Cenário de utilização de IPSec .....	39
Figura 11 - Processamento SRTP.....	45
Figura 12 - Estrutura de um pacote SRTP .....	45
Figura 13 - Infraestrutura de telefonia da UFSC.....	50
Figura 14 - Geração do par de chaves assimétricas com o openssl.....	55
Figura 15 - Geração do arquivo CSR com o OpenSSL .....	55
Figura 16 - Arquivos de chave e CSR .....	56
Figura 17 - Certificado utilizado no servidor .....	56
Figura 18 - Parâmetros para ativação de SSL no apache.....	57
Figura 19 - Instalando certificado digital da CA no telefone SoundPoint IP .....	58
Figura 20 - Certificado digital da CA instalado no telefone SoundPoint IP.....	58
Figura 21 - Aprovisionamento sem criptografia .....	59
Figura 22 - Handshake TLS simples .....	59
Figura 23 - Erro no handshake TLS, CA desconhecida .....	59
Figura 24 - Parâmetros para ativação de TLS mútuo no apache.....	60
Figura 25 - Handshake TLS mútuo .....	61
Figura 26 - Parâmetros para ativação do SRTP no telefone SoundPoint IP .....	62
Figura 27 - Parâmetros para ativação do SRTP no gateway Mediant 2000.....	64
Figura 28 - Fluxo de chamada SIP utilizando RTP.....	67
Figura 29 - Campos SDP de INVITE sem oferta de criptografia .....	67
Figura 30 - Conversão do tráfego RTP em fluxo de áudio compreensível .....	68
Figura 31 - Fluxo de chamada SIP utilizando SRTP .....	69
Figura 32 - Campos SDP de INVITE com oferta de criptografia .....	70
Figura 33 - Conversão do tráfego SRTP em fluxo de áudio não compreensível.....	71
Figura 34 - Fluxo de chamada SIP utilizando SRTP - telefone IP para gateway .....	72
Figura 35 - Fluxo de chamada SIP utilizando SRTP - gateway para telefone IP .....	72
Figura 36 - Tabela OUI em um switch D-Link.....	74
Figura 37 - Configuração de Voice VLAN no switch D-Link .....	74
Figura 38 - Aplicação de Voice VLAN nas portas do switch D-Link .....	75
Figura 39 - MACs na porta com Voice VLAN, switch D-Link .....	75
Figura 40 - Endereços IP entregues para telefone e computador no switch D-Link..	76
Figura 41 - Consulta de dispositivos conectados através de LLDP no switch Cisco.	76



Figura 42 - Configuração de Voice VLAN em switch Cisco.....	77
Figura 43 - MACs na porta com Voice VLAN, switch Cisco .....	77
Figura 44 - Endereços IP atribuídos para telefone o computador no switch Cisco ...	78

## LISTA DE TABELAS

Tabela 1 - Classes de resposta SIP .....	23
Tabela 2 - Dimensionamento de IPs para as redes de voz.....	78

## LISTA DE ABREVIATURAS E SIGLAS

ACL	Access Control List
AES	Advanced Encryption Standard
ATA	Adaptadores de Telefones Analógicos
CA	Certification Authority
CDR	Call Detail Record
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECDSA	Elliptic Curve Digital Signature Algorithm
FTP	File Transfer Protocol
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICP	Infraestrutura de Chave Pública
ICPEDU	Infraestrutura de Chaves Públicas para Ensino e Pesquisa
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISDN	Integrated Service Digital Network
ITI	Instituto Nacional de Tecnologia da Informação
LCR	Lista de Certificados Revogados
LLDP	Link-Layer Discovery Protocol
MAC	Media Access Control
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OUI	Organizationally Unique Identifier
PBX-IP	Private Branch Exchange IP
PKI	Public-Key Infrastructure
PoE	Power over Ethernet
PSTN	Public Switched Telephone Network
RA	Registration Authority

RFC	Request for Comments
RNP	Rede Nacional de Ensino e Pesquisa
RTCP	Real-Time Transport Control Protocol
RTP	Real Time Protocol
SDES	Simplified Data Encryption Standard
SDP	Session Description Protocol
SeTIC	Superintendência de Governança Eletrônica e Tecnologia da Informação e Comunicação
SIP	Session Initiation Protocol
SIPS	SIP Secure
SPIT	Spam over Internet Telephony
SRL	SIP Router Local
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UFSC	Universidade Federal de Santa Catarina
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>15</b>
1.1 OBJETIVOS .....	16
1.1.1 <i>Objetivo Geral</i> .....	16
1.1.2 <i>Objetivos Específicos</i> .....	16
1.2 ESCOPO DO TRABALHO .....	16
<b>2 FUNDAMENTAÇÃO TEÓRICA .....</b>	<b>18</b>
2.1 TELEFONIA IP .....	18
2.1.1 <i>Vantagens e desafios</i> .....	18
2.1.2 <i>Arquitetura</i> .....	19
2.1.3 <i>Codecs</i> .....	20
2.1.4 <i>Protocolos</i> .....	21
2.2 SEGURANÇA DA INFORMAÇÃO .....	25
2.2.1 <i>Pilares da segurança (CID)</i> .....	26
2.2.2 <i>Criptografia e autenticação</i> .....	27
2.2.3 <i>Assinatura Digital</i> .....	29
2.2.4 <i>Certificados Digitais</i> .....	30
2.2.5 <i>TLS</i> .....	35
2.2.6 <i>IPSEC</i> .....	37
2.3 SEGURANÇA EM TELEFONIA IP .....	39
2.3.1 <i>Ameaças existentes</i> .....	39
2.3.2 <i>Medidas de proteção</i> .....	41
2.3.3 <i>Protocolos para segurança em VoIP</i> .....	43
<b>3 TRABALHOS CORRELATOS .....</b>	<b>47</b>
<b>4 AMBIENTE DE ESTUDO .....</b>	<b>49</b>
4.1 AMBIENTE DE TELEFONIA .....	49
4.2 PROPOSTA DE TRABALHO .....	51
<b>5 IMPLEMENTAÇÕES DE SEGURANÇA .....</b>	<b>53</b>
5.1 CRIPTOGRAFIA E AUTENTICAÇÃO PARA APROVISIONAMENTO .....	53
5.1.1 <i>Geração e instalação do certificado digital</i> .....	54
5.1.2 <i>Implementação de criptografia</i> .....	57

5.1.3 Implementação de autenticação .....	59
5.2 CRIPTOGRAFIA DE VOZ.....	61
5.2.1 Configuração dos dispositivos .....	62
5.2.2 Testes e resultados.....	66
5.3 SEGMENTAÇÃO DA REDE VOIP.....	72
5.3.1 Configuração dos switches .....	73
5.3.2 Planejamento da rede de voz .....	78
<b>6 CONSIDERAÇÕES FINAIS .....</b>	<b>80</b>
<b>REFERÊNCIAS.....</b>	<b>82</b>
<b>APÊNDICE A - ARTIGO .....</b>	<b>85</b>

## 1 INTRODUÇÃO

Os meios de comunicação estão em constante avanço e a convergência digital torna-se cada vez mais presente. As redes IP são o meio de comunicação mais utilizado pelos serviços que necessitam transmitir dados, uma vez que possuem alta escalabilidade e abrangência, interligando pontos no mundo inteiro. Neste cenário, diversas mídias e serviços trafegam sobre a mesma rede, tais como sites, sistemas web, televisão, dentre tantos outros que constituem o cotidiano das pessoas e instituições.

Por muito tempo a telefonia foi baseada em comutação de circuitos, no qual a infraestrutura é dedicada e circuitos são reservados para o estabelecimento da comunicação. Porém, com os benefícios da comutação por pacotes, a telefonia adaptou-se e passou também a utilizar as redes IP como meio de transmissão de sinalização e áudio, surgindo assim o conceito de VoIP (*Voice over IP*).

Com tantos dados sendo transmitidos pela rede, muitas vezes em locais que não estão sob o domínio das pessoas interessadas, a preocupação com a segurança torna-se algo necessário. Informações sigilosas são transmitidas diariamente, estando suscetíveis às mais diversas ameaças, no caminho entre emissores e receptores. Agentes maliciosos estão a todo o momento buscando informações que podem lhes trazer alguma vantagem, ou ainda prejudicar o dono da informação. Para mitigar estas ameaças, mecanismos de segurança como criptografia e autenticação devem ser utilizados em sistemas que possuem algum tipo de informação sigilosa, como dados pessoais, financeiros e estratégicos para organizações.

Segundo Nakamura e Geus (2007, p. 26) “[...] novas tecnologias trazem consigo novas vulnerabilidades [...]”. Diante, portanto, deste novo ambiente de telefonia, onde conversas são transmitidas pelos mesmos meios que tantas outras informações, existe a necessidade de aplicar segurança também sobre as chamadas IP, uma vez que muitas delas podem transmitir informações sigilosas. Conversas entre duas ou mais pessoas podem envolver informações estratégicas, dados pessoais, senhas, e muitas outras informações privadas dos envolvidos.

Pretende-se com este trabalho realizar um estudo sobre segurança da informação aplicada em um ambiente de telefonia IP, abordando pontos de vulnerabilidade, ameaças existentes, mecanismos de defesa e protocolos envolvidos.

Tal estudo será aplicado no ambiente de telefonia IP institucional da Universidade Federal de Santa Catarina, que atualmente possui mais de metade de sua estrutura baseada na tecnologia VoIP.

## 1.1 OBJETIVOS

### *1.1.1 Objetivo Geral*

O objetivo deste trabalho é realizar um estudo sobre as vulnerabilidades existentes em um ambiente de telefonia IP, bem como as tecnologias e protocolos que ampliam a segurança de chamadas de voz sobre IP e demais comunicações realizadas entre os dispositivos que integram um sistema de telefonia. Este estudo será aplicado posteriormente ao ambiente de telefonia IP da UFSC, identificando-se pontos de vulnerabilidade e propondo melhorias de segurança.

### *1.1.2 Objetivos Específicos*

Os objetivos específicos deste trabalho são:

- Realizar uma revisão bibliográfica sobre a tecnologia VoIP e conceitos relacionados à segurança da informação;
- Apresentar as vulnerabilidades e ameaças existentes em um serviço de telefonia IP;
- Apresentar os protocolos e tecnologias de segurança da informação aplicáveis a um ambiente VoIP;
- Apresentar o ambiente de telefonia IP utilizado na UFSC;
- Identificar possíveis vulnerabilidades no ambiente real;
- Propor soluções de segurança da informação para as vulnerabilidades identificadas.

## 1.2 ESCOPO DO TRABALHO

Será realizada uma revisão bibliográfica sobre conceitos de telefonia IP, as tecnologias e protocolos utilizados, suas características, funcionalidades, vantagens



e desvantagens. Também serão abordados conceitos de segurança da informação, seus pilares e tecnologias, bem como os principais tipos de ataques e mecanismos de defesa aplicados sobre um serviço de telefonia IP.

O trabalho será composto também por uma etapa prática, com a apresentação do ambiente de telefonia IP da UFSC, sua abrangência, características, estrutura lógica e física, posteriormente identificando-se possíveis ameaças e propondo soluções de segurança que contribuam com a mitigação dos riscos.

## 2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo, são descritos os conceitos básicos relacionados à Telefonia IP e Segurança da Informação, estabelecendo a conexão entre as duas áreas e contextualizando o ambiente no qual o trabalho prático será desenvolvido.

### 2.1 TELEFONIA IP

Há muito tempo, a telefonia é um mecanismo de comunicação utilizado para conectar pessoas e instituições. Com o avanço da convergência de serviços e mídias sobre a rede IP, a telefonia também foi integrada, passando de comutação de circuitos dedicados para transporte sobre a rede.

#### *2.1.1 Vantagens e desafios*

Segundo Vetter (2015) a telefonia IP não está apenas substituindo a telefonia convencional, mas também agregando novos valores ao serviço, como a convergência de voz e dados, redução de custos com equipamentos, unificação de equipes de suporte, economia com chamadas de longa distância através da rede IP, integração com outros serviços computacionais, entre outras vantagens.

Entre os maiores desafios da telefonia IP está o alcance da qualidade de serviço até então oferecido pela telefonia convencional, que por utilizar circuitos dedicados, possui alta disponibilidade e não sofre as interferências comuns de uma rede IP, como atrasos, perdas de pacotes e *jitter*, fatores que impactam diretamente na qualidade dos serviços de voz.

Por atuar sobre a rede IP, a telefonia IP também se torna dependente de outros serviços, como DHCP (*Dynamic Host Configuration Protocol*) para distribuição de IPs entre os terminais, DNS (*Domain Name System*) para resolução de nomes, HTTP (*Hypertext Transfer Protocol*) e FTP (*File Transfer Protocol*) para transferência de arquivos. Da mesma forma que o tráfego de dados, a telefonia IP torna-se suscetível a vulnerabilidades da rede, como capturas não autorizadas, alterações de informações, ataques de negação de serviço, tornando-se a segurança um fator a ser tratado cada vez com mais atenção.

### 2.1.2 Arquitetura

Brito e Silva (2013) relatam que como a tecnologia VoIP ainda é emergente, é comum a existência de ambientes híbridos de telefonia convencional e IP. Nestes casos, os principais componentes encontrados são descritos a seguir.

- **Terminais telefônicos:** Dispositivos ou softwares que realizam a interface com o usuário para geração e recebimento de chamadas, digitalizando a sua voz e a transmitindo através de pacotes na rede IP. Telefones IP e *softphones* são exemplos de terminais muito utilizados, havendo ainda a existência de ATAs (Adaptadores de Telefones Analógicos) que realizam a conversão de sinalização e mídia analógica para IP.
- **PBX-IP:** Servidor que realiza o gerenciamento de chamadas na rede, administrando usuários, intermediando sua sinalização e realizando funções de controle a auditoria, como associação de privilégios a usuários e registros de chamadas.
- **Gateway de Mídia:** Equipamento responsável por realizar a conversão de sinalização e áudio entre a rede de telefonia IP e a rede de telefonia convencional e/ou a PSTN (*Public Switched Telephone Network*). Muitas operadoras já utilizam a sinalização SIP através da rede para conectar clientes, dispensando nestes casos o uso de gateways para conexão à PSTN

Esta é uma infraestrutura básica para o funcionamento de uma telefonia IP corporativa, porém outros componentes podem ser encontrados, como servidores de provisionamento de configurações, que centralizam as configurações dos terminais e possibilitam configurações automatizadas através da rede. Sistemas de call center, gravação e relatórios também podem ser encontrados integrando ambientes mais complexos e personalizados.

Vetter (2015, p.35) cita que há duas possibilidades de encaminhamento de fluxo de mídia entre dois terminais. O primeiro, apresentado na Figura 1-a, é através da

transmissão direta entre os terminais, sem a necessidade de passagem do áudio pelo servidor de telefonia, apenas pelos ativos de rede. O segundo, apresentado na Figura 1-b, é através da centralização do fluxo de mídia pela PBX-IP, processo chamado de mídia proxy. Este modelo permite maior controle e monitoramento sobre as chamadas, porém com maior custo de processamento e rede.

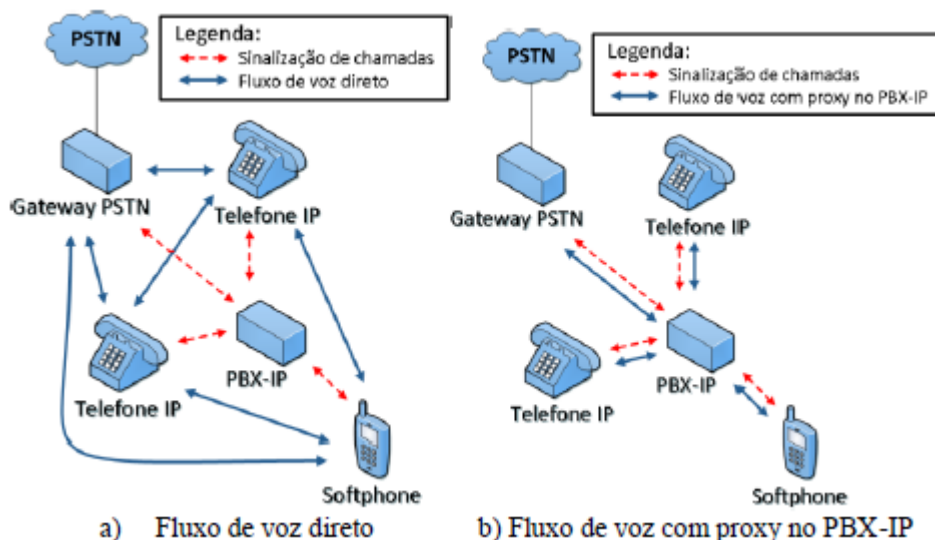


Figura 1 - Fluxo de mídia entre agentes SIP

Fonte: Vetter (2015)

### 2.1.3 Codecs

Codecs, acrônimo de Codificador/Decodificador, são dispositivos que implementam através de hardware ou software conversões de sinais analógicos em sinais digitalizados, por vezes compactados, podendo realizar também o processo inverso para retornar a informação em seu estado original. Há diferentes implementações de codecs para sinais de voz e vídeo no mercado, tendo cada um deles suas características relacionadas à taxa de transmissão pela rede, faixa de frequência do áudio e atraso no processamento.

Vetter (2015, p.39) cita que os codecs mais utilizados em ambientes de telefonia IP são o G.711, com características de baixa utilização de CPU e taxa de transferência de 64kbps, utilizado também pela telefonia convencional, e o codec G.729, que apresenta maior compactação da voz, resultando em uma taxa de transferência de 8kbps, sendo indicado para ambientes com restrição de banda.

Pelo fato da rede IP não oferecer garantias de entrega, alguns recursos extras podem ser implementados pelos codecs, como a detecção de perda de pacotes e seu preenchimento com áudio. Também podem detectar intervalos de silêncio em uma conversa, evitando transmiti-los pela rede para economia de banda (SILVA e JÚNIOR, 2013, p.9).

#### 2.1.4 Protocolos

Esta seção descreve os principais protocolos padrão utilizados em uma comunicação VoIP para sinalização, transferência de mídia e descrição de parâmetros de sessão.

### **SIP**

O SIP (*Session Initiation Protocol*) é um protocolo da camada de aplicação que permite o estabelecimento e gerência de sessões multimídia entre dois ou mais participantes, como chamadas de VoIP e videoconferências. O protocolo foi padronizado pela IETF através da RFC 2543 com o objetivo de ser simples, modular, extensível e de fácil integração aos demais serviços da rede (VETTER, 2015), sendo posteriormente atualizado para a RFC 3261.

O protocolo SIP se comunica de forma similar ao HTTP, através de requisições e respostas, baseadas em texto, entre cliente e servidor, neste contexto chamados de *User Agent Client* (UAC) e *User Agent Server* (UAS). Os UAC são aplicações encontradas em terminais de interface com o usuário, utilizados para iniciar e receber chamadas, como *softphones* e telefones IP. Já os UAS são aplicações centralizadas que tipicamente possuem as funções de SIP Register, gerenciando a localização e autenticação de usuários, SIP Proxy, realizando a gerência de permissões e encaminhamento de chamadas, e SIP Redirect, fornecendo informações relacionadas a outros servidores ou usuários da rede.

Em ambientes de telefonia com servidores SIP centralizados, as trocas de sinalizações mais comuns são para registro do usuário e estabelecimento de sessões. A realização de um registro segue o fluxo de troca de mensagens apresentado na Figura 2, onde inicialmente o cliente envia uma mensagem *REGISTER* para o

servidor, que em um primeiro momento nega a autenticação enviando a resposta 401 - *Unauthorized* e um *nonce* como desafio. O cliente então realiza novamente a solicitação de registro enviando suas credenciais e a resposta ao desafio, no qual o servidor valida os dados e responde com a mensagem 200 OK, caso tudo esteja correto (JORGE, 2017).

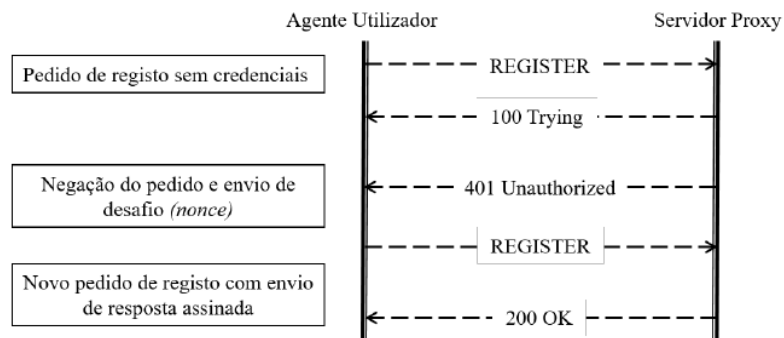


Figura 2 - Sinalização SIP para registro de usuário

Fonte: Jorge (2017)

Após um cliente estar devidamente autenticado no servidor Proxy, o mesmo poderá solicitar ao servidor o estabelecimento de uma chamada com outros usuários, ou clientes externos. Para o estabelecimento desta comunicação é realizada a troca de mensagens apresentada na Figura 3.

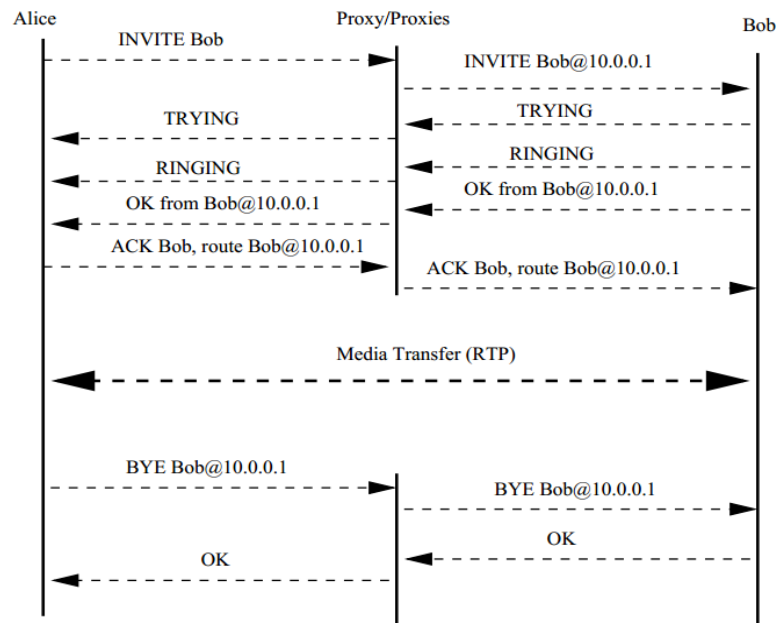


Figura 3 - Sinalização SIP para estabelecimento de sessão

Fonte: Brito (2013)

O cliente que deseja estabelecer uma chamada inicia o processo enviando uma mensagem INVITE ao servidor proxy, adicionando nos campos SDP (*Session Description Protocol*) do pacote, os parâmetros a serem negociados com o destino, como lista de codecs suportados e chaves para estabelecimento de conexões seguras. Ao receber a mensagem, o servidor proxy informa estar processando a requisição com a resposta 100 Trying, e então verifica as permissões do originador da chamada, localizando o endereço do agente destino na rede para encaminhar a ele o INVITE recebido.

Assim que recebe a mensagem, o agente destino responde com 100 Trying, informando que está processando a requisição, e ao começar a chamar para o usuário, responde com uma mensagem 180 Ringing, indicando para a origem que está aguardando atendimento. A resposta do destino pode ser diferente de acordo com o seu estado, como 486 BUSY caso esteja em outra chamada. Ao ocorrer o atendimento da chamada, o agente destino envia a mensagem 200 OK para a origem, que confirma o estabelecimento da sessão com um ACK. Após este processo, é iniciada a troca de áudio ou vídeo diretamente entre as partes, geralmente utilizando o protocolo RTP.

O agente que desligar a chamada primeiro irá enviar a mensagem BYE para o outro agente, indicando uma desconexão, e este responde com 200 OK confirmando a finalização da chamada. Estando o SIP Proxy intermediando a comunicação, ele também realiza a função de CDR (Call Detail Record) da chamada, armazenando informações como data e hora de início, duração e custo da chamada.

Como durante o estabelecimento de uma chamada podem ocorrer inúmeros imprevistos, como problemas de roteamento, destino não encontrado, redirecionamentos, etc, o protocolo prevê classes de respostas, de forma similar ao HTTP. As classes de resposta SIP estão descritas na Tabela 1.

Tabela 1 - Classes de resposta SIP

<b>Classe</b>	<b>Funcionalidade</b>
1xx	Informativo
2xx	Sucesso
3xx	Redirecionamento
4xx	Falha de requisição
5xx	Falha de servidor
6xx	Falha global

Fonte: Vetter (2015)

Brito e Silva (2013) citam o protocolo SIP como vantajoso sobre o anteriormente utilizado H323 por diversos fatores. Um deles é a velocidade, uma vez que utiliza menos trocas de mensagens para estabelecimento de chamadas e utiliza o protocolo UDP (*User Datagram Protocol*) para transporte, ao passo que o H323 utiliza o TCP (*Transmission Control Protocol*). Outro fator é a flexibilidade, devido ao SIP utilizar URLs indicando o protocolo em uso (`sip:nome@dominio.com.br`), desta forma podendo encaminhar chamadas para servidores que não utilizam SIP. Sua fácil depuração também é uma vantagem, uma vez que utiliza uma simples codificação baseada em texto, facilmente interpretada por softwares analisadores de protocolo.

O SIP geralmente é utilizado em conjunto com outros protocolos, como o SDP (*Session Description Protocol*) que dispõe de campos para descrição de informações sobre a sessão, como codec utilizado e endereços de origem e destino, o TLS para estabelecimento de sessões de forma criptografada e autenticada e o RTP para transmissão da mídia.

## **RTP**

O RTP (*Real Time Protocol*) é um protocolo padronizado pela RFC 3550 projetado para realização do transporte de mídias de tempo real através da rede, como VoIP e videoconferências. Possui características que o torna adequado para este uso, como a compensação de falhas da rede IP, tipicamente jitter e perda de sequência de pacotes, e a utilização do UDP como protocolo real de transporte. Uma vez que o UDP não é orientado a conexão, consegue-se uma transferência de dados com latência muito menor que o TCP. Atraso, *jitter*, e perda de pacotes são erros críticos para aplicações de voz e vídeo em tempo real, pois são diretamente percebidas pelo usuário, através de picotes de chamadas, eco e áudios atrasados.

Como o RTP não possui controle sobre qualidade de serviço, geralmente é utilizado em paralelo o RTCP (*Real-Time Transport Control Protocol*), protocolo que envia e recebe informações sobre a qualidade da sessão.

Tanto o RTP quanto o RTCP são protocolos que trafegam de forma aberta na rede, oferecendo desta forma riscos de segurança para os usuários. Um agente malicioso que realize a captura do tráfego na rede e utilize um software que implementa o codec utilizado na chamada, conseguirá facilmente montar o fluxo passante e assim realizar escutas não autorizadas. Como opções de segurança para



estes protocolos existem os protocolos SRTP e o SRTCP, capazes de agregar confidencialidade, autenticidade e proteção contra ataques de *replay* ao tráfego.

## SDP

O SDP (*Session Description Protocol*) é um protocolo padronizado pela IETF através da RFC 4566 utilizado para descrição e negociação de atributos durante o estabelecimento de sessões multimídias entre dois ou mais participantes, como chamadas de voz ou vídeo sobre IP. O SDP possui campos padronizados que servem para que outros protocolos de estabelecimento de sessões, como o SIP e o H323, possam transmitir informações como o tipo de mídia a ser transmitida, codec a ser utilizado, protocolo de transporte, endereçamento de IP e porta para entrega da mídia, chave criptográficas, entre outros dados necessários de acordo com o contexto.

## 2.2 SEGURANÇA DA INFORMAÇÃO

A informação pode ser gerada, armazenada e transmitida em diversos formatos, sejam documentos impressos, digitais, e-mails, conversas. Independente do formato e meio de transmissão, ela pode conter valores pessoais, estratégicos, financeiros para seus proprietários, precisando assim de proteção adequada. Coelho e Araujo (2014) definem que “Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”. Também destacam os seguintes conceitos relacionados à segurança:

- **Incidente de segurança:** qualquer evento que comprometa a segurança, como ataques a serviços, roubo e vazamento de informações.
- **Ativo:** elemento tangível ou intangível que tenha valor para a organização, como softwares, dados, equipamentos, pessoas, processos e serviços.
- **Ameaça:** evento que explora vulnerabilidades a fim de causar incidentes.
- **Vulnerabilidade:** fraqueza ou falha que possa ser explorada e comprometa a segurança de sistemas ou informações.
- **Risco:** combinação da probabilidade de um evento ocorrer e suas consequências.

- **Ataque:** qualquer ação que comprometa a segurança de uma organização.
- **Impacto:** consequência da ocorrência de um evento.

### 2.2.1 Pilares da segurança (CID)

O Manual de Segurança de Computadores do NIST (*National Institute of Standards and Technology*), citado por Stallings (2014), apresenta segurança de computadores com a seguinte definição:

Segurança de computadores é a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).

A definição do NIST aborda os três princípios centrais da segurança da informação: confidencialidade, integridade e disponibilidade, também conhecidas como tríade CID.

Confidencialidade é a propriedade que tem por objetivo restringir o acesso a informação apenas para as pessoas autorizadas, estando armazenada, em processamento ou em trânsito. Captura de dados sigilosos através da rede ou acesso não autorizado a um banco de dados são possíveis ataques contra a confidencialidade de um sistema, passíveis de serem combatidos através da implementação de políticas de controle de acesso e mecanismos de criptografia.

Integridade é a propriedade que visa garantir a manutenção das características originais de uma informação, em conteúdo ou legitimidade. Trata-se de garantir que os dados em uso são provenientes de uma fonte confiável e que os mesmos não foram alterados de forma ilícita. Interceptações de transferências bancárias e alterações de seus valores e destino são ataques que envolvem a integridade da informação. Estes ataques podem ser combatidos com a implementação de resumos criptográficos digitalmente assinados, recursos que garantem a integridade e autenticidade da informação.

Disponibilidade é a propriedade que objetiva garantir o pronto acesso às informações e recursos de um sistema a usuários devidamente autorizados. Ataques de negação de serviço são muito comuns para afetar a disponibilidade de sistemas,

podendo ser combatidos através do uso de sistemas de detecção de intrusão e firewalls.

A tríade CID forma o conjunto das principais características que gestores de segurança devem providenciar para seus ambientes computacionais. Suas implementações visam o combate contra os principais ataques a sistemas de informação, podendo estes ser passivos, em forma de capturas e monitoramento de tráfego, ou ativos, com alterações de mensagens ou indisponibilização de serviços aos usuários.

### 2.2.2 Criptografia e autenticação

Criptografia é a área de estudo sobre a transformação reversível de mensagens de texto claro em conteúdos incompreensíveis. Este recurso é utilizado para armazenamento e transmissão de informações sigilosas, garantindo a sua confidencialidade e autenticidade.

A criptografia simétrica é o modelo mais utilizado para transferências de dados, pois utiliza algoritmos simples e processamento eficiente para tratar grandes volumes de dados sem ocasionar atrasos. Conforme ilustrado na Figura 4, seu processo consiste na implementação de algoritmos de cifragem e decifragem que utilizam uma mesma chave secreta, pré-compartilhada entre o emissor e o destinatário, para ocultar a mensagem original em seu caminho.

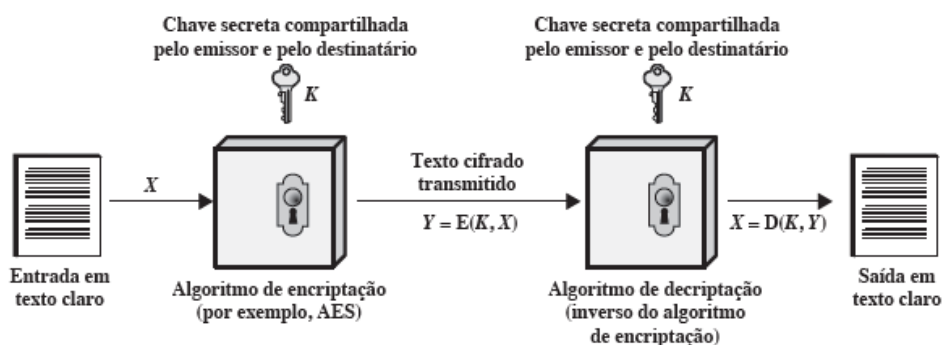


Figura 4 - Modelo simplificado de criptografia simétrica

Fonte: Stallings (2014)

Segundo Stallings (2014), existem dois requisitos para o uso seguro do modelo de criptografia simétrica:

1. O algoritmo de cifragem deve ser forte o suficiente para que um agente malicioso que possua diversos textos cifrados e seus respectivos textos claros não consiga decifrar novas mensagens ou descobrir a chave utilizada.
2. Tanto o emissor quanto o receptor precisam obter e armazenar a chave de maneira segura, uma vez que o seu vazamento permitirá a decifragem de toda a comunicação por terceiros.

Existem diferentes métodos para compartilhamento de chaves entre dois indivíduos, sendo mais comum a utilização do algoritmo Diffie Hellman com suas variantes e a utilização de criptografia assimétrica.

Criptografia assimétrica é implementada através de algoritmos que utilizam pares de chaves para cifrar e decifrar mensagens, sendo que uma chave cifra apenas o que o seu par correspondente consegue decifrar. O processo se dá com cada usuário gerando um par de chaves a ser utilizado na cifragem e decifragem de suas mensagens, disponibilizando uma delas publicamente e a outra armazenando de forma privada. Caso um usuário deseje enviar uma mensagem confidencial para o outro, basta cifrá-la com a chave pública do destinatário, pois apenas ele tem conhecimento da chave privada que poderá decifrá-la. Da mesma forma é possível garantir a autenticação sobre uma mensagem, cifrando a mesma com a sua própria chave privada, dessa forma o destino poderá decifrar a mensagem utilizando a chave pública da origem, tendo a garantia de que apenas o dono da chave privada poderia ter cifrado a mensagem (STALLINGS, 2014, p.202).

A Figura 5 ilustra o processo de envio de uma mensagem de forma a garantir tanto confidencialidade quanto autenticação, utilizando para isso os dois processos descritos anteriormente.

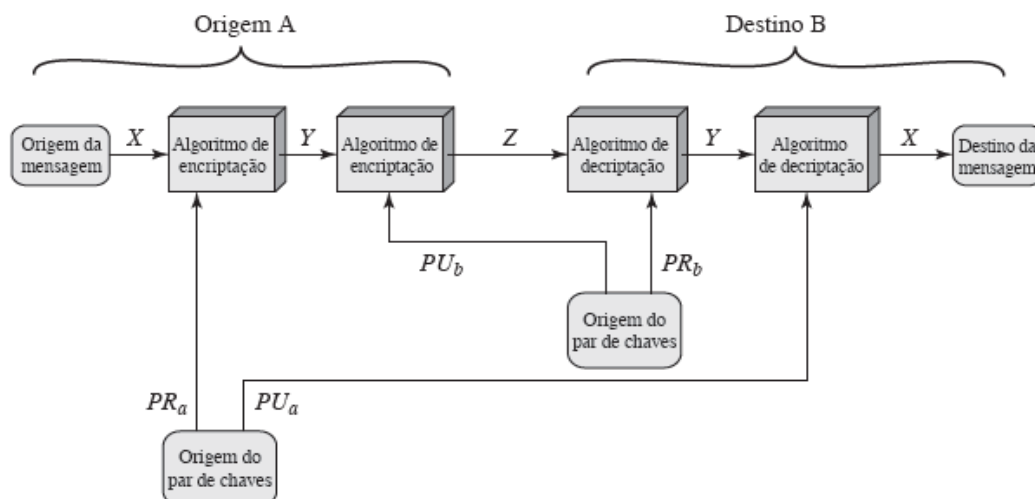


Figura 5 - Criptossistema de chave assimétrica: autenticação e sigilo

Fonte: Stallings (2014)

Ristic (2016, p.30) cita em suas recomendações de segurança para implantação básica de mecanismos de criptografia e autenticação o uso do algoritmo AES GCM para criptografia simétrica, uma vez que provê a melhor segurança oferecida pelo protocolo TLS 1.2. Cita ainda o interesse por utilizar chaves de 128 bits, pois possui segurança adequada para a maioria dos sistemas sem causar a perda de desempenho. Para autenticação, Ristic indica a utilização do algoritmo ECDSA, por ser mais rápido que o RSA, porém alerta não ser implementado por qualquer dispositivo, sendo o RSA mais comum.

### 2.2.3 Assinatura Digital

Assinaturas digitais são mecanismos utilizados para garantir a autenticidade e integridade de documentos ou mensagens digitais. Assim como assinaturas convencionais, ela é utilizada para afirmar quem foi o responsável pela geração e envio de uma informação, adicionando ainda a garantia de que não houve posterior alteração da mensagem.

O processo de assinatura digital sobre um documento ou bloco de dados qualquer consiste em duas etapas, conforme mostrado na Figura 6: a geração de um resumo hash criptográfico sobre a mensagem e em seguida a criptografia deste hash utilizando a chave privada do emissor.

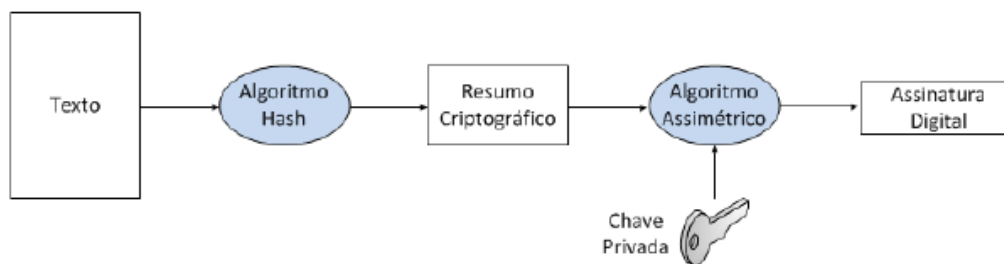


Figura 6 - Esquema simplificado de assinatura digital

Fonte: Santos (2013)

A utilização de algoritmo de hash possui duas finalidades, primeiramente pelo fato da criptografia assimétrica não possuir eficiência adequada para grandes quantidades de dados, fazendo do hash assim uma quantidade menor, porém suficiente de dados a serem criptografados. A segunda finalidade do uso de hash é a adição da garantia de integridade sobre a mensagem, uma vez que o receptor poderá comparar o resumo contido na assinatura da origem com o resumo que ele mesmo gera sobre a mensagem recebida.

A utilização de criptografia assimétrica garante a autenticidade do documento, pois uma vez que o hash foi cifrado com a chave privada do emissor, o receptor saberá que ninguém além dele foi quem gerou a mensagem (SANTOS, 2013).

#### 2.2.4 Certificados Digitais

Certificados Digitais são arquivos que possuem a principal finalidade de armazenar uma chave pública e associá-la ao seu proprietário. Como chaves públicas são cruciais em protocolos de comunicação segura, possibilitando recursos de criptografia e autenticação, sua legitimidade deve ser garantida.

A autenticidade de um certificado digital é garantida através da assinatura digital de seus dados por uma terceira parte confiável, chamada de autoridade certificadora (CA, do inglês *Certification Authority*), geralmente agências públicas ou instituições financeiras de confiança. Estas instituições são credenciadas a gerar certificados digitais para qualquer solicitante e assiná-los através da sua própria chave privada. A Figura 7 demonstra o processo de assinatura e validação de um certificado digital.

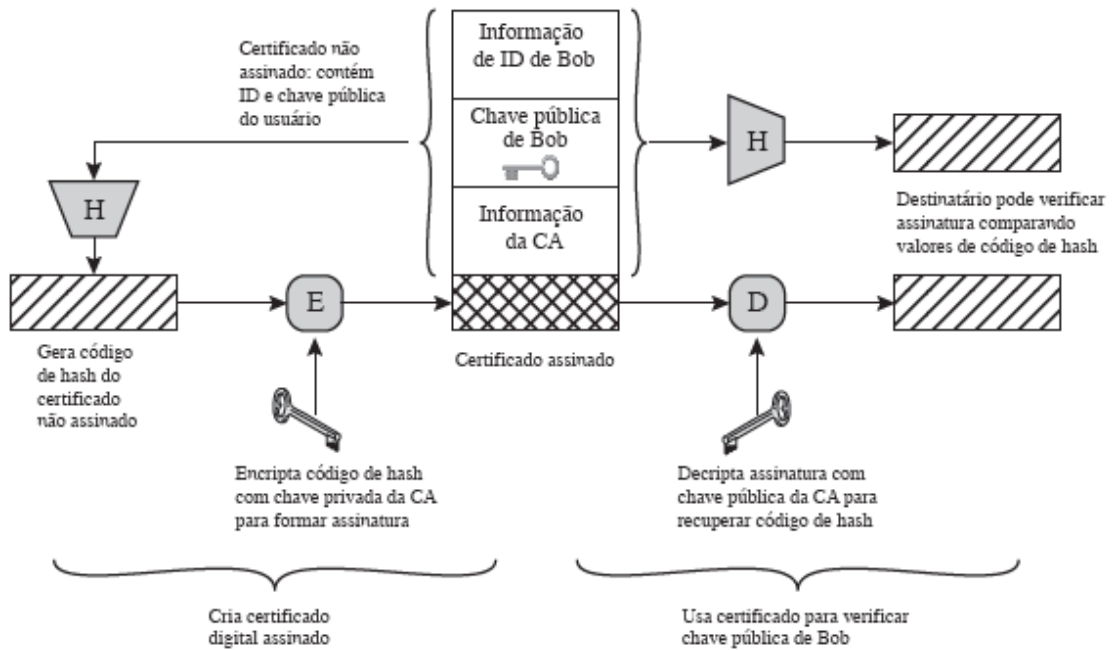


Figura 7 - Assinatura e validação de um certificado digital

Fonte: Stallings (2014)

Como apresentado na Figura 7, o certificado possui campos relacionados à identificação do proprietário, a sua chave pública e informações relacionadas à CA que está emitindo o certificado. Em seguida, para garantir a sua autenticidade, a CA gera um resumo hash destes dados, criptografa esse hash utilizando sua chave privada e anexa esta informação ao arquivo do próprio certificado. A sua posterior validação pelas entidades que desejam utilizar o seu conteúdo é realizada com a decifração do bloco de assinatura utilizando a chave pública da CA, a geração do mesmo resumo hash dos dados não cifrados, e então a comparação dos dois resumos hash. Caso os resumos sejam iguais, o certificado é válido, ou seja, não houve fraude ou perda de dados sobre seu conteúdo (STALLINGS, 2014).

Como visto, para o processo de validação de um certificado é necessário ter posse da chave pública da CA que o emitiu. Assim como os seus clientes, a CA também armazena sua chave pública através de certificado assinado por outra CA acima dela, portanto para funcionamento desta infraestrutura de certificação existe uma cadeia de Autoridades Certificadoras em formato hierárquico, onde a CA raiz gera o certificado digital da CA abaixo dela na hierarquia, e assim sucessivamente até alcançar os usuários que apenas precisam do certificado para utilização própria.

Além das Autoridades Certificadoras, instituições que geram os certificados, existem também as Autoridades de Registro (RA, do inglês *Registration Authority*),

que são instituições que recebem as solicitações de certificado digital e validam os dados de identificação do solicitante, como CPF no caso de pessoas físicas e CNPJ no caso de pessoa jurídica. Importante frisar que qualquer instituição pode gerar certificados como uma CA, porém há uma lista de Autoridades Certificadoras confiáveis, que são instituições credenciadas e auditadas por órgãos reguladores para que mantenham todas as políticas de segurança necessárias.

Segundo Stallings (2014) apud RFC 4949, o conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerenciar, armazenar, distribuir e revogar certificados digitais constitui uma Infraestrutura de Chave Pública (ICP), ou do inglês *Public-Key Infrastructure - PKI*, sendo seu principal objetivo permitir a aquisição segura, conveniente e eficiente de chaves públicas. O Instituto Nacional de Tecnologia da Informação (ITI) é o órgão federal brasileiro responsável por manter e auditar a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), sendo ele a AC-Raiz da cadeia de Autoridades Certificadoras regulamentadas (ITI, 2017).

Durante o processo de validação de certificado por um agente que precisa de sua chave pública, é importante a verificação da sua data de expiração e se o mesmo não foi revogado, ou seja, já foi um certificado válido em algum momento, porém não é mais garantido pela CA que o gerou. Stallings (2014) cita os motivos pelos quais certificados podem ser revogados:

- A chave privada do usuário foi comprometida;
- O certificado da CA foi comprometido;
- O proprietário deixou de ser certificado pela CA, por motivos de mudança de nome, quebra de requisitos de segurança exigidos pela CA, ou houve a substituição do certificado.

Cada CA é responsável por manter e disponibilizar uma Lista de Certificados Revogados (LCR) que ela tenha gerado. Esta lista deve conter a identificação da CA emissora, a data que a lista foi criada, a data da próxima lista que será emitida, e para cada certificado revogado deve haver o registro do seu número de série e a data da revogação (STALLINGS, 2014).

Santos (2013) cita que a verificação de certificados revogados pode ser realizada pelos usuários através da consulta da LCR inteira, disponibilizada pela CA,



ou através da consulta *online* a servidores da CA que forneçam o estado de um certificado através do protocolo OCSP (*Online Certificate Status Protocol*).

O padrão de certificado atualmente utilizado pelos principais protocolos de segurança é o X.509 versão 3. Ele é baseado no uso de criptografia de chave pública e assinaturas digitais, sem exigência de algoritmo específico, porém com recomendação de uso do RSA sobre o hash dos dados para sua assinatura. Os campos que compõem um certificado X.509 e uma lista de revogação são apresentados na Figura 8.

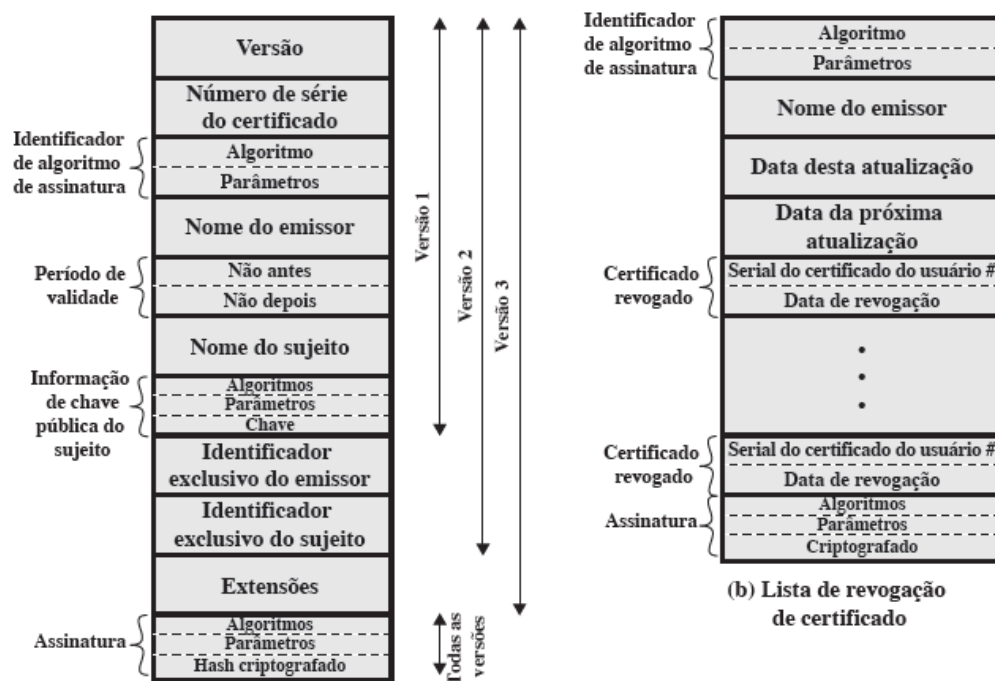


Figura 8 - Certificado digital formato X.509

Fonte: Stallings (2014)

Conforme apresentado na Figura 8, um certificado possui os seguintes campos:

- **Versão:** diferencia as versões do certificado, sendo 1 o default, 2 caso contenha o identificador do emissor ou do sujeito, e 3 caso contenha alguma extensão;
- **Número de série:** identificador único do certificado para a CA emissora;
- **Algoritmo de assinatura:** algoritmo e seus parâmetros utilizados na assinatura do certificado;
- **Nome do emissor:** nome da CA que criou e assinou o certificado;

- **Período de validade:** data de início e fim em que o certificado é considerado válido;
- **Nome do sujeito:** nome do usuário a quem o certificado se refere, dono da chave pública;
- **Chave pública do sujeito:** chave propriamente dita do proprietário do usuário, adicionada da informação do protocolo a ser utilizado para uso da mesma e parâmetros associados;
- **Id exclusivo do emissor:** código identificador único da CA, sendo opcional, para o caso de haver mais de uma CA com o mesmo nome;
- **Id exclusivo do sujeito:** código identificador único do sujeito (proprietário), sendo opcional, para o caso de haver mais de um sujeito com o mesmo nome;
- **Extensões:** conjuntos de um ou mais campos adicionados na versão 3 do protocolo. Esses campos possuem categorias, porém não são fixos como os demais que fazem a base deste padrão;
- **Assinatura:** código hash de todos os campos anteriores, sendo cifrado com a chave privada da CA. Inclui-se o algoritmo utilizado para assinatura.

A ICP-Brasil emite essencialmente duas categorias de certificado, sendo o tipo A utilizado para fins de autenticação, como sistemas de e-mail, VPN e documentos eletrônicos, e o tipo S, utilizado para atividades sigilosas como proteção de arquivos confidenciais e documentos. As duas categorias são subdivididas em 4 tipos, diferenciadas pelo processo de geração, o tipo de mídia que armazena o certificado e o prazo de validade do mesmo. As mais comuns são do tipo A1 e A3. Certificados A1 são gerados por software, armazenados em arquivos digitais, podendo ser depositados em diretórios comuns de qualquer sistema de arquivos, e são válidos por um ano. Já os certificados A3 são gerados por hardware, são armazenados em *SmartCards* ou *tokens*, e possuem duração de 3 anos. Aplicações comuns de certificados A1 são para uso de aplicações web, onde os certificados ficam em diretórios do próprio servidor, já certificados A3 são comuns para realização de assinaturas digitais de pessoas físicas, como em processos eletrônicos.

### 2.2.5 TLS

TLS (*Transport Layer Security*) é um protocolo cujo objetivo é prover confidencialidade e integridade para a comunicação entre duas aplicações através da rede de computadores. Padronizado pela IETF, sucede o protocolo SSL (*Secure Sockets Layer*) e está hoje em sua versão 1.2, documentado através da RFC 5246. Muito utilizado para transferência de dados sigilosos, como envios de email, logins e conversas privadas, o protocolo garante privacidade e integridade através do uso de criptografia simétrica, algoritmos de MAC e autenticação. Todos os parâmetros de sessão são negociados através de um *handshake* realizado na inicialização do protocolo, onde os algoritmos de criptografia, troca de chaves, integridade e autenticação são definidos. O *handshake* pode ser estabelecido em três níveis: normal, mútuo e resumido. O *handshake* simples requer autenticação apenas por parte do servidor, que envia o seu certificado digital para o cliente, já o *handshake* mútuo envolve a autenticação tanto do servidor quanto do cliente, com a troca de seus certificados. O *handshake* resumido é uma retomada de conexão realizada anteriormente, sem a necessidade de fazer novamente a autenticação entre as partes, reduzindo o tempo de processamento e podendo ser usada para recursos de *single sign-on*, ou logins unificados.

Hsieh e Leu (2017) descrevem o fluxo do *handshake* mútuo realizado pelo protocolo TLS, desde a requisição de comunicação pelo cliente até o início da troca de dados de forma criptografada com o servidor.

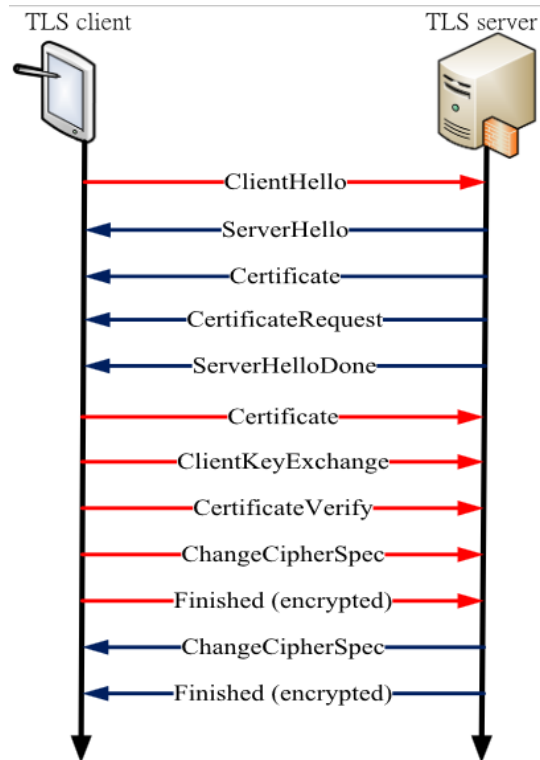


Figura 9 - Handshake TLS mútuo

Fonte: Hsieh e Leu (2017)

Conforme apresentado na Figura 9, inicialmente o cliente envia ao servidor uma mensagem “ClientHello”, contendo a versão do protocolo TLS, os algoritmos de compressão e a lista de *ciphersuites* que suporta, sendo cada *ciphersuite* um conjunto de parâmetros para criptografia, autenticação e integridade a ser utilizada na comunicação. Para proteção contra ataques de replay, também é enviado um número aleatório e o timestamp da mensagem.

Recebendo a mensagem, o servidor verifica se suporta a versão o protocolo, escolhe o algoritmo de compressão e a *ciphersuite* dentre as opções passadas pelo cliente. Em seguida retorna para o cliente a mensagem “ServerHello” com as informações dos parâmetros selecionados, adicionando também um número aleatório e o timestamp.

Em seguida, o servidor envia para o cliente o seu certificado digital, contendo sua chave pública, e solicita ao cliente que envie o seu certificado. Feito isto, indica a finalização da fase de negociação de parâmetros enviando a mensagem “ServerHelloDone” para o cliente.

Ao receber a requisição de certificado do servidor, o cliente envia seu certificado, contendo sua chave pública, garantindo assim a autenticação mútua entre

as partes. Caso o *handshake* não seja mútuo, apenas o certificado do servidor é passado para o cliente.

De posse do certificado do servidor, o cliente verifica a autenticidade do mesmo e, sendo este válido, utiliza a chave pública contida no certificado para cifrar uma chave prévia de sessão, referenciada geralmente como “*premastersecret*”. O cliente então envia esta chave prévia para o servidor através da mensagem “*ClientKeyExchange*”, e em seguida uma mensagem “*CertificateVerify*” com um valor derivado de todas as mensagens anteriores assinada com a sua chave privada. O servidor, contendo o certificado do cliente, verifica então a sua autenticidade e decifra a chave prévia de sessão recebida utilizando a chave pública do cliente.

Possuindo a chave prévia de sessão, tanto o cliente quanto o servidor utilizam esta chave em conjunto com o número aleatório passado no início do protocolo para calcular a chave definitiva, chamada de “*master\_secret*”, que será usada como parâmetro para a geração das chaves simétricas de autenticação e criptografia.

Ambas as partes então finalizam o *handshake* enviando as mensagens “*ChangeCipherSpec*”, informando que deste ponto em diante toda a comunicação será realizada utilizando os algoritmos negociados, e “*Finish*”, com o resumo das mensagens anteriores de forma já criptografada.

As principais informações trocadas em um *handshake* TLS estão contidas na ciphersuite negociada entre cliente e servidor, nela encontram-se os algoritmos de segurança a serem utilizados durante a transferência de dados entre as aplicações. As *ciphersuites* são representadas por strings concatenadas em sequência, descrevendo os algoritmos de troca de chaves, de criptografia, de MAC e hash, conforme o seguinte exemplo: TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256. Neste caso é definido que o algoritmo de troca de chaves será o ECDHE (variação de Diffie Hellman), com autenticação provida pelo RSA, o algoritmo de criptografia será o AES com 128 bits de chave no modo GCM, e a integridade/autenticação será realizada através de MAC utilizando internamente um hash SHA256.

### 2.2.6 IPSEC

IPSEC é um mecanismo de segurança utilizado para garantir autenticação, confidencialidade e gerenciamento de chaves na camada 3, ou seja, a camada IP,

sendo projetado para utilização tanto em redes IPv4 quanto IPv6. Entre suas aplicações, está o estabelecimento de Redes Virtuais Privadas (VPN), conexões remotas seguras, e adição de uma camada de segurança para provedores de serviço.

O IPSec permite a utilização de dois protocolos para fornecimento de segurança, o Authentication Header (AH), especificado pela RFC 4302, utilizado para autenticação de cabeçalhos, e Encapsulating Security Payload (ESP), especificado pela RFC 4302, utilizado para cifragem e autenticação. Segundo Stallings (2014, p.496), como o ESP fornece serviço de autenticação, o uso de AH é desaconselhado, estando ainda presente apenas por questões de compatibilidade.

O IPSec pode operar em dois modos: transporte e túnel. O modo transporte oferece segurança para os dados provenientes das camadas acima do IP, ou seja, é aplicado sobre o payload de um pacote IP, excluindo o seu cabeçalho. Portanto dados das aplicações, sessões e transporte são protegidas, mas o cabeçalho IP permanece visível. Este modo é principalmente utilizado quando implementado em dispositivos finais e provedores de serviço. O modo túnel, diferente do transporte, aplica a criptografia e autenticação sobre todo o pacote IP, incluindo seu cabeçalho. Como neste modo o ESP criptografa o cabeçalho IP, ele gera um novo cabeçalho de camada 3, permitindo ainda alterar as suas informações, como diferentes endereços IP de origem e destino, dando-lhe maior poder de segurança sobre o seu roteamento, não podendo nenhum roteador intermediário verificar o cabeçalho IP interno. O modo túnel geralmente é utilizado para comunicação entre roteadores ou firewalls, interligando segmentos de rede. Desta forma, as aplicações internas às redes não precisarão se preocupar com protocolos de segurança para trafegar pela Internet. Caso uma aplicação já implemente algum protocolo de segurança, o firewall poderá identificar e não aplicar o ESP sobre seus pacotes, realizando assim o *bypass* e economizando processamento (STALLINGS, 2014). A Figura 10 apresenta um ambiente no qual a utilização do IPSec garantiria proteção a um usuário fora da rede interna.

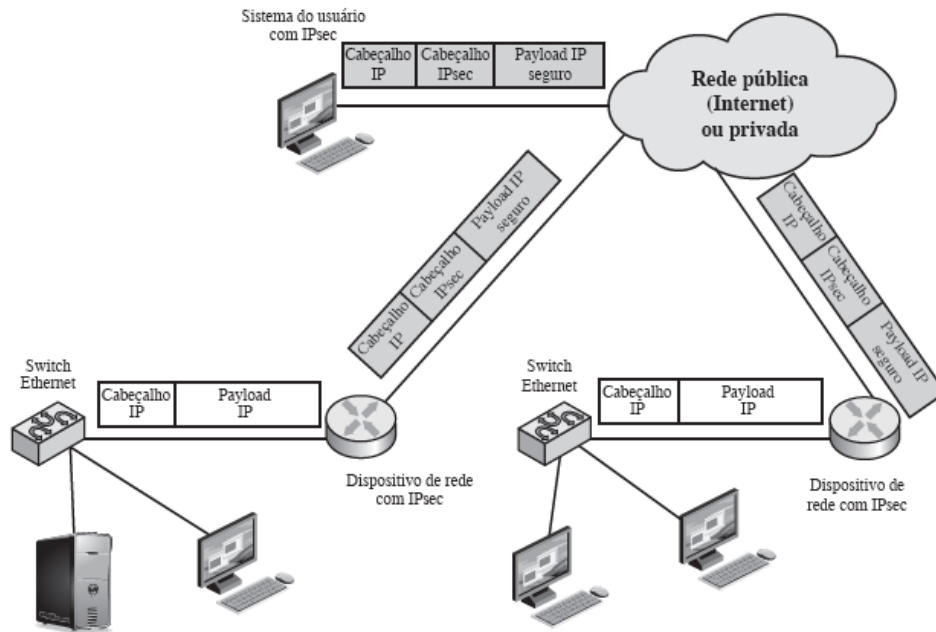


Figura 10 - Cenário de utilização de IPsec

Fonte: Stallings (2014)

## 2.3 SEGURANÇA EM TELEFONIA IP

O avanço da telefonia para a tecnologia VoIP trouxe consigo muitas vantagens, porém a convergência de tecnologia impacta no compartilhamento de vulnerabilidades. A utilização de uma rede IP traz para o VoIP ameaças que até então não existiam na telefonia convencional, tornando-a alvo tanto de ataques comuns de uma rede de dados quanto ataques direcionados ao serviço de voz.

Este capítulo descreve ataques que afetam diretamente o funcionamento do serviço de telefonia IP, bem como medidas de proteção existentes, que reduzem as vulnerabilidades e aumentam a sua segurança.

### 2.3.1 Ameaças existentes

A seguir são descritos os principais tipos de ataques direcionados à telefonia IP, tendo como pontos de entrada geralmente a infraestrutura de rede e os equipamentos de informática utilizados.

**Eavesdropping:** é um ataque comum a rede de dados, no qual agentes maliciosos encontram acesso a um ponto da rede e realizam a captura do tráfego

através de alguma ferramenta de *sniffing*, como o Wireshark. Com este ataque os agentes passam a ter acesso total aos dados que trafegam pelo segmento da rede. No caso da telefonia IP, que realiza a transmissão de sinalização e voz sobre a rede, o atacante passa a ter o poder de monitorar chamadas telefônicas, inclusive sequenciar os pacotes de voz e convertê-los para um formato audível, utilizando para isso um software que implemente o codec em uso. Os artigos de Rehman e Abbasi (2014, p.3) e Jorge (2017, p.22) citam que este ataque possui ainda mais relevância por servir de base para realização de outros ataques como homem do meio, sequestro de registros, alteração de mensagens e spams sobre a rede de telefonia.

**Denial of Service (DoS):** negação de serviço também é um ataque proveniente da rede de dados, em que agentes maliciosos enviam uma alta carga de requisições para servidores, esgotando sua capacidade de processamento, e assim indisponibilizando os seus recursos para os usuários legítimos. Como visto anteriormente, a infraestrutura de telefonia IP é constituída por servidores que exercem funções fundamentais para o funcionamento do ambiente, como proxy de sinalização. Assim como servidores web convencionais, estes servidores também estão situados na rede e podem ser alvo de ataques de negação de serviço.

**VoIP MAC Spoofing:** trata-se da falsificação do endereço MAC de um dispositivo malicioso. Neste ataque, o agente malicioso clona o MAC de um dispositivo válido na rede e se faz passar por ele perante os demais, podendo fingir ser o servidor, *gateways* ou terminais. Este ataque lhe dá poder para monitorar comunicações, obter informações confidenciais e utilizar serviços em nome de outro usuário.

**Código malicioso:** uma vez que usuários VoIP podem utilizar qualquer computador ou celular com um *softphone* para se registrar e utilizar os serviços de telefonia, os riscos que estes dispositivos possuem também alcançam o serviço de telefonia prestado. Uma vez que um computador possui um vírus, trojan ou outro código malicioso, os agentes SIP e a comunicação com o servidor VoIP podem ser manipulados.

**SQL Injection:** assim como servidores web, servidores de telefonia estão suscetíveis a injeção de SQL quando recebem informações dos clientes. Estes



ataques são realizados através da inserção de códigos SQL indesejáveis sobre as mensagens de autenticação para o servidor, que poderá executá-las e comprometer o serviço, com perdas ou alteração de tabelas do banco de dados.

**Uso indevido de recursos:** trata-se da utilização indevida dos recursos de telefonia por um agente malicioso que venha a descobrir os dados de autenticação de um usuário legítimo. Esta informação pode ser descoberta através de ataques de força bruta ou monitoramento da rede. Rehman e Abbasi (2014) citam em sua pesquisa sobre vulnerabilidades VoIP que a maior causa de vazamento de informações de usuários está na utilização de métodos fracos de autenticação, como o HTTP *Digest*, que utiliza apenas um mecanismo de hash com os dados dos usuários e uma string que é passada pelo servidor através da rede.

**Spam over Internet Telephony (SPIT):** trata-se do envio excessivo de requisições de chamadas indesejadas para um ou mais destinos, assim com existe para e-mail, porém com ainda mais frequência.

**SIP PortScan:** trata-se da varredura da rede em busca de dispositivos que respondem em portas de sinalização SIP, formando assim uma lista de possíveis alvos de outros ataques direcionados, como spams, spoofing ou monitoramento para descoberta de credenciais.

### *2.3.2 Medidas de proteção*

Como visto na seção 2.3.1, os serviços de telefonia IP estão suscetíveis a diversos ataques já comuns nas redes de dados, impactando sobre as principais propriedades da segurança: Confidencialidade, Integridade e Disponibilidade. Em seguida são descritas medidas de proteção que auxiliam no combate a estes ataques que, direta e indiretamente, podem afetar os serviços de telefonia IP.

**Criptografia do tráfego VoIP:** este é um dos principais recursos para se garantir confidencialidade em uma rede, evitando vazamento de informações, e no caso do VoIP, escutas ilegais. O estabelecimento de criptografia pode ser realizado

através de túneis VPN, com protocolos IPSec ou SSL por exemplo, que realizam a criptografia entre dois pontos independente do tráfego passante. Silva e Júnior (2013) citam em seu ambiente de testes, o uso de telefones que estabelecem túneis VPN com o servidor antes de transportarem dados de telefonia. O recurso de criptografia também pode ser implementado através de protocolos específicos para mídia, como o SRTP, e para a sinalização, como o SIP Secure.

**Autenticação eficiente de usuários:** esta é uma medida que pode aumentar a garantia de confidencialidade e disponibilidade de um sistema de telefonia IP. Rehman e Abbasi (2014, p.4) citam em seu artigo que a utilização de uma simples autenticação por HTTP *Digest* é o maior ponto vazamento de credenciais de um usuário, permitindo assim diversos ataques posteriores. Autenticações com o uso de TLS não envolvem usuário e senha e assim podem resultar em uma maior garantia de segurança.

**Segmentação do tráfego de voz:** a utilização de redes distintas para dados e voz facilita a gerência da telefonia e evita que o serviço possa ser afetado durante instabilidades ou ataques às demais redes, como SIP Scan, MAC Spoofing e negação de serviço. A separação de tráfego pode ser realizada através da configuração de VLANs nos *switches* utilizados.

VLAN (*Virtual LAN*) é um recurso documentado pelo padrão IEEE 802.1Q, utilizado para separar domínios de broadcast de forma virtual através do uso de tags identificadoras de domínios nos quadros de camada 2. Este mecanismo permite o transporte de diversas redes entre switches e a disponibilização de uma ou mais redes distintas entre suas portas (TANENBAUM, 2011).

**Controle do acesso ao segmento de voz:** recomenda-se a utilização de firewall especializado para restringir o acesso a rede onde encontram-se os servidores VoIP, permitindo requisições apenas de dispositivos legítimos que precisam se comunicar, como telefones IP da instituição. Além de firewall, pode-se também utilizar ACLs (Access Control Lists) para restringir o acesso à rede.

ACLs são regras configuradas em roteadores ou switches que permitem realizar filtros de tráfego, possibilitando, por exemplo, comunicação apenas entre IPs

e portas desejados. Este recurso é utilizado para manter redes críticas, como de servidores, mais restritas, evitando ataques e tentativas de acesso ilegítimo.

**Uso de endereços privados nos telefones IP:** esta medida reduz a possibilidade de monitoramento e ataques por agentes externos à rede. Caso o serviço precise se comunicar com a internet, o mesmo deve ser realizado através de roteamento por firewall e NAT (*Network Address Translation*).

### 2.3.3 Protocolos para segurança em VoIP

Em complemento às medidas de segurança listadas, a seguir são descritos protocolos criados e padronizados para implementar segurança sobre serviços de telefonia IP, como criptografia e autenticação adequada.

#### **SIPS**

O SIP Secure (SIPS) é uma integração entre os recursos de sinalização do SIP com a segurança fornecida pelo protocolo TLS, resultando no estabelecimento de sessões de forma segura. A troca de sinalização VoIP geralmente é transmitida sobre o protocolo UDP, porém o TLS não é aplicável sobre ele, portanto para o estabelecimento de sessões seguras é necessária a utilização do protocolo TCP para transporte, o que gera uma sobrecarga sobre o servidor proxy SIP. Para sinalizar que está tentando gerar uma comunicação segura, o SIP altera a identificação do protocolo em sua URI, ficando da seguinte forma: “sips:1234@exemplo.br” (GENEITAKIS, 2006, p.3).

A RFC 6347 descreve o DTLS (*Datagram Transport Layer Security*) como um protocolo que possibilita a criptografia de datagramas UDP. Diferente do protocolo TLS, que utiliza informações dos dados anteriores para poder cifrar ou decifrar o atual, o DTLS trata cada registro a ser cifrado ou decifrado isoladamente, contornando o impacto para perda de pacotes UDP, que não possuem retransmissão. Apesar de ser documentado por uma RFC, ele não é abordado pela documentação do SIPS, havendo apenas esboços de implementações abortados pela IETF.

A RFC 5630, que descreve a utilização do SIP Secure, cita que no uso do TLS é possível realizar autenticação apenas do servidor ou autenticação mútua com os terminais, porém este segundo processo exige a manutenção de uma infraestrutura de certificados para uma grande quantidade de usuários, sendo dificilmente aplicado.

## **SRTP**

O SRTP (*Secure Real-time Transport Protocol*) é um protocolo padronizado pela IETF através da RFC 3711 que possui o objetivo de prover segurança para tráfegos RTP (*Real-time Transport Protocol*) e RTCP (*Real-Time Transport Control Protocol*), garantindo confidencialidade, integridade, autenticação e proteção contra ataques de replay.

O SRTP trabalha intermediando a comunicação entre os dados que entram e saem da camada de aplicação e a camada de transporte, não impondo uma sobrecarga sobre os pacotes RTP, podendo assim alcançar alta taxa de transmissão e operar em ambientes heterogêneos de redes físicas ou *wireless*.

O protocolo garante a confidencialidade através do uso de criptografia simétrica, onde o algoritmo pré-definido para cifragem/decifragem é o AES no modo contador ou modo f8 (variação do modo Output Feedback - OFB). Já a autenticidade é realizada através de hash com chave sobre a mensagem enviada, sendo utilizado por padrão o algoritmo HMAC-SHA-1. Ataques de replay são evitados inserindo um índice de sequência sobre os pacotes enviados.

O método de cifragem do SRTP consiste na geração de uma chave pseudo-aleatória para cada pacote RTP, utilizando como parâmetros de entrada uma chave mestra (*MasterKey*) pré-compartilhada entre as partes, o índice de sequência do pacote RTP e a quantidade de vezes que esta sequência está se repetindo, gerando uma chave de sessão, ou *keystream*. A chave de sessão gerada é utilizada tanto para cifragem da mídia, quanto para realização da autenticação (ALEXANDER, WIJESINHA e KARNE, 2009).

A Figura 11 apresenta o processo de criptografia e autenticação realizado pelo SRTP.

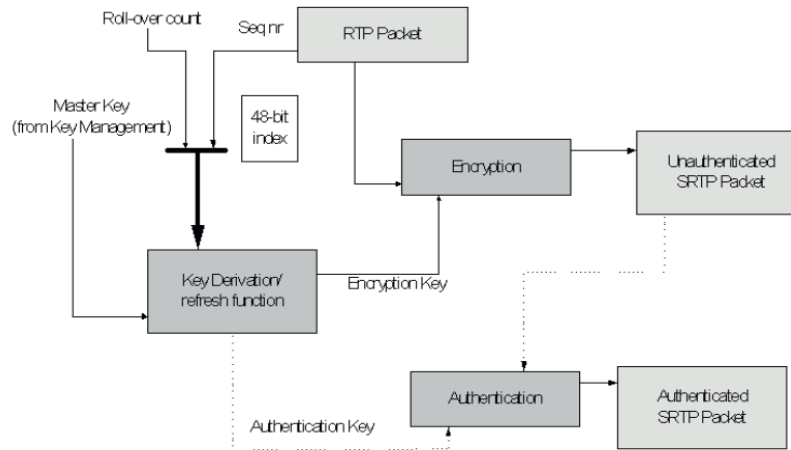


Figura 11 - Processamento SRTP

Fonte: Alexander, Wijesinha e Karne (2009)

Após passar pelo processo de cifragem o protocolo mantém o payload do pacote RTP com o mesmo tamanho e adiciona apenas dois novos campos ao pacote, sendo um campo opcional com a *masterkey* utilizada para cifragem e autenticação, e outro com a TAG resultante da autenticação do pacote. A Figura 12 apresenta o formato de um pacote SRTP, com as indicações de campos que são cifrados, campos que são autenticados, campos provenientes do RTP e campos adicionados pelo SRTP (HÉRCULES, 2014).

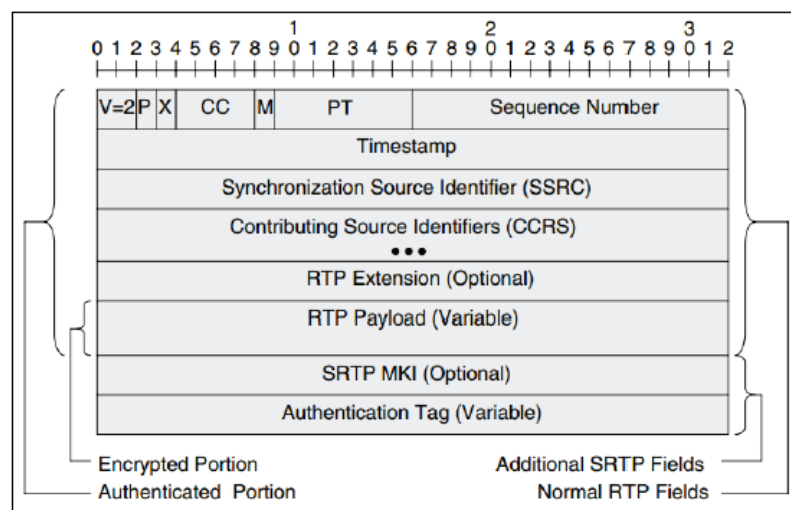


Figura 12 - Estrutura de um pacote SRTP

Fonte: Hércules (2014)

Conforme dito anteriormente, para a realização de todo o processo de criptografia e autenticação do SRTP é necessário haver uma chave pré-compartilhada

entre as entidades, porém o SRTP não especifica um protocolo para troca e gerenciamento de chaves, podendo cada aplicativo e servidor implementar um método diferente. Alguns possíveis métodos de gerenciamento de chave são o SDES (*Session Description Protocol Security Descriptions*), que transmite a chave através dos campos SDP no estabelecimento de uma sessão, o ZRTP, que negocia a chave utilizando Diffie Hellman sobre o canal de mídia, e o MIKEY (*Multimedia Internet KEYing*), estabelece um canal seguro para gerenciamento de chaves, podendo este canal ser estabelecido por uma variação de métodos, como Diffie Hellman, chaves públicas, ou chaves pré-compartilhadas. O método SDES utiliza os campos SDP durante o estabelecimento de uma sessão para o compartilhamento da chave criptográfica, sendo aconselhado neste caso a cifragem destes campos através de recursos como o TLS (ALEXANDER, WIJESINHA e KARNE, 2009).

O SRTP possibilita ainda a não utilização de criptografia e/ou autenticação, sendo passados campos “eNull” e “aNull” durante a negociação de parâmetros no início de uma chamada. A única obrigatoriedade é a utilização de autenticação nos pacotes RTCP, que realizam o controle de transferência da mídia.

## **ZRTP**

ZRTP é um protocolo padronizado pela IETF através da RFC 6189 que descreve procedimentos para acordo de chaves e criptografia para duas aplicações que desejam se comunicar através do protocolo RTP. Ele faz uso do método de Diffie Hellman para realizar a concordância de chaves e posterior uso do protocolo SRTP para realização da criptografia e autenticação das mensagens.

A diferença do ZRTP para os demais protocolos é que este realiza as operações de Diffie Hellman através do próprio fluxo de mídia RTP, tornando-se independente das sinalizações de estabelecimento de sessão (SIP, H323), de chaves pré-compartilhadas, de estrutura de chaves públicas, certificados ou qualquer sistema gerenciador de chaves.

### 3 TRABALHOS CORRELATOS

Durante o processo de pesquisa foi realizado o levantamento de temas relacionados à segurança da informação e telefonia IP, retornando alguns artigos e monografias com informações relevantes para fundamentação e desenvolvimento deste trabalho. Neles foram apresentados pontos de vulnerabilidade, potenciais ataques, mecanismos de defesa, avaliações de desempenho e estudos de caso sobre sistemas VoIP.

Rehman e Abbasi (2014) apresentam um artigo relatando uma análise de segurança do protocolo SIP sobre uma arquitetura VoIP. Tal análise foi realizada através de revisão da literatura, classificando ataques e mecanismos de defesa mais citados, e posterior execução de testes práticos de ataque sobre um servidor Asterisk. Seu estudo revela que a maioria dos ataques a ambientes VoIP foram bem sucedidos devido a deficiências do SIP, principalmente durante sua fase de autenticação no estabelecimento de sessões, com o uso comum do método HTTP *Digest*. Para combater esta vulnerabilidade, o autor propõe um esquema de autenticação de sessão utilizando o conceito de Single-Sign-On, onde os usuários SIP recebem do servidor um token criptográfico e os utilizam para posterior autenticação durante a inicialização de sessões.

Alexander, Wijesinha e Karne (2009) apresentam em seu artigo uma avaliação de desempenho do protocolo SRTP sobre chamadas VoIP, utilizando diferentes *softphones*, sistemas operacionais e parâmetros de criptografia e autenticação. Após monitoramento dos tempos de processamento, jitter e taxa de transferência para cada teste, conclui que a adição do SRTP não afeta significativamente a qualidade da voz; a autenticação é mais custosa do que a criptografia e; a utilização do SRTP aumenta em apenas 2% a taxa de transferência sobre a rede.

Silva e Júnior (2013) relatam em sua monografia a aplicação dos conceitos de segurança da informação sobre um ambiente de comunicações unificadas, focando em ambientes de telefonia IP. Os autores citam os principais ataques direcionados a telefonia IP e possíveis métodos de proteção a serem implementados para redução dos riscos. Posteriormente, os autores apresentam um estudo de caso avaliando as vulnerabilidades existentes em um ambiente com diferentes recursos de proteção,

realizando por fim o comparativo de qual rede implementa a melhor defesa contra ataques.



## 4 AMBIENTE DE ESTUDO

Este capítulo descreve o ambiente de telefonia utilizado na Universidade Federal de Santa Catarina, suas características e componentes. Em seguida são apresentadas as propostas de melhoria de segurança a serem desenvolvidas neste trabalho.

### 4.1 AMBIENTE DE TELEFONIA

O trabalho prático será aplicado no ambiente de telefonia utilizado na Universidade Federal de Santa Catarina, que possui uma rede híbrida composta por aproximadamente 5.000 ramais, sendo destes cerca de 70% IP e o restante analógicos. A infraestrutura de telefonia IP é centralizada na matriz, em Florianópolis, porém atende outros 4 campi situados nas cidades de Araranguá, Blumenau, Curitiba e Joinville.

Os principais componentes da infraestrutura de telefonia são apresentados na Figura 13 e detalhados a seguir:

- **PBX-IP Corporativa:** Servidor de registro e proxy SIP para os terminais telefônicos IP utilizados na instituição. Atua como central telefônica corporativa, gerenciando recursos como controle de privilégios, siga-me, captura de chamadas e emissão de mensagens. Existem dois servidores operando em redundância, garantindo a continuidade do serviço caso um deles fique indisponível.
- **PBX-IP Acadêmica:** Servidor de registro e proxy SIP, assim como a PBX corporativa, porém com a finalidade de servir a comunidade acadêmica (alunos, professores e servidores) através do uso de *softphones*. Sua maior vantagem é a possibilidade de gerar chamadas gratuitas para qualquer ramal da instituição.
- **SRL (SIP Router Local):** Servidor responsável por interligar todos os componentes SIP da rede (servidores e *gateways*), realizando o roteamento de

chamadas entre eles. Também trabalha em dualidade para garantir maior disponibilidade e balanceamento de carga.

- **Gateways TDM:** Equipamentos que intermediam a comunicação entre os dispositivos SIP e a telefonia convencional, realizando conexões com centrais analógicas e a PSTN.
- **Centrais legadas:** Centrais telefônicas utilizadas para gerenciamento de ramais analógicos da rede de telefonia convencional.
- **Gateways PSTN remotos:** Equipamentos situados nas unidades remotas da instituição para realizar a comunicação com a PSTN de cada cidade.
- **Fone@RNP:** Serviço de roteamento SIP fornecido pela RNP (Rede Nacional de Ensino e Pesquisa) para realização de chamadas IP com outras instituições nacionais, através da Internet.

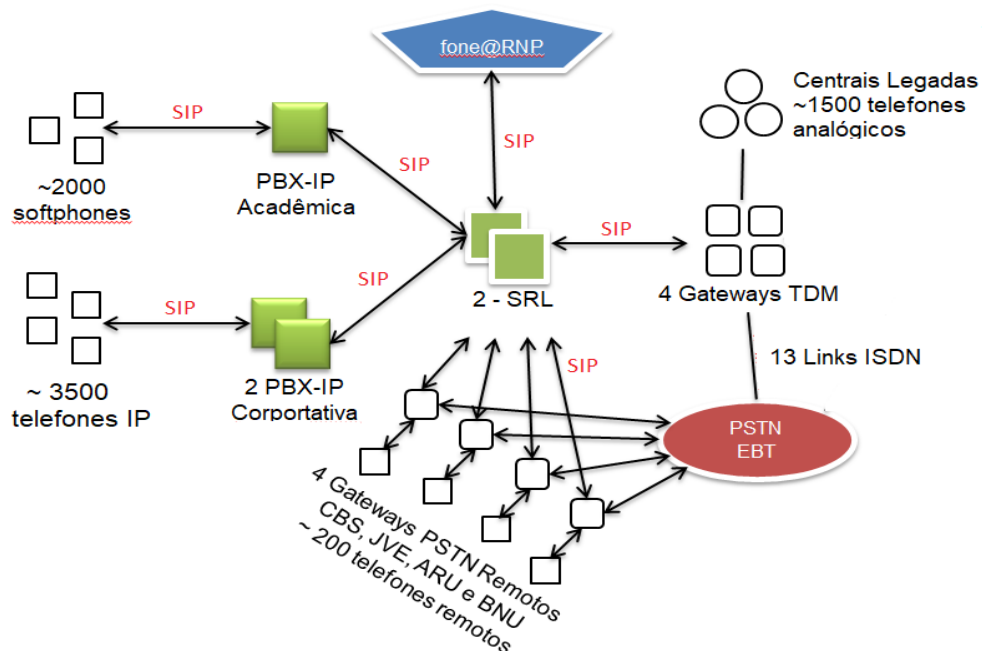


Figura 13 - Infraestrutura de telefonia da UFSC

Fonte: O autor

O serviço de telefonia IP corporativa utiliza em sua maioria telefones IP do fabricante Polycom, sendo o parque composto por cerca de 95% de aparelhos do

modelo SoundPoint 331 e VVX 201. Estes aparelhos possibilitam o download centralizado de configurações através de um servidor de provisionamento e realizam extensão da rede através de uma porta bridge, evitando a necessidade de duplicar a quantidade de pontos de rede em estações de trabalho com telefones e computadores.

O serviço de telefonia acadêmica é aberto para utilização de clientes SIP que o usuário desejar, sendo a grande maioria *softphones* instalados em computadores e smartphones, como o Zoiper, X-Lite e Linphone.

O protocolo de sinalização utilizado para estabelecimento de sessões entre os terminais telefônicos, servidores VoIP e *gateways* é o SIP, com o uso do protocolo SDP para descrição das sessões e o RTP para transmissão da voz.

#### 4.2 PROPOSTA DE TRABALHO

Tendo em vista que o serviço de telefonia acarreta em um custo financeiro para a instituição diretamente relacionado ao seu uso, através de faturas da operadora, o uso ilegal e indevido de seus recursos torna-se um fator crítico para a instituição. Foi identificado no ambiente de telefonia em estudo a utilização de protocolo HTTP para transporte de arquivos importantes entre o servidor centralizado de configurações e os terminais telefônicos, bem como a utilização do método HTTP *Digest* para autenticação dos dispositivos com o servidor, o que provê baixo grau de segurança, conforme citado no capítulo 2. Pretende-se, portanto, ampliar a segurança sobre o acesso e o transporte destas informações críticas através de criptografia e autenticação com o uso de certificados digitais, mitigando assim o uso indevido do serviço e falsificações de identidade.

O principal valor de um ambiente de telefonia está na comunicação proporcionada entre seus usuários e usuários externos, sendo que as conversas que ali trafegam podem conter informações confidenciais para as pessoas e a instituição. Uma das propostas deste trabalho é proporcionar o aumento da confidencialidade das chamadas através de criptografia da mídia, uma vez que atualmente é utilizado o protocolo RTP para transmissão de voz. Para isso serão estudados os protocolos suportados pelos dispositivos envolvidos, elaborado um ambiente de teste e avaliadas as possíveis implementações de segurança.

O serviço de telefonia é essencial para a instituição, providenciando a comunicação mínima necessária para o funcionamento de todos os serviços prestados por ela, seja para alunos, servidores ou comunidade. Sendo um serviço crítico e sensível a falhas e ataques sobre a rede, muitos autores recomendam o isolamento da rede VoIP das demais redes de dados utilizadas. Pretende-se, portanto, avaliar o atual isolamento da rede da telefonia IP sobre as demais redes da instituição e propor melhorias neste quesito de segurança, reduzindo assim riscos de indisponibilidade.

## 5 IMPLEMENTAÇÕES DE SEGURANÇA

Baseado nas propostas de trabalho descritas no capítulo 4, este capítulo apresenta as implementações de segurança desenvolvidas no ambiente de telefonia IP em estudo.

### 5.1 CRIPTOGRAFIA E AUTENTICAÇÃO PARA APROVISIONAMENTO

Como descrito no capítulo 4 do presente trabalho, o serviço de telefonia corporativa faz uso de um servidor de provisionamento para automatização do processo de configuração dos telefones IP, utilizados pela instituição. Atualmente, durante o processo de provisionamento, os dispositivos realizam o download de suas configurações através do protocolo HTTP, ou seja, em texto plano, ameaçando assim a confidencialidade destes dados, que possuem informações de identidade dos usuários e ramais. Além de uma transferência de arquivos em texto plano, foi identificada a utilização de uma autenticação baseada método *HTTP Digest* para acesso ao servidor, o que segundo autores citados nos capítulos 2 e 3 deste trabalho, é um método fraco de autenticação, baseado em usuário e senha, que se torna um ponto de vulnerabilidade do sistema.

As implementações propostas para mitigar as vulnerabilidades mencionadas e ampliar a segurança do sistema de provisionamento estão no uso de certificados digitais para criptografar os dados transferidos pela rede e tornar mais forte o método de autenticação entre os terminais telefônicos e o servidor.

A criptografia dos dados será providenciada através da alteração do protocolo HTTP por HTTPS para download de arquivos do servidor. Para isso será necessário a geração, instalação e configuração de um certificado digital no servidor web de provisionamento, sendo neste caso o Apache. Em complemento será necessário alterar o servidor DHCP da rede para que passe a direcionar a opção 160 para a nova URL de provisionamento.

A segurança de acesso aos dados também será ampliada através da implementação de TLS mútuo para autenticação dos dispositivos no servidor. Desta forma além de garantir que os terminais estão se comunicando com o servidor correto

também será garantido que o servidor está entregando os arquivos para um telefone homologado do ambiente e não para algum invasor.

### *5.1.1 Geração e instalação do certificado digital*

Para a implementação proposta neste trabalho foi solicitado um certificado digital para a AC UFSC, autoridade certificadora e de registro da universidade que possui seus certificados assinados pela ICPEDE (Infraestrutura de Chaves Públicas para Ensino e Pesquisa), que por sua vez são assinados pela autoridade certificadora GlobalSign, reconhecida mundialmente.

A ferramenta utilizada para a geração de um par de chaves para o servidor e o arquivo CSR (*Certificate Signing Request*) a ser enviado para a autoridade de registro foi o openSSL.

O primeiro passo para obtenção de um certificado digital é a geração do par de chaves pública e privada. RISTIC (2016, p.8) apresenta os parâmetros necessários para geração de um par de chaves, sendo eles:

- **Algoritmos de criptografia**, onde é indicado o uso de RSA, pois o algoritmo DSA possui limitação de tamanho da chave em 1024 bits e o ECDSA ainda não é amplamente suportado pelas CAs;
- **Tamanho da chave**, que considera 2048 bits um valor seguro, sendo uma chave menos suscetível a ataques de força bruta nos dias atuais;
- **Senha**, sendo uma palavra-chave utilizada para acesso posterior ao conteúdo do arquivo com a chave privada, muitas vezes habilitado para testes e homologações, mas posteriormente desabilitado para o servidor de produção.

A Figura 14 apresenta o processo de geração de um par de chaves utilizando os parâmetros citados.

```

root@pbx-homologa:/home/vitor/seg#
root@pbx-homologa:/home/vitor/seg# openssl genrsa -aes128 -out voip.ufsc.br.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
Enter pass phrase for voip.ufsc.br.key:
Verifying - Enter pass phrase for voip.ufsc.br.key:
root@pbx-homologa:/home/vitor/seg#
root@pbx-homologa:/home/vitor/seg#

```

Figura 14 - Geração do par de chaves assimétricas com o openssl

Fonte: O autor

Após criado o par de chaves, é necessária a geração de um arquivo CSR contendo os dados da instituição, domínio do endereço a ser acessado e a chave pública gerada anteriormente, sendo este arquivo o modelo formal de solicitação de certificado para autoridades de registro. A Figura 15 apresenta a geração do arquivo CSR utilizando a ferramenta openssl.

```

root@pbx-homologa:/home/vitor/seg#
root@pbx-homologa:/home/vitor/seg# openssl req -new -key voip.ufsc.br.key -out voip.ufsc.br.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:BR
State or Province Name (full name) [Some-State]:Santa Catarina
Locality Name (eg, city) []:Florianopolis
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UNIVERSIDADE FEDERAL DE SANTA CATARINA
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:*.voip.ufsc.br
Email Address []:.

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
root@pbx-homologa:/home/vitor/seg#
root@pbx-homologa:/home/vitor/seg#

```

Figura 15 - Geração do arquivo CSR com o OpenSSL

Fonte: O autor

O campo CN (*Common Name*) foi designado como \*.voip.ufsc.br, ou seja, este certificado será válido para utilização em qualquer subdomínio de voip.ufsc.br. Após os comandos apresentados, obtivemos então os arquivos de chave e CSR, conforme mostrado na Figura 16.

```

root@pbx-homologa:/home/vitor/seg# ls -l
total 8
-rw-r--r-- 1 root root 1050 Jul 17 20:50 voip.ufsc.br.csr
-rw-r--r-- 1 root root 1679 Jul 17 20:36 voip.ufsc.br.key
root@pbx-homologa:/home/vitor/seg#

```

Figura 16 - Arquivos de chave e CSR

Fonte: O autor

O arquivo CSR foi submetido para a AC UFSC e no dia seguinte foi recebido o certificado digital em formato PEM assinado pela AC raiz GlobalSign. A Figura 17 apresenta as informações gerais do certificado e a cadeia de assinaturas utilizadas até alcançar a AC raiz.

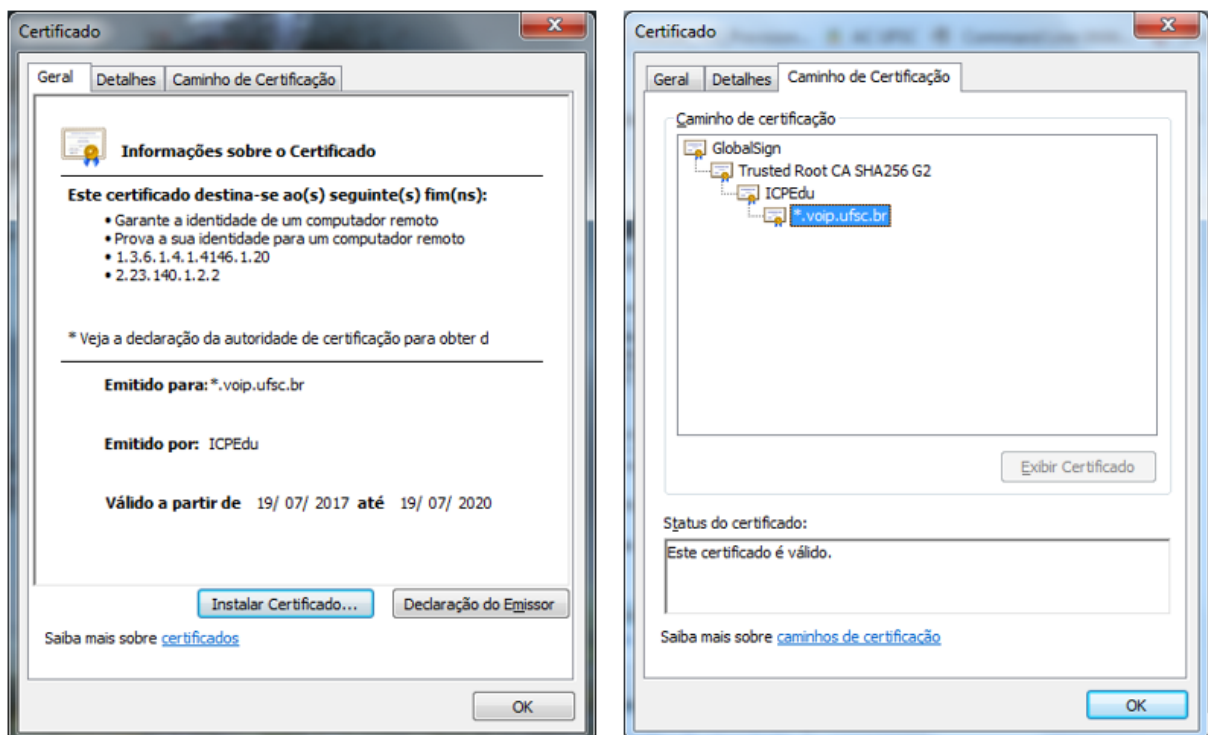


Figura 17 - Certificado utilizado no servidor

Fonte: O autor

Tendo o par de chaves e o certificado digital assinado por uma AC confiável, foi realizada a configuração do servidor web de provisionamento. Para que os telefones IP pudessem reconhecer a entidade certificadora raiz, foi necessário concatenar no mesmo arquivo PEM os certificados de toda a cadeia de assinaturas acima do certificado adquirido.



Nas configurações do Apache foi habilitado o módulo SSL e foram configurados os caminhos do certificado digital e chave privada correspondente, conforme exemplo apresentado na Figura 18.

```
SSLEngine on
SSLCertificateFile "/path/to/www.example.com.cert"
SSLCertificateKeyFile "/path/to/www.example.com.key"
```

Figura 18 - Parâmetros para ativação de SSL no apache  
Fonte: Fundação Apache (2017)

### 5.1.2 Implementação de criptografia

Os terminais telefônicos SoundPoint IP 331 e VVX 201 correspondem a cerca de 95% do total utilizado pela instituição, portanto os testes foram realizados com estes equipamentos.

Conforme apresentado no documento de atualização de certificados do fabricante para a versão de software 5.5, Polycom (2016, p. 6), utilizada nos telefones VVX, os aparelhos reconhecem o certificado da GlobalSign Root CA por padrão, portanto não houve necessidade de instalar certificado raiz nos terminais. Os aparelhos SoundPoint IP e sua versão de software 4.0 não reconhecem o certificado da GlobalSign, porém conforme o *AdminGuide* desta versão, Polycom (2011, p 280), é possível instalar o certificado da AC raiz no dispositivo e assim tornar o certificado do servidor confiável. As Figuras 19 e 20 demonstram o processo de instalação do certificado da CA no telefone através do download pela rede.



Figura 19 - Instalando certificado digital da CA no telefone SoundPoint IP

Fonte: O autor

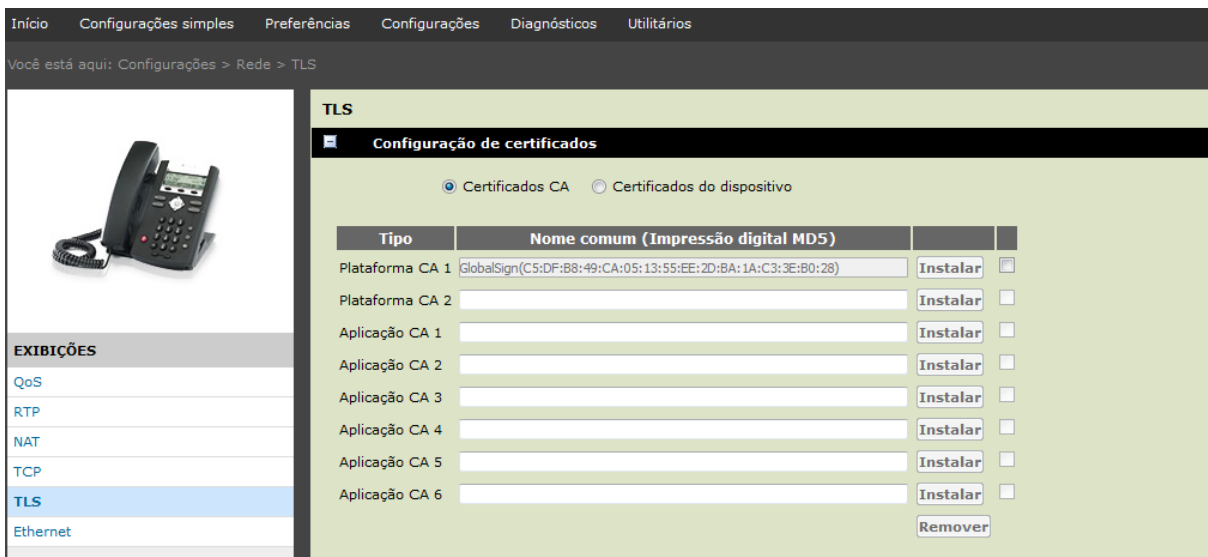


Figura 20 - Certificado digital da CA instalado no telefone SoundPoint IP

Fonte: O autor

Durante os testes de homologação foram coletados tráfegos na porta do telefone a fim de confirmar o funcionamento do *handshake* TLS e criptografia dos dados. Estes tráfegos foram analisados através da ferramenta *Wireshark*. Para apresentação dos resultados o IP do telefone foi substituído por 192.168.0.1 e o do servidor por 192.168.0.50.

A Figura 21 apresenta o tráfego de um provisionamento antes da implementação de criptografia, utilizando apenas o protocolo HTTP, sendo possível observar as requisições e respostas em texto plano.

No.	Source	Destination	Protocol	Info
3694	192.168.0.1	192.168.0.50	HTTP	GET /provisionamento-contatos/0004f...-directory.xml HTTP/1.1
3699	192.168.0.50	192.168.0.1	HTTP/XML	HTTP/1.1 200 OK
3827	192.168.0.1	192.168.0.50	HTTP	GET /0004f2... .cfg HTTP/1.1
3848	192.168.0.50	192.168.0.1	HTTP	HTTP/1.1 404 Not Found (text/html)
3911	192.168.0.1	192.168.0.50	HTTP	GET /SoundPointIPLocalization/Portuguese_Portugal/SoundPointIP-dictionary.xml HTTP/1.1

Figura 21 - Aprovisionamento sem criptografia

Fonte: O autor

Após a implantação do certificado e habilitação do HTTPS, o telefone passou a negociar os parâmetros de segurança através de um *handshake* TLS com o servidor, conforme apresentado no tráfego da Figura 22, e posteriormente transferir dados de forma criptografada.

No.	Source	Destination	Protocol	Info
839	192.168.0.1	192.168.0.50	TLSv1	Client Hello
841	192.168.0.50	192.168.0.1	TLSv1	Server Hello
844	192.168.0.50	192.168.0.1	TLSv1	Certificate, Server Hello Done
851	192.168.0.1	192.168.0.50	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
852	192.168.0.50	192.168.0.1	TLSv1	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
853	192.168.0.1	192.168.0.50	TLSv1	Encrypted Alert
854	192.168.0.50	192.168.0.1	TLSv1	Encrypted Alert

Figura 22 - Handshake TLS simples

Fonte: O autor

Para os aparelhos SoundPoint IP 331, antes de instalar o certificado da AC raiz o processo de *handshake* TLS era iniciado, porém ao receber o certificado do servidor os telefones respondiam informando não reconhecer o certificado recebido, conforme apresentado na Figura 23.

No.	Source	Destination	Protocol	Info
884	192.168.0.1	192.168.0.50	TLSv1	Client Hello
886	192.168.0.50	192.168.0.1	TLSv1	Server Hello
889	192.168.0.50	192.168.0.1	TLSv1	Certificate, Server Hello Done
892	192.168.0.1	192.168.0.50	TLSv1	Alert (Level: Fatal, Description: Unknown CA)

Figura 23 - Erro no handshake TLS, CA desconhecida

Fonte: O autor

### 5.1.3 Implementação de autenticação

Como visto nas Figuras 22 e 23, até o momento apenas o servidor envia a sua chave pública através do seu certificado digital para o telefone conferir se está se

comunicando com o interlocutor correto, porém o servidor não recebe o certificado do aparelho, o que o torna vulnerável a conexões de dispositivos indevidos. Para mitigar esta vulnerabilidade e aumentar a segurança de acesso ao servidor, foi implementado o *handshake* TLS mútuo, onde o servidor passa a autorizar acesso apenas para dispositivos que possuam certificado reconhecido.

Conforme informado no *AdminGuide* da Release 4.0, Polycom (2011, p 281), cada telefone possui um certificado digital instalado de fábrica, sendo este baseado no seu MAC e assinado pela autoridade certificadora Polycom Root CA. Como esta não é uma autoridade certificadora confiável por padrão em servidores web, é necessária a sua instalação no servidor. Conforme informado na mesma documentação do fabricante, o certificado digital da AC raiz que assina o certificado de cada aparelho é disponibilizado online através do endereço <http://pki.polycom.com>.

Após instalado o certificado da AC raiz do fabricante no servidor de provisionamento, foi configurado o Apache para solicitar o certificado a qualquer dispositivo que tente estabelecer uma conexão HTTPS, conforme parâmetros indicados na documentação online da Fundação Apache (2017), apresentados na Figura 24.

```
# require a client certificate which has to be directly  
# signed by our CA certificate in ca.crt  
SSLVerifyClient require  
SSLVerifyDepth 1  
SSLCACertificateFile "conf/ssl.crt/ca.crt"
```

Figura 24 - Parâmetros para ativação de TLS mútuo no apache

Fonte: Fundação Apache (2017)

Estando habilitado o *handshake* mútuo, foi coletado o tráfego na porta de um telefone e identificado que o servidor passou a solicitar o certificado do dispositivo que está realizando uma conexão. A Figura 25 apresenta a troca de mensagens entre o telefone e o servidor durante um *handshake* mútuo, onde o terceiro pacote mostra a solicitação de certificado pelo servidor, e o quarto pacote é a resposta do telefone enviando o seu certificado. O *handshake* ocorre normalmente até as mensagens de “EncryptedAlert”, onde cada dispositivo finaliza o *handshake* informando que deste ponto em diante passará a enviar dados criptografados.

No.	Source	Destination	Protocol	Info
987	192.168.0.1	192.168.0.50	TLSv1	Client Hello
989	192.168.0.50	192.168.0.1	TLSv1	Server Hello
992	192.168.0.50	192.168.0.1	TLSv1	Certificate, Certificate Request, Server Hello Done
1001	192.168.0.1	192.168.0.50	TLSv1	Certificate
1029	192.168.0.1	192.168.0.50	TLSv1	Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1031	192.168.0.50	192.168.0.1	TLSv1	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1033	192.168.0.1	192.168.0.50	TLSv1	Encrypted Alert
1034	192.168.0.50	192.168.0.1	TLSv1	Encrypted Alert

Figura 25 - Handshake TLS mútuo

Fonte: O autor

## 5.2 CRIPTOGRAFIA DE VOZ

A maioria dos ambientes de telefonia IP utiliza por padrão o protocolo RTP para transporte de mídia, sendo o mesmo também atualmente utilizado no ambiente de telefonia IP em estudo. Seguindo a proposta apresentada no capítulo 4, foram levantados os principais equipamentos que compõem a infraestrutura de voz sobre IP e identificado uma opção de segurança, possível de se implementar sem prejudicar a interoperabilidade.

No ambiente em estudo, toda a negociação de parâmetros de mídia é realizada entre os dispositivos VoIP finais, não havendo manipulação pelos *proxies* que estão no caminho, portanto dentro do ambiente apresentado no capítulo 4, os equipamentos que precisam estabelecer um protocolo seguro para mídia são os terminais telefônicos e os *gateways* de mídia, que realizam a conversão de mídia entre a rede IP e o ambiente TDM com as centrais analógicas e operadora.

Segundo o *AdminGuide* da versão 4.0, Polycom (2011, p. 283), o telefone SoundPoint IP disponibiliza a utilização do protocolo SRTP para criptografia de mídia, padronizado pela RFC 3711, e o processo de negociação de parâmetros de segurança seguindo a RFC 4568, que define a transmissão de atributos de segurança através de campos do protocolo SDP já utilizado pelo SIP.

Para os telefones VVX, o *AdminGuide* da versão 5.5, Polycom (2016, p. 266) também apresenta a disponibilidade do SRTP com o uso do SDP para negociação dos parâmetros de segurança.

Para os *gateways de mídia* do fabricante Audiocodes, a nota técnica de recomendações de segurança, Audiocodes (2011, p. 39) informa que os seus dispositivos também suportam as RFCs 3711 (SRTP) e 4568 (descrição de segurança através de SDP).

Havendo, portanto, a possibilidade de os três dispositivos *endpoints* IP implementarem as RFCs 3711 e 4568, será utilizado o SRTP como protocolo de criptografia de mídia e a utilização dos campos SDP para negociação de parâmetros de segurança.

Conforme descrito na própria RFC 4586, a sua implementação não garante segurança sobre os dados que insere nos campos SDP, sendo necessário para isso a utilização de outra técnica em complemento que cifre os pacotes SIP para que os parâmetros não sejam visualizados por terceiros. Esta implementação extra de segurança não está sendo abordada neste trabalho e será recomendada como trabalho futuro.

### 5.2.1 Configuração dos dispositivos

Por padrão os equipamentos responsáveis por criptografar a mídia não possuem esta funcionalidade ativa, por serem opcionais e consumirem processamento extra, porém eles possibilitam estas ativações através da configuração de alguns parâmetros. O *AdminGuide* versão 4.0, Polycom (2011, p. 284), indica quais são os parâmetros a serem configurados no telefone SoundPoint 331 para habilitação dos recursos de segurança de mídia, conforme apresentado na Figura 26.

Central Provisioning Server	template > parameter
Enable SRTP .....	sip-interop.cfg > sec.srtp.enable
Include secure media in SDP of SIP INVITE.....	sip-interop.cfg > sec.srtp.offer
Include crypto in offered SDP.....	sip-interop.cfg > sec.srtp.offer.*
Secure media stream required in all SIP INVITES .....	sip-interop.cfg > sec.srtp.require
Check tag in crypto parameter in SDP.....	sip-interop.cfg > sec.srtp.requireMatchingTag
Specify if the phone offers and/or requires: RTP encryption, RTP authentication, and RTCP encryption .....	sip-interop.cfg > sec.srtp.sessionParams.*

Figura 26 - Parâmetros para ativação do SRTP no telefone SoundPoint IP  
Fonte: Polycom (2011)

Os parâmetros de configurações podem ser alterados em arquivos XML em cada telefone ou para todos os aparelhos através do servidor de provisionamento

centralizado. A seguir, é apresentado o detalhamento de cada configuração necessária para o funcionamento do SRTP nos telefones IP.

- **SRTP Enable:** Parâmetro que habilita o telefone a aceitar as ofertas de SRTP quando recebe esta opção dentro de um INVITE de novas chamadas;
- **SRTP Offer:** Parâmetro que habilita o telefone a enviar a opção de chamada segura quando inicia uma ligação, enviando os parâmetros de segurança a serem negociados com o interlocutor através de um campo SDP do INVITE de uma nova chamada;
- **sec.srtp.offer.\*** : Parâmetro que indica quais crypto-suites serão ofertadas para o interlocutor quando iniciada uma nova chamada. As opções disponibilizadas pelo aparelho são AES\_CM\_128\_HMAC\_SHA1\_32 e AES\_CM\_128\_HMAC\_SHA1\_80, ou seja, implementam criptografia simétrica utilizando o algoritmo AES em modo contador e chave de 128 bits, podendo adicionar ao pacote SRTP tags de autenticação de 32 ou 80 bits através de HMAC-SHA1. Os campos que são cifrados e os autenticados em um pacote SRTP podem ser visualizados na Figura 12, localizada na sessão 2.3.3 deste trabalho.
- **SRTP Require:** Parâmetro que indica se o telefone irá aceitar apenas chamadas seguras ou também chamadas sem criptografia de mídia;
- **SRTP RequireMatchingTag:** Define se o aparelho irá validar se o campo tag da resposta de um INVITE é o mesmo presente em uma das opções ofertadas. Cada opção de criptografia enviada em um INVITE contém este campo identificador;
- **SessionParams:** Parâmetro que adiciona identificadores do uso de criptografia e autenticação sobre os pacotes de mídia. A princípio, apenas a autenticação sobre pacotes RTCP é obrigatória.

Para ativar o SRTP nos telefones Polycom com criptografia e autenticação, não deixando de aceitar chamadas sem oferta de segurança, os parâmetros foram configurados da seguinte forma:

```
sec.srtp.enable="1"
```

```
sec.srtp.offer="1"
```

```

sec.srtp.require="0"
sec.srtp.requireMatchingTag="1"
sec.srtp.offer.HMAC_SHA1_32="0"
sec.srtp.offer.HMAC_SHA1_80="1"
sec.srtp.sessionParams.noAuth.offer="0"
sec.srtp.sessionParams.noAuth.require="0"
sec.srtp.sessionParams.noEncrypRTCP.offer="0"
sec.srtp.sessionParams.noEncrypRTCP.require="0"
sec.srtp.sessionParams.noEncrypRTP.offer="0"
sec.srtp.sessionParams.noEncrypRTP.require="0"

```

O *AdminGuide* versão 5.5, Polycom (2016, p. 266), indica quais são os parâmetros a serem configurados no telefone VVX 201 para habilitação dos recursos de segurança de mídia. Como trata-se dos mesmos parâmetros informados para o telefone SoundPoint IP da versão 4.0, as configurações ficaram da mesma forma.

O *User'sGuide* da versão 6.4 do *gateway* Mediant 2000, Audiocodes (2011, p.438), apresenta as configurações disponíveis para ativação do SRTP em chamadas VoIP. Estas configurações podem ser realizadas através de uma interface web, conforme apresentado na Figura 27.

▼ General Media Security Settings	
⚡ Media Security	Disable ▼
Media Security Behavior	Preferable ▼
Authentication On Transmitted RTP Packets	Active ▼
Encryption On Transmitted RTP Packets	Active ▼
Encryption On Transmitted RTCP Packets	Active ▼
▼ SRTP Setting	
Master Key Identifier (MKI) Size	0
Enable symmetric MKI negotiation	Disable ▼
◆ SRTP offered Suites	
CIPHER SUITES AES CM 128 HMAC SHA1 80	<input checked="" type="checkbox"/>
CIPHER SUITES AES CM 128 HMAC SHA1 32	<input checked="" type="checkbox"/>
CIPHER SUITES ARIA CM 128 HMAC SHA1 80	<input checked="" type="checkbox"/>
CIPHER SUITES ARIA CM 192 HMAC SHA1 80	<input checked="" type="checkbox"/>

Figura 27 - Parâmetros para ativação do SRTP no gateway Mediant 2000

Fonte: Audiocodes (2011)



As configurações disponibilizadas por este equipamento são muito próximas às dos telefones IP, conforme detalhado a seguir.

**Media Security:** Habilita o recurso de segurança sobre a mídia através do SRTP;

**Media Security Behavior:** Define se o *gateway* tornará o uso de SRTP obrigatório para as chamadas ou aceitará o estabelecimento de chamadas utilizando o protocolo RTP quando o dispositivo com quem está estabelecendo uma sessão não suportar SRTP;

**Authentication On Transmitted RTP Packets:** Ativa a autenticação sobre os pacotes RTP;

**Encryption On Transmitted RTP Packets:** Ativa a criptografia sobre os pacotes RTP;

**Encryption On Transmitted RTCP Packets:** Ativa a criptografia sobre os pacotes RTCP;

**MKI Size:** MKI (Master Key Identifier) são identificadores de chave mestra possíveis de concatenar com a chave enviada no campo SDP. Utilizado para facilitar a manipulação e troca de chave caso alcance a sua vida útil. Chamadas de voz dificilmente chegam ao máximo de pacotes possíveis de cifrar por uma mesma chave, portanto este campo é mais utilizado em transmissões de vídeo. A RFC 4568, que padroniza a descrição de parâmetros de segurança sobre o SDP, apresenta este identificador como opcional. Seu tamanho pode ser de 0 a 4 bytes, valores possíveis de configurar neste campo. Caso o valor seja zero, o gateway nunca irá enviar um identificador.

**Enable symmetric MKI negotiation:** Habilita a negociação do identificador de chave mestra (MKI). Caso este campo esteja desativado, todas as chaves terão um identificador concatenado, se o tamanho selecionado no campo anterior for maior do que zero. Caso seja habilitado, o gateway irá concatenar um identificador apenas em respostas de INVITES que possuam chave mestra com identificadores.

**SRTP offered Suites:** Seleção de *crypto-suites* a serem ofertadas nos INVITES de novas chamadas geradas.

Em compatibilidade com as configurações ativadas nos telefones IP utilizados pela instituição, os parâmetros de segurança para o *gateway* ficaram com a seguinte configuração:

***Media Security: "Enable"***

***Media Security Behavior: "Preferable"***

***Authentication On Transmitted RTP Packets: "Active"***

***Encryption On Transmitted RTP Packets: "Active"***

***Encryption On Transmitted RTCP Packets: "Active"***

***MKI Size: "0"***

***Enable symmetric MKI negotiation: "Disable"***

***SRTP offered Suites: "CIPHER SUITES AES CM 128 HMAC SHA1 80"***

### 5.2.2 Testes e resultados

Para comprovar o funcionamento da implementação foram realizados testes de chamadas com a captura de tráfego sobre a porta que se encontra um telefone na rede e utilizada a ferramenta Wireshark para analisar os fluxos das chamadas. Durante os testes foram utilizados os seguintes equipamentos:

- Telefone IP VVX, apresentado com o IP 192.168.0.1 e ramal 7654;
- Telefone IP SoundPoint IP 331, apresentado com o IP 192.168.0.2 e ramal 2148;
- *Gateway de mídia* Mediant 2000, apresentado com o IP 192.168.0.10, realizando a interface com o ramal analógico 7586;
- PBX-IP, apresentada com os IPs 192.168.0.51 (virtual) e 192.168.0.52 (real).

Inicialmente foi capturado o tráfego de uma chamada da forma como ela é estabelecida atualmente, sem implementação de segurança sobre a mídia. A chamada foi gerada do telefone VVX para o SoundPoint, sem habilitação dos parâmetros de segurança. A Figura 28, obtida através da ferramenta Wireshark, apresenta o fluxo desta chamada. Nela é possível identificar cada mensagem de

estabelecimento de sessão SIP sobre o ponto de vista do telefone VVX, que está na porta onde o tráfego foi capturado.

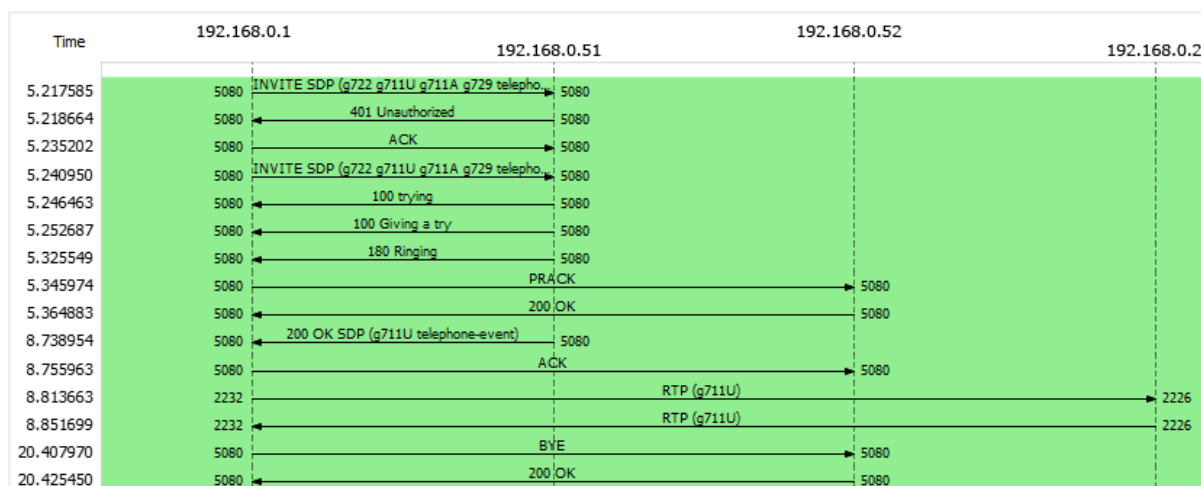


Figura 28 - Fluxo de chamada SIP utilizando RTP

Fonte: O autor

O fluxo apresentado inicia com o INVITE na primeira linha, onde são enviados os parâmetros de sessão para negociação com o destino. A Figura 29 apresenta o conteúdo SDP deste INVITE, com os valores padrão de estabelecimento de sessão, como identificação da origem, portas utilizadas, protocolo de mídia e opções de codec, porém sem os campos para descrição de parâmetros de segurança.

```

49 192.168.0.1 192.168.0.51 SIP/SDP Request: INVITE sip:2148@adm2.voip.ufsc.br;user=phone
<
> Ethernet II, Src: Polycom_85:85:85 (64:16:7f:85:85:85), Dst: IETF-VRRP-VRID_f8 (00:00:5e:00:00:08)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.51
> User Datagram Protocol, Src Port: 5080, Dst Port: 5080
v Session Initiation Protocol (INVITE)
  > Request-Line: INVITE sip:2148@adm2.voip.ufsc.br;user=phone SIP/2.0
  > Message Header
  v Message Body
    v Session Description Protocol
      Session Description Protocol Version (v): 0
      > Owner/Creator, Session Id (o): - 1505586946 1505586946 IN IP4 192.168.0.1
      Session Name (s): Polycom IP Phone
      > Connection Information (c): IN IP4 192.168.0.1
      > Time Description, active time (t): 0 0
      Session Attribute (a): sendrecv
      > Media Description, name and address (m): audio 2232 RTP/AVP 9 0 8 18 127
      > Media Attribute (a): rtpmap:9 G722/8000
      > Media Attribute (a): rtpmap:0 PCMU/8000
      > Media Attribute (a): rtpmap:8 PCMA/8000
      > Media Attribute (a): rtpmap:18 G729/8000
      > Media Attribute (a): fmp:18 annex=no
      > Media Attribute (a): rtpmap:127 telephone-event/8000

```

Figura 29 - Campos SDP de INVITE sem oferta de criptografia

Fonte: O autor

No fluxo da chamada apresentado na figura 28 também é possível identificar que o protocolo de transmissão de mídia utilizado foi o RTP, com codec G711, sem criptografia, com a troca de pacotes diretamente entre os *endpoints*. O software Wireshark, utilizado para analisar este tráfego, possui a capacidade de conversão de pacotes para fluxos de áudio, assim foi possível obter e ouvir o áudio da chamada, conforme representado graficamente na Figura 30.

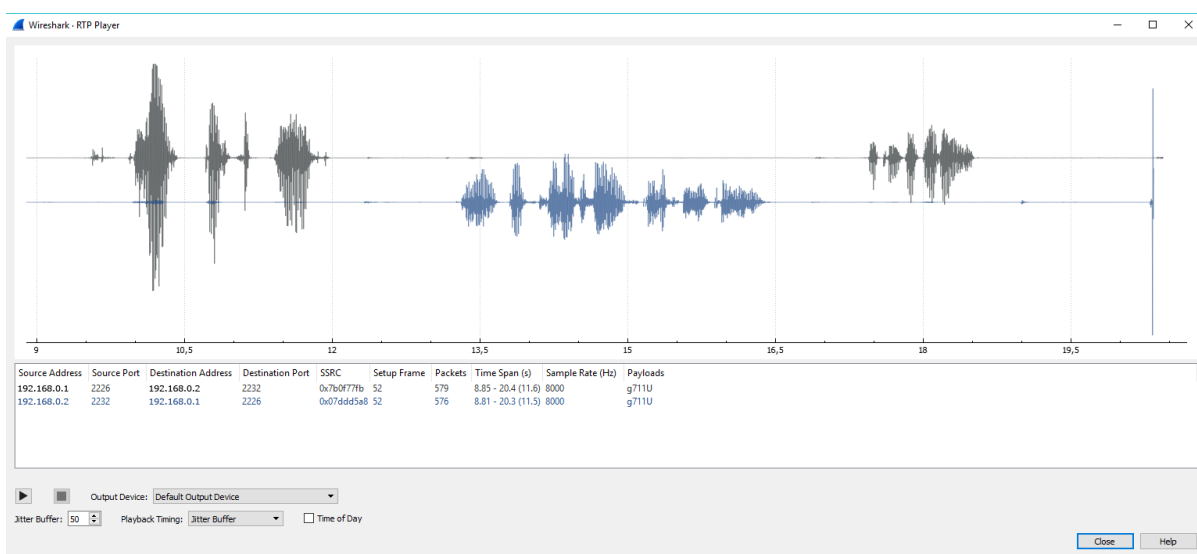


Figura 30 - Conversão do tráfego RTP em fluxo de áudio compreensível

Fonte: O autor

Uma vez analisadas as características de chamadas que trafegam no ambiente atual, foram aplicadas as configurações de segurança nos telefones IP e *gateway* e então realizados novos testes. A Figura 31 apresenta o fluxo de uma chamada realizada entre os mesmos telefones VVX e SoundPoint IP, agora com os parâmetros de segurança ativos.

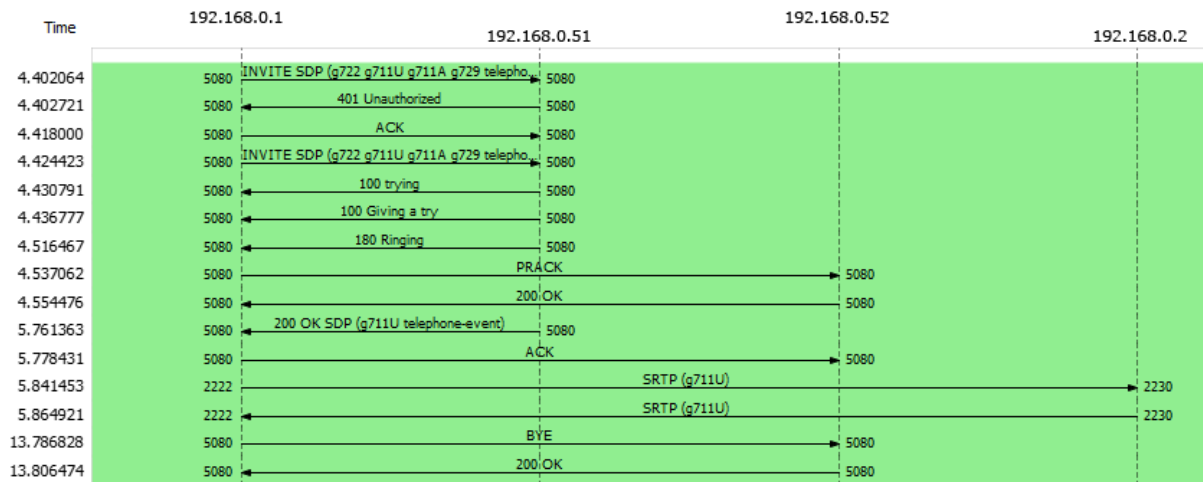


Figura 31 - Fluxo de chamada SIP utilizando SRTP

Fonte: O autor

É possível notar na Figura 31 que a própria ferramenta Wireshark identificou a utilização do protocolo SRTP e alterou a descrição do fluxo de mídia. Os parâmetros de sessão do INVITE desta chamada são apresentados na Figura 32, onde é possível identificar a oferta de dois perfis de mídia, a primeira RTP/SAVP (*Secure Audio Video Profile*) com parâmetros de criptografia, e a segunda RTP/AVP (*Audio Video Profile*), sem o campo SDP de segurança. Desta forma o destino poderá optar por aceitar uma chamada segura ou não.

```

<
> Request-Line: INVITE sip:2148@adm2.voip.ufsc.br;user=phone SIP/2.0
> Message Header
v Message Body
  v Session Description Protocol
    Session Description Protocol Version (v): 0
    > Owner/Creator, Session Id (o): - 1505592283 1505592283 IN IP4 192.168.0.1
    Session Name (s): Polycom IP Phone
    > Connection Information (c): IN IP4 192.168.0.1
    > Time Description, active time (t): 0 0
    Session Attribute (a): sendrecv
    > Media Description, name and address (m): audio 2222 RTP/SAVP 9 0 8 18 127
    > Media Attribute (a): crypto:3 AES_CM_128_HMAC_SHA1_80 inline:4AdwakUJzLH4hRbDVdX3bB2Pjgge/903c3ii/xaz
    > Media Attribute (a): rtpmap:9 G722/8000
    > Media Attribute (a): rtpmap:0 PCMU/8000
    > Media Attribute (a): rtpmap:8 PCMA/8000
    > Media Attribute (a): rtpmap:18 G729/8000
    > Media Attribute (a): fmtp:18 annexb=no
    > Media Attribute (a): rtpmap:127 telephone-event/8000
    > Media Description, name and address (m): audio 2222 RTP/AVP 9 0 8 18 127
    > Media Attribute (a): rtpmap:9 G722/8000
    > Media Attribute (a): rtpmap:0 PCMU/8000
    > Media Attribute (a): rtpmap:8 PCMA/8000
    > Media Attribute (a): rtpmap:18 G729/8000
    > Media Attribute (a): fmtp:18 annexb=no
    > Media Attribute (a): rtpmap:127 telephone-event/8000

```

Figura 32 - Campos SDP de INVITE com oferta de criptografia

Fonte: O autor

Conforme apresentado na RFC 4568, o atributo adicional no protocolo SDP para descrição de parâmetros de segurança é chamado “crypto”, e é constituído com o seguinte padrão de dados:

`a=crypto:<tag><crypto-suite><key-params> [<session-params>]`

**<tag>**: número decimal único utilizado para identificar o conjunto de atributos de segurança;

**<crypto-suite>**: identificador que descreve os algoritmos de criptografia e autenticação a ser utilizado;

**<key-params>**: armazena um ou mais parâmetros de chave de acordo com a crypto-suite associada. Geralmente carrega a chave mestra concatenada com o salt. Também pode conter o tempo de vida da chave mestra;

**<session-params>**: campo opcional que pode conter parâmetros extras como definição para desativação de criptografia e autenticação.

Após coleta do tráfego desta chamada utilizando o protocolo SRTP, foi utilizada a ferramenta Wireshark novamente para converter os pacotes de mídia em fluxo de

áudio, e o resultado foi a geração de um áudio apenas de ruído, graficamente representado pela Figura 33.

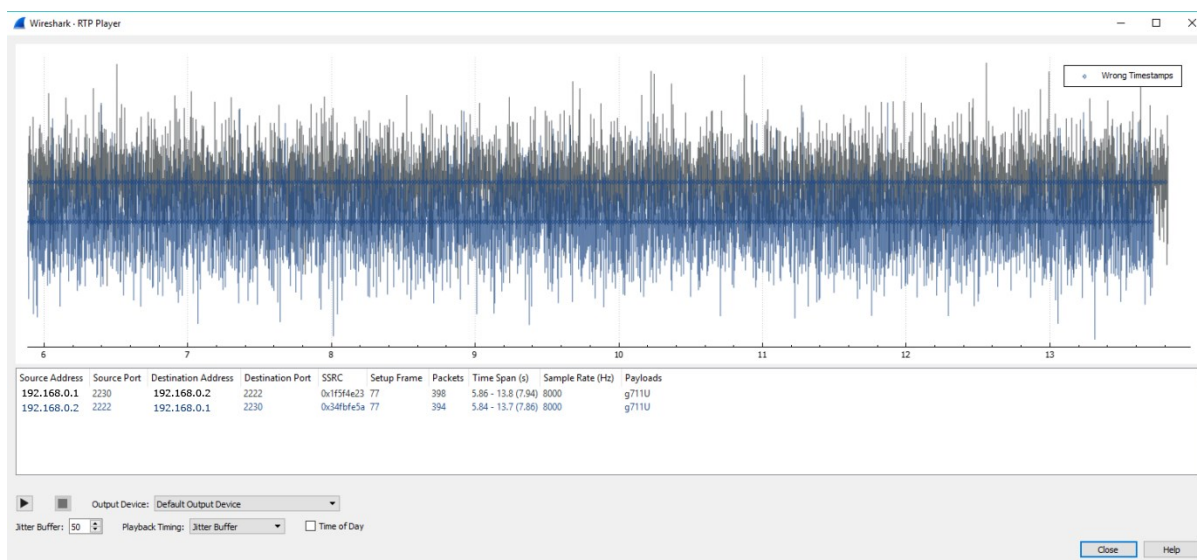


Figura 33 - Conversão do tráfego SRTP em fluxo de áudio não compreensível

Fonte: O autor

Em seguida, foram realizados testes com chamadas entre telefones IP e telefones analógicos, neste caso com o *gateway* de mídia realizando a interface entre o ambiente VoIP e o TDM. Conforme apresentado no capítulo 4, as chamadas que trafegam entre a PBX-IP e o *gateway* necessariamente passam pelo componente SRL, que além de realizar SIP *proxy*, também realiza *media proxy*, ou seja, centraliza o fluxo de mídia entre os demais componentes. Apesar da centralização de mídia, o SRL não altera características negociadas entre os terminais VoIP, como codec ou protocolo de mídia. A Figura 34 apresenta o fluxo de uma chamada VoIP gerada do telefone IP VVX para o *gateway* de mídia, e a Figura 35 apresenta uma chamada saindo do *gateway* para o telefone IP. Como o tráfego foi coletado na porta do telefone e o SRL, de IP 192.168.0.20, realiza *media proxy*, o fluxo de áudio apresentado na figura é entre o telefone IP e o SRL, porém este é apenas um intermediário, sendo o *gateway* que realiza a negociação de parâmetros de segurança.

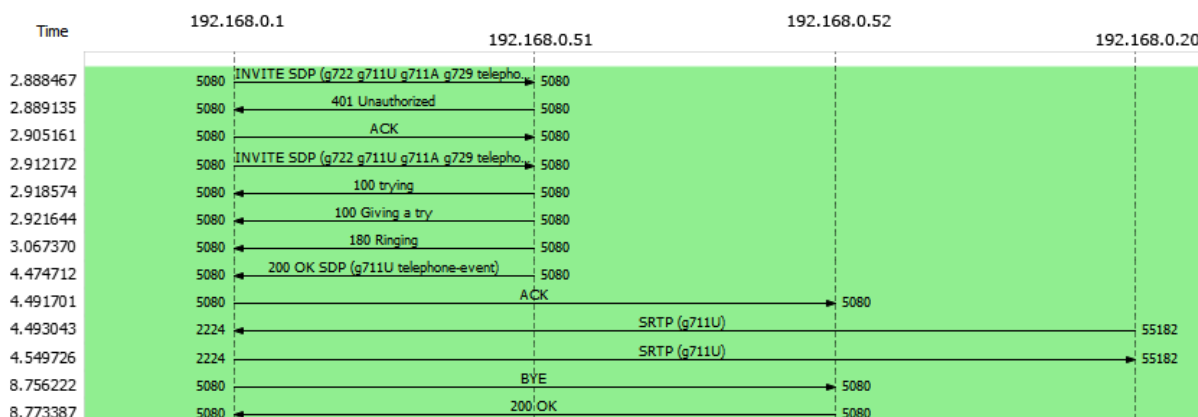


Figura 34 - Fluxo de chamada SIP utilizando SRTP - telefone IP para gateway

Fonte: O autor

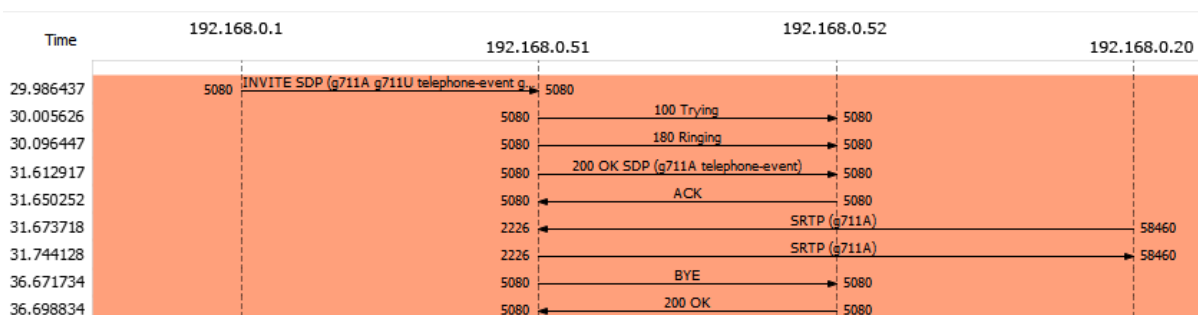


Figura 35 - Fluxo de chamada SIP utilizando SRTP - gateway para telefone IP

Fonte: O autor

Os testes entre telefones IP e gateway também foram bem sucedidos, com a mídia sendo criptografada de ponto a ponto.

### 5.3 SEGMENTAÇÃO DA REDE VOIP

Conforme apresentado no capítulo 4 deste trabalho, o ambiente de telefonia em estudo é composto por servidores, *gateways* e terminais SIP. Dentre estes componentes, os servidores e os *gateways* estão em uma rede dedicada para telefonia, utilizando ACLs para controle de acesso externo. Já os terminais telefônicos IP estão distribuídos por toda a instituição através das mesmas sub-redes de navegação utilizadas pelos computadores, sendo estas mais abertas devido à diversidade de serviços que podem acessar.

Estando os terminais VoIP em sub-redes de dados, estes apresentam maior vulnerabilidade a ataques externos. Além de estarem suscetíveis a ataques de negação de serviço, os terminais telefônicos tornam-se potenciais pontos de entrada



para agentes maliciosos ao sistema de telefonia, uma vez que são dispositivos autorizados a utilizar os recursos providos. A inserção de códigos maliciosos nos terminais pode gerar degradação do serviço, chamadas indesejadas e ainda custos financeiros para a instituição.

Busca-se, portanto, uma solução que atenda os seguintes requisitos:

- Isolar a rede dos aparelhos telefônicos IP dos demais dispositivos da rede;
- Possibilitar a restrição de acesso aos telefones baseado em IPs e portas;
- Manter o compartilhamento de portas dos switches entre telefones e computadores.

A solução encontrada que atende os requisitos mencionados é a implementação de Voice VLAN nos switches da rede. Este recurso permite distribuir uma rede dedicada para os dispositivos de telefonia, sendo esta identificada com uma tag de VLAN até o switch de borda, que deverá detectar automaticamente a presença de telefones IP em suas portas e então passar esta rede adequadamente.

### 5.3.1 Configuração dos switches

O parque de rede camada dois da universidade é composto em sua maioria por switches gerenciáveis dos fabricantes D-Link e Cisco, portanto o trabalho será limitado a implementações nos equipamentos destes fabricantes, sendo que ambos disponibilizam o recurso de VoiceVLAN.

Conforme apresentado no manual do usuário, D-Link (2009, p. 122), o switch D-Link implementa segmentação do tráfego de voz através da verificação do MAC de origem dos quadros que recebe nas portas de acesso. O switch verifica se os três primeiros octetos do MAC se encontram na tabela de OUI (*Organizationally Unique Identifier*) previamente configurada e caso positivo, marca os quadros com a tag da VLAN de voz.

OUIs são números de 24 bits que identificam de forma única os fabricantes ou vendedores de dispositivos de rede. Este número forma o início do MAC de cada dispositivo que é conectado na rede. A Figura 36 apresenta a tabela OUI em um switch

D-Link utilizado para testes, onde foram cadastradas as duas OUIs utilizadas por telefones IP Polycom, 0004f2 e 64167f.

```
SeTIC_ [redacted]# show voice_vlan oui-table
OUI      Description
-----  -
00:04:f2 Polycom UFSC
00:0b:82 Grandstream
00:0e:08 Linksys
64:16:7f Polycom UFSC 2
SeTIC_ [redacted]#
```

Figura 36 - Tabela OUI em um switch D-Link

Fonte: O autor

Uma mesma porta pode, portanto, possuir uma VLAN para dados e uma VLAN para voz, com o switch separando os tráfegos de acordo com o MAC dos quadros que recebe. A Figura 37 apresenta a configuração de uma Voice VLAN de tag 10 em um switch D-Link.

```
SeTIC_ [redacted]# show voice_vlan
Voice VLAN Status      : Enabled
Voice VLAN Untagged    : Disabled
Voice VLAN VID         : 10
Voice VLAN NAME        : v10
802.1p Priority        : 6
Remark 802.1p Priority : Disabled
Voice VLAN Aging Time  : 1440
SeTIC_ [redacted]#
```

Figura 37 - Configuração de Voice VLAN no switch D-Link

Fonte: O autor

Estando a Voice VLAN criada no switch, ela deve ser associada às portas onde poderão ser conectados dispositivos VoIP. Os testes foram realizados na porta 13 do switch, portanto a Voice VLAN foi associada a ela, conforme apresentado na Figura 38.

```

SeTIC_0a_SalaRedes[110]# config voice_vlan add 2:13 untagged

Success.
SeTIC_0a_SalaRedes[110]# show voice_vlan ports 2:(12-14)

Port Mode      Security Untagged Voice VLAN Membership
-----
2:12 disabled disabled disabled excluded
2:13 auto disabled enabled excluded
2:14 disabled disabled disabled excluded

SeTIC_0a_SalaRedes[110]#

```

Figura 38 - Aplicação de Voice VLAN nas portas do switch D-Link

Fonte: O autor

Com a habilitação de Voice VLAN nas portas de acesso do switch, caso um telefone seja conectado, receberá IP da rede de voz. Quando um computador for conectado na porta PC deste telefone, o telefone continuará na rede de voz e o computador irá se conectar a rede de dados, uma vez que o MAC do computador não está cadastrado na tabela OUI na qual o switch associa a VLAN de voz.

Para realização do teste foi conectado um telefone IP de MAC iniciando com 00:04:f2 na porta 2:13 do switch e um computador de MAC iniciando com 70:71:bc conectado na porta PC do telefone. Com a configuração de Voice VLAN os quadros do telefone devem ser marcados com a tag 10, resultando no recebimento de um IP da rede 192.168.10.0/24 já o computador deve ter seus quadros marcados com a tag 12, fazendo com que receba um IP da rede de dados 192.168.12.0/24.

A Figura 39 apresenta os MACs dos dois equipamentos sobre a porta 2:13 do switch e a Figura 40 apresenta os IPs que cada equipamento obteve.

```

SeTIC_0a_SalaRedes[110]# show fdb port 2:13

VID  VLAN NAME      MAC Address      Port  Type
----  -
10   v10             00:04:f2:5a:00:04  2:13  dynamic
12   v12             70:71:bc:22:00:00  2:13  dynamic

SeTIC_0a_SalaRedes[110]#

```

Figura 39 - MACs na porta com Voice VLAN, switch D-Link

Fonte: O autor

```

SeTIC-251#show arp | inc 7071.bc14
Internet 192.168.12.68          0    7071.bc14 ARPA   Vlan12
SeTIC-251#
SeTIC-251#show arp | inc 0004.f2c9
Internet 192.168.10.21        6    0004.f2c9 ARPA   Vlan10
SeTIC-251#

```

Figura 40 - Endereços IP entregues para telefone e computador no switch D-Link

Fonte: O autor

Os switches Cisco implementam a descoberta de dispositivos através do protocolo LLDP (*Link-Layer Discovery Protocol*). O protocolo LLDP é definido pelo padrão IEEE 802.1AB e permite que dispositivos diretamente conectados comuniquem entre si, através da camada 2, quais são as suas principais funções e capacidades, dentre elas se são dispositivos de telefonia, *bridges* ou roteadores. O protocolo permite informar também dados relacionadas a gerenciamento de energia PoE (Power over Ethernet) e VLAN, possibilitando automatização de configurações entre dispositivos.

A Figura 41 apresenta uma consulta resumida realizada em um switch Cisco no qual são detectados os dispositivos vizinhos que respondem a este protocolo, sendo um deles um telefone IP Polycom. Os telefones utilizados no ambiente de telefonia respondem no campo “Capability” as opções T e B, correspondentes a Telephone e Bridge, uma vez que estes dispositivos possuem uma porta para estender a rede até um computador.

```

SeTIC-251#show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf      Hold-time  Capability  Port ID
Polycom SoundPoint IGi1/0/17       112        B,T         0004.f2c9
SeTIC-Sala4[251    Gi1/0/24       104        B           1:23
sala4-Infoway      Gi1/0/12       99         S           0024.1d
Total entries displayed: 3
SeTIC-251#

```

Figura 41 - Consulta de dispositivos conectados através de LLDP no switch Cisco

Fonte: O autor

Conforme apresentado na Figura 41, o telefone informa no campo *Capability* as informações “B,T”, correspondentes a *Telephone* e *Bridge*. Possuindo esta informação, o switch identifica que há um telefone na porta e insere a tag da Voice

VLAN nos quadros que encaminha e recebe do telefone, permanecendo com a tag da rede de dados para o computador. O protocolo LLDP permite ainda que o telefone identifique a VLAN de voz utilizada e se autoconfigure para trabalhar reconhecendo e inserindo a tag da Voice VLAN, o que não ocorre com o switch D-Link, que precisa remover a tag do quadro quando passa para a porta do telefone.

Como o protocolo LLDP já vem habilitado por padrão nestes switches e nos telefones, basta apenas ter a VLAN criada no switch e então configurá-la como Voice VLAN nas portas de acesso. A Figura 42 apresenta a configuração de Voice VLAN na porta 17 do switch Cisco.

```
SeTIC-#configure terminal
SeTIC-(config)#interface gigabitEthernet 1/0/17
SeTIC-(config-if)#switchport access vlan 12
SeTIC-(config-if)#switchport voice vlan 10
SeTIC-(config-if)#
SeTIC-#show running-config in gi1/0/17 | inc switchport
switchport access vlan 12
switchport trunk allowed vlan 12
switchport mode access
switchport voice vlan 10
SeTIC-#
```

Figura 42 - Configuração de Voice VLAN em switch Cisco

Fonte: O autor

Após realizadas as configurações, foram feitos testes de separação do tráfego conectando um telefone IP e um computador na porta 17 do switch. A Figura 43 apresenta os MACs que estão na porta 17, e a Figura 44 apresenta os IPs atribuídos a estes MACs pelo DHCP.

```
SeTIC-#show mac address-table interface gi 1/0/17
Mac Address Table
-----
Vlan    Mac Address      Type           Ports
----    -
12      7071.bc         DYNAMIC        Gi1/0/17
10      0004.f2         DYNAMIC        Gi1/0/17
Total Mac Addresses for this criterion: 2
SeTIC-#
```

Figura 43 - MACs na porta com Voice VLAN, switch Cisco

Fonte: O autor

```

SeTIC-251#show arp | inc 0004.f2c9
Internet 192.168.10.21          19  0004.f2c9  ARPA  Vlan10
SeTIC-251#
SeTIC-251#show arp | inc 7071.bc14
Internet 192.168.12.68        1   7071.bc14  ARPA  Vlan12
SeTIC-251#

```

Figura 44 - Endereços IP atribuídos para telefone o computador no switch Cisco

Fonte: O autor

### 5.3.2 Planejamento da rede de voz

Como a universidade possui aproximadamente 3500 telefones IP, uma única rede com todos estes dispositivos geraria um tráfego de *broadcast* muito grande, podendo inclusive esgotar a capacidade da tabela de MACs suportada pelos switches e forçando os mesmos a processarem constantemente descobertas de MACs em suas portas, gerando ainda mais broadcast sobre a rede. A solução é a criação de domínios de broadcast de no máximo 512 IPs, adotando assim sete sub-redes de voz. Estas redes podem ser distribuídas por blocos de ambientes físicos da universidade, como centros e campi.

Atualmente, a rede da universidade não possui disponível sete faixas contínuas de 512 IPs, portanto, uma alternativa pode ser criar novas sub-redes de telefonia, utilizando IPs privados. Recomenda-se a utilização de faixa de IP classe B, pois possuem a quantidade de redes e hosts suficientes para a criação das sub-redes necessárias, com possibilidades de posterior expansão. Um exemplo de dimensionamento de IPs para as redes de voz pode ser observado na Tabela 2.

Tabela 2 - Dimensionamento de IPs para as redes de voz

TAG	Rede	Máscara	Broadcast	Host mínimo	Host máximo	nº hosts
3001	172.16.0.0	255.255.254.0	172.16.1.255	172.16.0.1	172.16.1.254	510
3002	172.16.2.0	255.255.254.0	172.16.3.255	172.16.2.1	172.16.3.254	510
3003	172.16.4.0	255.255.254.0	172.16.5.255	172.16.4.1	172.16.5.254	510
3004	172.16.6.0	255.255.254.0	172.16.7.255	172.16.6.1	172.16.7.254	510
3005	172.16.8.0	255.255.254.0	172.16.9.255	172.16.8.1	172.16.9.254	510
3006	172.16.10.0	255.255.254.0	172.16.11.255	172.16.10.1	172.16.11.254	510
3007	172.16.12.0	255.255.254.0	172.16.13.255	172.16.12.1	172.16.13.254	510

Fonte: O autor

Com a criação das setes sub-redes indicadas, haverá IPs para 3570 telefones, com a escalabilidade de se adicionar novas sub-redes na sequência. Para operacionalização destas novas faixas de IP, é necessário a criação de novos escopos no DHCP, configuração de roteamento para as demais redes, implementação de ACLs para controle de acesso e configuração das novas VLANs em todos os switches da universidade.

Com a segmentação da rede de voz, as ACLs poderão realizar as seguintes restrições de acesso:

- Restringir a comunicação SIP dos terminais apenas para o servidor PBX-IP, que realiza SIP proxy de todas as chamadas;
- Restringir a comunicação com as redes de dados apenas para portas de mídia, já que este tráfego é realizado diretamente entre os terminais e alguns deles poderão ainda ficar nessas redes, seja por não estarem sob a gerência da SeTIC, ou por estarem em switches sem suporte a Voice VLAN;
- Restringir tráfego de serviços de rede, como NTP, apenas para a rede de servidores;
- Permitir demais acessos apenas para a rede de gerência da SeTIC.

A realização de chamadas com outras instituições através do Fone@RNP não é prejudicada, pois nestes casos há a realização de SIP proxy e media proxy no servidor SRL, que possui IP válido na rede de servidores de telefonia.

## 6 CONSIDERAÇÕES FINAIS

A pesquisa realizada sobre segurança da informação e telefonia IP proporcionou a compilação de informações e geração de conhecimento necessário para elaboração de três propostas para implementação de medidas de segurança do ambiente de telefonia IP da Universidade Federal de Santa Catarina.

A proposta de segurança sobre os dados de provisionamento demonstrou-se eficaz e viável. Através do uso de certificado digital assinado por uma AC confiável foi possível estabelecer uma transmissão de dados criptografada entre o servidor e os clientes. A autenticação dos dispositivos no servidor através de certificados também apresentou funcionamento adequado, permitindo acesso apenas aos equipamentos desejados e bloqueando possíveis tentativas de acesso indevido.

A proposta de criptografia de voz através do protocolo SRTP é viável e funciona. Com os pacotes de mídia cifrados entre os terminais, não foi possível reconstituir o fluxo de áudio compreensível através de uma captura e ordenação de conteúdo. Além de prover confidencialidade nas chamadas, a utilização do SRTP também mostrou-se adequada devido a diversidade de dispositivos que o implementam, reduzindo assim problemas de interoperabilidade. Durante os testes não foi notada qualquer degradação do áudio.

A proposta de segmentação da rede de voz através de Voice VLAN também é efetiva. O recurso possibilitou a distribuição dinâmica de uma rede dedicada para dispositivos VoIP, provendo maior isolamento e segurança contra ataques de acesso indevido e negação de serviço. Com a possibilidade de compartilhamento de portas dos switches entre telefones e estações de trabalho, mesmo havendo a necessidade inicial de configurar todos os ativos de rede, esta solução resulta na economia de tempo com a posterior disponibilização automática de portas. Também resulta na manutenção da portabilidade dos terminais telefônicos e economia de milhares de pontos de rede, garantindo, portanto, uma implantação transparente e sem custos adicionais.

O protocolo SRTP possui a finalidade de cifrar exclusivamente a mídia de uma chamada, não tratando a confidencialidade de sinalização SIP e campos SDP, responsável pelo gerenciamento das sessões. Como trabalho futuro é proposto o estudo de uma metodologia para criptografia da sinalização SIP e sua aplicação no



ambiente de telefonia apresentado, havendo como opções os protocolos SIPS, TLS, IPSec, entre outros.

Foi identificado no ambiente de telefonia IP, servidores Asterisk sem suporte a criptografia, necessitando estes serem customizados com as devidas bibliotecas e configurações para suportarem SRTP. Sugere-se posteriormente o estudo do servidor Asterisk, com o levantamento de requisitos e implementações necessárias para o suporte à criptografia de mídia e sinalização.

A segmentação da rede VoIP viabiliza além do aumento de segurança, através do controle de acesso e restrições de tráfego, também a priorização de tráfego. Desta forma, propõe-se estudar também possíveis implementações no ambiente para priorização do tráfego VoIP sobre os demais serviços, uma vez que a telefonia IP é um serviço de tempo real e sua qualidade está diretamente relacionada a disponibilidade da rede.

A execução deste trabalho contribui com a geração de conhecimento tanto para a instituição quanto para a comunidade acadêmica. As soluções foram aplicadas sobre equipamentos proprietários, porém as tecnologias e protocolos são públicos e podem ser utilizados em qualquer outro ambiente.

## REFERÊNCIAS

ALEXANDER, Andre L.; WIJESINHA, Alexander L.; KARNE, Ramesh. **An Evaluation of Secure Real-Time Transport Protocol (SRTP) Performance for VoIP**. 2009 Third International Conference On Network And System Security, [s.l.], p.1-1, 2009. IEEE. <http://dx.doi.org/10.1109/nss.2009.90>.

APACHE, Fundação. **SSL/TLS Strong Encryption: How-To**. Disponível em: <[https://httpd.apache.org/docs/2.4/ssl/ssl\\_howto.html](https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html)>. Acesso em: 27 ago. 2017

AUDIOCODES. **Mediant 2000: User's Manual**. 2011. Disponível em: <[http://www.audiocodes.com/filehandler.ashx?fileid=2059222&usg=AFQjCNGNf\\_tqg1fg1Ee815u9GsYDD4PLZA](http://www.audiocodes.com/filehandler.ashx?fileid=2059222&usg=AFQjCNGNf_tqg1fg1Ee815u9GsYDD4PLZA)>. Acesso em: 27 ago. 2017.

AUDIOCODES. **Tchnical Note: Recommended Security Guidelines**. 2011. Disponível em: <[www.audiocodes.com/filehandler.ashx?fileid=1477052&usg=AFQjCNFKJdJuD\\_RP Pixp6nkKIHdxI4kZWw](http://www.audiocodes.com/filehandler.ashx?fileid=1477052&usg=AFQjCNFKJdJuD_RP Pixp6nkKIHdxI4kZWw)>. Acesso em: 27 ago. 2017.

COELHO, Flávia Estévia Silva; ARAUJO, Luiz Geraldo Segadas de; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação**. Rio de Janeiro: Rnp/esr, 2014. 220 p.

GENEITAKIS, Dimitris et al. Survey of security vulnerabilities in session initiation protocol. **Ieee Communications Surveys & Tutorials**, [s.l.], v. 8, n. 3, p.68-81, 2006. Institute of Electrical and Electronics Engineers (IEEE). <http://dx.doi.org/10.1109/comst.2006.253270>.

HÉRCULES, LuisAntonio Leiva. **Impacto no Desempenho em Aplicações de Tempo Real Utilizando Criptografia**. 2014. 71 f. TCC (Graduação) - Curso de Engenharia de Computação, Universidade Federal do Rio Grande do Sul, Porto Alegre, 2014.

HSIEH, Wen-bin; LEU, Jenq-shiou. **Implementing a secure VoIP communication over SIP-based networks**. *Wireless Networks*, [s.l.], v. 23, 25 abr. 2017. Springer Nature. <http://dx.doi.org/10.1007/s11276-017-1512-3>.

**Instituto Nacional de Tecnologia da Informação**. Disponível em: <[www.itl.gov.br](http://www.itl.gov.br)>. Acesso em: 17 ago. 2017.

JORGE, Bruno Tiago Correia. **Segurança e Privacidade numa Infraestrutura de VoIP**. 2017. 89 f. Dissertação (Mestrado) - Curso de Engenharia Eletrotécnica e de Computadores, Universidade do Porto, Porto, 2017.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

POLYCOM. **Certificate Updates for Polycom UC Software 5.5.0**. 2016. Disponível em: <<http://support.polycom.com/content/dam/polycom->

support/products/Voice/business\_media\_phones/other-documents/en/ucs-cert-update.pdf>. Acesso em: 27 ago. 2017.

POLYCOM. **Polycom UC Software 5.5.0**. 2016. Disponível em: <[http://support.polycom.com/content/dam/polycom-support/products/Voice/business\\_media\\_phones/setup-maintenance/en/uc\\_admin\\_550.pdf](http://support.polycom.com/content/dam/polycom-support/products/Voice/business_media_phones/setup-maintenance/en/uc_admin_550.pdf)>. Acesso em: 27 ago. 2017.

POLYCOM. **Polycom UC Software Administrator's Guide**. 2011. Disponível em: <[http://support.polycom.com/global/documents/support/setup\\_maintenance/products/voice/spip\\_ssp\\_vvx\\_Admin\\_Guide\\_UCS\\_v4\\_0\\_0.pdf](http://support.polycom.com/global/documents/support/setup_maintenance/products/voice/spip_ssp_vvx_Admin_Guide_UCS_v4_0_0.pdf)>. Acesso em: 27 ago. 2017.

D-LINK. **User Manual: DGS 3100 Series**. Disponível em: <[ftp://ftp2.dlink.com/PRODUCTS/DGS-3100-24/REVA/DGS-3100-24\\_MANUAL\\_3.60\\_EN.PDF](ftp://ftp2.dlink.com/PRODUCTS/DGS-3100-24/REVA/DGS-3100-24_MANUAL_3.60_EN.PDF)> Acesso em: 27 ago. 2017.

REHMAN, Ubaid Ur; ABBASI, Abdul Ghafoor. Security analysis of VoIP architecture for identifying SIP vulnerabilities. **2014 International Conference On Emerging Technologies (icet)**, [s.l.], dez. 2014. IEEE. <http://dx.doi.org/10.1109/icet.2014.7021022>.

RISTIC, Ivan. **OpenSSL Cookbook**. 2. ed. Londres: FeistyDuckLimited, 2016

[RFC 2543] J. Rosenberg et al; **SIP: Session Initiation Protocol**. IETF: Março 1999.

[RFC 3261] J. Rosenberg et al; **SIP: Session Initiation Protocol**. IETF: Junho 2002.

[RFC 3550] H. Schulzrinne et al; **RTP: A Transport Protocol for Real-Time Applications**, IETF: Julio 2003.

[RFC 3711] M. Baugher et al; **The Secure Real-time Transport Protocol (SRTP)**, IETF: Março 2004.

[RFC 4566] M. Handley et al; **SDP: Session Description Protocol**, IETF: Julio 2006.

[RFC 4568] F. Andreassen et al; **Session Description Protocol (SDP) Security Descriptions for Media Streams**, IETF: Julio 2006.

[RFC 5246] T. Dierks; E. Rescorla. **The Transport Layer Security (TLS) Protocol Version 1.2**, IETF: Agosto 2008.

[RFC 5630] F. Audet; **The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)**, IETF: Outubro 2009.

[RFC 6189] P. Zimmermann et al. **ZRTP: Media Path Key Agreement for Unicast Secure RTP**, IETF: Abril 2011.

[RFC 6347] E. Rescorla et al. **Datagram Transport Layer Security Version 1.2**, IETF: Janeiro 2012.

SANTOS, Douglas Bayer. **Sistema Gerenciador de Certificados de Atributo X.509**. 2013. 83 f. TCC (Graduação) - Curso de Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2013.

SILVA, Fernando de Britto e; JESUS JÚNIOR, Silvio Mário Cândido de. **Análise dos aspectos de segurança da informação em um ambiente de comunicações unificadas**. 2013. 65 f. TCC (Graduação) - Curso de Engenharia de Redes de Comunicação, Universidade de Brasília, Brasília, 2013.

STALLINGS, William. **Criptografia e segurança de redes: Princípios e práticas**. 6. ed. São Paulo: Pearson Education do Brasil, 2014.

TANENBAUM, Andrew S.; WETHERALL, D. **Redes de computadores**. 5. ed. São Paulo: Pearson, 2011. xvi, 582 p. ISBN 9788576059240.

VETTER, Murilo. **Sistema de monitoramento de qualidade em serviços de telefonia IP**. 2015. 112 f. Dissertação (Mestrado) - Curso de Ciência da Computação, Universidade Federal de Santa Catarina, Florianópolis, 2015.

## APÊNDICE A - ARTIGO

### Propostas de segurança para o ambiente de telefonia IP da Universidade Federal de Santa Catarina

Vitor Augusto Schweitzer

Departamento de Informática e Estatística  
Universidade Federal de Santa Catarina (UFSC) – Florianópolis, SC - Brasil

vaschweitzer@gmail.com

**Abstract.** *This work presents a study on the application of information security in IP telephony environments, aiming at the elaboration and validation of proposals that contribute to the security of the telephony service at Universidade Federal de Santa Catarina. With the constant replacement of the university's conventional telephony by VoIP, it was identified the need for improvements in its Confidentiality, Integrity and Availability requirements, essential security factors for the maintenance of services provided over the IP network. This work resulted in the application of three proposals at specific points in the system. Digital certificates were used to implement authentication and encryption for centralized data access and transfer on a provisioning server, securely distributing endpoint configurations. Voice traffic was encrypted by enabling the SRTP protocol on VoIP devices, increasing the confidentiality of calls. VoIP network isolation was planned by implementing Voice VLAN over switches, enabling traffic restriction and reducing the risk of intrusion and denial of service attacks. All the proposals were tested in the current telephony environment of the institution, concluding that all are applicable and may contribute to the security of the service provided.*

**Resumo.** *Este trabalho apresenta um estudo sobre a aplicação de segurança da informação em ambientes de telefonia IP, objetivando a elaboração e validação de propostas que contribuem para a segurança do serviço de telefonia da Universidade Federal de Santa Catarina. Com a constante substituição da telefonia convencional da universidade pelo VoIP, identificou-se a necessidade de melhorias nos seus quesitos de Confidencialidade, Integridade e Disponibilidade, fatores de segurança essenciais para manutenção de serviços prestados sobre a rede IP. O trabalho resultou na aplicação de três propostas em pontos específicos do sistema. Certificados digitais foram utilizados para implementação de autenticação e criptografia para acesso e transferência de dados centralizados em um servidor de provisionamento, distribuindo de forma segura as configurações de terminais telefônicos. O tráfego de voz foi criptografado através da habilitação do protocolo SRTP nos dispositivos VoIP, aumentando a confidencialidade das chamadas. O isolamento da rede VoIP foi planejado através da implementação de Voice VLAN sobre os switches,*

*possibilitando a restrição de tráfego e reduzindo riscos de invasões e ataques de negação de serviço. Todas as propostas foram testadas no atual ambiente de telefonia da instituição, concluindo-se que todas são aplicáveis e poderão contribuir para a segurança do serviço prestado.*

## 1. Introdução

Por muito tempo a telefonia foi baseada em comutação de circuitos, topologia no qual a infraestrutura é dedicada e circuitos são reservados para o estabelecimento da comunicação. Porém, com os benefícios da comutação por pacotes, a telefonia adaptou-se e passou também a utilizar as redes IP como meio de transmissão de sinalização e áudio, surgindo assim o conceito de VoIP (*Voice over IP*).

Diante deste novo ambiente de telefonia, onde informações do serviço e conversas são transmitidas pelos mesmos meios que tantas outras informações, muitas vezes em locais que não estão sob o domínio das pessoas interessadas, a preocupação com a segurança torna-se essencial.

Os protocolos padronizados para o funcionamento básico de um sistema de telefonia IP, geralmente SIP (*Session Initiation Protocol*) para sinalização e RTP (*Real Time Protocol*) para transporte de mídia, não foram projetados para garantir segurança sobre a comunicação, e sim viabilizar o estabelecimento das sessões de forma simples. Ambientes maiores de telefonia IP acabam se tornando mais complexos, com o aumento de servidores e comunicações via rede.

O avanço da telefonia para a tecnologia VoIP trouxe consigo muitas vantagens, porém a convergência de tecnologias impacta também no compartilhamento de vulnerabilidades. A utilização de uma rede IP traz para o VoIP ameaças que até então não existiam na telefonia convencional, tornando-a alvo de ataques comuns a uma rede de dados, como *Eavesdropping*, *Denial of Service*, injeção de códigos maliciosos, entre outros.

Para mitigar estas ameaças, mecanismos de segurança como criptografia e autenticação são utilizados em sistemas que possuem algum tipo de informação sigilosa, dados pessoais, financeiros e estratégicos para organizações, portanto a telefonia IP também necessita de mecanismos de proteção que ampliem a sua confidencialidade, integridade e disponibilidade.

Entre os mecanismos de segurança que se enquadram a sistemas de telefonia IP estão a criptografia de sinalização e voz, autenticação eficiente de usuários, uso de certificados digitais, segmentação do tráfego VoIP sobre as demais redes, controle de acesso à redes, e implementação de protocolos que provem maior segurança do que os padrões adotados, como o SRTP (*Secure Real-time Transport Protocol*), que fornece criptografia sobre os pacotes de mídia, o SIPS (*SIP Secure*), que provê criptografia sobre os pacotes de sinalização e o HTTPS, que provê transferência de dados de forma segura.

Este artigo descreve a associação de vulnerabilidades existentes em sistemas e redes de telefonia IP com o ambiente real de telefonia IP da Universidade Federal de Santa Catarina, buscando identificar pontos de vulnerabilidade e propor mecanismos de proteção que possam mitigar tais riscos. A sessão 2 apresenta trabalhos correlatos sobre segurança em ambientes de telefonia IP, utilizados como referencial para estudos sobre

ameaças e mecanismo de proteção. A sessão 3 apresenta o ambiente de telefonia onde o estudo foi aplicado, as vulnerabilidades encontradas e as propostas de segurança implementadas. A sessão 4 decorre as conclusões e considerações finais do trabalho realizado.

## 2. Trabalhos correlatos

Durante o processo de pesquisa foi realizado o levantamento de temas relacionados à segurança da informação e telefonia IP, retornando alguns artigos e monografias com informações relevantes para fundamentação e desenvolvimento deste trabalho. Neles foram apresentados pontos de vulnerabilidade, potenciais ataques, mecanismos de defesa, avaliações de desempenho e estudos de caso sobre sistemas VoIP.

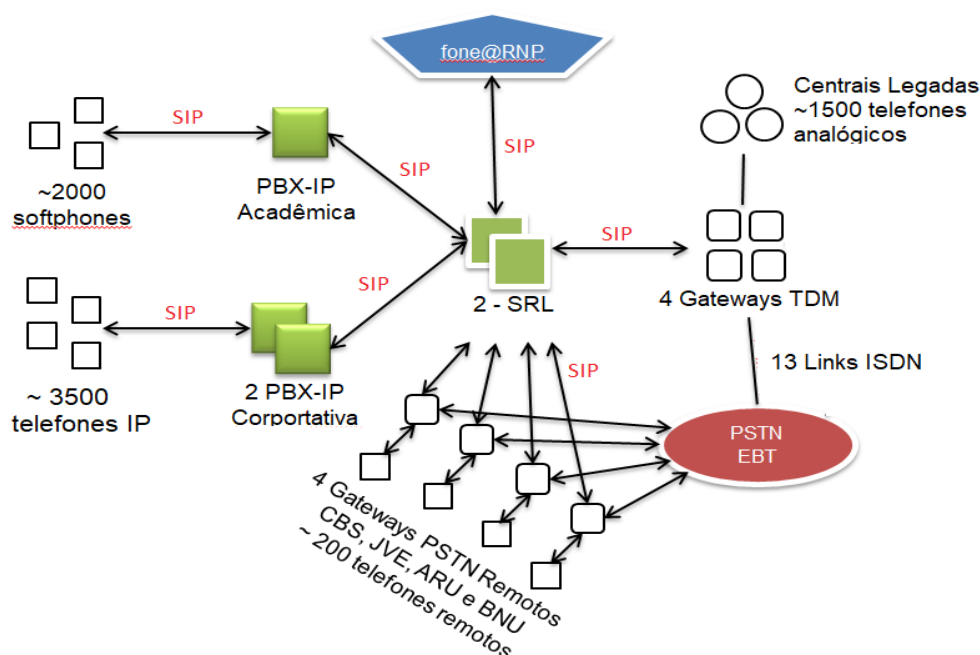
Rehman e Abbasi (2014) apresentam um artigo relatando uma análise de segurança do protocolo SIP sobre uma arquitetura VoIP. Tal análise foi realizada através de revisão da literatura, classificando ataques e mecanismos de defesa mais citados, e posterior execução de testes práticos de ataque sobre um servidor Asterisk. Seu estudo revela que a maioria dos ataques a ambientes VoIP foram bem sucedidos devido a deficiências do SIP, principalmente durante sua fase de autenticação no estabelecimento de sessões, com o uso comum do método HTTP *Digest*. Para combater esta vulnerabilidade, o autor propõe um esquema de autenticação de sessão utilizando o conceito de Single-Sign-On, onde os usuários SIP recebem do servidor um token criptográfico e os utilizam para posterior autenticação durante a inicialização de sessões.

Alexander, Wijesinha e Karne (2009) apresentam em seu artigo uma avaliação de desempenho do protocolo SRTP sobre chamadas VoIP, utilizando diferentes *softphones*, sistemas operacionais e parâmetros de criptografia e autenticação. Após monitoramento dos tempos de processamento, jitter e taxa de transferência para cada teste, conclui que a adição do SRTP não afeta significativamente a qualidade da voz; a autenticação é mais custosa do que a criptografia e; a utilização do SRTP aumenta em apenas 2% a taxa de transferência sobre a rede.

Silva e Júnior (2013) relatam em sua monografia a aplicação dos conceitos de segurança da informação sobre um ambiente de comunicações unificadas, focando em ambientes de telefonia IP. Os autores citam os principais ataques direcionados a telefonia IP e possíveis métodos de proteção a serem implementados para redução dos riscos. Posteriormente, os autores apresentam um estudo de caso avaliando as vulnerabilidades existentes em um ambiente com diferentes recursos de proteção, realizando por fim o comparativo de qual rede implementa a melhor defesa contra ataques.

## 3. Ambiente e propostas

O ambiente de telefonia da Universidade Federal de Santa Catarina é composto por uma rede híbrida de aproximadamente 5.000 ramais, sendo cerca de 70% IP e o restante analógico. A infraestrutura de telefonia IP é centralizada na matriz, porém atende outros 4 campi em cidades distintas. Os principais componentes da infraestrutura de telefonia são apresentados na Figura 1, e descritos em sequência.



**Figura 1 - Infraestrutura de telefonia da UFSC**

- **PBX-IP Corporativa:** Servidor de registro e proxy SIP para os terminais telefônicos IP. Atua como central telefônica corporativa, gerenciando recursos como controle de privilégios, siga-me e captura de chamadas;
- **PBX-IP Acadêmica:** Servidor de registro e proxy SIP similar a PBX corporativa, porém com a finalidade de servir a comunidade acadêmica (alunos, professores e servidores) chamadas gratuitas para qualquer ramal da instituição;
- **SRL (SIP Router Local):** Servidor responsável por interligar todos os componentes SIP da rede (servidores e *gateways*), realizando o roteamento de chamadas entre eles.
- **Gateways TDM:** Equipamentos que intermediam a comunicação entre os dispositivos SIP e a telefonia convencional, realizando conexões com centrais analógicas e a PSTN.
- **Centrais legadas:** Centrais telefônicas utilizadas para gerenciamento de ramais analógicos da rede de telefonia convencional.
- **Gateways PSTN remotos:** Equipamentos situados nas unidades remotas da instituição para realizar a comunicação com a PSTN de cada cidade.
- **Fone@RNP:** Serviço de roteamento SIP fornecido pela RNP (Rede Nacional de Ensino e Pesquisa) para realização de chamadas IP com outras instituições nacionais, através da Internet.

O protocolo de sinalização utilizado para estabelecimento de sessões entre os terminais telefônicos, servidores VoIP e *gateways* é o SIP, com o uso do protocolo SDP (*Session Description Protocol*) para descrição das sessões e o RTP para transmissão da voz. Os terminais telefônicos são compostos em 95% de telefones IP do fabricante Polycom. As configurações e atualizações destes aparelhos são baixadas de forma centralizadas em um servidor de aprovisionamento.

Sobre o ambiente apresentado foram identificados pontos de baixa segurança e então elaboradas três propostas que visam aumentar a confidencialidade, integridade e



disponibilidade do sistema. A primeira proposta apresenta a implementação de criptografia e autenticação com o uso de certificados digitais para o provisionamento de telefones IP. A segunda proposta corresponde a habilitação de criptografia de mídia sobre as chamadas telefônicas. A terceira proposta apresenta a implementação de Voice VLAN em switches camada dois para segmentação da rede de voz e dados. As três propostas foram elaboradas e testadas sobre um ambiente de testes, porém com equipamentos utilizados no ambiente de produção, portanto validando implementações possíveis de serem implantadas.

### 3.1. Provisionamento seguro

O serviço de telefonia corporativa faz uso de um servidor de provisionamento para automatização do processo de configuração e atualização dos telefones IP utilizados pela instituição. Atualmente, o processo de provisionamento é realizado através de transferências de arquivos utilizando o protocolo HTTP, ou seja, em texto plano, ameaçando assim a confidencialidade de dados importantes. Além disso, foi identificada a utilização de autenticação baseada método *HTTP Digest* para acesso ao servidor, o que segundo Rehman e Abbasi (2014) é um método fraco, baseado em usuário e senha, tornando-se um ponto de vulnerabilidade do sistema.

A proposta para mitigar as vulnerabilidades mencionadas consiste na utilização de certificados digitais para estabelecimento de uma comunicação segura entre o servidor e os terminais telefônicos, criptografando os dados transferidos pela rede e provendo um método mais forte de autenticação.

A criptografia dos dados foi implementada através da substituição do protocolo HTTP por HTTPS para realização da transferência dos arquivos do servidor para os telefones. Para isso foi necessária a geração, instalação e configuração de um certificado digital no servidor web de provisionamento. Em complemento foi necessário alterar o escopo da rede no servidor DHCP passando a direcionar a opção 160 para a nova URL de provisionamento.

Para obtenção do certificado digital foi utilizada a ferramenta OpenSSL para geração do par de chaves assimétricas e o arquivo CSR (*Certificate Signing Request*) a ser enviado para a autoridade de registro. A solicitação de certificado então foi realizada para a AC UFSC, autoridade certificadora e de registro da universidade que possui seus certificados assinados pela ICPEDEU (Infraestrutura de Chaves Públicas para Ensino e Pesquisa), que por sua vez são assinados pela autoridade certificadora GlobalSign, reconhecida mundialmente.

Tendo o par de chaves e o certificado digital assinado por uma AC confiável, foi realizada a configuração do servidor web de provisionamento. Para que os telefones IP pudessem reconhecer a entidade certificadora raiz, foi necessário concatenar no mesmo arquivo PEM os certificados de toda a cadeia de assinaturas acima do certificado adquirido. Nas configurações do servidor web foi habilitado o módulo SSL e configurados os caminhos do certificado digital e chave privada correspondente.

A segurança de acesso ao servidor foi ampliada através da implementação de TLS mútuo para autenticação dos dispositivos no servidor. Desta forma além de garantir que os terminais estão se comunicando com o servidor correto também é garantido que o servidor está entregando os arquivos para um telefone homologado do ambiente e não para algum invasor.

Para o estabelecimento do TLS mútuo foram utilizados certificados digitais que cada aparelho telefônico recebe de fábrica, baseado em sua identificação única de MAC e assinado pelo fabricante. O certificado da AC Raiz disponibilizado pelo fabricante foi instalado no servidor web, e nas configurações do servidor foi habilitada a solicitação de certificado para qualquer dispositivo que tente estabelecer uma conexão HTTPS.

Para comprovar a validade da proposta foram realizados testes através da coleta de tráfego na porta de um telefone, antes e depois das implementações realizadas.

A Figura 1 apresenta o tráfego de um provisionamento antes da implementação de criptografia, utilizando apenas o protocolo HTTP, sendo possível observar as requisições e respostas em texto plano.

No.	Source	Destination	Protocol	Info
3694	192.168.0.1	192.168.0.50	HTTP	GET /provisionamento-contatos/0004f2- directory.xml HTTP/1.1
3699	192.168.0.50	192.168.0.1	HTTP/XML	HTTP/1.1 200 OK
3827	192.168.0.1	192.168.0.50	HTTP	GET /0004f2- .cfg HTTP/1.1
3848	192.168.0.50	192.168.0.1	HTTP	HTTP/1.1 404 Not Found (text/html)
3911	192.168.0.1	192.168.0.50	HTTP	GET /SoundPointIPLocalization/Portuguese_Portugal/SoundPointIP-dictionary.xml HTTP/1.1

**Figura 45. Provisionamento sem criptografia**

Após a implantação do certificado e habilitação do módulo SSL no servidor, o telefone passou a negociar os parâmetros de segurança através de um *handshake* TLS, conforme apresentado no tráfego da Figura 2, e posteriormente transferir dados de forma criptografada.

No.	Source	Destination	Protocol	Info
839	192.168.0.1	192.168.0.50	TLSv1	Client Hello
841	192.168.0.50	192.168.0.1	TLSv1	Server Hello
844	192.168.0.50	192.168.0.1	TLSv1	Certificate, Server Hello Done
851	192.168.0.1	192.168.0.50	TLSv1	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
852	192.168.0.50	192.168.0.1	TLSv1	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
853	192.168.0.1	192.168.0.50	TLSv1	Encrypted Alert
854	192.168.0.50	192.168.0.1	TLSv1	Encrypted Alert

**Figura 46. Handshake TLS simples**

Após a habilitação do TLS mútuo e instalação do certificado da AC raiz dos telefones no servidor, foi coletado um novo tráfego, apresentado na figura 3. Neste tráfego é possível visualizar a troca de mensagens entre o telefone e o servidor durante um *handshake* mútuo, onde o terceiro pacote trata-se da solicitação de certificado pelo servidor, e o quarto pacote é a resposta do telefone enviando o seu certificado. O *handshake* ocorre normalmente até as mensagens de “EncryptedAlert”, onde cada dispositivo finaliza o *handshake* informando que deste ponto em diante passará a enviar dados criptografados.

No.	Source	Destination	Protocol	Info
987	192.168.0.1	192.168.0.50	TLSv1	Client Hello
989	192.168.0.50	192.168.0.1	TLSv1	Server Hello
992	192.168.0.50	192.168.0.1	TLSv1	Certificate, Certificate Request, Server Hello Done
1001	192.168.0.1	192.168.0.50	TLSv1	Certificate
1029	192.168.0.1	192.168.0.50	TLSv1	Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
1031	192.168.0.50	192.168.0.1	TLSv1	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
1033	192.168.0.1	192.168.0.50	TLSv1	Encrypted Alert
1034	192.168.0.50	192.168.0.1	TLSv1	Encrypted Alert

**Figura 3. Handshake TLS mútuo**

### 3.2. Criptografia de voz

A maioria dos ambientes de telefonia IP utiliza por padrão o protocolo RTP para transporte de mídia, sendo o mesmo protocolo utilizado no ambiente em estudo. O protocolo RTP transmite a mídia de forma aberta na rede, sendo portando um risco contra a confidencialidade das conversas transmitidas. Pretende-se, portanto, validar e propor um mecanismo que agregue confidencialidade e autenticidade ao tráfego de mídia.

No ambiente em estudo, toda a negociação de parâmetros de mídia é realizada entre os dispositivos VoIP finais, não havendo manipulação pelos *proxies* que estão no caminho, portanto os equipamentos que precisam acordar um protocolo seguro para mídia são os terminais telefônicos e os *gateways* de mídia. Dentre estes equipamentos, foi levantado que mais de 95% dos telefones IP utilizados, bem como os *gateways* de mídia suportam o protocolo SRTP como opção de transporte de mídia, sendo este, portanto, possível de se implementar sem prejudicar a interoperabilidade do ambiente.

Por padrão os equipamentos responsáveis por criptografar a mídia não possuem esta funcionalidade ativa, por ser um recurso opcional e consumir processamento extra, porém possibilitam a ativação através da configuração de alguns parâmetros. Os equipamentos do ambiente foram, portanto, configurados para adicionar a opção de chamada segura com o uso de SRTP, mantendo a oferta de chamada aberta com RTP no mesmo INVITE. Também foram configurados para aceitarem preferencialmente chamadas seguras quando recebem as duas opções. Desta forma é possível garantir a interoperabilidade com equipamentos que apenas implementam o protocolo RTP.

Para validar o funcionamento da implementação foram realizados testes de chamadas com a captura de tráfego sobre a porta que se encontra um telefone na rede e utilizada a ferramenta Wireshark para analisar os fluxos das chamadas. Durante os testes foram utilizados os seguintes equipamentos:

- Telefone IP VVX, apresentado com o IP 192.168.0.1;
- Telefone IP SoundPoint IP 331, apresentado com o IP 192.168.0.2;
- PBX-IP, apresentada com os IPs 192.168.0.51 (virtual) e 192.168.0.52 (real).

Inicialmente foi capturado o tráfego de uma chamada da forma como ela é estabelecida atualmente, sem implementação de segurança sobre a mídia. A Figura 4, obtida através da ferramenta Wireshark, apresenta o fluxo de uma chamada gerada do telefone VVX para o SoundPoint IP. Nela é possível identificar cada mensagem de estabelecimento de sessão SIP sobre o ponto de vista do telefone VVX, bem como a utilização do protocolo RTP e codec G711 para transmissão de mídia diretamente entre os *endpoints*.

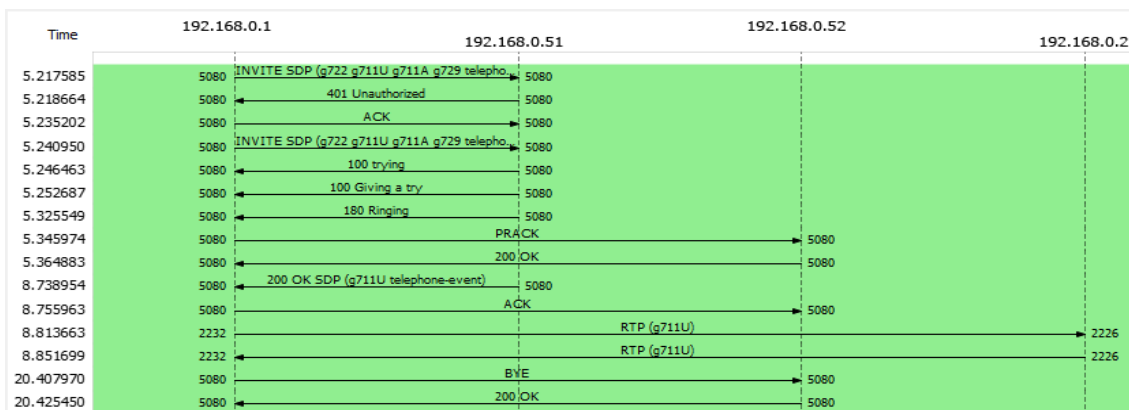


Figura 4. Fluxo de chamada SIP utilizando RTP

O fluxo apresentado na Figura 4 inicia com o INVITE na primeira linha, onde são enviados os parâmetros de sessão para negociação com o destino. A Figura 5 apresenta o conteúdo SDP deste INVITE, com os campos padrões para estabelecimento de sessão, como identificação da origem, portas utilizadas, protocolo de mídia e opções de codec.

```

49 192.168.0.1 192.168.0.51 SIP/SDP Request: INVITE sip:2148@adm2.voip.ufsc.br;user=phone
<
> Ethernet II, Src: Polycom_85: (64:16:7f:85: ), Dst: IETF-VRRP-VRID_f8 (00:00:5e: )
> Internet Protocol Version 4, Src: 192.168.0.1 , Dst: 192.168.0.51
> User Datagram Protocol, Src Port: 5080, Dst Port: 5080
v Session Initiation Protocol (INVITE)
  > Request-Line: INVITE sip:2148@ .ufsc.br;user=phone SIP/2.0
  > Message Header
  v Message Body
    v Session Description Protocol
      Session Description Protocol Version (v): 0
      > Owner/Creator, Session Id (o): - 1505586946 1505586946 IN IP4 192.168.0.1
      Session Name (s): Polycom IP Phone
      > Connection Information (c): IN IP4 192.168.0.1
      > Time Description, active time (t): 0 0
      Session Attribute (a): sendrecv
      > Media Description, name and address (m): audio 2232 RTP/AVP 9 0 8 18 127
      > Media Attribute (a): rtpmap:9 G722/8000
      > Media Attribute (a): rtpmap:0 PCMU/8000
      > Media Attribute (a): rtpmap:8 PCMA/8000
      > Media Attribute (a): rtpmap:18 G729/8000
      > Media Attribute (a): fmtp:18 annexb=no
      > Media Attribute (a): rtpmap:127 telephone-event/8000
  
```

Figura 47. Campos SDP de INVITE sem oferta de criptografia

O software Wireshark, utilizado para analisar este tráfego, possui a capacidade de conversão de pacotes para fluxos de áudio, assim foi possível obter e ouvir o áudio da chamada, conforme representado graficamente na Figura 6.

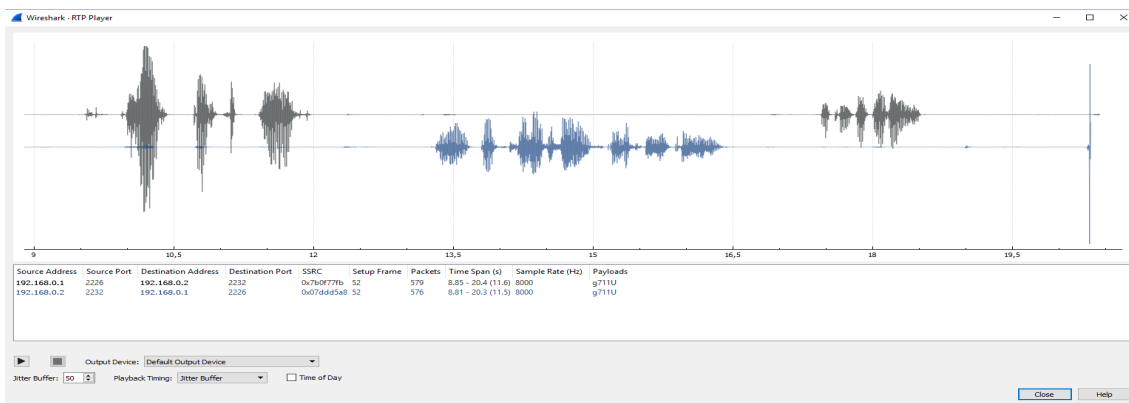
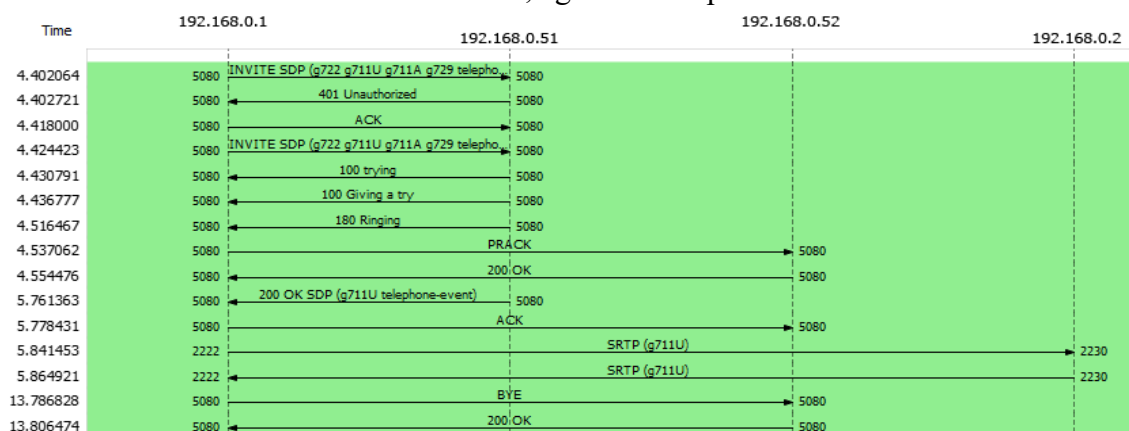


Figura 6. Conversão do tráfego RTP em fluxo de áudio compreensível

Após aplicadas as configurações de segurança nos telefones IP e *gateway*, novos testes foram realizados. A Figura 7 apresenta o fluxo de uma chamada realizada entre os mesmos telefones VVX e SoundPoint IP, agora com o protocolo SRTP habilitado.



**Figura 7. Fluxo de chamada SIP utilizando SRTP**

É possível notar na Figura 7 que houve a substituição do protocolo de mídia para SRTP. Os parâmetros de sessão do INVITE desta chamada são apresentados na Figura 8, onde é possível identificar a oferta de dois perfis de mídia, a primeira RTP/SAVP (*Secure Audio Video Profile*), com parâmetros adicionais de criptografia, e a segunda RTP/AVP (*Audio Video Profile*), com os mesmos campos da chamada realizada anteriormente. Desta forma o destino poderá optar por aceitar uma chamada segura ou não.

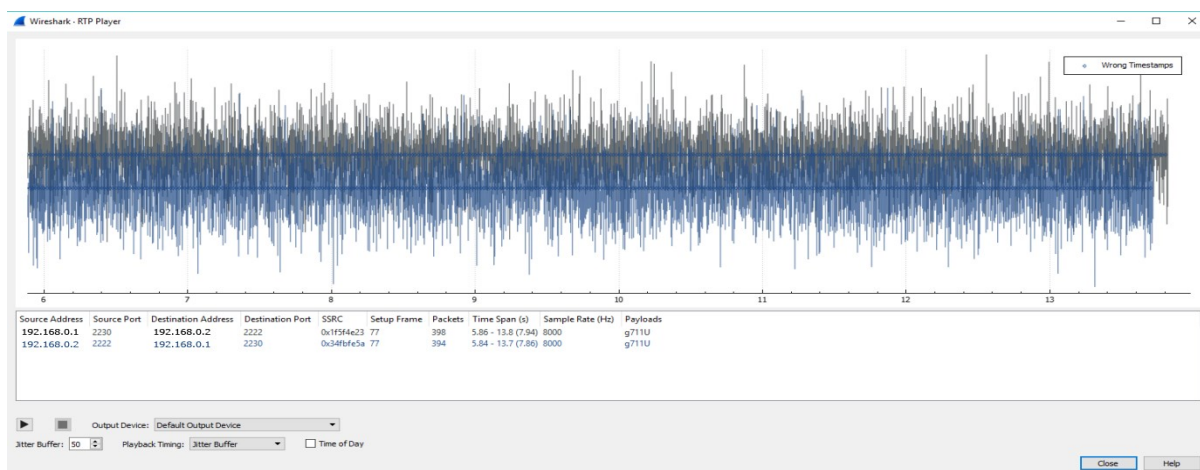
```

<
Request-Line: INVITE sip:2148@adm2.voip.ufsc.br;user=phone SIP/2.0
Message Header
Message Body
  Session Description Protocol
    Session Description Protocol Version (v): 0
    Owner/Creator, Session Id (o): - 1505592283 1505592283 IN IP4 192.168.0.1
    Session Name (s): Polycom IP Phone
    Connection Information (c): IN IP4 192.168.0.1
    Time Description, active time (t): 0 0
    Session Attribute (a): sendrecv
    Media Description, name and address (m): audio 2222 RTP/SAVP 9 0 8 18 127
    Media Attribute (a): crypto:3 AES_CM_128_HMAC_SHA1_80 inline:4AdwakUJzLH4hrbDvDX3bB2Pjgge/903c3ii/xaZ
    Media Attribute (a): rtpmap:9 G722/8000
    Media Attribute (a): rtpmap:0 PCMU/8000
    Media Attribute (a): rtpmap:8 PCMA/8000
    Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute (a): fmp:18 annex=no
    Media Attribute (a): rtpmap:127 telephone-event/8000
    Media Description, name and address (m): audio 2222 RTP/AVP 9 0 8 18 127
    Media Attribute (a): rtpmap:9 G722/8000
    Media Attribute (a): rtpmap:0 PCMU/8000
    Media Attribute (a): rtpmap:8 PCMA/8000
    Media Attribute (a): rtpmap:18 G729/8000
    Media Attribute (a): fmp:18 annex=no
    Media Attribute (a): rtpmap:127 telephone-event/8000

```

**Figura 8. Campos SDP de INVITE com oferta de criptografia**

Após coleta do tráfego desta chamada utilizando o protocolo SRTP, foi utilizada novamente a ferramenta Wireshark para converter os pacotes de mídia em fluxo de áudio, e o resultado foi a geração de áudio apenas em formato de ruído, graficamente representado pela Figura 9.



**Figura 9. Conversão do tráfego SRTP em fluxo de áudio não compreensível**

Os testes entre telefones IP e gateway também foram bem sucedidos, com a mídia sendo criptografada de ponto a ponto.

### 3.3. Segmentação da rede VoIP

O ambiente de telefonia em estudo é composto por servidores, *gateways* e terminais SIP. Dentre estes componentes, os servidores e os *gateways* estão em uma rede dedicada para telefonia, utilizando ACLs para controle de acesso externo. Já os terminais telefônicos IP estão distribuídos por toda a instituição através das mesmas sub-redes de navegação utilizadas pelos computadores, sendo estas mais abertas devido à diversidade de serviços que podem acessar.

Estando os terminais VoIP em sub-redes de dados, estes apresentam maior vulnerabilidade a ataques externos. Além de estarem suscetíveis a ataques de negação de serviço, os terminais telefônicos tornam-se potenciais pontos de entrada para agentes maliciosos ao sistema de telefonia, uma vez que são dispositivos autorizados a utilizar os recursos providos. A inserção de códigos maliciosos nos terminais pode gerar degradação do serviço, chamadas indesejadas e ainda custos financeiros para a instituição.

Buscou-se, portanto, uma solução que atenda os seguintes requisitos:

- Isolar a rede dos aparelhos telefônicos IP dos demais dispositivos da rede;
- Possibilitar a restrição de acesso aos telefones baseado em IPs e portas;
- Manter o compartilhamento de portas dos switches entre telefones e computadores.

A solução encontrada que atende os requisitos mencionados é a implementação de Voice VLAN nos switches da rede. Este recurso permite distribuir uma rede dedicada para os dispositivos de telefonia, sendo esta identificada com uma tag de VLAN até o switch de borda, que deverá detectar automaticamente a presença de telefones IP em suas portas e então passar esta rede adequadamente.

O parque de rede camada dois da universidade é composto em sua maioria por switches gerenciáveis dos fabricantes D-Link e Cisco, portanto o trabalho limitou-se a implementações nos equipamentos destes fabricantes, sendo que ambos disponibilizam o recurso de Voice VLAN.

O switch D-Link implementa segmentação do tráfego de voz através da verificação do MAC de origem dos quadros que recebe nas portas de acesso. O switch verifica se os três primeiros octetos do MAC se encontram na tabela de OUI (*Organizationally Unique Identifier*) previamente configurada e caso positivo, marca os quadros com a tag da VLAN de voz. Uma mesma porta pode, portanto, possuir uma VLAN para dados e uma VLAN para voz, com o switch separando os tráfegos de acordo com o MAC dos quadros que recebe. A Figura 10 apresenta a tabela OUI de um switch D-Link utilizado para testes, onde estão cadastrados OUIs de alguns fabricantes.

```
SeTIC_01-2011-01-11# show voice_vlan oui-table

OUI      Description
-----
00:04:f2 Polycom UFSC
00:0b:82 Grandstream
00:0e:08 Linksys
64:16:7f Polycom UFSC 2

SeTIC_01-2011-01-11#
```

Figura 10. Tabela OUI em um switch D-Link

Com a habilitação de Voice VLAN nas portas de acesso do switch, caso um telefone seja conectado, receberá IP da rede de voz, enquanto um computador conectado na porta PC deste telefone permanecerá na rede de dados, uma vez que o MAC do computador não está cadastrado na tabela OUI na qual o switch associa a VLAN de voz.

Os switches Cisco implementam a descoberta de dispositivos através do protocolo LLDP (*Link-Layer Discovery Protocol*). O protocolo LLDP é definido pelo padrão IEEE 802.1AB e permite que dispositivos diretamente conectados comuniquem entre si, através da camada 2, quais são as suas principais funções e capacidades, dentre elas se são dispositivos de telefonia, *bridges* ou roteadores. O protocolo permite informar também dados relacionadas a gerenciamento de energia PoE (Power over Ethernet) e VLAN, possibilitando automatização de configurações entre dispositivos.

A Figura 11 apresenta uma consulta resumida realizada em um switch Cisco no qual são detectados os dispositivos vizinhos que respondem a este protocolo, sendo um deles um telefone IP Polycom. Os telefones utilizados no ambiente de telefonia respondem no campo “Capability” as opções T e B, correspondentes a *Telephone* e *Bridge*, uma vez que estes dispositivos também possuem uma porta para estender a rede até um computador.

```
SeTIC_01-2011-01-11#show lldp neighbors
Capability codes:
  (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
  (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf         Hold-time  Capability  Port ID
Polycom SoundPoint IGil/0/17          112        B,T         0004.f2
SeTIC-Sala4[251    Gil/0/24           104        B           1:23
sala4-Infoway      Gil/0/12           99         S           0024.1d

Total entries displayed: 3

SeTIC_01-2011-01-11#
```

Figura 48. Consulta de dispositivos conectados através de LLDP no switch Cisco

Conforme apresentado na Figura 11, o telefone informa no campo *Capability* as informações “B,T”, correspondentes a *Telephone* e *Bridge*. Possuindo esta informação, o switch identifica que há um telefone na porta e insere a tag da Voice VLAN nos quadros que recebe do telefone, mantendo quadros sem tag para o computador. O protocolo permite ainda que o telefone identifique a VLAN de voz utilizada e se autoconfigure para trabalhar reconhecendo e inserindo a tag da Voice VLAN, o que não ocorre com o switch D-Link, que precisa remover a tag do quadro quando passa para a porta do telefone.

Como a universidade possui aproximadamente 3500 telefones IP, uma única rede com todos estes dispositivos geraria um tráfego de *broadcast* muito grande. A solução proposta está na criação de domínios de broadcast de no máximo 512 IPs, adotando assim sete sub-redes de voz. Estas redes podem ser distribuídas por blocos de ambientes físicos da universidade, como centros e campi.

Atualmente, a rede da universidade não possui disponível sete faixas contínuas de 512 IPs, portanto, uma alternativa está na criação de novas sub-redes utilizando IPs privados. Recomenda-se a utilização de faixas de IP classe B, pois possuem a quantidade de redes e hosts suficientes para a criação das sub-redes necessárias, com possibilidades de posterior expansão. Um exemplo de dimensionamento de IPs para as redes de voz pode ser observado na Tabela 1.

**Tabela 1. Dimensionamento de IPs para as redes de voz**

TAG	Rede	Máscara	Broadcast	Host mínimo	Host máximo	nº hosts
3001	172.16.0.0	255.255.254.0	172.16.1.255	172.16.0.1	172.16.1.254	510
3002	172.16.2.0	255.255.254.0	172.16.3.255	172.16.2.1	172.16.3.254	510
3003	172.16.4.0	255.255.254.0	172.16.5.255	172.16.4.1	172.16.5.254	510
3004	172.16.6.0	255.255.254.0	172.16.7.255	172.16.6.1	172.16.7.254	510
3005	172.16.8.0	255.255.254.0	172.16.9.255	172.16.8.1	172.16.9.254	510
3006	172.16.10.0	255.255.254.0	172.16.11.255	172.16.10.1	172.16.11.254	510
3007	172.16.12.0	255.255.254.0	172.16.13.255	172.16.12.1	172.16.13.254	510

Com a criação das setes sub-redes indicadas, haverá IPs para 3570 telefones, com a escalabilidade de se adicionar novas sub-redes na sequência. Para operacionalização destas novas faixas de IP, é necessário a criação de novos escopos no DHCP, configuração de roteamento para as demais redes, implementação de ACLs para controle de acesso e configuração das novas VLANs em todos os switches da universidade.

Com a segmentação da rede de voz, as ACLs poderão realizar as seguintes restrições de acesso:

- Restringir a comunicação SIP dos terminais apenas para o servidor PBX-IP, que realiza SIP proxy de todas as chamadas;
- Restringir a comunicação com as redes de dados apenas para portas de mídia, já que este tráfego é realizado diretamente entre os terminais e alguns deles poderão ainda ficar nessas redes;
- Restringir tráfego de serviços de rede, como NTP, apenas para a rede de servidores;
- Permitir demais acessos apenas para a rede de gerência.



#### 4. Considerações finais

A proposta de segurança sobre os dados de provisionamento demonstrou-se eficaz e viável. Através do uso de certificado digital assinado por uma AC confiável foi possível estabelecer uma transmissão de dados criptografada entre o servidor e os clientes. A autenticação dos dispositivos no servidor através de certificados também apresentou funcionamento adequado, permitindo acesso apenas aos equipamentos desejados e bloqueando possíveis tentativas de acesso indevido.

A proposta de criptografia de voz através do protocolo SRTP é viável e funciona. Com os pacotes de mídia cifrados entre os terminais, não foi possível reconstituir o fluxo de áudio compreensível através de uma captura e ordenação de conteúdo. Além de prover confidencialidade nas chamadas, a utilização do SRTP também mostrou-se adequada devido a diversidade de dispositivos que o implementam, reduzindo assim problemas de interoperabilidade. Durante os testes não foi notada qualquer degradação do áudio.

A proposta de segmentação da rede de voz através de Voice VLAN também é efetiva. O recurso possibilitou a distribuição dinâmica de uma rede dedicada para dispositivos VoIP, provendo maior isolamento e segurança contra ataques de acesso indevido e negação de serviço. Com a possibilidade de compartilhamento de portas dos switches entre telefones e estações de trabalho, mesmo havendo a necessidade inicial de configurar todos os ativos de rede, esta solução resulta na economia de tempo com a posterior disponibilização automática de portas. Também resulta na manutenção da portabilidade dos terminais telefônicos e economia de milhares de pontos de rede, garantindo, portanto, uma implantação transparente e sem custos adicionais.

As soluções foram aplicadas sobre equipamentos proprietários, porém as tecnologias e protocolos são públicos e podem ser utilizados em qualquer outro ambiente.

#### Referências

- Alexander, A., Wijesinha, A. e Karne, R. (2009) “An Evaluation of Secure Real-Time Transport Protocol (SRTP) Performance for VoIP”. Em: Third International Conference On Network And System Security, [s.l.], p.1-1.
- F. Audet. (2009) “[RFC 5630] The Use of the SIPS URI Scheme in the Session Initiation Protocol (SIP)”.
- H. Schulzrinne et al. (2003) “[RFC 3550] RTP: A Transport Protocol for Real-Time Applications”.
- J. Rosenberg et al. (2002) “[RFC 3261] SIP: Session Initiation Protocol.”
- M. Baugher et al. (2004) “[RFC 3711] The Secure Real-time Transport Protocol (SRTP)”.
- M. Handley et al. (2006) “[RFC 4566] SDP: Session Description Protocol”
- Rehman, U. e Abbasi, G. (2014) “Security analysis of VoIP architecture for identifying SIP vulnerabilities”. Em: International Conference On Emerging Technologies (icet), [s.l.].
- Silva, F. e Jesus Júnior, S. (2013) “Análise dos aspectos de segurança da informação em um ambiente de comunicações unificadas.”. Em: TCC (Graduação) - Curso de Engenharia de Redes de Comunicação, Universidade de Brasília.