UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE ESPECIALIZAÇÃO EM TECNOLOGIAS, GERÊNCIA E SEGURANÇA DE REDES DE COMPUTADORES

ANDRÉ SCOMAZZON ANTONIAZZI

Segurança em VoIP: Ameaças, Vulnerabilidade e as Melhores Práticas de Segurança

Trabalho de Conclusão apresentado como requisito parcial para a obtenção do grau de Especialista

Prof. Dr. João Netto
Orientador

Prof. Dr. Sérgio Luis Cechin
Prof. Dr. Luciano Paschoal Gaspary
Coordenadores do Curso

Porto Alegre, dezembro de 2008.

AGRADECIMENTO

Ao amigo e colega de profissão Juliano Murlick pelo incentivo e apoio que foram fundamentais na decisão de realizar esse curso de especialização.

Ao amigo e colega de profissão Sony Ribeiro Stachlewski pela experiência e conhecimento compartilhados sempre muito prestativo em me auxiliar nos meus primeiros passos no mundo de Voz sobre IP.

Ao Dr. João Netto, pela orientação que me possibilitou concluir esse trabalho.

A minha família, pelo amor incondicional, pelo incentivo e apoio incessantes, pelos valores morais transmitidos, por tudo que sou.

Em especial, à querida Fernanda pela compreensão com que tem convivido e suportado minhas angustias e minha ausência nessa etapa da minha vida.

A todos, meu singelo agradecimento.

"O pessimista se queixa do vento, o otimista espera que ele mude e o realista ajusta as velas."

William George Ward

SUMÁRIO

LISTA DE ABREVIATURAS E SIGLAS

ACK	Acknowledge
AES	Advanced Encryption Standard
AH	Authentication Header
AOR	Address Of Register
ARP	Address Resolution Protocol
DDOS	Distributed Denial of Service
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DOS	Denial Of Service
DP	Disponibilidade Planejada
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	Internet Protocol Security
ITU-T	International Telecommunications Union – Telecommunication Standardization Sector
MAC	Media Access Control

MCU	Multipoint Control Unit
MEGACO	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MIME	Multipurpose Internet Mail Extensions
MIKEY	Multimedia Internet Keying
MKI	Master Key Identifier
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PING	Packet Inter-Network Groper
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standards
QOS	Quality of Service
RAS	Registration, Admission and Status
RDSI	Rede Digital de Serviços Integrados
RFC	Request For Comment
RPC	Remote Procedure Call
RPTC	Rede Pública de Telefonia Comutada
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
SA	Security Association
SCTP	Stream Control Transmission Protocol
SDP	Session Description Protocol
SIMPLE	Session Initiation Protocol for Instant Messaging, and Presence Leveraging Extensions
SIP	Session Initiation Protocol
SIPS	Session Initiation Protocol Secure
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SRTCP	Secure Real-Time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol

SSL	Secure Socket Layer
SYN	Synchronize
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
VOIP	Voice Over Internet Protocol
VPN	Virtual Private Network

LISTA DE FIGURAS

LISTA DE TABELAS

RESUMO

A tecnologia de voz sobre IP (VoIP) há algum tempo não é mais apenas uma novidade. Cada vez mais as pessoas e as organizações estão usufruindo os benefícios da convergência dos sistemas de comunicação de voz para as redes IP. Essa mudança está ocorrendo, sobretudo devido às inúmeras vantagens que a tecnologia promove, seja na redução dos custos envolvidos em infra-estrutura, que passa a ser compartilhada com a rede de dados, seja na disponibilização de novos serviços. Somado a esses fatores, a crescente evolução da infra-estrutura de rede que passou a fornecer bandas cada vez maiores a preços acessíveis com mecanismos mais eficientes de qualidade de serviço, possibilitou um ambiente fértil para a proliferação das aplicações de voz sobre IP. Contudo, a segurança das informações nesse cenário passa a ser um desafio. Pois, juntamente com as inúmeras ameaças e vulnerabilidade que todas as aplicações que operam na rede IP estão sujeitas, somam-se inúmeras outras que nasceram com a descrição dos protocolos que formam os serviços e as aplicações de voz sobre IP. Sendo assim, esse trabalho visa descrever as principais ameaças e vulnerabilidades que afetam o VoIP ao mesmo tempo em que traz um panorama das melhores práticas de segurança que podem ser empregadas a fim de tornar essa tecnologia mais confiável e segura.

Palavras-Chave: VoIP, Segurança, Vulnerabilidades, Ameaças

VoIP Security: Threats, Vulnerabilities and Security Best Practices

ABSTRACT

Voice over IP technology (VoIP) has become increasingly common lately. More and more people and companies are enjoying the benefits of the convergence of voice communication systems for IP networks. Such a change is taking place mainly because of the several advantages offered by this technology, either regarding the reduction of infrastructure costs, since infrastructure is shared by the data network, or in terms of availability of new services. In addition to these factors, the increasing progress of the network infrastructure, which has been providing broader bands at reasonable prices and more efficient mechanisms of service quality, made it possible to create a fertile environment that promoted the proliferation of voice over IP applications. However, in this scenario, information security has become a challenge, since, besides the countless threads and vulnerabilities involving the applications that operate on the IP network, there are several other threads created because of the description of the protocols that constitute the voice over IP services and applications. Therefore, the objective of this study is to describe the main threads and vulnerabilities affecting VoIP and, at the same time, to present an overview of the security best practices available to make this technology more reliable and safer.

Keywords: VoIP, Security, Vulnerabilities, Threats

1 INTRODUÇÃO

A possibilidade de transmissão de serviços de voz sobre a rede IP, tecnologia conhecida pela sigla VoIP – *Voice over IP*, tem se mostrado uma solução bastante atraente no mercado de comunicação mundial. As altas tarifas cobradas pelos serviços de telefonia convencionais atrelada a uma infra-estrutura de comutação de circuitos que pouco tem evoluído nos últimos anos, pouco combinam com a expectativa dos consumidores frente aos avanços e necessidades de comunicação do mundo moderno.

Em contrapartida, a convergência dos serviços de voz para as redes de dados proporciona, além da economia de recursos devido à consolidação de uma plataforma de rede integrada, um aumento de produtividade na medida em que essa integração facilita a interação e o controle sobre a informação com os diferentes serviços e aplicações de uma plataforma tecnológica unificada.

Todavia, a migração do serviço de voz de um sistema de telefonia convencional para o sistema de voz sobre IP deve ser planejada com muita cautela, sobretudo em relação a aspectos de segurança. Afinal, as aplicações de VoIP além de herdarem todas as ameaças que afetam as redes de dados, também estão vulneráveis a ameaças atreladas à própria tecnologia.

Sendo assim, o objetivo deste trabalho é alertar sobre os aspectos de segurança que afetam os serviços e aplicações de voz sobre IP, apresentando suas principais ameaças e vulnerabilidade ao mesmo tempo em que apresenta um panorama das melhores práticas de segurança que podem ser empregadas a fim de tornar essa tecnologia mais confiável e seguro.

Com esse intuito, o trabalho foi dividido da seguinte forma: no Capitulo 2 serão apresentados os princípios fundamentais e alguns conceitos de Segurança da Informação. No capítulo 3 serão apresentadas uma visão geral acerca da tecnologia VoIP, alguns dos principais protocolos e uma breve descrição do funcionamento de cada um deles. Já no capítulo 4 serão discutidas as principais ameaças e vulnerabilidade que afetam os serviços e aplicações de voz sobre IP, enquanto que no capítulo 5 serão analisadas as melhores práticas que podem ser adotadas como forma de proteção contra essas ameaças e vulnerabilidades. Por fim, no capítulo 6 serão feitas as considerações finais do trabalho.

2 SEGURANÇA DA INFORMAÇÃO

Esse tópico tem como objetivo apresentar ao leitor alguns conceitos e fundamentos envolvidos em segurança da informação.

2.1 Conceito

Segundo a norma ABNT NBR ISO/IEC 17799:2005, segurança da informação é definida como a proteção da informação, nas diversas formas que ela pode existir, de uma série de ameaças com o objetivo de garantir a continuidade do negócio, minimizar o risco ao negócio e maximizar o retorno sobre o investimento e as oportunidades de negócio.

2.2 Princípios fundamentais de segurança

A segurança da informação está calcada sobre três princípios fundamentais que são: a disponibilidade, a integridade e a confidencialidade das informações de um dado negócio. Estes três princípios fundamentais, muitas vezes referenciados na literatura por tríade AIC (*availability*, *integrity* e *confidenciality*) ou tríade CID, servem de base para a definição do modelo de segurança que fornecerá as proteções necessárias para atender aos objetivos do negócio. Todos os controles de segurança, mecanismos e proteções são implementados para fornecer um ou mais desses princípios e todos os riscos, ameaças e vulnerabilidades são mensurados com base na probabilidade de que um ou mais deles sejam comprometidos (HARRIS, 2008). Além dos princípios fundamentais já referenciados, outras propriedades como a autenticidade e o não-repúdio complementam a segurança da informação (ISO/IEC 17799:2005).

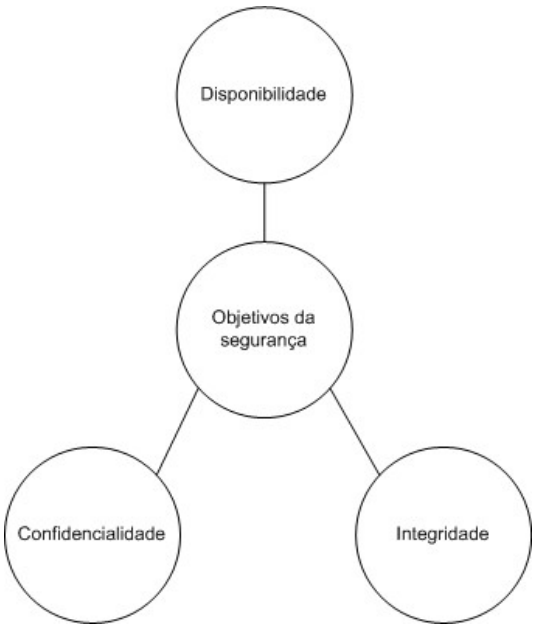

Figura 2.1: Tríade CID

2.2.1 Disponibilidade

Disponibilidade pode ser definida como a probabilidade de um sistema estar em funcionamento e pronto para uso em um dado instante de tempo. Dependendo do valor dessa probabilidade os sistemas são classificados como de Disponibilidade básica, alta ou contínua. O cálculo da disponibilidade é dado pela formula DP = MTBF/(MTBF+MTTR) onde:

- DP é a Disponibilidade Planejada;
- MTBF é o tempo médio entre a ocorrência de uma falha e a próxima, representando também o tempo de funcionamento do serviço de TI diante da necessidade do negócio até a falha seguinte, e
- MTTR é o tempo para reparar e disponibilizar o serviço de TI para seu estado de funcionamento normal.

Valores de DP entre 99% e 99,9% representam sistemas de disponibilidade básica e se caracterizam por não possuir nenhum mecanismo tanto de hardware como de software para mascarar eventuais falhas. Sistemas de alta disponibilidade possuem DP entre 99,9% e 99,999%, valores muitas vezes atingidos mediante o uso de mecanismos especializados para a detecção, recuperação e mascaramento de falhas. Acima dos valores especificados têm-se sistemas que mesmo quando ocorram paradas programadas ou não programadas eles sempre permanecem disponíveis. Geralmente são caracterizados como sistemas de missão crítica onde qualquer parada ocasiona prejuízo ao negócio (MAGALHÃES, 2007).

"O gerenciamento da disponibilidade garante que os serviços estarão disponíveis sempre que forem solicitados e deve estar alinhado com a demanda do negócio, custos requeridos, configuração e complexidade da infra-estrutura de TI, processo e procedimentos utilizados pelos serviços de TI, fatores humanos e eventos externos" (MAGALHÃES, 2007).

2.2.2 Integridade

Integridade é o princípio que trata da legitimidade e consistência da informação no que se refere às permissões para modificação de seu conteúdo as quais são definidas pelo proprietário da informação e devem ser garantidas durante todo o seu ciclo de vida. (STEWART, 2008)

A integridade pode ser vista de três perspectivas:

- Sujeitos não autorizados devem ser impedidos de realizar modificações.
- Sujeitos autorizados devem ser impedidos de realizar modificações não autorizadas, tais como erros.
- A informação, esteja ela armazenada, em trânsito ou em processamento, deve ser legítima, consistente e verificável (STEWART, 2008).

Para garantir a integridade de um sistema, além de um rígido controle de acesso, um sistema de *log* de atividade deve ser empregado para assegurar que somente usuários autorizados possam acessar seus respectivos recursos (STEWART, 2008).

2.2.3 Confidencialidade

Confidencialidade é o princípio que assegura a proteção da informação contra o acesso e divulgação não autorizados esteja ela armazenada, em processamento ou em trânsito. Lembrando que a violação da confidencialidade pode ocorrer não somente por modo deliberado na forma de ataques como captura de tráfego de rede, engenharia social e *port scan*, mas também de modo acidental por erro humano, imperícia ou negligência (STEWART, 2008).

Segundo Porter, "a criptografia e a codificação de dados são exemplos de métodos usados para garantir a confidencialidade da informação durante sua transmissão entre origem e destino" (2006, p.13).

Além da criptografia, outros mecanismos como controle de acesso restrito, rígidos processos de autenticação e treinamento podem auxiliar na garantia da confidencialidade da informação (STEWART, 2008).

2.2.4 Autenticidade

Pode ser classificada como uma sub-propriedade da integridade. A Autenticidade trata da legitimidade da informação esteja ela no formato eletrônico ou físico. É muito utilizada em mecanismos de controle de acesso, em comunicações e transações eletrônicas assim como na autenticação de documentos. A assinatura digital é um exemplo de instrumento utilizado para se garantir a autenticidade da informação e a identidade de quem se intitula proprietário dela (STEWART, 2008).

2.2.5 Não-repudio

Não-Repúdio é a propriedade da segurança que garante que o emissor de uma mensagem enviada eletronicamente não poderá negar sua autoria posteriormente. Assim como na autenticidade, a assinatura digital é freqüentemente usada como instrumento para se obter tal garantia (STEWART, 2008).

2.3 Definições de Segurança

Esse tópico visa apresentar algumas definições de segurança importantes para o entendimento da segurança em redes VoIP.

2.3.1 Vulnerabilidade

Caracteriza os sistemas que podem ser explorados de forma mal intencionada e sem as devidas permissões em virtude de falhas latentes não protegidas ou má configuração em seus componentes. Essas vulnerabilidades podem estar relacionadas a softwares, hardwares e processos e possibilitam que alguém mal intencionado comprometa o funcionamento do sistema. (HARRIS, 2008)

2.3.2 Ameaça

Define como uma vulnerabilidade pode ser explorada. A entidade que tira proveito de uma vulnerabilidade para explorar um sistema é definida como agente da ameaça. Esse agente pode ser uma pessoa, um processo ou um evento natural do mundo físico. Ex. Invasor, vírus, queda de energia, raio. (HARRIS, 2008)

2.3.3 Risco

"É definida como a probabilidade de um agente de ameaça tirar vantagens de uma vulnerabilidade e os impactos resultantes no negócio" (HARRIS, 2008, p.62). Como exemplo, um ambiente computacional utilizando software de antivírus desatualizado tem um risco maior de ser contaminado por vírus e, conseqüentemente, de queda de produtividade.

2.3.4 Proteção

É usada para reduzir o risco potencial. Pode ser um elemento de software, hardware ou procedimento que tenta eliminar as vulnerabilidades ou diminuir a probabilidade que elas sejam exploradas pelos agentes de ameaças. Ex. Firewall, antivírus, política de senhas fortes, etc. (HARRIS, 2008).

2.3.5 Incidente

É caracterizado quando um agente de ameaça consegue de fato explorar uma vulnerabilidade provocando a violação de um dos princípios fundamentais da segurança (Tríade AIC) (HARRIS, 2008).

3 VOZ SOBRE IP

VoIP - *Voice over Internet Protocol* – é a tecnologia que permite o estabelecimento de uma comunicação de voz pela rede IP graças a técnicas de conversão de sinais de áudio analógicos em sinal digitais (BATES, 2002).

Em comparação com a Rede Pública de Telefonia Comutada – RPTC - que utiliza circuitos comutados na prestação dos seus serviços, e que, por essa razão trabalha com uma banda de tamanho fixo dedicada do início ao fim de uma ligação, a Telefonia sobre IP usa a rede de dados e compartilha a banda com outras aplicações e seus tráfegos na rede IP (BATES, 2002).

A intercomunicação entre os diferentes produtos da indústria do VoIP só foi possível graças a aceitação por parte delas dos padrões de protocolos de sinalização e mídia especificados por organizações como a IEEE, IETF, 3GPT e ITU-T (THERMOS, 2007).

Protocolos de sinalização são usados para estabelecer, manter e encerrar chamadas além de servir de suporte à bilhetagem e parâmetros de negociação da chamada como portas de mídia, chave de criptografia e *codecs*. Adicionalmente são responsáveis pela interoperabilidade entre dispositivos já que são usados para negociar os *codecs* que fazem a conversão entre sinais de áudio analógicos em pacotes digitais (THERMOS, 2007).

Já os protocolos de mídia são usados para realizar a transferência fim a fim dos pacotes. RTP (Real Time Protocol) é o protocolo de *stream* de mídia freqüentemente utilizado em VoIP. Como exemplo de protocolos de sinalização pode-se citar SIP, MGCP e H.323 (THERMOS, 2007).

3.1 Protocolos VoIP

Em uma chamada VoIP são utilizados três protocolos na camada de aplicação do modelo TCP/IP:

NTP – *Network Time Protocol* – é usado para verificar se os sinais são transmitidos e recebidos numa janela de tempo aceitável para a qualidade do serviço.

RTP – *Real Time Protocol* – fornece funcionalidade de transporte fim a fim para os sinais de voz encapsulados nos pacotes VoIP.

RTCP – *Real Time Control Protocol* – fornece controle simplificado para assegurar a entrega dos pacotes de VoIP enviados via RTP.

Já na camada de transporte, por se tratar de uma aplicação em tempo real em que a rapidez na entrega dos pacotes (que deve ocorrer na ordem de nanosegundos) é mais

importante que a garantia de sua entrega no destino, o protocolo utilizado é o UDP (*User datagram protocol*) (KELLY, 2005).

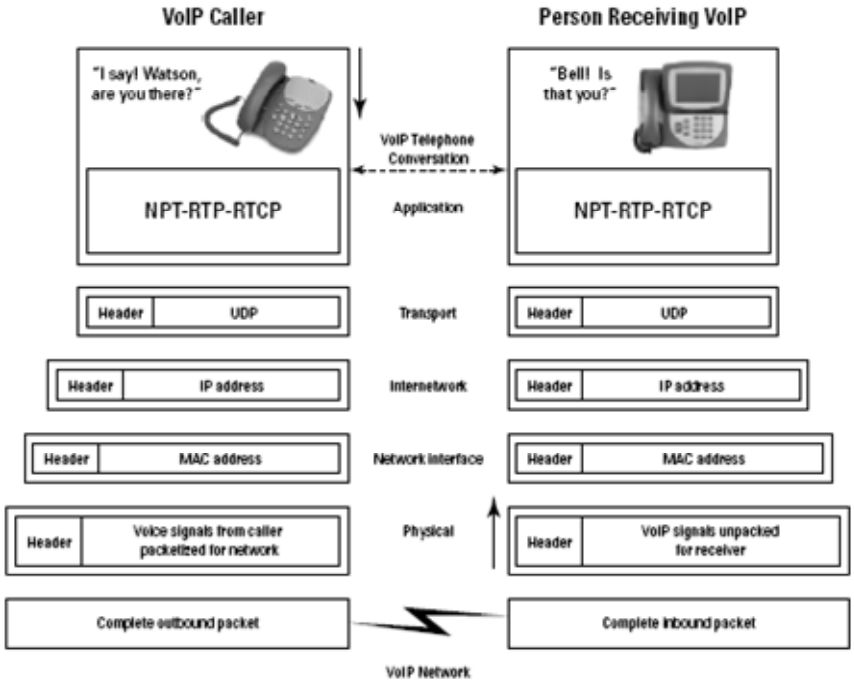

Figura 3.1: Fluxo de uma ligação VoIP pelas camadas do modelo TCP/IP (KELLY, 2005)

Apesar das vantagens econômicas da convergência de voz na rede IP proporcionada principalmente pela diminuição do custo envolvido no gerenciamento e manutenção de infra-estruturas de rede distintas para tráfego de voz e dados, a tecnologia de VoIP passa a herdar todas as vulnerabilidades intrínsecas das aplicações que operam sobre redes TCP/IP. (THERMOS, 2007)

3.1.1 H.323

H.323 é o conjunto de protocolos e especificações elaborados pela *International Telecommunications Unit* (ITU) para a comunicação em tempo real de áudio, vídeo e dados sobre a rede IP (PORTER, 2007).

Esse padrão, que foi criado com a finalidade de garantir a compatibilidade e interoperabilidade entre os equipamentos de Telefonia IP de diferentes fabricantes, permite uma variedade de configurações na comunicação multimídia, contudo, a comunicação de áudio é obrigatória enquanto que a comunicação de vídeo e dados é opcional (TUCKER, 2005).

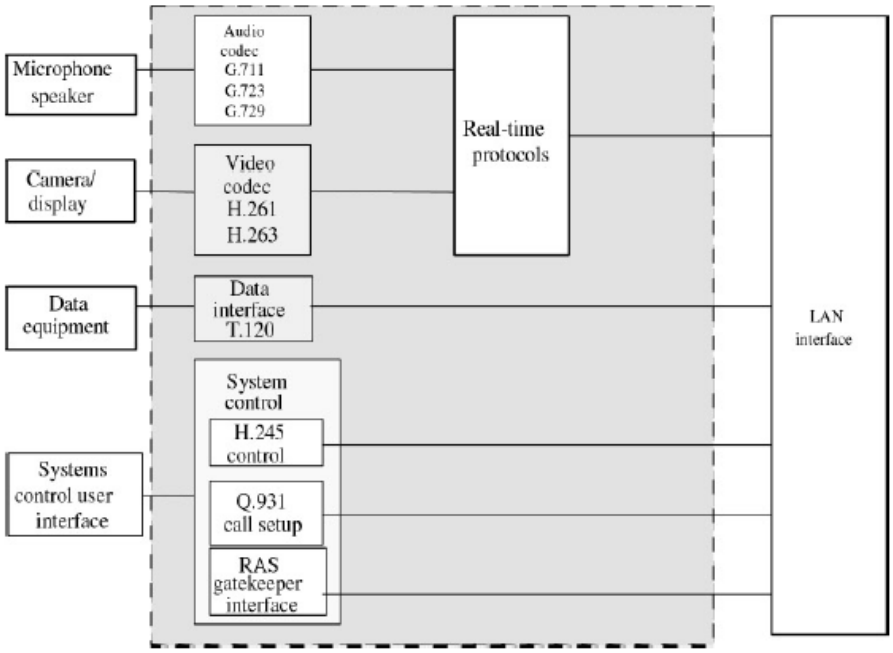

Figura 3.2: Visão geral dos elementos e protocolos do padrão H.323 (BATES, 2002)

O H.323 define quatro tipos de componentes:

- Terminais – são os dispositivos com os quais os usuários interagem na comunicação (telefones, *softphones*, câmeras de vídeo, etc.).
- Gateways – é um elemento opcional na infra-estrutura de rede sobre IP que tem a função de negociar a sinalização e o transporte da mídia servindo como interface entre outros tipos de rede (RPTC, RDSI, etc.)
- Gatekeepers – sua principal função é traduzir os endereços dos nomes simbólicos em endereços IP na infra-estrutura de rede do H.323. Adicionalmente gerencia serviços e recursos de rede prestados aos terminais através do protocolo RAS. (Ex. controle de banda, gerenciamento da zona controle de admissão no H.323). Assim como o gateway ele é opcional e muitas vezes estão no mesmo dispositivo físico na rede.
- MCU's – é o dispositivo que possibilita o estabelecimento de uma conferencia multiponto entre três ou mais terminais (PORTER, 2007).

Além destes componentes, o padrão H.323 define um conjunto de protocolos específicos para cada necessidade envolvida na comunicação de VoIP.

- H.225/Q931 – protocolos usados na sinalização e configuração da chamada entre terminais
- H.225/RAS – protocolos usados na sinalização e configuração de chamadas entre *gatekeepers* ou entre um terminal e um *gatekeeper*.
- H.245 – protocolo de controle da chamada que negocia parâmetros do tipo de mídia e de compatibilidade entre os terminais que desejam iniciar uma comunicação

- RTP e RTCP – usados para o transporte fim a fim dos pacotes envolvidos na comunicação no padrão H.323
- Codecs (G.711, G.723.1 e G.729) – protocolos usados na compressão de áudio (PORTER, 2007).

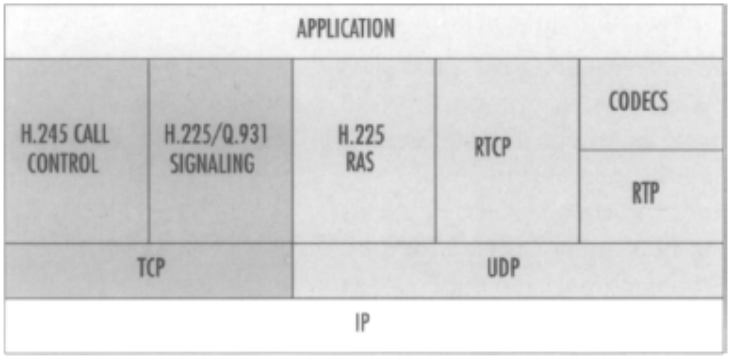

Figura 3.3: Pilha de protocolos H.323 (PORTER, 2007)

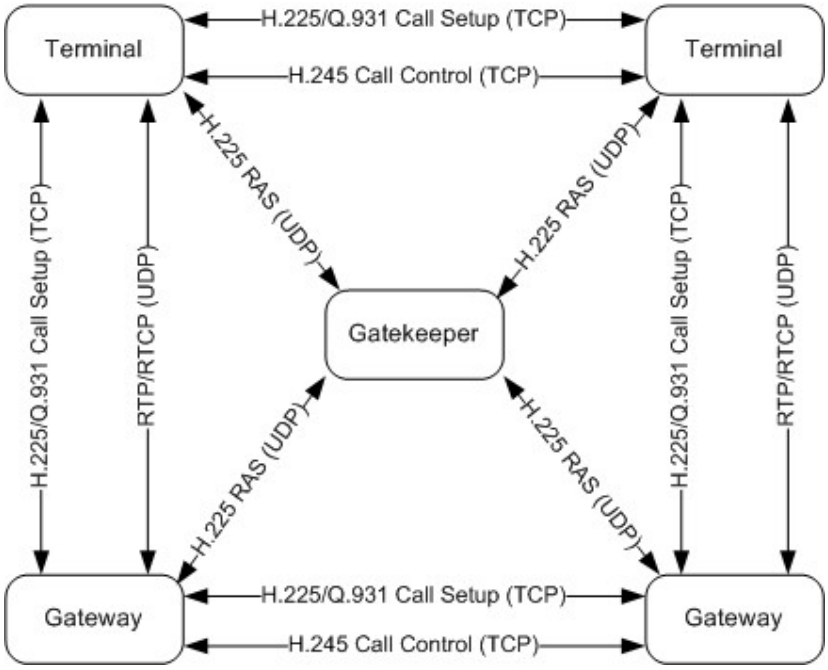

Figura 3.4: Fluxo de comunicação entre componentes definidos pelo padrão H.323 (PORTER, 2007)

3.1.2 SIP

Session Initiation Protocol é um protocolo de nível de aplicação especificado pela *Internet Engineering Task Force* (IETF) para o estabelecimento, manutenção e encerramento de sessões de comunicação em tempo real na rede IP. Diferentemente do padrão H.323 que é um protocolo binário, o SIP é baseado em código texto e, seguindo a filosofia da IETF, foi concebido para ser simples (GREGORY, 2006). Outra diferença está na sua independência para com o protocolo da camada de transporte. Mensagens SIP podem ser transportadas tanto por TCP como por UDP, além de SCTP e TLS. (SINNREICH, 2006). Seu funcionamento elementar é muito parecido com o HTTP, ou seja, utiliza-se de um modelo de requisições e respostas baseadas em texto para o desempenho de suas funções. Outra característica do SIP é ser bastante modular e extensível facilitando sua integração com outros ambientes de comunicação. (GREGORY, 2006)

Além disso, o SIP usa um único endereço para identificar o usuário em todas as suas comunicações. É o chamado *address of register* (AOR) que é o único endereço que liga o usuário a todos os serviços e dispositivos de comunicação que ele utiliza. Como complemento, o SIP usa um mecanismo chamado *Uniform Resource Identifier* (URI) que estabelece um esquema de mapeamento para cada agente de usuário. Em outras palavras, o usuário será conhecido por um único endereço (Ex. sip:nome@dominio.com) independentemente do dispositivo que ele estiver usando e cada dispositivo por sua vez terá seu próprio URI (Ex. phone sip:514200@dominio.com;user=phone) (GREGORY, 2006).

A arquitetura do SIP é composta pelos seguintes elementos:

- Agentes de usuários - são os dispositivos ou programas utilizados para estabelecer a comunicação entre os usuários finais. Um agente de usuário pode estabelecer uma comunicação diretamente com outro agente sem a necessidade de servidores SIP. Para isso basta que eles saibam a URI e o IP de cada dispositivo envolvido na comunicação.
- Servidores SIP – são elementos de rede centralizados que fornecem uma infra-estrutura para serviços de roteamento, registro, autenticação/autorização, localização e presença no ambiente SIP (GREGORY, 2006).

Os servidores SIP podem ser assim classificados:

- Servidor de Registro – é o servidor encarregado por fazer a autenticação e o registro dos usuários que ficam online. Nesse servidor ficam armazenadas as identidades lógicas dos usuários e seus dispositivos (URI) usados para a comunicação.
- Serviço de Localização – é um banco de dados que mantém um registro dos usuários e de suas localizações. Ele recebe dados de entrada do servidor de registro e repassa informações para os servidores de redirecionamento e de Proxy para o correto mapeamento do endereço lógico dos usuários em seus endereços físicos.
- Servidor de Redirecionamento – servidor responsável por redirecionar as requisições SIP para um usuário que está fora do seu domínio.

- Servidor Proxy – sua função básica é fazer o roteamento da sinalização das chamadas indicando os servidores intermediários para se alcançar o agente de usuário de destino. Atua na sinalização como se fosse o originador da chamada e repassa as respostas para o solicitante. Após o estabelecimento da sessão, a comunicação é feita diretamente entre as partes.
- Servidor de Presença – tem como função aceitar, armazenar e distribuir informações de presença dos usuários no ambiente SIP. Trabalha em conjunto com o *Session Initiation Protocol for Instant Messaging, and Presence Leveraging Extensions* (SIMPLE), padrão que é usado para gerenciar mensagens instantâneas e informações de presença dos usuários no ambiente SIP. (GREGORY;PORTER; 2006)

Para o estabelecimento da sessão SIP são usados os seguintes métodos:

- *Register* – usado para registra o usuário
- *Invite* – convidar alguém para uma sessão de multimídia
- *Ack* – confirmação de uma requisição de estabelecimento de sessão
- *Cancel* – cancelamento de uma transação
- *Bye* – encerramento de uma sessão ou transação
- *Options* – Consulta de compatibilidades
- *Info* – usado para troca de informações intermediárias como dígitos discados
- *Messages* – usado para mensagens curtas de serviço e mensagem instantânea
- *Notify* – usado para notificar eventos e atualização de registro
- *Subscribe* – usado para a subscrição de notificação de eventos
- *Update* – usado para atualização das informações de uma sessão (SINNREICH, 2006)

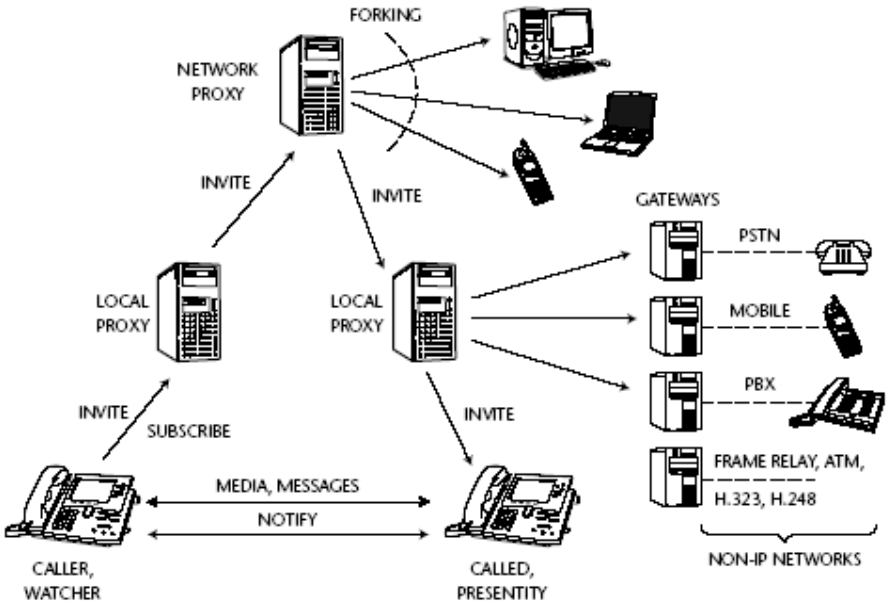

Figura 3.5: Visão geral do SIP (SINNREICH, 2006)

A arquitetura SIP pode ser cliente-servidor quando os agentes de usuário fazem requisições para algum servidor SIP ou *pear-to-pear* quando os agentes estabelecem uma sessão e passam a trocar mensagens diretamente entre si. (PORTER, 2006)

Além de configurar e gerenciar as sessões, o SIP também tem a função de determinar a localização, disponibilidade e compatibilidades entre os agentes de usuários envolvidos na comunicação (PORTER, 2006).

3.1.3 MGCP e H.248

Media Gateway Control Protocol é o padrão especificado pela IETF em 1998 com a função de servir de gateway entre os sistemas de telefonia IP e as redes de telefonia convencionais (RPTC, RDSI, etc.). É um protocolo baseado em texto usado sobre a camada de transporte UDP. Sua função é gerenciar os gateways do ambiente SIP.

Em 2000 a ITU-T especificou o protocolo H.248 cuja função foi mover o controle da sinalização do equipamento de gateway de mídia para um controlador de Gateway. Apesar de ser bastante similar ao MGCP, o H.248 trouxe alguns avanços em relação ao padrão da IETF conforme segue:

- Avanços no suporte a serviços de multimídia em multipontos;
- Suporte a TCP e UDP no nível de transporte;
- Suporte a codificação baseada em texto ou binária para dar suporte a ambos os padrões (IETF e ITU-T)

Para fornecer segurança, ambos os protocolos podem usar IPSec para permitir criptografia do fluxo de streaming entre os equipamentos terminais da comunicação (PORTER, 2006).

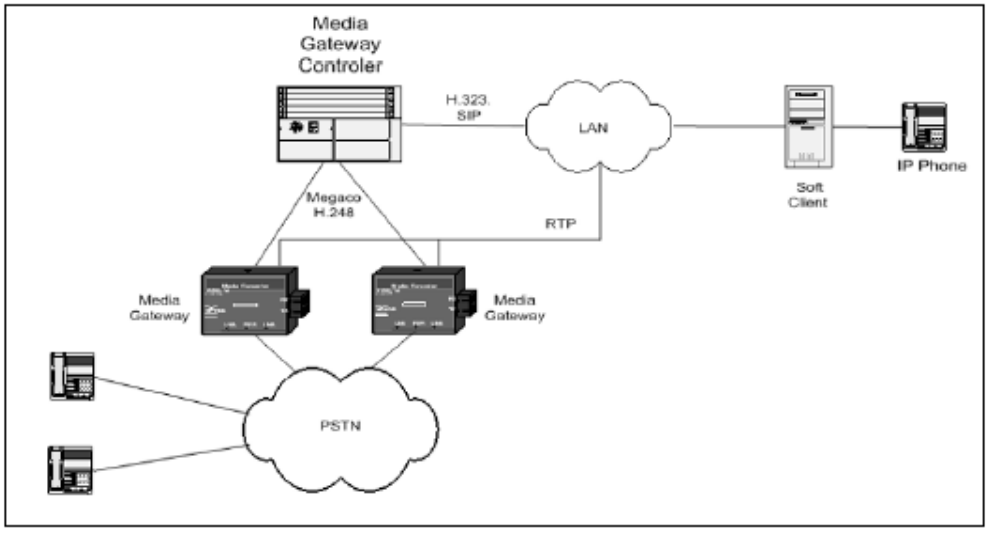

Figura 3.6: Infra-estrutura típica de uso do H.248 (PORTER, 2006)

4 AMEAÇAS E VULNERABILIDADES EM VOIP

O objetivo desse tópico é descrever as principais ameaças e vulnerabilidades em redes VoIP.

4.1 Interrupção e Abuso de Serviço

Estão enquadradas nessa categoria as ameaças que afetam a disponibilidade do serviço VoIP. Os ataques são direcionados a elementos da infra-estrutura de rede (dispositivos ou serviços) que o VoIP depende para funcionar. Como exemplo, pode-se citar ataques aos servidores SIP, aos roteadores de rede ou mesmo ao serviço de DNS da rede. E podem ser disparados tanto remotamente como localmente através de instruções maliciosas. (THERMOS, 2007)

4.1.1 Negação de serviço (DoS)

Esse ataque conhecido mundialmente pelo acrônimo DoS (*Denied of Service*) pode ser direcionado para várias camadas da infra-estrutura do ambiente VoIP. Seu principal objetivo é provocar a interrupção ou degradação do serviço alvo. No caso do VoIP, o ataque pode ser direcionado tanto para o sistema operacional dos servidores como também para os serviços de rede (THERMOS, 2007). Dentre os tipos de ataques de negação de serviço, destacam-se os baseados em:

- Inundação - consiste em enviar uma sobrecarga de mensagens para um destino com o objetivo de comprometer seu funcionamento.
- Pacotes deformados – processo conhecido como *Fuzzing* que gera um pacote deformado aleatoriamente ou semi-aleatoriamente e que pode comprometer um dispositivo alvo.

4.1.1.1 DDoS

Ataques de negação de serviço também podem ser organizados de forma sincronizada de diferentes origens com foco em um alvo. Esse tipo de ataque conhecido como DDoS (*Distributed Denied of Service*) geralmente utiliza programas maliciosos como vírus e worms para infectar equipamentos de terceiros que serão usados para compor o ataque (THERMOS, 2007).

4.1.1.2 SIP Flooding

É o ataque por inundação em que muitas mensagens *INVITE* são endereçadas ao um usuário SIP. Esse ataque degrada o desempenho dos servidores S*IP proxies* que terão

que tratar essas requisições e suas respostas além de impossibilitar que o usuário alvo consiga efetuar ligações (THERMOS, 2007).

4.1.1.3 SIP Signalling Loop

Outro ataque conhecido de DoS é o *SIP Signalling Loop* que afeta sistemas que não implementam mecanismos de detecção de *looping*. Esse ataque consiste em registrar dois usuários em domínios de SIP distintos, sendo que no cabeçalho de contato de cada registro há dois valores, cada um apontando para um destes usuários só que no domínio contrário. Quando o SIP Proxy de um domínio recebe o INVITE para um desses usuários, ele irá gerar duas mensagens de INVITE uma para cada usuário no outro domínio. Já o SIP Proxy do outro domínio por sua vez, ao receber esses dois INVITE's irá gerar quatro novas mensagens de INVITE para o outro domínio. Assim, o numero de mensagens irá crescer na ordem de uma potencia de base dois e rapidamente pode comprometer o sistema SIP (THERMOS, 2007).

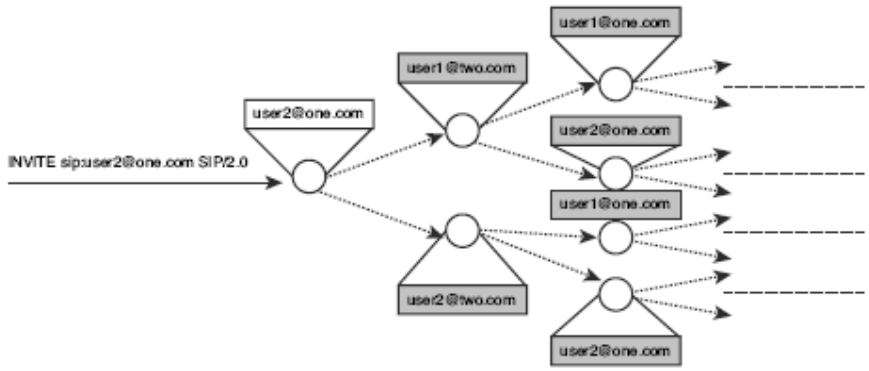

Figura 4.1: Ilustração de um ataque SIP Signalling Loop (THERMOS, 2007)

4.1.1.4 VoIP Packet Replay Attack

Consiste em capturar e reenviar pacotes VoIP fora de seqüência o que gera um atraso e uma progressiva degradação na qualidade das chamadas.

4.1.1.5 QoS Modification Attack

Consiste em modificar os campos referentes a QoS (802.1Q VLAN tag ou ToS bits) no header do pacote IP anulando o controle de QoS da rede e comprometendo o serviço VoIP.

4.1.1.6 VoIP Packet Injection

Caracterizado pelo envio de pacotes VoIP falsificados para terminais injetando fala, ruídos, e lacunas nas chamadas ativas (PORTER, 2007).

4.2 Violação de Acesso

Essa categoria descreve as ameaças em que serviços e elementos de rede são acessados sem a devida permissão. Freqüentemente esse tipo de ataque é usado como primeiro passo para outros ataques. O acesso indevido é geralmente obtido através de vulnerabilidades como *buffer overflow*, ou seja, com o uso de instruções que exploram falhas no controle da pilha de memória do sistema para obter acesso privilegiado, além de falhas de configuração e um fraco controle de acesso a rede e sinalização. Dentre os método utilizados pode-se destacar:

- impersonificação – descobrir ou roubar senha de outra pessoa e usá-la para acesso ao sistema
- Ataque do homem do meio (*man in the middle*) – técnica de ataque que permite ao atacante interceptar uma sessão válida de um usuário e se apropriar dela após a autenticação
- Comprometimento total – permite ao atacante o acesso total ao sistema e geralmente está relacionado ao uso de softwares maliciosos como vírus e *worms*.

Vale ressaltar que a violação de acesso que está muito associada a sistemas operacionais pela exploração de suas vulnerabilidades, também pode ocorrer em nível de aplicação (serviços do VoIP) pelo manipulação das mensagens de sinalização e de mídia e em nível de camadas de transporte e rede pela manipulação do tráfego de rede (THERMOS, 2007).

As principais vulnerabilidades exploradas na infra-estrutura VoIP são:

- Configuração padrão dos serviços e dispositivos - os controles de segurança geralmente vêm desabilitados por padrão
- Uso de senhas e contas de gerenciamento padrão
- Ausência de controles de acesso nas interfaces de gerenciamento e nos serviços (FTP, Telnet, RPC, etc.)

4.2.1 Ataque de dicionário na autenticação SIP

Essa técnica tem como objetivo obter as credenciais de acesso de um usuário válido em um sistema de telefonia SIP através da utilização de um ataque de força bruta. Através dessa técnica, um atacante pode enviar inúmeras requisições de registro (método REGISTER do SIP) com identificação (IDs) e senhas a partir de um arquivo de dicionário. Uma vez descoberta a senha, o atacante pode usar ela para acessar o serviço (THERMOS, 2007).

4.3 Escuta e análise de tráfego

Estão enquadradas nessa categoria as ameaça que afetam a confidencialidade do serviço VoIP. Segundo a VoIPSA, *eavesdropping*, como é designada essa ameaça, compreende os métodos de ataque que permitem ao atacante monitorar a sinalização e o tráfego de dados VoIP sem alterá-los. Basicamente essas técnicas de ataque objetivam a

busca de informações para o aperfeiçoamento de ataques posteriores. Esse tipo de ameaça é sempre possível quando a sinalização e o tráfego de dados da chamada não estiverem criptografados.

Existem vários métodos para realizar a escuta do tráfego VoIP. Programas analisadores de tráfego ou *sniffers* são ferramentas que podem ser utilizadas para essa finalidade. Contudo, o atacante precisa estar inserido no segmento de rede entre os terminais que se comunicam ou, terá que usar alguma técnica de envenenamento (*poisoning*) de ARP para conseguir interceptar os pacotes da comunicação antes que eles sejam transmitidos ao destino correto (THERMOS, 2007)

4.3.1 ARP Poisoning

Também conhecido como ARP *Spoofing*, essa técnica de ataque explora uma vulnerabilidade do nível de rede do modelo TCP/IP. ARP é o protocolo responsável por fazer o mapeamento entre o endereço físico da interface de rede e o endereço IP. O princípio desse ataque consiste em alterar (envenenar) esse mapeamento através da manipulação da tabela ARP dos equipamentos da rede. Para isso, o atacante envia uma mensagem de *broadcast* na rede publicando um novo MAC (*Media Access Control*) para o IP que ele deseja interceptar. Esse método de ataque é também conhecido como "ataque do homem do meio" (*man in the middle*) (THERMOS, 2007)

4.3.2 VLAN hopping

É uma técnica de ataque que possibilita a escuta de tráfego quando estão envolvidos segmentos de redes distintos. Há dois ataques conhecidos que utilizam essa técnica: *switch spoofing* e *doubletagging*. Ambos exploram a vulnerabilidade em switches de rede cujas portas de *trunk* são mal configuradas (THERMOS, 2007).

4.3.3 Ataque ao protocolo MGCP

É outro método utilizado para a realização de escuta indevida no fluxo de dados de uma chamada. Através do envio de mensagens de sinalização MGCP para um gateway RPTC, um atacante pode manipular o estado das conexões ativas desviando seus fluxos RTP para um host intermediário antes de serem encaminhados aos verdadeiros destinos (THERMOS, 2007).

4.4 Mascaramento

É uma categoria especial de ameaça visto que as técnicas de mascaramento podem também ser usadas para realizar outros tipos de ameaças como violação de acesso, interrupção de serviços e fraude. É caracterizada pela habilidade do atacante em se fazer passar por um usuário, dispositivo ou serviço a fim de obter acesso a rede, seus dispositivos e informações trafegadas. Esse tipo de ameaça pode comprometer a disponibilidade, a integridade e a confidencialidade dos serviços de VoIP. A impersonificação é um tipo especial de mascaramento em que o atacante pode comprometer a segurança do sistema seja através da falsificação de serviços e dispositivos de rede básicos na infra-estrutura VoIP, seja se fazendo passar por outra pessoa através da captura ou roubo das credencias de acesso da vítima. Esse tipo de ataque pode ocorrer contra usuários, dispositivos, serviços e aplicações de rede.

- Impersonificação dos serviços e aplicações – método mais sofisticado de ataque. Envolve uma coordenação maior de elementos e está relacionado aos

tipos de ataque que tiram vantagens de vulnerabilidades que impactam no roteamento dos protocolos de sinalização.

- Impersonificação dos dispositivos – elementos de rede como telefones, servidores DNS, registradores SIP e gateways de mídia e sinalização podem ser impersonificados com o objetivo de coletar e desviar seus tráfegos de rede.
- Impersonificação do assinante – caracteriza a impersonificação em que o atacante mascara sua identidade utilizando-se de credenciais capturadas ou de acesso a dispositivos de um assinante de um serviço para realizar seu ataque.

Os métodos de mascaramento mais utilizados em ambientes de VoIP são direcionados à manipulação das mensagens de sinalização embora métodos tradicionalmente conhecidos como clone de endereços IP e MAC e *spoofing* de IP também são utilizados (THERMOS, 2007)

4.4.1 Seqüestro de chamada

No cabeçalho da requisição *Register* em um sistema SIP há um registro com informações de contato (*Contact*) que é usado pelo Proxy SIP para rotear as ligações para o dispositivo do usuário. O ataque de seqüestro de chamada pode ser realizado através da alteração das informações de IP contidas nesse registro. Com essa alteração, as ligações que deveria ser encaminhadas para o dispositivo do usuário, são desviadas para o dispositivo do atacante (THERMOS, 2007).

Contact: 201-853-0102 <sip:12018530102@192.168.1.3:5061>;expires=60

Endereço IP que pode ser alterado pelo atacante para desviar chamadas.

4.4.2 Impersonificação de elementos de rede

Um exemplo dessa vulnerabilidade ocorre com os *Call Managers*. Esses dispositivos são responsáveis entre outras coisas por fazer o gerenciamento das ligações de entrada e saída entre a rede VoIP e a rede pública de telefonia (RPTC). Através de uma implementação do protocolo MGCP um atacante pode manipular a sinalização das mensagens e redirecionar o tráfego das ligações para um *Call manager* falso (THERMOS, 2007)

Tabela 4.1: Possíveis ataques de mascaramento contra VoIP

Alvo	Objetivo	Método
Usuário	Fraude	Obter as credenciais do usuário por meio de outro ataque e usá-las para efetuar ligações fraudulentas Obter acesso físico ou remoto à um dispositivo do usuário

		Manipular mensagens de sinalização para desviar tráfego
DNS	Redirecionar as requisições de sessão para um dispositivo não autorizado	Envenenamento de cache de DNS Violação de acesso com o objetivo de manipular as configurações de elementos da rede
Gateway de Sinalização	Desviar o tráfego da sinalização e conseqüentemente as chamadas	Manipular remotamente a sinalização para desviar o tráfego (Ataque no protocolo MGCP) Violação de acesso com o objetivo de manipular as configurações de elementos da rede
Gateway de Mídia	Desviar tráfego da mídia	Manipular remotamente a sinalização para desviar o tráfego (Ataque no protocolo MGCP) Violação de acesso com o objetivo de manipular as configurações de elementos da rede
Proxy SIP	Obter credenciais de usuários Desviar o tráfego da sinalização e conseqüentemente as chamadas	Manipular remotamente a sinalização para desviar o tráfego (manipulação das sessões pelo *spoofing* de mensagens de sinalização como *Refer* e *Invite*) Violação de acesso com o objetivo de manipular as configurações de elementos da rede
SIP Registra	Obter credenciais de usuários	Ataque de spoofing nas requisições de registro Violação de acesso com o objetivo de manipular as configurações de elementos da rede

Gatekeeper H.323	Obter credenciais de usuários Obter informações do tráfego da chamada	Ataque de spoofing nas requisições de registro Violação de acesso com o objetivo de manipular as configurações de elementos da rede
Soft switch	Desviar o tráfego da sinalização e conseqüentemente as chamadas Obter informações do tráfego da chamada	Violação de acesso com o objetivo de manipular as configurações de elementos da rede

Fonte: THERMOS, 2007, p.111

Visualizando a Tabela 4.2 há uma relação de ataques e como cada um deles impacta nos princípios de segurança da informação.

Tabela 4.2: Lista dos principais ataques contra as redes VoIP

Nível	Ataque	Confidencialidade	Integridade	Disponibilidade
Interface de rede	Ataque físico	X		X
	ARP Cache	X	X	X
	Envenenamento ARP			X
	MAC Spoofing	X	X	X
Internet	IP spoofing			
	Dispositivo	X	X	X
	Redirecionamento por IP spoofing	X	X	X
	Deformação de pacotes	X	X	X
	Fragmentação IP			X
Transporte	Envenenamento TCP/UDP			X
	TCP/UDP Reply	X	X	
Aplicação	Inserção de servidores DHCP e TFTP		X	
	Envenenamento ICMP			X

	SIP			
	Seqüestro de registro SIP	X	X	X
	Seqüestro MGCP	X	X	X
	Modificação de mensagem SIP	X	X	X
	Inserção RTP			
	Deformação de Métodos			X
	Spoofing de cabeçalho	X	X	X
	Ataque de Cancel/Bye			X
	Método de redirecionamento	X		X
	RTP			
	Redirecionamento de SDP			X
	Criptografia	X	X	X
	Configuração padrão	X	X	X
	Serviços desnecessários	X	X	X
	Buffer overflow	X	X	X
	DNS			X

Fonte: MCGANN & SICKER, 2005, p.2

5 MELHORES PRÁTICAS DE SEGURANÇA EM REDES VOIP

O objetivo desse tópico é descrever as recomendações e melhores práticas a serem adotadas nas redes de VoIP para minimizar os riscos frente as já conhecidas ameaças e vulnerabilidades.

5.1 Controles de segurança na rede VoIP

Nesse tópico serão abordados alguns mecanismos utilizados na arquitetura da rede de computadores a fim de fornecer aspectos que reforcem a segurança de redes que utilizam serviço de Voz sobre IP.

5.1.1 Virtual Local Area Network (VLAN)

O objetivo com a utilização de VLAN é permitir a segmentação lógica da rede criando domínios de colisão e de broadcast distintos entre o tráfego de dados e o tráfego de voz. Dessa forma, previne-se que problemas em um segmento de rede interfiram no outro e vice-versa. Ataques de negação de serviço ou mesmo instabilidades na rede de dados provocados pela atuação de pragas virtuais como vírus e *worms* terão seus efeitos minimizados com a segregação das redes promovida com o uso de VLAN. Além de aspectos de segurança, a separação dos segmentos de broadcast favorece o desempenho na medida em que reduz significativamente o tráfego de rede e, conseqüentemente, proporciona maior banda passante (PORTER, 2007).

Adicionalmente, VLAN podem ser implementadas juntamente com mecanismos de QoS a fim de separar e priorizar os tráfegos de voz sobre IP. Apesar de existirem protocolos proprietários que implementam VLAN, o padrão foi definido pela IEEE através do protocolo 802.1Q (PORTER, 2007).

Embora a utilização de VLAN tenha como objetivo agregar segurança ao ambiente de rede VoIP, cabe ressaltar que a má configuração dos dispositivos de rede que implementam esse recurso podem trazer vulnerabilidades aos serviços. Basta recordar o tópico 4.3.2 que trata da vulnerabilidade de VLAN Hopping (PORTER, 2007)

Outra consideração se faz necessária quanto ao uso de *Softphones* (software instalado nas estações de trabalho que simulam telefone IP). Se a estação de trabalho na qual o *softphone* estiver instalado possuir uma única interface de rede, significa que o software irá compartilhar a rede de dados para trafegar o fluxo de voz. Dessa forma, não será possível utilizar o conceito de VLAN para separação dos tráfegos de dados e voz. Embora seja possível fazer essa separação utilizando uma segunda interface de rede

com a estação roteando aos tráfegos de voz e dados para segmentos distintos, não se recomenda o uso desses softwares em ambientes de VoIP em virtude da complexidade de configuração e administração desse ambiente e das vulnerabilidades que ele está sujeito (PORTER, 2007).

5.1.2 Firewall, IDS e IPS

A utilização de equipamentos como firewalls, IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*) visam proteger segmentos de rede contra ameaças externas. Esses equipamentos são estrategicamente inseridos na infra-estrutura de rede de modo que todo tráfego entre os segmentos de redes que se deseja proteger seja inspecionado (PORTER, 2007)

A função do firewall é bloquear todo o tráfego de rede que não esteja de acordo com a política de segurança implementada por suas regras de acesso. O processamento do tráfego pelo firewall é realizado através de uma técnica denominada filtro de pacote. Esse processo consiste em analisar informações contidas no cabeçalho de cada pacote que atravessa o firewall como endereços IP, portas e tipo de protocolos a fim de identificar os pacotes legítimos. Ainda sobre esse processo, os firewalls podem ser classificados em *Stateless* e *Stateful. Stateless* são os firewalls que não guardam informações em memória sobre o estado das conexões. Já os firewalls *Stateful*, mantém em memória uma tabela de estados das conexões e, dessa forma, conseguem diferenciar pacotes iniciando uma nova conexão (*NEW*) de pacotes de conexões já estabelecidas ou relacionadas (*ESTABLISHED/RELATED*). Além da habilidade de verificar e barrar pacotes com número de seqüência incorreto. Como benefício, esse tipo de firewall é mais eficiente para detectar e bloquear pacotes maliciosos (PORTER, 2007).

IDS e IPS são sistemas capazes de detectar tráfego malicioso mesmo que esses tenham sido considerados legítimos pela política de segurança de firewalls. Através de uma arquitetura composta por sensores, unidade de detecção e uma base de conhecimento, esses sistemas analisam os protocolos dos pacotes até as camadas do nível de aplicação. Existem três métodos de detecção utilizados por esses sistemas que são os baseados em assinaturas, em anomalia e em análise do protocolo *stateful* (PORTER, 2007).

Os sistemas baseados em assinatura utilizam uma base de dados, que deve ser atualizada periodicamente, com as instruções referentes aos conhecidos ataques, o que inclui, por exemplo, assinaturas contra ataques ao Code Red, NIMDA, DoS, buffer overflows e outras vulnerabilidades (PORTER, 2007).

Sistemas de detecção de intrusão baseados em anomalias funcionam com base no comportamento da rede. Distorções observadas nesse comportamento são indícios de que algo está errado. Apesar de ser um método muito eficiente para detectar ataques como Port Scan e DoS, falso-positivos podem ocorrer se o padrão de comportamento da rede não for mapeado adequadamente (PORTER, 2007).

Já os sistemas baseado em análise do protocolo *stateful* fazem a analisa dos protocolos dos pacotes até as camadas do nível de aplicação e verificam se eles estão em conformidade com os perfis de comportamento estabelecidos pelas RFC's e *vendors* de cada protocolo (PORTER, 2007).

A diferença básica entre IDS e IPS é que, enquanto o IDS apenas tem como ação gerar eventos e alarmes aos administradores da segurança da rede, os IPS são mais pró-ativos e capazes de tratar os alertas realizando, eles próprios, ações de bloqueios.

Embora sejam muito úteis para a proteção contra ataques que visam a negação de serviços com foco em dispositivos da infra-estrutura de rede VoIP, tanto os firewalls como os IDS e IPS adicionam latência e complexidade ao tráfego VoIP na rede.

5.1.3 Qualidade do Serviço – *QoS (Quality of Service)*

O emprego de técnicas de Qualidade de Serviço é fundamental para o bom funcionamento do serviço VoIP. Qualidade de Serviço visa entregar um nível de serviço garantido para o usuário da rede, o que inclui uma largura de banda garantida e um valor máximo de atraso e *Jitter* (BATES, 2002). Em uma transmissão de dados, atraso é o tempo que a informação leva para trafegar entre sua origem e o seu destino. Em se tratando de Voz sobre IP, a origem é o emissor da voz, ou seja, aquele que fala enquanto que o destino é o receptor ou aquele que ouve. Esse atraso é denominado atraso de uma via e os valores aceitáveis de atraso não devem ultrapassar os 150ms segundo recomendações da ITU. Já o *Jitter* é a variação do atraso (BATES, 2002).

O objetivo ao se utilizar técnicas de QoS é garantir o bom desempenho do fluxo de voz mesmo em momentos que a rede esteja em condições desfavoráveis. Rede congestionadas, seja em decorrência de uma ataque de DoS ou pela ação de pragas virtuais ainda podem ter uma excelente qualidade no fluxo de voz quando utilizadas políticas de QoS apropriadas (PORTER, 2007).

5.2 Segurança na Sinalização

Como foi visto no item 4, muitos ataques são direcionados ao processo de sinalização entre os componentes de uma rede VoIP. Esses ataques, se bem sucedidos podem ocasionar desvio e seqüestro de chamadas violando os princípios de integridade e confidencialidade das informações trafegadas no ambiente. Sendo assim, esse tópico tem como objetivo apresentar mecanismos utilizados para fornecer segurança contra as ameaças e vulnerabilidades relacionadas ao processo de sinalização em redes de voz sobre IP.

5.2.1 Autenticação SIP

O mecanismo de autenticação SIP é usado para fornecer segurança ao processo de requisições de mensagens envolvendo o registro e o inicio e fim de sessões (métodos *REGISTER e INVITE*). Na Figura 5.1 é ilustrado o fluxo de mensagens envolvidas no processo de registro, estabelecimento e término de uma chamada SIP com autenticação.

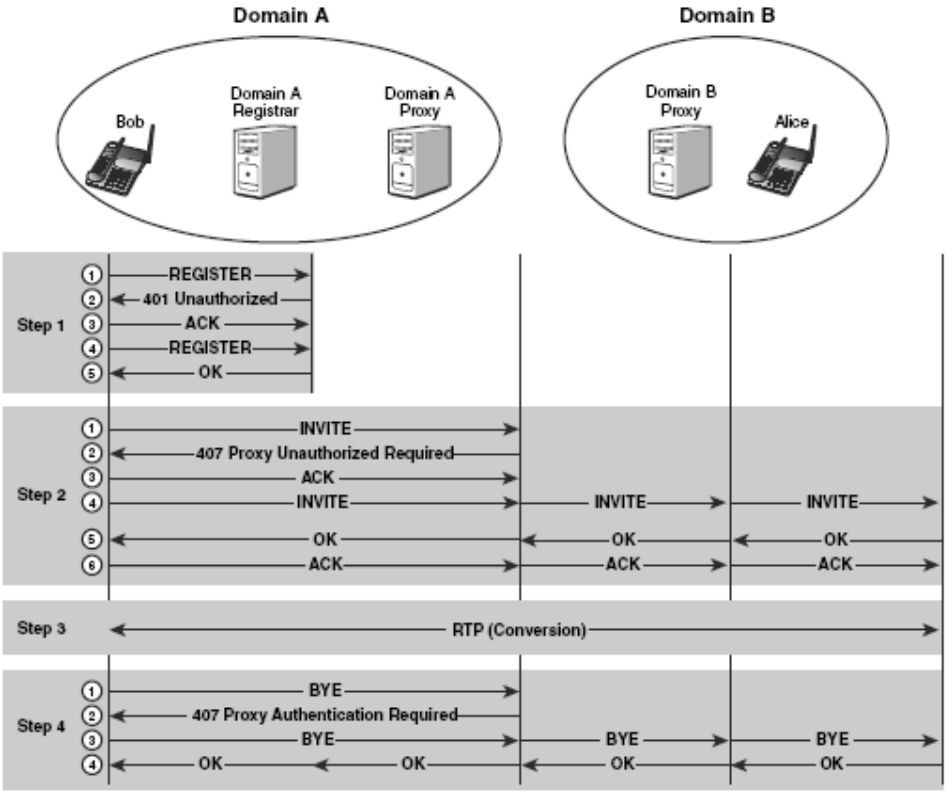

Figura 5.1: Autenticação SIP no registro, inicio e término de uma chamada (THERMOS, 2007)

Após receber a tentativa de registro, o servidor de registro retorna ao agente de usuário uma mensagem *401 Unauthorized message* solicitando um desafio para a sua autenticação. Em seguida, o agente de usuário envia uma nova mensagem de requisição de registro acrescida de um MD5 *digest* que será usado na autenticação. Caso a autenticação seja realizada com sucesso, as informações do dispositivo e do usuário são atualizadas (URI do usuário e IP do dispositivo atual) e é retornada uma mensagem de OK. Processo semelhante ocorre para inicio e termino da chamada com o método INVITE e BYE respectivamente. A autenticação SIP é opcional e pode ser implementada separadamente para cada método SIP. Por exemplo, pode-se optar pela autenticação nos métodos REGISTER e INVITE sem tê-la nos métodos BYE e CANCEL. Contudo, esse tipo de escolha pode abrir oportunidades para ataques como inicio e termino de chamadas sem autorização (THERMOS, 2007).

Como proteção contra ataques de *message replay* e mascaramento, a autenticação por desafio deve ser utilizada em todas as mensagens que se destinam a criar, modificar e encerrar sessões. Contudo, algumas mensagens como CANCEL e BYE não são protegidas pela utilização de MD5. Como alternativa recomenda-se a utilização de criptografia para as mensagens de sinalização através de protocolos como TLS, IPSec e S/MINE (THERMOS, 2007).

5.2.2 IP Security - IPSec

Internet Protocol Security (IPsec) é uma extensão do protocolo IP descrito pela IETF para operar no nível de rede do modelo OSI com a finalidade de prover autenticidade, confidencialidade e integridade na comunicações fim a fim de aplicações que utilizam a rede IP (THERMOS, 2007).

O IPsec pode operar de duas formas diferentes:

- Modo Transporte – somente a carga útil do pacote IP é protegida. O cabeçalho fica intacto.
- Modo Túnel – todo o pacote IP é protegido por criptografia. Nesse modo há a necessidade de um novo cabeçalho IP para fazer o encaminhamento do pacote.

A Figura 5.2 apresenta os dois métodos que o IPsec oferece para proteção da informação.

Para garantir a segurança, o IPSec utiliza dois protocolos, o *Authentication Header* (AH) e o *Encapsulating Security Payload* (ESP). O AH fornece autenticação e integridade enquanto que a ESP adicionalmente a esses atributos fornece também a confidencialidade da carga útil do pacote. Os protocolos AH e ESP podem ser utilizados em conjunto ou individualmente (GREGORY, 2007).

Além disso, outros dois protocolos desempenham funções importantes ao IPsec. O *IP Payload Compression* (IPcomp) usado para aumentar o desempenho na medida em que comprime os pacotes antes da criptografia, e o *Internet Key Exchange* (IKE) que é utilizado para negociar a troca segura de chaves de criptografia (STEWART, 2008).

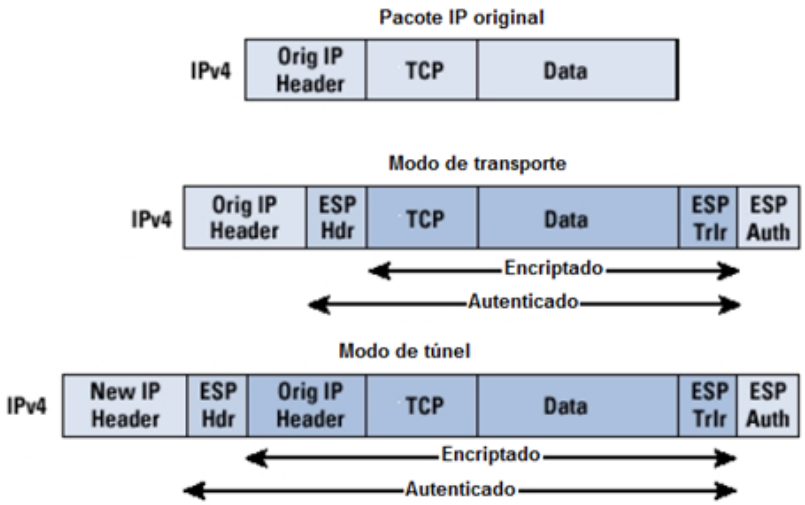

Figura 5.2: Modos de funcionamento do IPSEC

Em redes de voz sobre IP o IPsec pode fornecer confidencialidade, integridade e autenticação para mensagens de sinalização e de mídia, criando túneis seguros entre as entidades participantes da comunicação. Contudo, a formação do túnel IPSec acrescenta atraso tanto no estabelecimento da chamada como no transporte da mídia o que muitas vezes torna inviável a suas utilização. A Figura 5.3 demonstra o uso de IPSec em um ambiente de SIP informando os tempos de atraso medidos em estudo pela *Telecordia Technologies* em nome da NIST – *National Institute of Standards and Technology* (THERMOS, 2007).

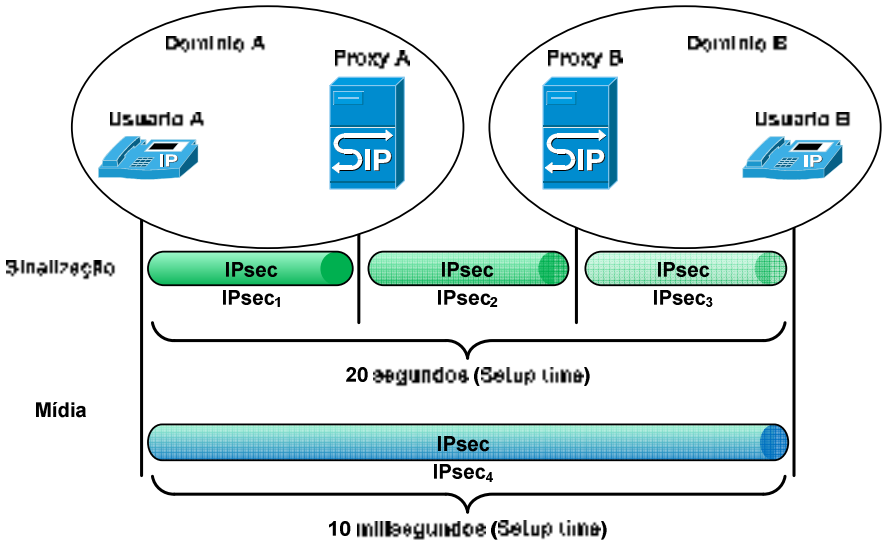

Figura 5.3: IPSec em ambiente SIP (THERMOS, 2007)

O que se percebe por esse estudo realizado pela *Telecordia Technologies* é que usar IPSec no processo de sinalização de uma chamada fim a fim é inviável em virtude do

tempo gasto para a formação dos túneis entre cada *hop* envolvido na comunicação. O estudo demonstra que uma chamada entre domínios SIP usando dois servidores Proxy leva cerca de 20 segundos para ser estabelecida. O padrão tolerável para esse processo é em torno de 250ms. Contudo, se o túnel IPSec fim a fim já estiver estabelecido, a transmissão da mídia e das mensagens de sinalização sofre um atraso desprezível (cerca de 10ms) o que faz da utilização de túneis IPSec uma alternativa viável (THERMOS, 2007).

Mesmo estando na camada de rede, o IPsec é orientado a conexão, pois as chaves de criptografia são utilizadas e trocadas por períodos de tempo, a fim de garantir a segurança, num processo que se assemelha a uma espécie de conexão que é denominada de *security association* (SA). O SA é um canal *simplex*, logo para uma comunicação bi-direcional, são necessários dois SAs, um para cada direção. Ainda, se for utilizado o AH com o ESP, serão necessários quatro SAs (GREGORY, 2007).

Como ponto forte pode-se citar:

- suporte aos protocolos UDP, TCP, SIP e RTP por operar na camada de rede;
- proteção a ataques de grampo, mascaramento, DoS entre outros;
- garante confidencialidade, integridade, autenticação, e não repúdio.

Limitações:

- o IPsec requer grande esforço de implementação devido a sua complexidade e exigências de infra-estrutura;
- exige uma infra-estrutura de PKI para garantir autenticação, integridade e confidencialidade de dispositivos de borda, mas não necessariamente para o centro da rede VoIP;
- os componentes intermediários da rede devem ser confiáveis; não apresenta escalabilidade para grandes redes e aplicações distribuídas (por exemplo, conferência) (THERMOS, 2007).

5.2.3 Transport Layer Security - TLS

Protocolo criptográfico especificado pela IETF para fornecer segurança na comunicação fim a fim em redes TCP/IP. Assim como o IPSec, também é utilizado para a criação de VPN's (*Virtual Private Network*) contudo, oferece esse serviço a uma camada acima do IPSec, ou seja, à camada de transporte.

O TLS é um protocolo independente do nível de aplicação, baseado em sessão, utilizado para criptografar conexões TCP, com a capacidade de oferecer autenticação mutua (cliente-servidor), confidencialidade e integridade às aplicações baseadas em redes IP (GREGORY, 2007).

Ele é composto por duas camadas:

a) *TLS Record Protocol* – camada inferior cuja função é garantir a segurança da conexão. Nessa camada é realizado o encapsulamento e transmissão de todas as mensagens dos protocolos dos níveis superiores. Ao transmitir uma mensagem, o protocolo de registro realiza a fragmentação dos dados, opcionalmente faz sua compressão, aplica uma função de integridade (MAC - *Message Authenticating*

Code), faz a criptografia e a transmissão das mensagens. No receptor ocorre o processo inverso.

b) *TLS Handshake Protocol* – camada cuja função é negociar os parâmetros de segurança que serão usados pela camada de registro para o estabelecimento de conexões seguras. Dentre esses parâmetros estão os métodos de compressão, criptografia (DES, RC4, etc.) e integridade (MD5, SHA, etc.) que serão utilizados, o tamanho do *hash* e a troca dos certificados e *master key* usados entre cliente e servidor. A Figura 5.4 exemplifica o *TLS Handshake*.

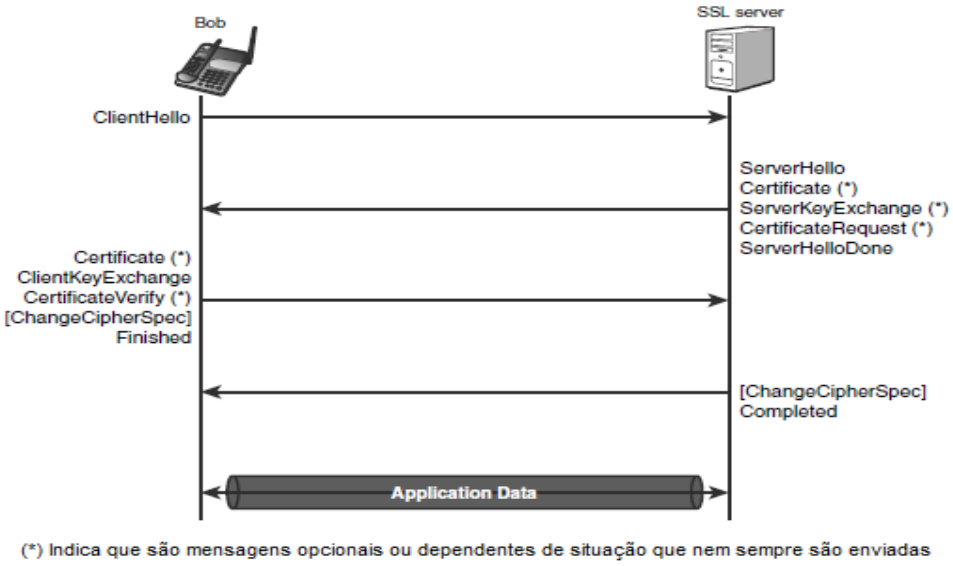

Figura 5.4: Negociação TLS (TLS Handshake) (THERMOS, 2007)

Contudo, o TLS foi concebido para dar suporte aos protocolos confiáveis da camada de transporte como TCP e SCTP, ou seja, possui limitações quando se trata de aplicações que usam UDP como é o caso das mensagens SIP. Para contornar isso foi especificado pela RFC 4347 o *Datagram Transport Layer Security* - DTLS que será visto em detalhe no item 5.2.4.

As mensagens de sinalização, contudo, podem ser protegidas com a utilização de TLS. A RFC SIP recomenda essa prática como forma de evitar ataques de *eavesdropping, message replay*, manipulação de mensagens, entre outros. SIPS URI (secure SIP ou SIP over TLS) protege as mensagens de sinalização uma vez que elas são criptografadas e transmitidas com o uso de TLS. Adicionalmente, o TLS fornece a autenticação mútua através do uso de certificados digitais o que reforça a segurança contra ataques de *man-in-the-midle* (THERMOS, 2007).

As diferenças entre o SIPS e o SIP estão:

- Na sintaxe URI que ficou definida como *sips:alice@domain-b.com;*
- No protocolo de transporte que ficou sendo o TLS ao invés do TCP/UDP;
- Na porta utilizada que ficou sendo a 5061 ao invés da 5060.

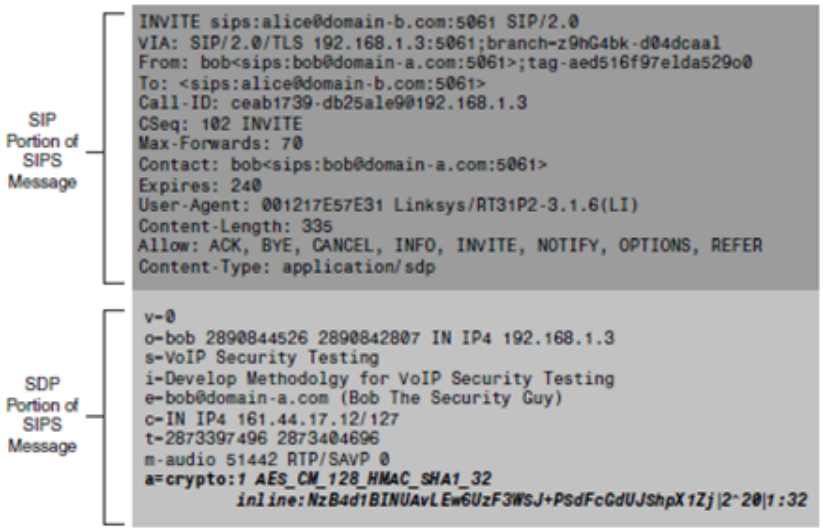

Figura 5.5: Exemplo de mensagem SIPS (THERMOS, 2007)

Uma das limitações do uso de TLS para proteção da sinalização SIP está no fato de que ele não suporta confidencialidade fim a fim para usuários conectados em *SIP proxies* intermediários. Para esse caso, em cada segmento deve ser estabelecida uma conexão TLS distinta. Assim, cada SIP Proxy precisa analisar o cabeçalho do pacote SIP a fim de saber para onde encaminhá-lo, feito isso, a conexão segura é finalizada e uma nova sessão é criada para o próximo *hop*. Veja Figura 5.6

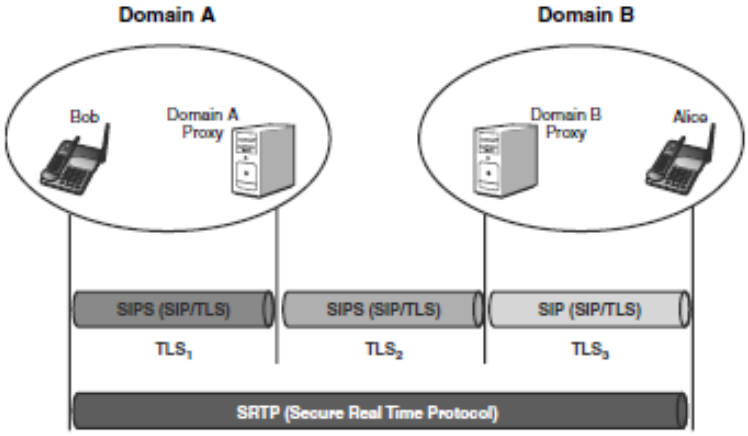

Figura 5.6: Exemplo de tunelamento SIPS entre hops (THERMOS, 2007)

Como ponto forte pode-se citar:

- Suporte a autenticação mutua com uso de certificados;
- Fornece confidencialidade e integridade como proteção contra ataques de *eavesdropping, message reply* e manipulação de mensagens;

- Proteção na negociação das chaves de criptografia;
- Baixo impacto no desempenho se comparado ao uso de IPSec;

Limitações:

- Requer infra-estrutura de PKI;
- Não fornece confidencialidade fim a fim diretamente. Requer a finalização e a criação de uma nova sessão a cada *hop;*
- Não pode ser usado com UDP;
- É suscetível a ataques de negação de serviço por inundação TCP e reset de conexão.

5.2.4 DTLS

Datagram Transport Layer Security é o protocolo descrito pela RFC 4347 para atender as limitações do TLS no fornecimento de um serviço de transporte seguro às aplicações que utilizam UDP como protocolo de transporte fim a fim na rede IP. Embora seja similar ao TLS em muitos aspectos, o que inclui a limitação de necessitar que uma nova conexão seja estabelecida para garantir a proteção das mensagens SIP entre cada *hop*, o DTLS tem como diferencial a capacidade de tratar aspectos da comunicação UDP não confiável como a perda e o reordenamento dos pacotes (THERMOS, 2007).

O TLS apresenta deficiências quanto ao tratamento de perdas de pacotes durante o *handshake* do protocolo (o que provoca a perda da conexão) assim como na detecção de pacotes duplicados. O DTLS foi especificado para superar essas limitações.

Para o tratamento de perdas de pacotes, o DTLS utiliza um mecanismo de retransmissão baseado em temporizador. Ou seja, se uma mensagem é enviada e não há retorno durante certo período de tempo, a mensagem é retransmitida. Veja Figura 5.7.

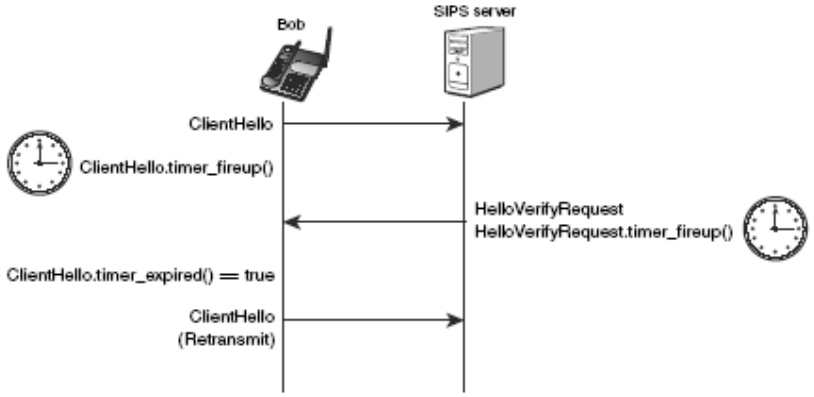

Figura 5.7: Mecanismo de retransmissão do DTLS (THERMOS, 2007)

Outro mecanismo de proteção utilizado pelo DTLS é o *Stateless Cookies*. Essa técnica consiste em incluir um *cookie* nas respostas que o servidor gera para as

requisições que ele recebe a fim de verificar se elas são originadas de um cliente verdadeiro e não de um impostor. Esse mecanismo é útil para evitar ataques de negação de serviço onde o atacante falsifica o endereço IP para inundar a vitima com respostas do servidor.

5.2.5 S/MIME

Secure/Multipurpose Internet Mail Extensions é um padrão especificado pela IETF através da RFC 3851 para fornecer autenticidade, integridade e confidencialidade para protocolos de aplicação como SMTP e SIP. O MIME é largamente utilizado em sistemas de e-mail para tratar formatos complexos (não ASCII) de mensagens e caracteres encapsulados dentro do protocolo SMTP. Em suma, o MIME define uma série de mecanismos para codificar e representar essas mensagens de formatos complexos como arquivos multimídia e caracteres lingüísticos anexados dentro de outros protocolos como SMTP ou SIP (THERMOS, 2007).

O S/MIME é uma versão do MIME que incorpora em sua estrutura o padrão de criptografia de chaves públicas (PKCS) a fim de prover segurança para os protocolos de aplicação que o utilizam. Diferente do TLS e o DTLS, que englobam toda a mensagem SIP em suas estruturas, o S/MIME é mais flexível e permite ser mais granular na proteção das informações das mensagens SIP (THERMOS, 2007). Assim, ele possibilita que equipamentos intermediários da rede interpretem a parte não criptografada sem a necessidade de decodificar todo pacote (PORTER, 2007). Além disso, ele pode ser usado com UDP e TCP, ou seja, é mais flexível que os método usando IPSec , TLS e DTLS na proteção fim a fim (THERMOS, 2007).

Na Figura 5.8 é ilustrada uma mensagem SIP com a parte SDP criptografada com uso do S/MIME. Essa opção protege informações como as portas UDP, chaves de criptografia para mídia (SRTP) e propriedades sobre o escopo da sessão (THERMOS, 2007).

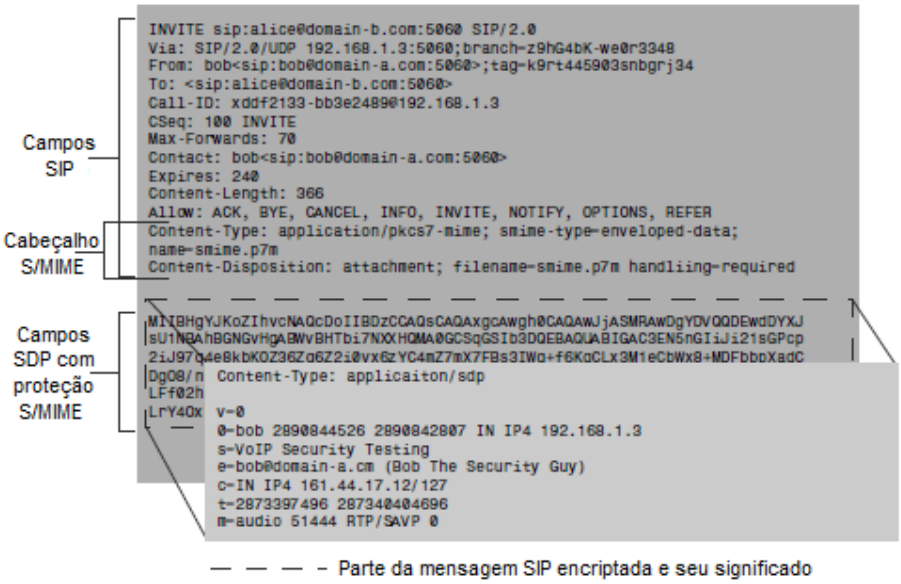

Figura 5.8: SIP com a parte SDP criptografada usando S/MIME (THERMOS, 2007)

Outro método utilizado é encapsular a mensagem SIP com o S/MIME fornecendo um nível adicional de privacidade para o usuário final uma vez que esse método permite ocultar as informações do originador da chamada. A porção da mensagem SIP sem a criptografia (campos "*To*", "*From*", "*Call-ID*", "*Cseq*" e "*Contact*") é utilizada pelos intermediários para rotear a mensagem ao destino, porém, quando a mensagem chega ao destinatário, ele utiliza os campos criptografados para tratar esta mensagem, verificando sua identidade através das chaves e certificados e sua integridade através da assinatura digital. Com essa característica, é possível manter a confidencialidade fim a fim da mensagem (THERMOS, 2007). A Figura 5.9 ilustra uma mensagem SIP encapsulada.

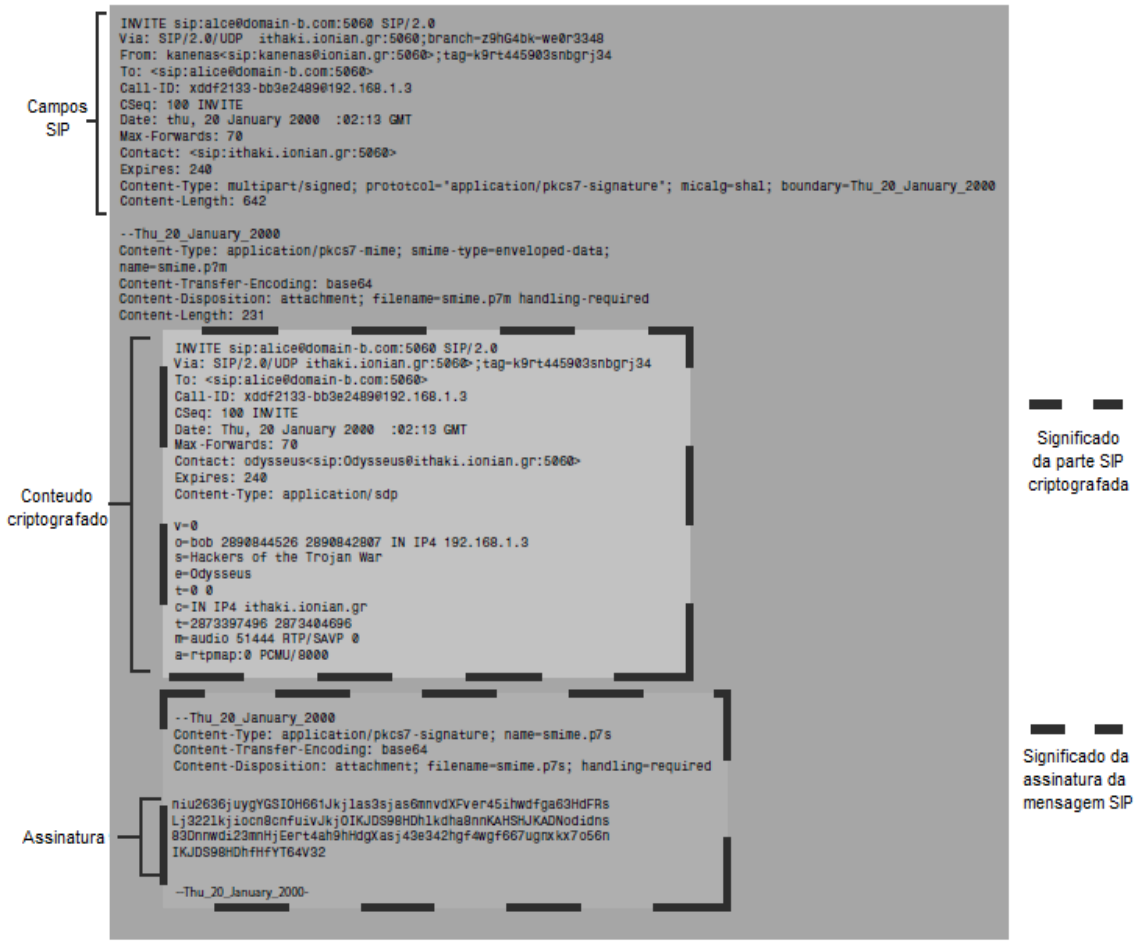

Figura 5.9: Mensagem SIP encapsulada com proteção S/MIME (THERMOS, 2007)

As implementações SIP que utilizam o S/MIME devem ter suporte aos algoritmos de criptografia (DES, 3DES e RC2), ao protocolo de criptografia de chave publica (RSA), ao algoritmo de assinatura digital (SHA1), a certificados digitais (X.509) (HARRIS 2008) (STEWART, 2008).

Como ponto forte pode-se citar:

- É independente do protocolo da camada de transporte, tem suporte a UDP e TCP;
- É mais flexível na proteção das mensagens SIP se comparado a métodos com IPSec, TLS e DTLS;
- Fornece autenticidade, confidencialidade e integridade fim a fim

Limitações:

- Necessidade de maior esforço de implementação, devido a sua complexidade e requerimentos de infra-estrutura (exige PKI) (THERMOS, 2007).

5.2.6 H.323

Para questões de segurança como autenticação e integridade a ITU-T especificou o padrão H.235 para trabalhar em conjunto com os demais protocolos da serie H. Esse padrão especifica perfis de segurança que podem ser combinados para atender aos serviços de segurança como autenticação, integridade, confidencialidade, irrevogabilidade, controle de acesso e gerenciamento de chave de criptografia. (PORTER, 2007).

O perfil H.235.1, por exemplo, presta suporte a serviços de autenticação e integridade. A autenticação é suportada através do compartilhamento de chave secreta ou de métodos de chave pública com uso de certificados que são implementados juntamente com os protocolos de controle e de sinalização como o H.245 e o H.225. Outros perfis tratam da criptografia através da utilização de algoritmos de chave simétrica como DES, 3DES e AES que podem ser usados juntamente com o fluxo RTP. Além disso, TLS e IPSec são recomendados para fornecer segurança aos níveis 4 e 3 da pilha TCP/IP respectivamente (PORTER, 2007)

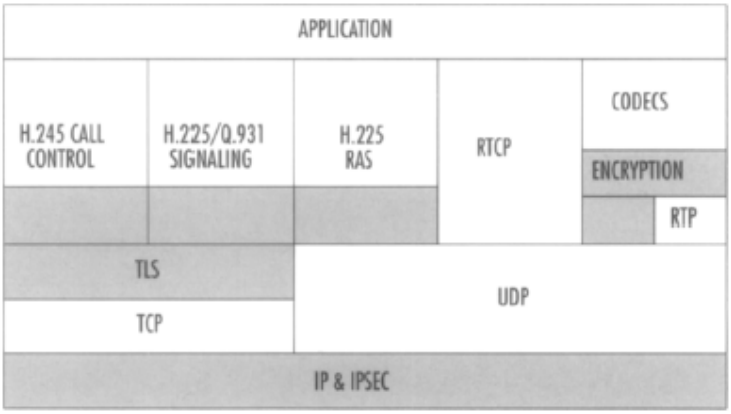

Figura 5.10: Pilha com utilização das recomendações do padrão H.235 (PORTER, 2007)

A Tabela 5.1 apresenta uma breve descrição de cada perfil de segurança especificado pela H.235.

Tabela 5.1: Perfis de segurança do padrão H.235

Recomendação	Descrição
H.235.0	Estrutura de segurança para a série H (H.323 e outros baseados em H.245) sistemas de multimídia
H.235.1	Baseline security profile
H.235.2	Signature security profile
H.235.3	Hybrid security profile
H.235.4	Direct and selective routed call security
H.235.5	Security profile for RAS authentication using weak shared

	secrets
H.235.6	Voice encryption profile with “native” H.235/H.245 key management
H.235.7	MIKEY + SRTP security profile
H.235.8	Key exchange for SRTP on secure signaling channels
H.235.9	Security gateway support for H.323

Fonte: THERMOS, 2007, p.194

Com pontos fortes do H.235 pode-se citar:

- Habilidade de incorporar o material das chaves de criptografia para proteção das mensagens de sinalização e mídia através das mensagens de configuração da chamada (*call setup*);
- Suporte a segurança em tráfego *unicast* e *multicast;*
- Fornece proteção contra ataques de DoS, *man-in-the-middle, spoofing,* seqüestro de chamada e escuta indevida *(eavesdropping)* dependendo da combinação dos perfis do H.235 utilizados;

Limitações:

- É mais complexo de implementar se comparado com o SIP;
- Como não é muito utilizada, a interoperabilidade entre produtos de fabricantes diferentes pode ser um problema.

5.2.7 MGCP

O protocolo MGCP não fornece nenhum controle de segurança, dessa forma, é muito recomendado utilizar protocolos de segurança como é o caso do IPSec para fornecer alguma proteção ao MGCP. Se não for implementada nenhuma proteção, um atacante pode facilmente enviar mensagens de sinalização para desconectar chamadas, desviar o fluxo RTP para outro host ou mesmo o fluxo de uma conferencia sem que os participantes tomem conhecimento (THERMOS, 2007)

Recomenda-se para a proteção de ataques ao MGCP:

- Reforçar o controle de acesso a rede (ACL) para restringir o acesso a portas do MGCP. Essa prática evita a tentativa maliciosa de manipulação de sessões existentes;
- Reforçar a relação um-para-um entre call manager (ou call agents) e os gateways da RPTC na troca de mensagens MGCP;
- Quando suportado, habilitar IPSec para a criptografia do tráfego entre call manager e o gateway RPTC.

5.3 Segurança no fluxo da mídia

Como foi visto no item 3, embora existam diferente protocolos de sinalização usados para estabelecer uma sessão de VoIP (SIP, H.323 e MGCP são alguns exemplos), o protocolo padrão utilizado para a troca de fluxo de mídia é o RTP (*Real Time Protocol*). Contudo, se o RTP for utilizado sem os devidos cuidados, o fluxo de mídia poderá ficar vulnerável a ataques de interceptação e manipulação que comprometerão princípios de integridade e confidencialidade das informações trafegadas no ambiente. Sendo assim, esse tópico tem como objetivo apresentar mecanismos utilizados para fornecer segurança contra as ameaças e vulnerabilidades relacionadas ao processo de fluxo de mídia em redes de voz sobre IP.

5.3.1 SRTP e SRTCP

Secure Realtime Transport Protocol (SRTP) é o padrão especificado pela IETF através da RFC 3711 para fornecer confidencialidade, integridade e autenticação ao tráfego de mídia em tempo real em aplicações multimídia (áudio e vídeo). Adicionalmente ele também fornece proteção às mensagens RTCP (*Realtime Transport Control Protocol)* que tem como função fornecer informações referentes a QoS como atraso*, jitter* e quantidade de pacotes transmitidos aos participantes de uma sessão RTP. Pelo fato das mensagens RTCP e RTP serem transmitidas separadamente, inclusive cada protocolo usa portas de serviços distintas, ambas precisam estar protegidas por algum mecanismo de segurança, pois, caso o RTCP não esteja protegido, o tráfego poderá ser manipulado ocasionando a interrupção ou degradação do serviço VoIP (THERMOS, 2007).

A confidencialidade do fluxo de mídia RTP é garantida pela utilização de criptografia na carga útil dos pacotes transmitidos. Dessa forma, antes que seja enviado qualquer fluxo de mídia é necessário que haja uma negociação das chaves criptográficas entre as partes envolvidas na comunicação. Para esse fim, foram propostos diversos protocolos de gerenciamento de chaves, cada um com seus prós e contras, sendo que os mais utilizados comercialmente são o MIKEY e o *Sdescriptions*. A recomendação é combinar o SRTP com o mecanismo de troca de chaves que tenha o suporte mais adequado com os requerimentos do ambiente (THERMOS, 2007).

Enquanto que o algoritmo criptográfico padrão utilizado pelo SRTP para garantir a confidencialidade do fluxo RTP é o AES (*Advanced Encryption Standard*) com chaves de 128 ou 256 bits de comprimento, a integridade e a autenticação são fornecidas pelo algoritmo SHA-1 de 160 bits. O MAC (*message authentication code*) é calculado pelo *hash* de todo conteúdo do pacote RTP (cabeçalho RTP e carga útil criptografada) e seu valor é incluído no campo *Authentication tag*. O uso desse campo é recomendado para fornecer proteção contra ataques de repetição (*message reply*). Já o campo *Master Key Identifier* (MKI) que é opcional, pode ser utilizado como forma de recuperar ou verificar a chave mestre utilizada numa sessão como também verificar a autenticidade da carga útil do pacote SRTP associada a ela. Na Figura 5.11 é ilustrado o formato do pacote SRTP (THERMOS, 2007).

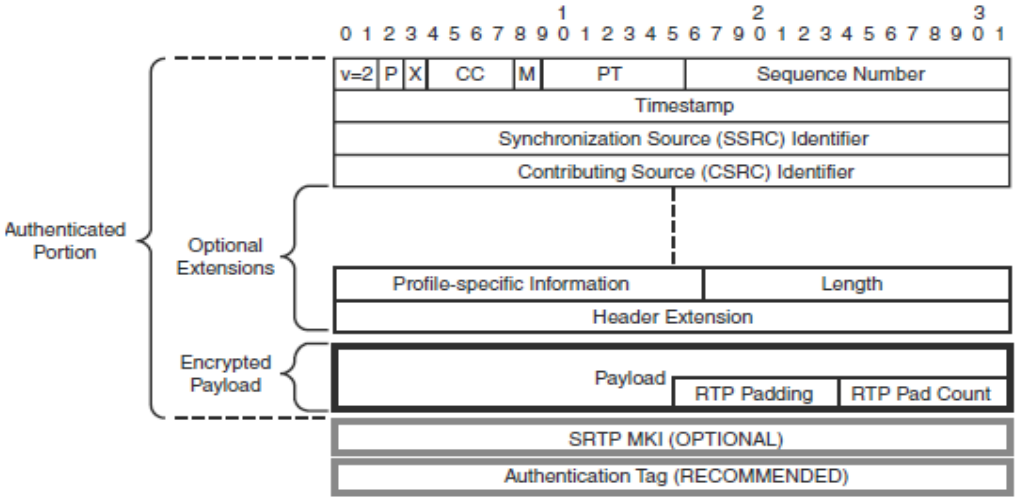

Figura 5.11: Pacote SRTP (THERMOS, 2007)

No SRTCP também há o campo *Authentication tag* e o *Master Key Identifier* (MKI) utilizados no SRTP, contudo, além destes campos há dois cabeçalhos adicionais: *SRTCP index*, utilizado para contar a seqüência dos pacotes, evitando ataques de repetição (*replay attacks*) e o *Encrypt-flag* (E), que indica se o corpo RTCP foi criptografado (THERMOS, 2007). A Figura 5.12 ilustra o formato do pacote SRTCP.

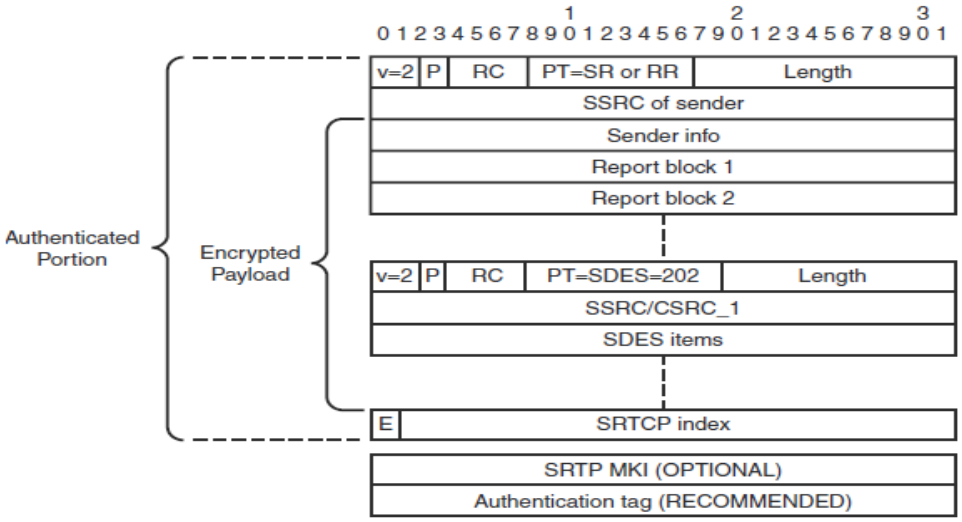

Figura 5.12: Pacote SRTCP (THERMOS, 2007)

6 CONCLUSÃO

Embora já tenha se firmado como uma tecnologia de comunicação alternativa aos sistemas convencionais de telefonia baseados em redes de circuitos comutados, em termos de segurança o VoIP ainda tem muito a evoluir. Conforme foi visto no capítulo 4, as ameaças e vulnerabilidades estão por toda a parte, presentes em todos os elementos de infra-estrutura que compõem a arquitetura da solução de voz sobre IP. Seja um hardware, um software, um protocolo de comunicação ou mesmo os próprios usuários, todos esses elementos possuem alguma vulnerabilidade que pode ser explorada se não forem utilizadas as devidas proteções.

Seja um usuário desavisado que acaba fornecendo informações para um atacante, seja um equipamento de rede mal configurado ou sem as devidas atualizações de *firmaware*, até mesmo a falta de conhecimento sobre os riscos que afetam a tecnologia de VoIP utilizada, todas essas variáveis influenciam na segurança do ambiente de telefonia IP. Conseqüentemente, as soluções de segurança devem abranger cada uma dessas variáveis indistintamente, pois um item que seja negligenciado pode comprometer todo o ambiente e colocar a perder todo investimento realizado.

Apesar desse cenário, foi visto no capitulo 5 que existem diversos mecanismo de proteção cada um direcionado a uma vulnerabilidade ou a um conjunto delas. Ataques que visam comprometer a disponibilidade dos serviços VoIP, como técnicas de negação de serviço, tem como alvo elementos da infra-estrutura, seja servidores SIP, Gatekeepers, DNS ou mesmo equipamentos de rede como roteadores e switches. Como forma de prevenir esses ataques e outros baseados em violação de acesso, foi visto que é muito recomendada a segmentação da rede separando os fluxos de dados dos fluxos de voz além da utilização de equipamentos como firewalls IDS e IPS.

Para os ataques que visam comprometer a confidencialidade e a integridade das informações trafegadas em redes VoIP, os quais geralmente são direcionados ao fluxo de sinalização e ao transporte fim a fim da mídia, as proteções existentes são baseadas em técnicas de criptografia como o TLS, DTLS, S/MIME, IPSec, SRTP e SRTCP. Contudo, a técnica escolhida deve ser muito bem avaliada segundo aspectos de desempenho e complexidade de implementação além da sua interoperabilidade entre equipamentos, pois, o que se percebe é que não há um padrão claramente definido pela indústria no que se refere a esses mecanismos de criptografia e isso dificulta a implementação das soluções.

Como recomendação fica evidente a adoção de uma política de segurança sólida, que não se restrinja somente as vulnerabilidades conhecidas e que seja periodicamente atualizada. Além disso, é importantíssimo que essa política de segurança seja baseada em camadas, até porque os ataques não se concentram apenas em uma técnica de

exploração das vulnerabilidades, mas em um conjunto delas e qualquer brecha pode comprometer a segurança de todo o ambiente.

Relativo aos aspectos de segurança, fica evidente que a tecnologia de VoIP tem muito a amadurecer. Contudo, se seguidas algumas recomendações ela atualmente já pode ter um grau de segurança satisfatório e se apresenta como uma forma viável e promissora ao progresso da comunicação mundial.

REFERÊNCIAS

BATES, R. J. **Broadband Telecommunications Handbook.** 2nd ed. [S.l.]: McGraw−Hill, 2002.

BAUGHER, M. et al. **The Secure Real-time Transport Protocol (SRTP)**: RFC 3711. [S.l.]: IETF, 2004.

DIERKS, T.; RESCORLA, E. **The Transport Layer Security (TLS) Protocol -** version 1.1: RFC 4346. [S.l.]: IETF, 2006.

GREGORY, P. **SIP Communications For Dummies®.** Hoboken: Wiley Publishing, 2006.

HARRIS, S. CISSP **All-in-One Exam Guide.** 4th ed. [S.l.]: McGraw−Hill, 2008.

KELLY, T. **VoIP for Dummies**. Hoboken: Wiley Publishing, 2005.

KENT, S.; SEO, K. **Security Architecture for the Internet Protocol**: RFC 4301. [S.l.]: IETF, 2005.

MAGALHÃES, I. L. **Gerenciamento de serviços de TI na prática**: uma abordagem com base na ITIL. São Paulo: Novatec , 2007.

MCGANN, S.; SICKER, D. C. **An Analysis of Security Threats and Tools in SIP-Based VoIP Systems**. [S.l.]: University of Colorado at Boulder, 2005.

PORTER, T.; GOUGH, M. **How to Cheat at VolP Security**. Rockland: Syngress Publishing, 2007.

RAMSDELL, B. **Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification:** RFC3851. [S.l.]: IETF, 2004

SINNREICH, H. **Internet Communications Using SIP:** Delivering VoIP and Multimedia Services with Session. Indianapolis: Wiley Publishing, 2006.

SOARES, L. F. **Redes de Computadores:** das LANs, MANs e WANs às redes ATMs. Rio de Janeiro: Campus, 1995.

STEWART J. M.; TITTEL E.; CHAPPLE M. **CISSP:** Certified Information Systems Security Professional Study Guide. 4th ed. [S.l.]: Wiley Publishing, 2008.

TANEMBAUM, A. S. **Redes de Computadores.** 4.ed. Rio de Janeiro: Campus, 2003.

THERMOS, P.; TAKANEN, A. **Securing VoIP networks** : threats, vulnerabilities, countermeasures. Boston: Pearson Education, 2007.

TUCKER, G. S. **Voice Over Internet Protocol (VoIP) and Security**. [S.l.]: SANS Institute, 2004.