

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN**

BRUNO CÉSAR CÂMARA DE FARIAS

**SEGURANÇA APLICADA À VOIP: ESTUDO DAS
VULNERABILIDADES E SUAS SOLUÇÕES**

**NATAL/RN
2010**

BRUNO CÉSAR CÂMARA DE FARIAS

**SEGURANÇA APLICADA À VOIP: ESTUDO DAS
VULNERABILIDADES E SUAS SOLUÇÕES**

Monografia apresentada à Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte - FARN, como parte dos requisitos para obtenção do título de Especialista em Redes de Computadores.

Orientador:

Aluizio Ferreira da Rocha Neto (M.Sc.)

**NATAL/RN
2010**

BRUNO CÉSAR CÂMARA DE FARIAS

SEGURANÇA APLICADA À VOIP: ESTUDO DAS
VULNERABILIDADES E SUAS SOLUÇÕES

Monografia apresentada e aprovada em _____ de _____ de _____, pela banca
examinadora composta pelos seguintes membros

Aluizio Ferreira da Rocha Neto (M.Sc.)
Orientador

Membro examinador

Membro examinador

RESUMO

Diversas novas tecnologias estão surgindo no mercado para otimizar as operações de empresas e facilitar a vida das pessoas. Uma das áreas que mais têm avançado é a área de telecomunicações. Está acontecendo uma revolução no sistema de telefonia utilizado atualmente, cujas bases foram criadas há mais de 100 anos. A atual rede de circuitos comutados está gradativamente sendo substituída pela rede de pacotes comutados como o VOIP, que originalmente só era utilizada para o tráfego de dados. Esta mudança é benéfica para todos, pois reduz custos e acrescenta novas funcionalidades ao sistema de telefonia pública, porém, é preciso estar atento para os diversos desafios que esta nova tecnologia traz consigo, dentre eles o desafio de garantir no mínimo a mesma segurança que existe no sistema de telefonia atual. É importante que se tenha conhecimento das ameaças envolvidas com a tecnologia, para que se possa tomar as medidas necessárias para proteção da infraestrutura VOIP instalada e como consequência disso, garantir que a infraestrutura seja compatível com as três premissas da Segurança da Informação: Confiabilidade, Integridade e Disponibilidade. Este trabalho apresenta os problemas de segurança que estão relacionados as tecnologias VOIP e também suas soluções com ênfase no protocolo SIP.

Palavras-chave: VoIP .Segurança. SIP.

ABSTRACT

Diverse new technologies are appearing in the market to optimize the operations of companies and to facilitate the life of the people. One of the areas that more have advanced is the area of telecommunications. A revolution in the system of telephony is happening used currently, whose bases had been created have 100 years more than. The current net of commuted circuits is gradual being substituted for the net of commuted packages as the VOIP, that originally was only used for the traffic of data. This change is beneficial for all, therefore it reduces costs and it adds new functionalities to the system of public telephony, however, is necessary to be intent for the diverse challenges that this new technology brings obtains, amongst them the challenge to at least guarantee the same security that exists in the system of current telephony. It is important that if it has knowledge of the involved threats with the technology, so that if can take the necessary measures for protection of installed infrastructure VOIP and as consequence of this, to guarantee that the infrastructure is compatible with the three premises of the Security of the Information: Trustworthiness, Integrity and Availability. This work presents the security problems that are related technologies VOIP and also its solutions with emphasis in protocol SIP.

Word-key: VoIP. Security. SIP.

LISTA DE ABREVIATURAS

DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	IP Security Protocol
ITU-T	International Telecommunication Union
MIME	Multipurpose Internet Mail Extensions
MITM	Man in the Middle
PABX	Private Automatic Branch Exchange
PBX	Private Branch Exchange
PSTN	Public Switched Telephone Network
RTCP	Real-Time Transport Control Protocol
RTP	Real-Time Transport Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SPIT	Spam over IP Telephony
SRTP	Secure Real-time Transport Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport layer security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
ZRTP	Zimmermann Real-Time Transport Protocol

SUMÁRIO

1 INTRODUÇÃO	8
1.1 OBJETIVOS	9
1.2 ORGANIZAÇÃO DO TRABALHO	9
2 REFERENCIAL TEÓRICO	10
2.1 VOIP	10
2.1.1 Conceito.....	10
2.2 PROTOCOLOS USADOS NOS SERVIÇOS VOIP	12
2.3 PROTOCOLO SIP	13
2.3.1 Agente Usuário Cliente	14
2.3.2 Agente Usuário Servidor	15
2.3.3 Servidor Proxy.....	15
2.3.4 Servidor de Redirecionamento	16
2.3.5 Servidor de Registro	17
2.3.6 Endereçamento	18
2.3.7 As Vantagens do SIP	18
2.4 SEGURANÇA.....	19
2.4.1 Definição Acadêmica de Segurança	19
2.4.2 Segurança da Informação	20
3 RISCOS DE SEGURANÇA ATRIBUÍDOS AO VOIP	21
3.1 ATAQUES ATRIBUÍDOS AO VOIP	21
3.2 TIPOS DE ATAQUES EM UM AMBIENTE VOIP	22
3.2.1 DOS (<i>denial of service</i>)	22
3.2.2 DDOS (<i>distributed denial of service</i>).....	22
3.2.3 SIP Cancel/Bye DoS.....	23
3.2.4 SIP Bombing	23
3.2.5 Ataque ao Servidor Proxy	24
3.2.6 Ataque <i>Man in the Middle</i>	24
3.2.7 SPIT (<i>Spam over IP Telephony</i>).....	25
3.2.8 Caller ID Spoofing	25
4 SOLUÇÕES DE SEGURANÇA APLICADAS AO VOIP	27
4.1 TRANSPORT LAYER SECURITY APLICADO AO SIP	27
4.2 PROTOCOLO SRTP (SECURE REAL TIME PROTOCOL)	28
4.3 PROTOCOLO ZRTP	28
4.4 S/MIME APLICADO AO SIP.....	29
4.5 INTRUSION PREVENTION SYSTEM VOICE OVER IP	29
4.6 INTRUSION DETECTION SYSTEM	29
4.7 FIREWALL APLICADO AO VOIP.....	29
4.8 VLA (VIRTUAL LOCAL AREA /ETWORK)	29
5 CONCLUSÃO.....	30
REFERÊNCIAS	31

1 INTRODUÇÃO

Atualmente, presenciamos que cada vez mais novas tecnologias surgem em nosso cotidiano. Uma delas aparece com o avanço de formas da comunicação por voz e não estamos falando diretamente de telefone, mas de uma tecnologia que acompanha o avanço da Internet e suas aplicações. Uma dessas aplicações surgiu para revolucionar o sistema de telefonia.

Voz sobre IP, comumente chamada de VoIP, Telefonia IP ou Telefonia de Banda Larga, é uma tecnologia utilizada por grande parte das empresas e usuários domésticos que permite que sejam realizadas chamadas telefônicas através de uma rede de computadores como a Internet. Essa tecnologia converte sinais analógicos de voz em pacotes de dados digitais e suporta transmissões bi-direcionais em tempo real de conversas telefônicas usando o Internet Protocol conhecido como IP.

Surgiu em 1995, quando Israelenses interessados no assunto desenvolveram um sistema para computadores domésticos com o intuito de realizar comunicação por voz através da Internet. Em seguida, uma empresa chamada Vocaltec Inc lançou seu primeiro software para a comunicação de voz sobre IP, batizado de Internet Phone Software (INFO EXAME, 2005).

Em 1996, surgiu a Free World Dialup, uma associação onde estudiosos do assunto desenvolveram um software que admitiu usuários, estando conectados à Internet, realizar chamadas telefônicas a partir de computadores para telefones convencionais (SISNEMA, 2008).

Passado alguns anos, em 1998, surgiram os Gateways, equipamentos com a capacidade de interligar os aparelhos convencionais de telefones ao sistema VoIP e assim dispensar o uso de computadores em meio as conexões. No final da década de 90, houve uma crescente oferta dos Gateways devido à padronização dos protocolos de sinalização (SISNEMA, 2008).

No Brasil, um grupo de trabalho da rede nacional de pesquisa desenvolveu experimentos associados ao VoIP. Com esses experimentos, surgiu então, a implantação de um serviço que fez com que redes de organizações também pudessem usufruir dos serviços com a utilização de PABX, estações de trabalho e telefones IP.

Com toda essa revolução, os usuários do sistema gozam do baixo custo em relação à telefonia tradicional. Porém, o VoIP ainda necessita de alguns requisitos que são

indispensáveis para uma boa qualidade do serviço e um deles é a banda de dados suficiente para que a qualidade da transmissão não seja degradada (SISNEMA, 2008).

Com o serviço da rede de banda larga mais acessível, o sistema de voz sobre IP se torna mais vantajoso tanto para empresas como para usuários domésticos, à medida que o sistema de telefonia tradicional acaba por se tornar menos viável.

Contudo, paralelamente com o considerável aumento da demanda, também surgiram significativos problemas, sendo que um deles é a falta de segurança. O VoIP deverá sempre receber atenção especial no quesito segurança, pois este serviço compartilha a rede de dados mundial de computadores (Internet) para a transmissão de voz.

1.1 OBJETIVOS

O objetivo geral desse trabalho é a caracterização da tecnologia, apresentando seus protocolos, segurança, riscos e ameaças as quais a tecnologia VoIP está sujeita. Sejam essas, diretas a tecnologia VoIP ou ainda direcionadas aos protocolos e sistemas operacionais que compõem a infraestrutura de suporte, que atualmente, possuem diversas vulnerabilidades e fragilidades.

Contribuindo, dessa forma, para a construção de redes VoIP mais seguras e estáveis, tornando possível o crescimento e avanço dessa tecnologia cada vez mais em comparação a telefonia tradicional.

1.2 ORGANIZAÇÃO DO TRABALHO

Este trabalho está dividido da seguinte forma, no Capítulo 2 será apresentado o Referencial Teórico da Tecnologia VoIP; no Capítulo 3, serão apresentados os Riscos de Segurança Atribuído ao VoIP; no Capítulo 4 será apresentado as Soluções de Segurança Aplicadas ao VoIP e finalmente as Conclusões.

2 REFERENCIAL TEÓRICO

2.1 VOIP

Desde sua invenção, os sistemas de telefonia substancialmente não mudaram muito. É óbvio que novas tecnologias foram aperfeiçoando o sistema como um todo, mas no geral a funcionalidade permaneceu a mesma. Ao decorrer dos anos, os provedores de serviços de telefonia fizeram inúmeras mudanças no sistema, sem que os usuários finais percebessem, acabam não sabendo como o sistema todo funciona, mas têm certeza de duas coisas: o velho aparelho telefônico ainda é usado e os provedores de serviços cobram por qualquer adição de novos serviços na rede (PORTER, 2006).

Nos anos 90, um número considerável de pesquisadores, seja por motivos educacionais ou comerciais, aprofundaram o interesse em levar voz e vídeo para as redes IP, especialmente nas Intranets e na própria Internet. Essa tecnologia é comumente chamada hoje em dia de VoIP e é, em miúdos, o processo de fracionar áudio e vídeo em pequenas partes, transmitindo essas pequenas partes por uma rede IP, e remontando essas pequenas partes novamente no destino, para assim se estabelecer a comunicação entre dois pontos de áudio e vídeo (PORTER, 2006).

A idéia do VoIP certamente não é inovadora, pois existem documentos de pesquisa e patentes existentes há décadas e demonstrações do conceito dado há anos atrás. A partir dos anos 90 a Internet foi popularizando-se de tal forma que a quantidade de pessoas conectadas à grande rede crescia de forma exponencial. Antes disso, a Internet era limitada somente à ambientes acadêmicos de pesquisa (PORTER, 2006).

2.1.1 Conceito

Voice over Internet Protocol, mais conhecido por VoIP, é a tecnologia que permite a utilização das redes IP, como a própria Internet, para o transporte de voz. Esta tecnologia está cada vez mais sendo adotada por empresas e até mesmo por usuários domésticos, pois traz algumas vantagens em relação à telefonia tradicional (VOIP REVIEW, 2004).

Para falar sobre VoIP, é preciso falar um pouco sobre a PSTN (Public Switched Telephony Network), em português, Rede de Telefonia Comutada Pública. Há muitos anos, a rede de telefonia tradicional vem evoluindo e possibilitando uma comunicação de voz confiável e de qualidade entre as pessoas. Esta evolução trouxe diversos benefícios e novas funcionalidades aos usuários, mas mesmo assim, não trouxe mudanças tão significativas como o surgimento do VoIP (NEWPORT NETWORKS, ...).

A PSTN é uma rede de circuitos comutados, que cria um circuito dedicado com uma banda de 64 kbps garantida para o tráfego de voz entre os assinantes, já a tecnologia VoIP é baseada na rede de pacotes comutados, e utiliza diversos pacotes IP para a transmissão de voz (JESZENSKY, 2004).

Na rede de telefonia tradicional, cada chamada deve ter um circuito dedicado de 64 kbps, e este circuito fica ativo e “preso” por toda a chamada, ou seja, mesmo que em um determinado momento não exista tráfego de áudio (as duas pessoas estão em silêncio), nenhuma outra aplicação pode utilizar estes 64 kbps alocados para a ligação. Na rede de pacotes comutados, como as baseadas no protocolo IP, as ligações não possuem um circuito dedicado, (embora existam protocolos que procuram garantir uma banda exclusiva para o tráfego de voz) e sim dividem toda a banda disponível com diversas outras aplicações que também precisam transmitir por determinado meio (JESZENSKY, 2004).

O VoIP captura a voz do interlocutor, e através da utilização de CODECs (compression/decompression) específicos para a voz humana, comprime a voz do interlocutor para que a mesma possa ser transmitida utilizando uma quantidade menor de banda (AUDIO CODES, 2007).

Esta voz comprimida é dividida em pequenas amostras, geralmente variando entre 10 e 40 milissegundos, e colocada em pacotes IP para ser transmitida através da rede. Conforme os pacotes vão chegando ao receptor, o processo inverso é feito, ou seja, o telefone retira as pequenas amostras de áudio dos pacotes IP e remonta a mensagem de voz original (AUDIO CODES, 2007).

Existem diversos CODECs para a utilização em VoIP, mas os mais comuns são os CODECs ITU-T G.711 e o G.729 (AUDIO CODES, 2007).

O G.711 comprime a voz para ser transmitida em canais de 64 kbps, a mesma banda que as chamadas utilizam no sistema de telefonia tradicional. Este CODEC é o que oferece a melhor qualidade de voz atualmente, mas como utiliza uma quantidade razoável de banda, é utilizado em ambientes que disponibilizam uma grande quantidade de banda para as

aplicações, como em redes locais corporativas, que costumam ser formadas por equipamentos que fornecem 100 Mbps na porta de cada usuário (AUDIO CODES, 2007).

Já o G.729 comprime a voz para ser transmitida em 8 kbps, o que otimiza bastante a utilização do links de dados disponível, embora sacrifique um pouco a qualidade da voz. Este CODEC é o mais utilizado quando a quantidade de banda é baixa, como em links com a Internet (AUDIO CODES, 2007).

2.2 PROTOCOLOS USADOS NOS SERVIÇOS VOIP

A tecnologia VoIP utiliza diversos protocolos, sendo eles divididos em três principais categorias: Protocolos de Sinalização, Protocolos de Transporte e Protocolos de Suporte.

Protocolos de Sinalização: são responsáveis pela sinalização, ou seja, são os protocolos que realizam todo o controle das chamadas. Estes protocolos são os responsáveis por iniciar e finalizar as chamadas, realizar o registro dos usuários dentre outras funções. Os mais comuns são a família de protocolos ITU-T H.323 e IETF SIP (Session Initiation Protocol). O protocolo H.323 é o mais utilizado hoje em dia nos sistemas de telefonia IP corporativos, pois possui uma vasta lista de funcionalidades, mas o SIP está tomando destaque no mercado pois é um protocolo padrão, que tem foco em garantir a interoperabilidade entre fabricantes diferentes (TELECO, ...).

Protocolos de Transporte: tanto o H.323 quanto o SIP utilizam-se dos mesmos protocolos para o transporte de áudio. Estes protocolos são o RTP (Realtime Transport Protocol) e o RTCP (Realtime Control Transport Protocol) (TELECO, ...).

Protocolos de Suporte: Protocolos de suporte são os diversos protocolos que participam de um sistema de telefonia IP, alguns protocolos são o TFTP (Trivial File Transfer Protocol), utilizado para carregar o firmware e configurações de telefones IP, o DHCP (Dynamic Host Configuration Protocol), utilizado para entregar as configurações de IP dos telefones e o DNS (Domain Name System), utilizado principalmente pelo SIP para localizar os usuários na rede, é o protocolo mais utilizado nos tempos atuais. A próxima seção dará maior ênfase ao protocolo SIP (TELECO, ...).

2.3 PROTOCOLO SIP

O protocolo de Iniciação de Sessão (SIP) foi criado pelo IETF (Internet Engineering Task Force) com a finalidade de sinalizar sistemas de multimídia (JESZENSKY, 2004).

Este protocolo possui características semelhantes ao protocolo HTTP (Hyper Text Transfer Protocol), pois utiliza também o modelo requisição/reposta para dar início às sessões de comunicação interativa entre os usuários e estabelecer chamadas e conferência através da rede de dados utilizando o protocolo TCP/IP. Oferece também menos questões de interoperabilidade e, além disso, suporta todas as formas de comunicação de tempo real, podendo ser utilizado para todos os serviços, tais como roteamento e mecanismos inerentes à Internet (SIPCENTER,...).

Com seu surgimento na década de 90, o protocolo H.323, muito utilizado para os mesmos fins foi abandonado, pois o SIP trouxe a vantagem de dinamicamente adicionar ou remover usuários em uma sessão. Com o desenvolvimento deste protocolo, pode-se integrar nas sessões de administração vários conteúdos, e somando todas estas vantagens ele tornou-se rapidamente um padrão nos serviços VoIP. Uma de suas características é ter facilitado a integração dos serviços relacionados à Internet, pois este protocolo promove a interoperabilidade nas aplicações, facilita a constituição, alteração e execução da comunicação entre as sessões individuais ou de múltiplos participantes (SIPCENTER,...).

Em síntese, ele é capaz de controlar os meios de comunicação durante uma sessão realizando as adaptações adequadas quando requisitadas, melhorando a capacidade dos usuários interagirem entre si.

A partir dos protocolos utilizados na Internet, como o SMTP e o HTTP, com o intuito de estabelecer, alterar e terminar chamadas de um ou mais usuários em uma rede e acabar com a necessidade de se ter uma central de comutação para completar as chamadas ou interligar os usuários. Também é considerado um protocolo simples, pois possui apenas seis métodos e é independente do protocolo de transporte. O SIP contém cinco componentes em sua estrutura, que serão citados e comentados nos próximos tópicos (TELECO,...).

A figura 1 mostra como é uma arquitetura básica de uma rede VoIP.

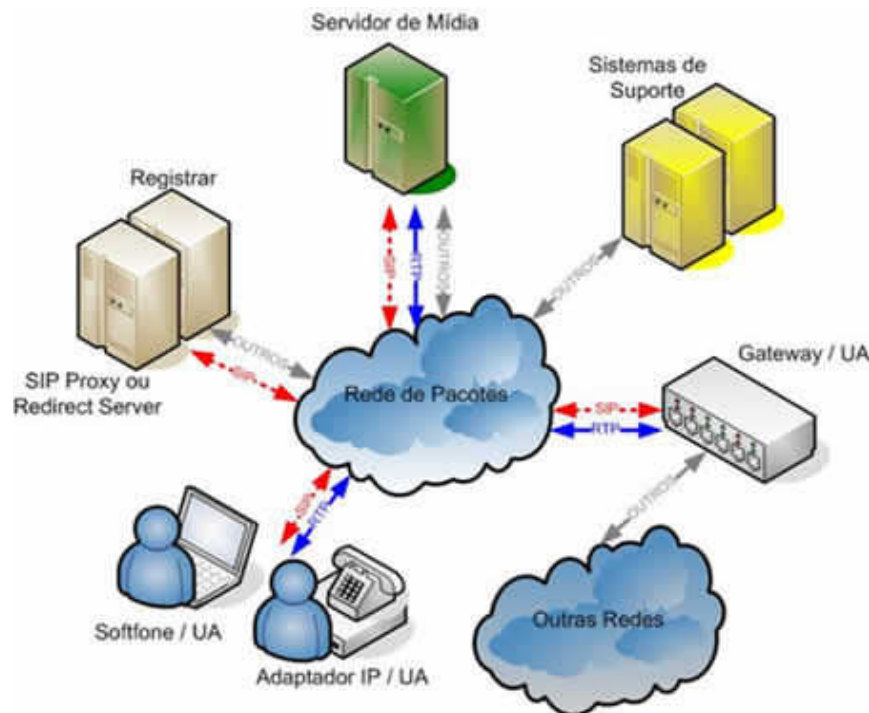


Fig 1: Arquitetura básica de uma rede VoIP.

Fonte: (TELECO,...)

2.3.1 Agente Usuário Cliente

Agente Usuário Cliente é um dos componentes que interagem com cliente e é responsável por gerar requisições (IETF RFC 2543, ...). Algumas das requisições são:

- Register: sua função é registrar o endereço SIP e o IP do usuário no Servidor de Registro;
- Invite: sua função é convidar um agente usuário para iniciar uma sessão;
- Bye: sua função encerrar uma sessão;
- Ack: sua função é fazer com que o Agente aceite uma sessão;
- Cancel: utilizado para cancelar buscas.

Quando a sessão SIP é iniciada pelo Agente Usuário Cliente, dados fundamentais para o pedido, como a porta de comunicação, o protocolo e o endereço IP são requisitados pelo Agente Usuário Servidor, para onde o pedido está sendo enviado. O Agente usuário Cliente também é capaz de utilizar as informações contidas no pedido URI para determinar o curso do pedido do SIP (IETF RFC 2543, ...).

2.3.2 Agente Usuário Servidor

O Agente Usuário Servidor tem a função de hospedar a aplicação responsável por receber os pedidos SIP de um Agente Usuário Cliente e enviar uma resposta ao pedido. Este Servidor pode emitir múltiplas repostas ao Agente Usuário Cliente e não necessariamente uma única resposta. Essa comunicação é realizada entre ambos os usuários como cliente/servidor (IETF RFC 2543, ...).

2.3.3 Servidor Proxy

O Servidor Proxy, como na maioria das aplicações, atua como mediador nas solicitações dos serviços requisitados em uma sessão. O Proxy no SIP é responsável pelas requisições ao Agente Usuário Servidor e fornecê-las ao Agente Usuário Cliente. Essa solicitação pode percorrer vários Servidores Proxy até chegar ao seu destino final. É também elemento chave de um IP PBX, que é um componente que trata da configuração das chamadas SIP em um sistema VoIP (IETF RFC 2543,...).

Outras funções de um Proxy em uma sistema VoIP são:

- Analisar pedidos de percurso para facilitar a localização do usuário;
- Autenticar e autorizar usuários de serviços de call-routing;
- Programar políticas e fornecer recursos para outros servidores;
- Traduzir endereços;
- Aplicar políticas de segurança e realizar roteamento de mensagens.

A figura 2 mostra um Servidor Proxy recebendo uma requisição INVITE do remetente da chamada e encaminhando-a a um Agente Usuário.

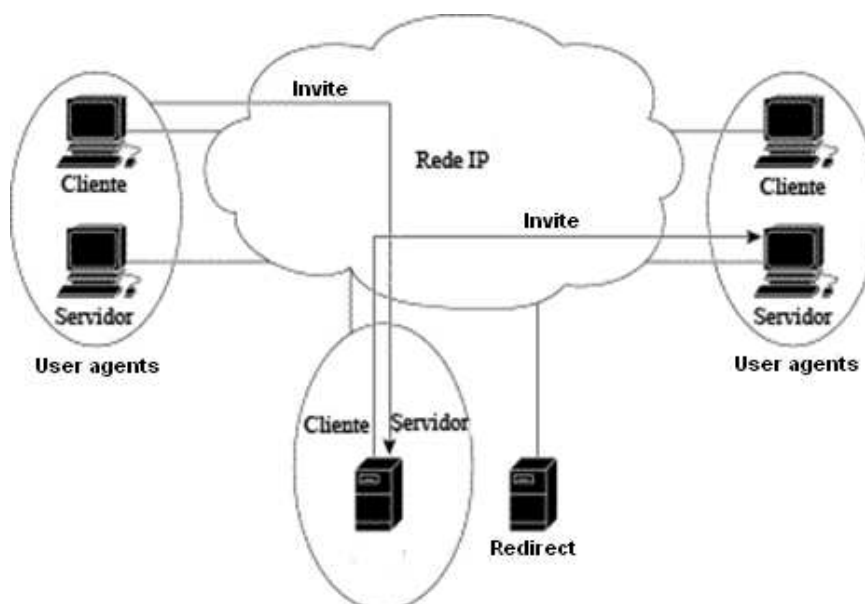


Fig 2: Servidor Proxy.
Fonte: (NATIONAL INSTITUTES,)

2.3.4 Servidor de Redirecionamento

O Servidor de Redirecionamento fornece reorientação aos usuários ao mudarem temporariamente a sua localização geográfica para serem localizados pela mesma identidade, disponibilizando listagens de endereços para que os clientes sejam encontrados. Também realiza mapeamento de endereços e executa a atualização do campo Request URL (IETF RFC 2543, ...).

A figura 3 ilustra um cliente enviando uma requisição INVITE ao Servidor de Redirecionamento e a troca de informações necessárias para realizar o redirecionamento do pedido.

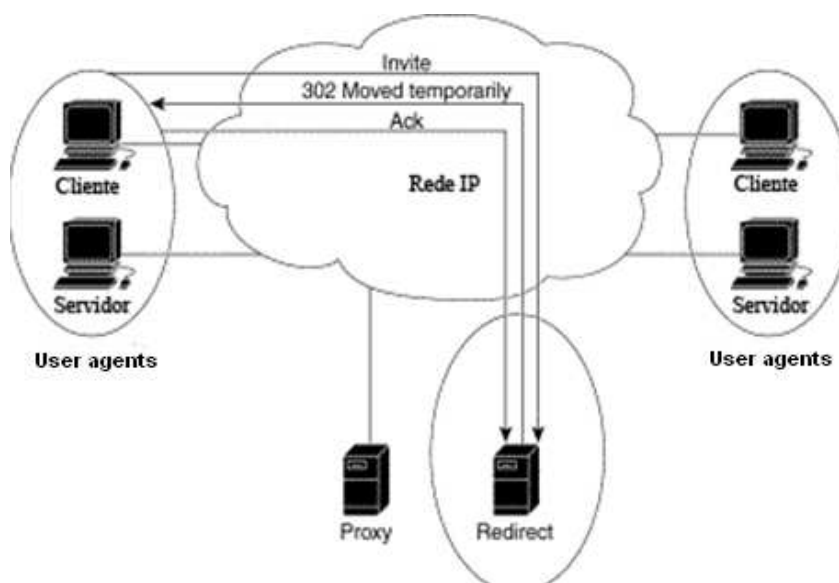


Fig 3: Servidor de Redirecionamento.
Fonte: (NATIONAL INSTITUTES,)

2.3.5 Servidor de Registro

O Servidor de Registro disponibiliza aos usuários a alteração do endereço em que eles são localizados. Isto é possível através do envio do comando SIP REGISTER, que é um pedido de mudança de um endereço ao Servidor.

Os Servidores de Registro armazenam a localização lógica dos usuários dentro de domínios e subdomínios.

Outra função é receber as atualizações sobre a localização de cada usuário e executar a autorização dos nomes, comparados aos servidores DNS de uma rede Web.

Também possibilitam o diálogo ponto a ponto com outros Agentes sem a necessidade do uso dos serviços proporcionados pelos servidores. Qualquer um dos Agentes do SIP precisam primeiramente registrar-se no Servidor de Registro para que possam dar início as chamadas em um ambiente VoIP. Os dados a referentes a localização devem sempre ser renovados, baseando-se no tempo de expiração dos registros (IETF RFC 2543,).

Na figura 4 podemos observar como é realizada a comunicação entre um telefone IP com o Servidor de Registro. O telefone IP envia um comando REGISTER em seguida, recebe uma resposta de confirmação do servidor.

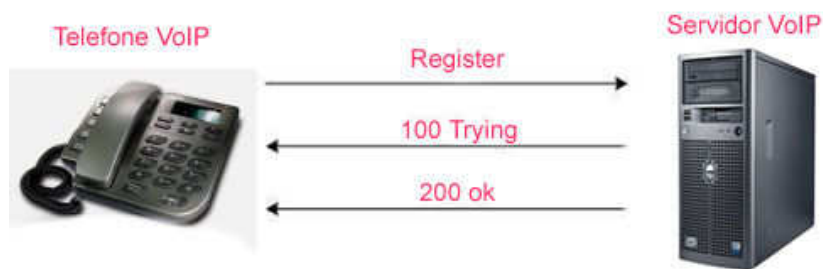


Fig 4: Comunicação com um Servidor de Registro.
Fonte: (WALLINGFORD, 2005).

2.3.6 Endereçamento

Para se realizar uma transmissão de voz em uma sessão é preciso que haja uma forma do originador da chamada encontrar o destinatário. Para que isso ocorra, é preciso que haja um endereçamento dos usuários através de servidores que disponibilizam uma URL SIP para cada usuário. A URL SIP é semelhante a um endereço de e-mail que o cliente deve escolher e criar (cliente@host). O cliente pode ser identificado por um nome ou número de telefone a escolher o host pode ser um endereço numérico de rede (IETF RFC 2543,).

2.3.7 As Vantagens do SIP

Comparado com as soluções existentes, as vantagens do SIP podem se resumidas em simplicidade e conectividade global. O protocolo possui uma estrutura menos complexa que seus predecessores e seus serviços são escaláveis, pois o protocolo emprega as potencialidades inerentes da Internet, como por exemplo, o roteamento e não necessita ser um único ponto focal para o tráfego. Mesmo em uma rede de maior arquitetura a vantagem pode ser mantida.

A maior vantagem de se utilizar este protocolo é a habilidade de se conseguir a conectividade global. Qualquer usuário que publique seu endereço SIP na Internet pode ser localizado, diferente dos serviços de mensagens instantâneas como Messenger, em que o usuário necessita registrar-se em um servidor central (VOIP REVIEW, 2004).

Em outras palavras, os usuários SIP não necessitam de um fornecedor de serviço, mas apenas de acesso a Internet.

2.4 SEGURANÇA

2.4.1 Definição Acadêmica de Segurança

Uma das definições do dicionário Michaelis para a palavra segurança é “certeza”, ou seja, pode-se dizer que segurança é a previsibilidade do futuro, um futuro sem riscos. O desconhecido traz insegurança para o ser humano.

Segurança é um termo muito genérico, e o seu significado é mais bem analisado quando se categoriza os tipos de segurança existentes. Alguns exemplos de segurança que podem ser citados são:

Segurança Física – Trata de manter ativos físicos em segurança, ou seja, evitar o roubo ou danos à computadores, equipamentos eletrônicos, e até o próprio imóvel de uma pessoa física, jurídica ou estado.

Segurança da Informação – Trata de manter as informações em segurança. A informação é um bem intelectual, não é um ativo tangível, portanto precisa de uma abordagem diferente para sua segurança em relação aos ativos fixos.

Segurança da Computação – Trata a segurança de sistemas computacionais, ou seja, visa garantir que os computadores e seus aplicativos funcionem apenas da forma esperada e conhecida, e conseqüentemente garante a segurança dos dados ali armazenados ou em trânsito.

Segurança Doméstica – Trata a segurança residencial de pessoas físicas, visando garantir a integridade do imóvel, dos ativos e das pessoas ali presentes.

Segurança Pública – Trata a segurança em um nível público, ou seja, para todas as pessoas de uma sociedade. Este tipo de segurança geralmente deve ser garantido pelo estado.

Segurança do Trânsito – Trata da segurança de motoristas e pedestres, visando garantir a integridade física e a vida destas pessoas evitando acidentes.

É importante notar que não é possível prover segurança utilizando-se apenas uma das abordagens, pois todas elas acabam se relacionando entre si e de alguma forma acabam sendo interdependentes.

2.4.2 Segurança da Informação

Atualmente a informação é o bem de maior valor existente, e boa parte desta informação se encontra em formato eletrônico. O conceito de informação é algo muito relativo, assim como a determinação do valor da informação. Um exemplo disso é que, uma informação escrita não significa muito para alguém que não saiba ler, e, as informações de uma empresa do ramo agropecuário não têm tanto valor para uma empresa de telecomunicações (IETF RFC 3261,).

Informação é poder, no competitivo mercado da nossa Era da informação, a posse de determinada informação pode fazer toda a diferença para o sucesso ou o fracasso de uma empresa. Devido a este fato, é cada vez mais importante garantir a segurança destas informações (TECH-FAQ ,).

Na sociedade da informação, ao mesmo tempo em que a informação é considerada o principal patrimônio de uma organização, a mesma está também sob constante risco, como nunca esteve antes. Com isso a segurança da informação tornou-se ponto crucial para sobrevivência das instituições. Atualmente as informações contidas em sistemas computacionais são consideradas recursos críticos, tanto para concretização de negócios e tomada de decisões. Nunca foi tão fácil atacar os sistemas informatizados, já que os sistemas de informação institucionais estão conectados em redes externas. Outro aspecto a ser considerado pela gerência é que os sistemas de informática, para operarem de forma adequada e garantirem a segurança das informações da organização, necessitam de ambientes controlados, protegidos contra desastres naturais (incêndio, terremoto, enchente), falhas estruturais (interrupção no fornecimento de energia elétrica, sobrecargas elétricas), sabotagens, fraudes, acessos não autorizados e outros. Segurança é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança (IETF RFC 3261, ...).

Em outras palavras, concluímos que Segurança da Informação agrega valor ao negócio e garante o Retorno sobre o Investimento.

3 RISCOS DE SEGURANÇA ATRIBUÍDOS AO VOIP

Se tratando do aumento de usuários que utilizam a tecnologia VoIP para se comunicar, é evidente a preocupação quanto a segurança oferecida pelo sistema.

Vários líderes e institutos de investigação indicam que esta tecnologia é a próxima grande tendência da telefonia. Mas com as novas oportunidades que este serviço trouxe para a telefonia, também surgiram problemas, ou seja, a falta de segurança (DRABIK, 2003).

A principal preocupação decorre do fato de que este serviço está integrado à rede mundial de computadores (Internet) que sempre esteve exposta a ameaças, e não possui uma estrutura física dedicada somente para o serviço de voz.

Atualmente, a arquitetura da Internet não pode por si só oferecer o mesmo nível de segurança física como a telefonia tradicional (PSTN). Por isso há várias exigências a serem seguidas nas questões relacionadas à segurança.

No entanto existem soluções para aumentar a confiabilidade nos serviço. Nos tópicos seguintes serão comentados alguns problemas que o VoIP enfrenta e algumas soluções aplicadas para evitar problemas relacionados a esta tecnologia.

3.1 ATAQUES ATRIBUÍDOS AO VOIP

Os ataques atribuídos ao VoIP geralmente são divididos em categorias, que podemos citar:

Disponibilidade - Garante o armazenamento, o transporte dos dados e acesso a sistemas de informação sempre que os usuários autorizados solicitarem. Os ataques que são direcionados à disponibilidade, geralmente são classificados como uma negação de serviço. Os tipos podem variar como consumo de banda, ataques de roteamento, etc.

Integridade - Este tipo de ataque pode alterar a voz em uma conversa, conteúdos de dados, senhas, configuração e outras informações armazenadas no sistema. Muitos utilizam criptografia e algoritmos que ajudam na manutenção da integridade, mas mesmo que este tipo de defesa atenua as ameaças, ainda existem vulnerabilidades.

Confidencialidade - É uma questão importante em se tratando dos sistemas VoIP, quando comparado com a telefonia tradicional (PSTN). Refere-se à proteção dos dados contra

usuários não autorizados. Em outras palavras, a perda de confidencialidade poderia ser uma escuta de uma conversa por meio de serviços telefônicos.

3.2 TIPOS DE ATAQUES EM UM AMBIENTE VOIP

3.2.1 DOS (*denial of service*)

Este tipo ataque acarreta negação de serviço, ou seja, a indisponibilidade ou perda de qualidade, que é muito comum em uma rede de dados. O ataque pode ser realizado com a exploração de falhas ou consumo de memória excessiva em equipamentos, ou sobrecarregando o processamento ou banda de uma rede de dados (ÁUDIO CODES, 2007).

Quando um computador sofre um ataque do tipo DoS, ele não está sendo invadido e sim sobrecarregado.

3.2.2 DDOS (*distributed denial of service*)

DDoS é também um ataque do tipo DoS, mas com uma diferença, ele ocasiona um impacto maior ao alvo, pois utiliza-se de várias máquinas para realizar o ataque.

Para que este tipo de ataque tenha forte impacto, é necessário que um grande número de máquinas (computadores) estejam envolvidas, e para que isto aconteça, é preciso inserir programas DDoS em vírus de computador ou programas maliciosos que estejam encarregados de atingir uma grande quantidade de computadores conectados à Internet. Após serem espalhados e alojados nas máquinas, esses programas geralmente agem em segundo plano, fazendo com que o usuário não perceba que sua máquina esteja realizando uma tarefa que não é do seu conhecimento. Como este ataque parte de vários pontos, fica difícil saber de onde ele se originou. Em outras palavras, quando uma máquina de um usuário é infectada, ela acaba se tornando um zumbi. Os zumbis recebem instruções sobre qual alvo será atacado por intermédio de uma máquina mestre (PORTER, 2006).

A figura 5 nos mostra um atacante se apossando do computador de uma vítima, e a partir deste computador, que é chamado de mestre, outros são instruídos a atacar um só ponto.

Com isso, o ataque poderá ganhar maior impacto sobre o alvo e assim, acarretar um grande problema.

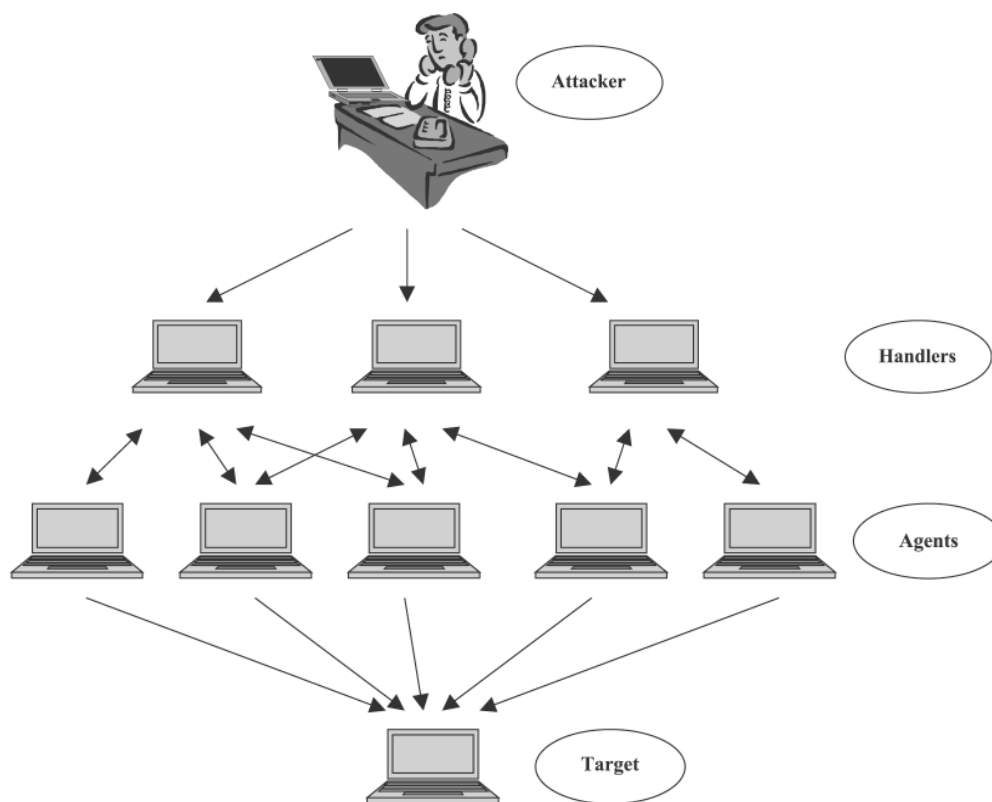


Figura 5: Ataque Distributed Denial of Service.
Fonte: (IETF RFC 3261,).

3.2.3 SIP Cancel/Bye DoS

É um ataque onde o invasor simula uma mensagem de desconexão do tipo CANCEL ou BYE em uma chamada. O objetivo principal é evitar que o usuário realize uma chamada ou até mesmo interromper uma sessão que esteja em andamento. Para que um SIP CANCEL se torne eficiente, é preciso que o ataque seja lançado entre o tempo disponível na emissão do método INVITE e na recepção do último ACK (TELECO,).

3.2.4 SIP Bombing

O ataque SIP Bombing transmite uma grande quantidade de mensagens forjadas em uma sessão VoIP. A telefonia IP é muito sensível às questões de disponibilidade. Sendo

assim, uma quantidade de mensagens acima do normal exigirá muito dos recursos computacionais para a decodificação e interpretação dos dados (TELECO, ...).

Com o sistema ocupado com o processamento de falsas mensagens, as válidas serão processadas em um ritmo mais lento ou até mesmo perdidas, afetando o seu desempenho.

Equipamentos do tipo telefones IP podem apresentar problemas, como queda de conexões quando submetidos a um excesso de tráfego, resultando algum nível de paralisação do serviço. Em se tratando aos softphones, esses são mais adaptados ao problema.

3.2.5 Ataque ao Servidor Proxy

O Servidor Proxy do SIP é um recurso essencial em um sistema baseado no protocolo SIP, pois é responsável pelo tratamento entre todos os parâmetros e pedidos SIP, incluindo Gateways, telefones SIP, e outros recursos.

Quando os serviços são descontinuados, toda rede envolvida será afetada, impedindo usuários de realizar e receber chamadas.

Estes ataques prejudicam total ou parcialmente o funcionamento dos componentes que compõem o sistema. Isto significa que alguns ou todos os seus usuários não serão capazes de realizar ou receber chamadas.

3.2.6 Ataque Man in the Middle

Man in the Middle ou MITM (homem no meio) é um ataque que captura, lê e modifica mensagens VoIP sem deixar nenhuma evidência de que os dados foram alterados para quem está em ambas as extremidades de uma conversa. Normalmente, o atacante se introduz no meio de uma comunicação (CONTENT VERIFICATION, ...).

Este ataque que é feito entre a comunicação e é um dos mais difíceis de ser detectado e com isso, o atacante pode tomar posse de senhas, desviar tráfego de dados, injetar e modificar pacotes, etc. Existem diferentes áreas de ataques, sendo alguns são realizados na rede local, ou seja, o atacante e a vítima estão na mesma rede (CONTENT VERIFICATION, ...).

A figura 6 mostra a entidade "A" enviando dados para a "B" pelo caminho determinado na sessão. A entidade "M" altera o curso, com isso os dados passam por ela antes de chegar ao seu destino.



Fig 6: Ataque Man in the Middle.
Fonte: (Guardian, 2007).

3.2.7 SPIT (Spam over IP Telephony)

Em um ataque SPIT, o atacante envia mensagens ou gravações indesejadas para os usuários VoIP, muitas vezes oferecendo produtos ou serviços não solicitados. Isto é possível graças a softwares específicos que efetuam automaticamente ligações simultaneamente para vários usuários (VOIP NEWS, ...).

A NEC Corporation desenvolveu um sistema com o nome de VoIP SEAL, com a finalidade de barrar Spams. Este sistema identifica e bloqueia as chamadas enviadas por geradores de Spams antes mesmo que eles cheguem até a vítima. Em uma simulação realizada pela NEC com o VoIP SEAL, foi constatado que 99% dos ataques foram detectados e bloqueados (SECURITY PRO NEWS, ...).

Este tipo de ataque não é considerado um problema de grandes proporções, pois o uso do VoIP ainda não se tornou uma grande tendência no ambiente da telefonia. No entanto, estudiosos do assunto dizem que nos próximos anos com o aumento da utilização desta tecnologia, os ataques do tipo SPIT terão maior impacto e automaticamente a qualidade dos serviços VoIP poderá sofrer uma degradação, pois o envio de Spams podem causar consumo excessivo de banda (GUARDIAN, 2007).

3.2.8 Caller ID Spoofing

Caller ID Spoofing é um ataque que permite ao atacante mascarar uma identificação telefônica. Este tipo de ataque pode ser aplicado tanto no VoIP quanto na telefonia convencional ou telefonia móvel (SECURITY FOCUS, ...).

Atualmente, existem tecnologias que permitem que o interlocutor altere sua identidade e se apresente com falsos nomes e números, e por existirem equipamentos que interligam a telefonia convencional com o VoIP, este ataque pode partir de qualquer lugar do mundo (ASTERISK VOIP NEWS,).

A figura 7 mostra uma situação em que o usuário recebe uma ligação. Ao atender, o identificador do telefone exibe um número de uma instituição de sua confiança, mas por trás disto, há um atacante praticando um golpe, fazendo- se passar pela instituição, que no caso é um Banco Financeiro.

A partir daí, o usuário passa tudo que é requisitado por quem está do outro lado da ligação, como por exemplo, dados confidenciais, senhas, etc.

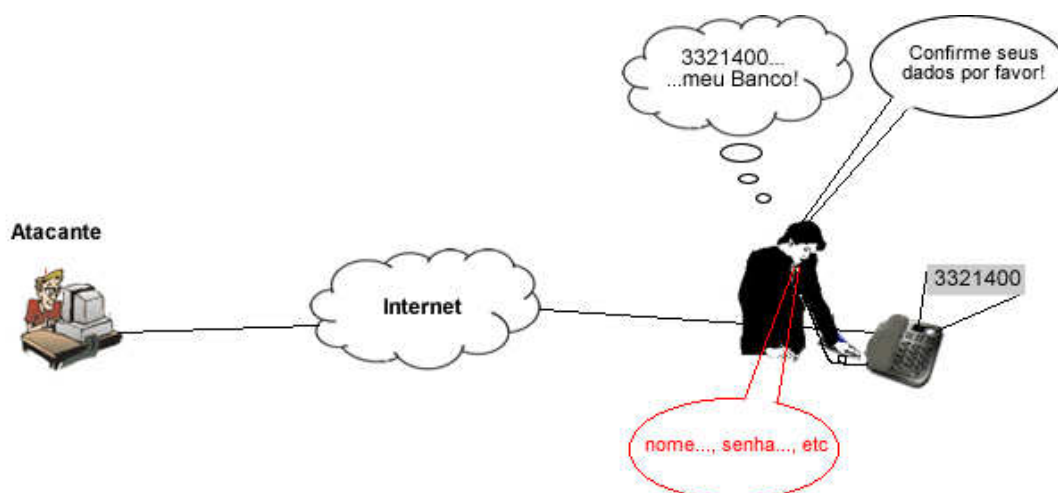


Fig 7: Ataque Call ID Spoofing.
Fonte: (SECURITY FOCUS,).

Para evitar que se caia em um ataque deste tipo, é necessário que entre o cliente e a instituição haja mecanismos de segurança ou regras de identificação antes mesmo do cliente passar seus dados confidenciais para quem está do outro lado da ligação.

4 SOLUÇÕES DE SEGURANÇA APLICADAS AO VOIP

Atualmente, a maioria das principais operadoras de telefonia estão se preparando para adotar o VoIP. No entanto, com a promessa de uma demanda maior no consumo dos serviços, também aumentará o risco de violações generalizadas. Com a utilização em massa, os usuários tanto de empresas quanto domésticos estão sujeitos aos mesmos riscos que sempre estiveram envolvidos à rede de dados (Internet).

O ambiente na Internet, pode ser particularmente considerado um oponente ao VoIP, por várias razões. Uma delas, é que os mecanismos de proteção nunca foram suficientes para resguardar uma aplicação, e isto significa que qualquer dispositivo VoIP corre o risco de sofrer violações.

As formas de se aplicar segurança são classificadas em protocolo, procedimentos, arquitetura e sistemas especializados, que serão estudados nos próximos tópicos.

4.1 TRANSPORT LAYER SECURITY (TLS) APLICADO AO SIP

O principal objetivo do protocolo TLS é estabelecer uma comunicação privada e manter a integridade dos dados durante a sessão. O protocolo permite que aplicações cliente/servidor se comuniquem de uma forma segura, projetada para impedir escutas, adulteração e falsificação de mensagens (TECH-FAQ,).

O protocolo é composto por duas camadas, o TLS Record e o TLS Handshake e utilizam criptografia simétrica. A criptografia simétrica é fornecida para cada conexão (TECH-FAQ,).

O TLS Handshake é um protocolo auxiliar que roda sobre o nível 4, negociando as chaves e não carrega dados de aplicação.

O TLS Record garante que os dados que estão sendo trocados entre as entidades não sejam alterados. O protocolo pode ser usado com ou sem criptografia, garantindo a segurança dos dados para que não sejam modificados e outras pessoas não autorizadas tenham acesso enquanto estiverem sendo transmitidos (PORTER, 2006).

4.2 PROTOCOLO SRTP (SECURE REAL TIME PROTOCOL)

O SRTP foi desenvolvido por peritos de comunicações da Cisco e da Ericsson, e foi publicado formalmente em março de 2004 pelo IETF (*Internet Engineering Task Force*). Sua função é manter a confidencialidade, autenticidade e proteção contra retransmissões fraudulentas dos pacotes RTP e RTCP. É também ideal para proteger o tráfego de voz sobre IP, pois pode ser utilizado em conjunto com o cabeçalho de compressão e não tem nenhum efeito sobre o IP quando se trata de qualidade de serviço (JOHNSTON, 2004).

Estes fatores proporcionam vantagens significativas, em especial para o tráfego de voz.

Outra vantagem, é que ele pode ser implantado em aplicativos pequenos que possuam poucos códigos de execução. Com essas propriedades, ele é favorável nas implementações em dispositivos móveis com memória limitada (JOHNSTON, 2004).

4.3 PROTOCOLO ZRTP

O protocolo ZRTP foi desenvolvido por Phil Zimmermann, com a cooperação de Alan Johnston e Jon Callas. Este protocolo foi baseado no RTP e utiliza protocolo Diffie Hellman para fornecer criptografia nas sessões (HANDLEY, 1998).

Em uma sessão VoIP, o ZRTP intercepta e filtra todos os pacotes de voz dos usuários, detecta o início de uma chamada e em seguida aplica criptografia. Este protocolo traz também outra vantagem ao usuário, pois informa quando uma chamada é segura (HANDLEY, 1998).

4.4 S/MIME APLICADO AO SIP

O S/MIME é uma solução de criptografia utilizando-se o sistema de chave pública e privada, desenvolvida para prover autenticação, integridade da mensagem, não repúdio e confidencialidade para serviços de e-mail. Apesar de ter sido desenvolvido para a utilização com mensagens de e-mail, o S/MIME pode ser utilizado também para mensagens HTTP e SIP (PORTER, 2006).

4.5 INTRUSION PREVENTION SYSTEM VOICE OVER IP

O Intrusion Prevention System é usado para monitorar a atividade de uma rede ou sistema com o objetivo de prevenir ataques. Quando um ataque é detectado pelo IPS, ele responde imediatamente, bloqueando o ataque antes mesmo que se prejudique a integridade dos dados (WALLINGFORD, 2005).

4.6 INTRUSION DETECTION SYSTEM

Intrusion Detection System monitora elementos em uma rede contra ataques do tipo DoS e Call Fraud, consultando regras contidas em uma base de dados ou também através de definições ditadas pela rede (UNDERSTANDING, 1998)

A maioria destes sistemas utiliza uma orientação à detecção de assinaturas de ataques e são muitos eficientes com relação a ataques já conhecidos, mas falham ao se deparar com novos tipos de ataques (UNDERSTANDING, 1998).

4.7 FIREWALL APLICADO AO VOIP

São sistemas desenvolvidos com a finalidade de prevenir acessos não autorizados a sistemas VoIP, podendo ser aplicado tanto em software quanto em hardware, ou em conjunto com ambos (UNDERSTANDING, 1998).

4.8 VLA (VIRTUAL LOCAL AREA /ETWORK)

Manter a voz e dados separados em VLANs é uma boa alternativa para aumentar o desempenho e a segurança no ambiente. A melhor maneira para garantir a segurança de voz entre VLANs, é utilizando filtros e Firewalls, com isso podemos impedir ataques do tipo DoS e Spoofing (VOIP-INFO.ORG, ...).

5 CONCLUSÃO

Na implantação de um sistema de voz sobre IP, devem ser criteriosamente analisados todos os fatores que efetivamente impactam na disponibilidade e a qualidade do serviço, além das ameaças à segurança da rede e da comunicação.

Apesar do grande número de ataques que podem afetar a disponibilidade, integridade e confidencialidade do serviço VoIP, quase sempre causando prejuízos aos usuários e corporações, a quantidade de ataques ainda é pequena. No entanto, com a popularização deste serviço, e a ampliação do seu uso no mercado corporativo, este número tende a aumentar, assim como ocorreu com o serviço de telefonia celular e correio eletrônico, e a segurança deve sempre permear as discussões relativas à implementação de serviços de voz sobre IP.

A utilização do protocolo SIP para a implementação de telefonia VoIP é, sob muitos aspectos, vantajosa, já que alia o baixo consumo de banda da rede com a simplicidade do endereçamento por URLs. O estabelecimento e o encerramento das sessões multimídia, também é simples e efetuada por pacotes UDP. Estas características fazem das redes SIP as preferidas atualmente para a implantação de telefonia sobre IP em redes convergentes.

Esta simplicidade, no entanto, exige um maior cuidado com a segurança da rede, principalmente porque o desempenho é crítico quando se trata do tráfego de voz.

A segmentação da rede em Vlan's (Virtual LAN's ou Redes Virtuais), separando tráfego de dados e tráfego de voz, além de criptografia e autenticação confiável, são a base da implementação de segurança em uma rede VoIP. Outras ferramentas, no entanto, podem ser utilizadas, desde que não diminuam substancialmente o desempenho da rede.

Como é concluído, "projetar, implementar, e operar VoIP de forma segura é um esforço complexo que exige uma preparação cuidadosa". Por esse motivo sugere-se que a análise das vulnerabilidades do serviço e a mensuração do custo-benefício das diferentes opções disponíveis antecede todas as ações de implementação e melhoria de segurança planejadas para um serviço de voz sobre IP.

Desta forma, conclui-se que a segurança sobre sistemas VoIP será cada vez mais requisitada conforme o seu crescimento e expansão e o protocolo SIP atualmente é um dos mais aptos para atingir todas estas expectativas, sejam elas corporativas, domésticas ou em qualquer outra área onde aplicações VoIP estiverem rodando.

REFERÊNCIAS

ABNF Grammar for SDP - Session Description Protocol. 2007. Disponível em: <http://www.tech-invite.com/Ti-sdp-abnf.html>

ASTERISK VOIP NEWS. VoIP Security: Scenarios, challenges, and counter measures. Disponível em: http://www.asteriskvoipnews.com/voip_security/voip_security_scenarios_challenges_and_counter_measures.html.

AUDIO CODES. AudioCodes' CPE Basic Technical Training. Version 5. 2007

INFO EXAME n. 228, março 2005. Disponível em: <http://info.abril.com.br/edicoes/228/index.shl>.

CONTENT VERIFICATION. Man In The Middle Attack. Disponível em: <http://www.contentverification.com/man-in-the-middle/index.html>.

CONVERGÊNCIA VOIP.SIP. Disponível em: <http://www.convergenciavoip.com.br/tag/sip/>.

DATA CONECTION. Session Border Controller Software Disponível em: <http://www.dataconnection.com/sbc/default.htm>.

DRABIK, John. The Seven Faces of the OSI Network Model: Part 1. CommsDesigner, 2003. Disponível em: http://www.commsdesign.com/design_corner/OEG20030415S0027

GUARDIAN. Why VoIP is the next target for spammers. Disponível em: <http://www.guardian.co.uk/technology/2007/nov/01/news.hacking>.

HANDLEY, M. RFC 2327 - SDP: Session Description Protocol. IETF. 1998. Disponível em: <http://www.ietf.org/rfc/rfc2327.txt>

IETF. RFC 2543. Disponível em: <http://www.ietf.org/rfc/rfc2543.txt> .

IETF. RFC 3261. Disponível em: <http://www.ietf.org/rfc/rfc3261.txt>.

JESZENSKY, PAUL JEAN ETIENNE. Sistemas Telefônicos. São Paulo, Manole, 2004.

JOHNSTON, Alan B. Understanding the Session Initiation Protocol. Norwood, MA. Artech House. 2004

NATIONAL INSTITUTES of Standards and Technology. Disponível em: <http://www.nist.gov/>.

NEWPORT NETWORKS. White Paper - IPsec in VoIP Networks. Disponível em: <http://www.newport-networks.com/whitepapers/IPsec-1.html>.

PORTER, Thomas. Practical VoIP Security, Andrew Williams Page Layout and Art, Canadá, publicado em 2006, ISBN: 1597490601.

SECURITY FOCUS. New Caller I.D. Spoofing Site Opens. Disponível em: <http://www.securityfocus.com/news/9822>.

SECURITY FOCUS. Two attacks against VoIP. Disponível em: <http://www.securityfocus.com/infocus/1862>.

SECURITY PRO NEWS. ,EC To Seal Out VoIP Spits. Disponível em: <http://www.securitypronews.com/insiderreports/insider/spn-49-20070129NECTSealOutVoIPSpit.html>.

SIPCENTER. What is SIP introduction. Disponível em: <http://www.sipcenter.com/sip.nsf/html/What+Is+SIP+Introduction>.

SISNEMA INFORMÁTICA. Voz sobre IP o que mudou? Disponível em: <http://sisnema.com.br/Materias/idmat018623.htm> Acesso em 01/2008.

TECH-FAQ. O que é IKE? Disponível em: <http://www.tech-faq.com/lang/pt/ike.shtml>.

TELECON. Segurança VoIP: Soluções. Disponível em: http://www.teleco.com.br/tutoriais/tutorialsegvoip/pagina_4.asp.

UNDERSTANDING the OSI Reference Model. MSI Communications. 1998.<http://www.psotec.net/osi.html>

VOIP NEWS, VoIP Spam Is Called SPIT. Disponível em:
<http://www.voipnews.com/feature/voip-spam-spit-030408/>.

VOIP REVIEW. History of VoIP. 2004. Disponível em:
<http://www.voipreview.org/news.details.aspx?nid=51>

VOIP UFSC, Uso de Voz sobre IP na Universidade. Disponível em:
http://voip.npd.ufsc.br/docs/artigo_voip.pdf.

VOIP-INFO.ORG. Virtual LAN, for VoIP networks. Disponível em:
<http://www.voipinfo.org/wiki/view/VLAN>.

WALLINGFORD, Theodore. Switching to VoIP. Sebastopol, CA. O'Reilly Media. 2005.