SEGURANÇA EM AMBIENTES VOIP: RISCOS E VULNERABILIDADES

Eder Leandro Cabral

Especialização de Redes e Segurança de Sistemas

Pontifícia Universidade Católica do Paraná

Porto União, novembro de 2010

Resumo

A tecnologia de Voz sobre IP (VoIP) vem crescendo muito nos últimos anos, entretanto, um dos principais problemas enfrentados por esse ambiente refere-se às questões de segurança. Sendo assim é fundamental encontrar mecanismos que auxiliem na segurança, oferecendo proteção, visando garantia e qualidade do serviço, pois o voip possui diversas vulnerabilidades e existe o desafio de garantir a qualidade e segurança das ligações iguais ou superiores as chamadas proporcionadas pelo sistema de telefonia convencional. Este trabalho tem como objetivo fazer uma apresentação da tecnologia voip, de uma forma geral explicar como a ela funciona, apresentar as questões de segurança como riscos, vulnerabilidades, formas de ataque e mecanismos que devem ser adotadas para melhorar a segurança desta tecnologia.

1. Definição Sobre Voip (Voice Over IP)

Nos dias atuais a internet não nos possibilita apenas a transmissão de dados, agora também é possível fazer chamadas telefônicas através da Internet, utilizando Voip, que abre novas possibilidades para chamadas com custos razoáveis trazendo benefícios significativos para os consumidores e se torna cada vez mais acessível [3].

O VoIP começou a ser desenvolvido no começo da década de 90, mas só de alguns anos pra cá começou a ganhar força. Primeiramente as empresas foram às beneficiadas implantando sistemas de VoIP para interligarem filiais. Atualmente, além das empresas qualquer usuário que possua Internet pode usufruir deste serviço.

Esta tecnologia permite estabelecer conversas telefônicas em uma rede IP, similar ao provido pelo serviço telefônico fixo comutado, onde transforma a voz no modo convencional em pacotes IP para ser transmitida pela rede de dados.

No inicio das implementações do VoIP as reclamações eram constantes com relação à qualidade da comunicação, mas com o passar do tempo tanto a qualidade quanto o desempenho do serviço foram melhorados, ficando difícil achar distinção entre o VoIP e o serviço tradicional de telefonia comutada [4]. Isso se deve a alta disponibilidade da banda larga que é a maior responsável pelo aumento no consumo do VoIP, pois as operadoras cada vez mais estão disponibilizando banda e por preços bem acessíveis.Desta forma os recursos do voip funcionam perfeitamente com qualidade, pois é uma aplicação critica, onde a perda de pacotes e atrasos não são tolerados.

2. Funcionamento do Voip

A tecnologia VoIP transforma os sinais de voz analógicos em pacotes de dados para transmissão na internet, sendo estes compactados antes de serem transmitidos. No destino os pacotes são convertidos novamente dessa vez em sinais de som analógicos e enviados ao receptor [5].

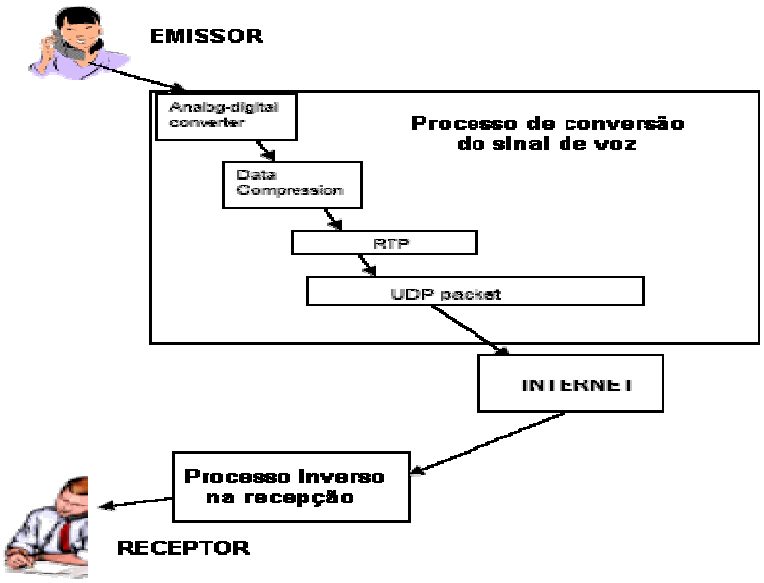

Figura 1: Processo de conversão do sinal de voz [13].

O voip possibilita a comunicação de voz entre os telefones tradicionais da rede de telefonia pública e os computadores, equipamentos que se encontrem conectados em uma rede IP e que disponibilizem este recurso.

> "Voz sobre IP (VoIP) é um conjunto de tecnologias que usam a internet ou redes IP privadas para a comunicação de voz, substituindo ou complementando os sistemas de telefonia convencionais "[4]

Para o bom funcionamento do voip, ele necessita de uma conexão com a internet de boa qualidade, sendo que determinadas conexões de banda larga possuem uma péssima qualidade na transmissão. Em conseqüência destas conexões deficientes, quando pacotes são perdidos ou atrasados em algum ponto da rede, existe uma queda momentânea da voz na conversação. Isso acontece com freqüência em redes bastante congestionadas ou onde existem grandes distâncias entre os pontos de conexão.

Como hoje o acesso à internet é cada vez mais difundido, principalmente em empresas, o voip não encontra muitas dificuldades no seu funcionamento, no que tange a qualidade do sinal.

Segue abaixo descrição dos modos de funcionamento do voip [14]:

- Computador a computador: Neste modo é quando você faz uma ligação do seu computador para outro computador, utilizando programas como Skype. Tudo que você fala no microfone é transformado em pacotes e transmitidos através da Internet.

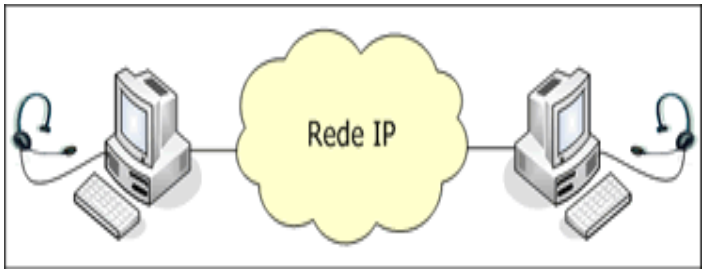

Figura 2: Ligação voip de computador para computador [14].

- Computador para rede de telefonia convencional: O segundo modo é quando você faz uma ligação para um telefone ou celular convencional. Da mesma forma tudo o que se fala é transformado em pacotes, e estes trafegam através da Internet até chegarem aos telefones e serem transformadas em sinais analógicos.

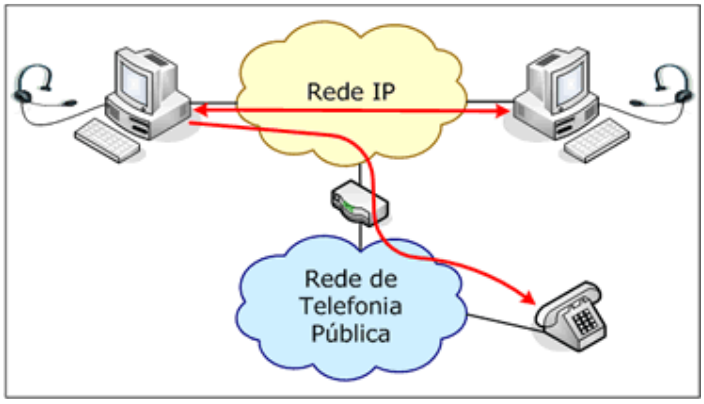

Figura 3: Ligação voip de computador para telefonia publica [14].

- Recebimento de ligações vindas da rede publica: O terceiro modo apresenta outra funcionalidade alem de fazer ligações, permitindo também o recebimento de ligações pela linha voip.

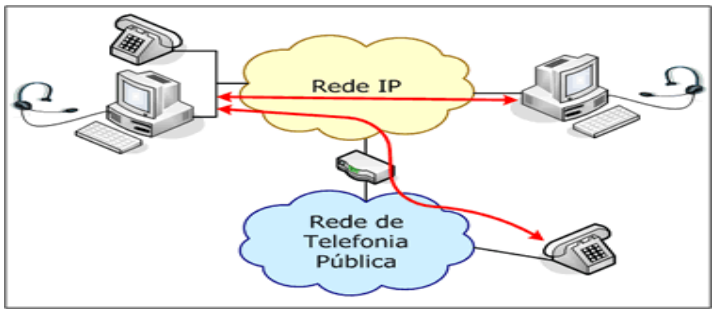

Figura 4: Recebimento de ligações vindas da rede publica [14].

3. Equipamentos VOIP

Os equipamentos voip permitem que o sinal da telefonia convencional seja transformado em pacotes para trafegar em redes IP e vice-versa. Os mais populares que podem ser utilizados com VoIP são os telefones IP, gateways digitais e adaptadores ATA. Abaixo segue descrição de cada equipamento:

- ATA (Adaptador para telefone analógico): Equipamento que permite que os telefones convencionais possam se conectar a uma rede IP, fazendo a conversão do sinal. Uma extremidade e conectado no serviço de banda larga e o outro ao telefone convencional ou centrais PABX:

Figura 5: Adaptador ATA [15]

- Telefone IP: São aparelhos semelhantes ao telefones convencionais, porem com funcionalidades para converter os sinais analógicos em pacotes IP, para transmissão na internet. Possui uma porta RJ45, onde permite a sua conexão diretamente a uma rede TCP/IP.

Figura 6: Telefone IP [15]

- Gateway Digital: Equipamento semelhante ao adaptador ATA citado acima, porem com funcionalidades de PABX, que permite conectar vários telefones convencionais a rede IP. A maioria destes equipamentos possui oito portas de saída para telefones convencionais.

Figura 7: Gateway Digital [15]

4. Protocolos

4.1 Protocolo de Sinalização

Os protocolos de sinalização são os responsáveis pelo controle de ligações entre elementos de uma rede, fazendo a negociação entre duas máquinas ou equipamentos que desejam estabelecer uma comunicação. Estes protocolos são responsáveis pela procura da máquina ou equipamento desejado, assim como pelo controle de fluxo e negociação de quais codificadores serão utilizados.

> Um protocolo de sinalização para VoIP deve especificar a codificação da voz, a configuração das chamadas, o transporte de dados, o modo de autenticação, segurança, métodos utilizados na comunicação, cabeçalho, endereçamento, sintaxe da mensagem [16].

Estes protocolos são essenciais para que os elementos da uma rede possam trocar informações de controle e gerenciamento do serviço, estabelecendo e desconectando chamadas, transportando informações necessárias para localizar usuários e negociar funcionalidades.

4.1.1 Protocolo H.323

O H323 é um conjunto de padrões da ITU-T que define um conjunto de protocolos para o fornecimento de comunicação de áudio e vídeo em uma rede, estabelecendo procedimentos para comunicação de áudio ponto a ponto em tempo real em uma rede comutada por pacotes que não provê garantia de QoS. Além disso, estabelece padrões para codificação e decodificação de fluxos de dados de áudio e vídeo, garantindo que produtos baseados no padrão H.323 de um fabricante sejam compatíveis com produtos H.323 de outros fabricantes [8].

> O padrão H.323 é um conjunto de protocolos verticalizados para sinalização e controle da comunicação entre terminais que suportam aplicações de áudio (Voz), vídeo ou comunicação de dados multimídia. É uma recomendação guarda-chuva do ITU-T que define padrões para comunicação multimídia através de redes que não oferecem Qualidade de Serviço (QoS) garantida [10].

H.323 é considerado um padrão amplamente utilizado em sistemas de videoconferência e sistemas de comunicação multimídia de maneira geral. Hoje a maioria das redes utilizadas possui uma infra-estrutura com protocolo de transporte baseado em pacotes, desta forma a adoção do padrão H.323 permite que sejam utilizadas aplicações multimídia sem requerer mudanças na estrutura de redes .

4.1.2 Protocolo SIP (Session Initiation Protocol)

SIP é um protocolo de sinalização de voip usado para estabelecer, modificar e finalizar chamadas telefônicas, negociando os termos e as condições de uma seção, alem de auxiliar na localização dos participantes da mesma[7].

> O SIP é um protocolo de sinalização para estabelecer chamadas e conferências através de redes via Protocolo IP. O estabelecimento, mudança ou término da sessão é independente do tipo de mídia ou aplicação que será usada na chamada; uma chamada pode utilizar diferentes tipos de dados, incluindo áudio e vídeo[17]

O SIP estabelece chamadas e conferências especificando os componentes da arquitetura de sinalização como clientes e servidores, sendo os quatro principais componentes dessa arquitetura o SIP User Agent, SIP Proxy Server, SIP Redirect Server e SIP Register Server [7]:

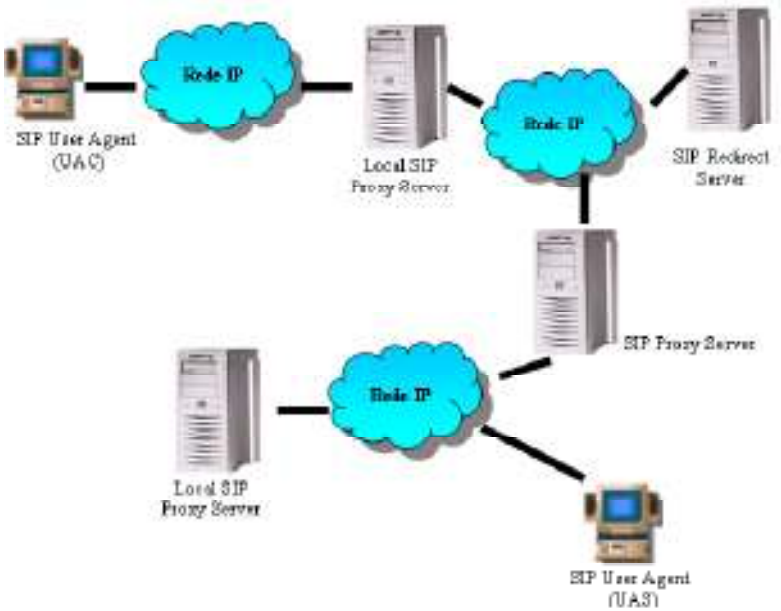

Figura 8: Arquitetura do protocolo SIP [7].

- Agente Usuário (User Agent): O User Agent é o terminal SIP ou o software de estação final, formado por uma parte cliente (User agent client), capaz de iniciar requisições SIP, e por uma parte servidor (User agent server), capaz de receber e responder as requisições.

- Servidor Proxy (Proxy server): Componente que age tanto como um servidor quanto um cliente, possibilitando fazer requisições em benefícios de outros que não podem fazer as requisições diretamente, sendo que o cliente envia as requisições e o servidor retorna a resposta para o cliente.

- Servidor de Redirecionamento (Redirect Server): Componente que redireciona chamadas, tratando adequadamente parâmetros como endereços, não aceitando e nem iniciando chamadas.O servidor de redirecionamento recebe a chamada de um agente usuário e retorna uma localização alternativa para o agente usuário contatar.

- Servidor de registro (Register Server): Componente utilizado para armazenar informações das requisições SIP do tipo REGISTER, mantendo atualizadas estas informações, trabalhando em conjunto com o servidor de redirecionamento e o servidor Proxy sobre a localização dos usuários.

Normalmente, os servidores de redirecionamento orientam os servidores proxy com respeito ao próximo passo na rota para o receptor da mensagem SIP. Essa operação é feita com base em um plano de identificação para determinar onde a mensagem SIP deve ser enviada.

4.2 Protocolo de Transporte

4.2.1 RTP (Real Time Transport Protocol)

O protocolo RTP foi projetado para transportar dados em aplicações de tempo real como áudio e vídeo, fazendo controle de atraso, variação do atraso e seqüência do fluxo, com intuito de garantir que a voz seja decodificada corretamente.

O protocolo RTP tenta fazer com que os pacotes sejam recebidos conforme a ordem de envio, aplicando números de seqüência de pacotes IP para reconstituir as informações de voz ou de vídeo, provendo o transporte fim-a-fim das informações multimídia, fazendo uma interface entre a camada de aplicação e de transporte [5]. Este protocolo não reserva recursos nem garante qualidade de serviço (QoS), porém é freqüentemente utilizado em paralelo com o RTCP (RTP Control Protocol) permitindo que tenha certa monitoração da comunicação.

4.2.2 RTCP (*RTP* Control Protocol)

O RTCP é um protocolo de controle, sendo complementar para RTP e gerencia informações sobre perdas de pacote e latência na rede, contribuindo para que a distribuição dos dados ocorra de uma maneira escalável ao ponto de permitir grandes transmissões e também provendo certo controle e identificação dos participantes da comunicação [10].

O RTCP realiza basicamente quatro funções [18]:

- Prover informações quanto à qualidade da distribuição de dados;
- Manter um identificador em nível de transporte (CNAME);
- A taxa em que os pacotes são enviados pode ser calculada a partir do número de participantes;
- Manter informações sobre o controle de sessão;

O RTP não garante a qualidade para serviços em tempo real, não fornecendo sozinho nenhum mecanismo para assegurar a entrega ou a ordenação dos pacotes. Mas permite que sejam adicionados mecanismos de segurança, quando necessários, bem como controle de fluxo e congestionamento

5. Segurança em Voip

Conforme citado anteriormente neste artigo, o voip vem crescendo a cada dia, proporcionando grandes vantagens a seus utilizadores, não substituindo a telefonia convencional, mas cada vez mais obtendo espaço no mercado. Na proporção que o voip cresce, junto com ele vem às ameaças a esta tecnologia, que como qualquer outra está suscetível a riscos e vulnerabilidades.

O voip já possui riscos e vulnerabilidades inerentes a rede IP, na qual os riscos são imensos, aliados com riscos e vulnerabilidades específicos. Como o voip roda sobre a rede IP, não deve ser considerado como uma aplicação qualquer deste ambiente, pois voip necessita de uma atenção especial, sendo um serviço complexo que funciona em tempo real. Sendo assim, a sua estabilidade é um ponto fundamental para que não haja comprometimento na qualidade do serviço [11].

Como o voip necessita de alta disponibilidade, os ambientes que envolvem o voip devem sempre estar bem protegidos com mecanismos que auxiliem na identificação e combate as ameaças que possam vir a causar danos ao serviço. Assim que identificado qualquer tipo de ameaça, esta deve ser contida por estes mecanismos de defesas da rede e a vulnerabilidade que estavam dando condições para o ataque deve ser eliminada, para assim impedir novos ataques [11].

> "Os mesmos tipos de ataques que afetam as redes de dados podem afetar as redes de VoIP.Conseqüentemente, o conteúdo de comunicações por VoIP fica vulnerável a ataques, hackers, alterações, interceptações ou redirecionamentos" [6].

A segurança é muito importante ao implementar VoIP, porque cada elemento da infra-estrutura está acessível na rede, bem como qualquer computador, e pode ser atacado ou utilizado como ponto de lançamento de ataques a toda a rede. Se um atacante tiver êxito no seu ataque, pode passar a ter a acesso a servidores voip, provocar instabilidade do serviço, roubo de identidade, escutas telefônicas, redirecionamento de chamadas e seqüestro de sessão.

5.1 Ataques Sobre a Tecnologia Voip

Abaixo segue a descrição de alguns tipos de ataques que podem ser aplicados sobre voip:

5.1.1 Invited flood

O invite flood é um ataque que tem como objetivo o envio de várias mensagens ao servidor SIP, para iniciar conexões, fazendo algumas modificações. Este tipo de ataque ocorre quando um atacante consegue enviar várias solicitações para um gateway VOIP ou para o administrador de chamadas do sistema, desta forma há um acumulo de solicitações, fazendo com que o sistema não consiga mais atender novas requisições, devido à ausência de recursos disponíveis [2].

5.1.2 Registration Hijack (Seqüestro de registro)

Neste tipo de ataque o atacante substitui o registro de um usuário legitimo de uma seção, faz a alteração do mesmo por um falso e se passa como usuário verdadeiro, assim

o atacante faz com que todas as chamadas entrantes sejam enviadas para o usuário falso [2].

5.1.3 Call Eavesdropping (Escuta telefônica)

Call Eavesdropping é o tipo de ataque onde uma pessoa não autorizada possui acesso ao meio de comunicação e consegue escutar ou interpretar o trafego que passa pela rede. Através desta escuta o individuo consegue obter nomes de usuários, senhas e números de telefones, assim controlar o plano de chamadas. Também podendo ter acesso a informações sigilosas e fazer proveito destas informações futuramente. Neste tipo de ataque os dados não são alterados, mas a confidencialidade das informações fica comprometida [2]

5.1.4 SPIT (SPAM over internet Telephony)

SPIT é uma ameaça à segurança com o potencial para preencher caixas de correio de voz com mensagens indesejadas da mesma maneira que o spam enche as caixas de entrada de e-mail, onde se recebe mensagens não solicitadas com ofertas de produtos e serviços [2].

5.1.5 IP Spoofing

IP spoofing é uma técnica que consiste em mascarar pacotes IP utilizando endereços de remetentes falsificados. Esta técnica permite assim a um atacante enviar pacotes sem que seja identificado. Não se trata de uma mudança de endereço IP, mas de um disfarce do endereço IP em nível dos pacotes emitidos, fazendo assim crer que o pacote veio de outro endereço, desta forma pode ser usado por atacantes para quebrar medidas de segurança.

5.1.6 Toll Fraud (Chamadas Sem Tarifação)

Toll Fraud, neste tipo de ameaça, novas configurações são exploradas com a intenção de fazer chamadas gratuitas, que não sejam tarifadas, ou que sejam tarifadas para um terceiro. Esse tipo de ataque é um dos mais críticos,pois caso o ataque demore a ser descoberto pode causar prejuízos financeiros enormes pelas ligações não autorizadas.

5.1.7 Session Tear down

Ataque de negação de serviço onde o atacante observa a sinalização de uma chamada, com o intuito de enviar falsas mensagens para terminar ou impedir uma chamada.

5.2 Causas de Problemas de Segurança em Voip

- Implementações básicas sem segurança mínima.
- Equipamentos mal gerenciados.
- Arquitetura de rede VoIP mal projetada.
- Falha em procedimentos operacionais.
- Inexistência de uma política de segurança.

- Falta de suporte técnico adequado.
- Excesso de confiança nos fabricantes.

6. Mecanismos de Segurança em Voip

O fator essencial para segurança é entender os riscos envolvidos a tecnologia para que os controles adequados e as melhores decisões sobre o seu tratamento possam ser tomadas, tudo isso com intuito de obter maior conhecimento sobre estes problemas de segurança existentes, podendo assim implementar serviços de modo que a sua disponibilidade não seja comprometida, juntamente com a garantia da confidencialidade e integridade das informações

As alternativas para melhorar a resistência de uma infra-estrutura VoIP frente aos diferentes ataques que o serviço pode estar exposto são diversas, mas todas elas tem custos ou impactos que devem ser cuidadosamente analisados antes de optar por uma ou outra alternativa. É importante ressaltar que, a princípio, não há uma receita de bolo para qual o conjunto capaz de prover o melhor custo-benefício [12].

Na verdade, não existe uma solução simples que possa garantir a absoluta segurança de VoIP, mas ainda assim de alguma forma a minimizar os riscos e melhorando a estratégia de segurança.

Abaixo algumas orientações que podem ajudar na segurança da tecnologia VOIP [6] [9]:

- Separar VoIP e dados**:** Separar o trafego de dados e voip é uma alternativa para melhorar a segurança, pois a partir da separação de dados e voip, pode-se utilizar ferramentas especificas para cada serviço.Algumas ferramentas utilizadas para segurança de dados não conseguem proteger totalmente voip, sendo necessário adotar ferramentas especificas para proteção deste serviço.

- Vigilância**:** Os envolvidos na segurança devem ficar atentos para que mantenham a estrutura voip sempre bem atualizada, principalmente com relação aos softwares utilizados.

- Novas ameaças: Ficar atento a novas ameaças que podem surgir no mundo voip, para que a partir delas novos mecanismos devem ser adotados para sua proteção.

- Bloquear o uso suspeito de VoIP**:** Utilizar equipamentos e softwares que sejam confiáveis, não comprometendo a rede de dados e voip.Determinados equipamentos e softwares não provem segurança mínima para seu funcionamento, fazendo com que a segurança do voip fique comprometida.

- Segurança da rede**:** Utilizar ferramentas adequadas para monitorar a rede, identificando qualquer atividade suspeita que possa vir a comprometer a segurança. Se a segurança da rede for comprometida, o voip também fica vulnerável as estas ameaças.

- Autenticação de operações remotas: Terminais de VoIP podem ser atualizados e gerenciados remotamente. É essencial que somente pessoal autorizado em localizações autorizadas, com base nos endereços de IP e nomes de usuário únicos tenham acesso a estes terminais.

- Firewall especializado para VOIP: O uso de um firewall especializado permite o controle do acesso ao segmento de rede onde está instalado o "Call Manager", fazendo o filtro de todo o tipo de tráfego que seja enviado à rede de voz e não seja necessário para o funcionamento destes serviços.

- Endereços IP privativos e inválidos: Os equipamentos voip da rede devem ser configurados com IPs inválidos. Isso dificultará as ações dos atacantes em monitorar o trafego de voz de fora da rede interna, evitando também o mapeamento de qualquer vulnerabilidade existente na rede voip.

- Configurar os equipamentos voip com endereços IP estáticos, associados ao MAC Address: O controle de acesso através de MAC Address vinculados a um IP é uma forma de garantir que somente os MAC autorizados a operar na rede tenham a permissão para tal.Este controle de acesso fará com que o equipamento voip antes de receber as configurações passe por uma autenticação e só recebera as configurações se seu Mac estiver na lista de controle de acesso.

- Utilizar servidores DHCP separados para voz e dados: Configurar servidores DHCP separados para voz e dados, ou seja, utilizar um servidor DHCP para os segmentos de voz e outro para os segmentos de dados. Esta medida garante que se um atacante disparar qualquer tipo de ataque contra um servidor que fornece configurações a uma rede de dados não interfira também no funcionamento da rede voip e da mesma forma para servidores DHCP para voip, onde não interfiram na rede de dados.

- Monitorar os endereços MAC no segmento de voz: Utilizar ferramentas para monitoramento dos MAC Addresses dos dispositivos utilizados na rede voip.Estas ferramentas permitem o controle de qualquer alteração feita na associação entre endereço IP e endereço MAC, reforçando a segurança da rede voip.

- Monitorar o desempenho e status dos serviços de VoIP: Adotar controles de monitoramento da rede voz, para que sejam identificadas instabilidades, atrasos e latências, que venham prejudicar a qualidade e disponibilidade do serviço de voz.

- Auditar o uso dos recursos: O controle sobre os equipamentos voip é um fator muito importante, pois través deles é possível identificar o nível da qualidade de serviços destes equipamentos e sua utilização. Este controle é possível através do registro de informações sobre as sessões, como data e horário do início e término, duração, origem, destino. Com estas informações os administradores conseguem fazer uma análise do desempenho destes equipamentos.

- Criptografar o tráfego de VoIP: A criptografia do trafego de voz na rede e uma ótima forma de garantir que indivíduos não autorizados violem a confidencialidade das conversações.

7. Vantagens da Tecnologia VOIP

- Economia na conta telefônica: O grande fator motivacional para utilização do voip é a redução de custo nas ligações, sendo possível reduzir drasticamente a sua conta telefônica, pois o custo das ligações voip é muito inferior ao custo das ligações pela telefonia convencional;

- Custo Zero: Determinadas ligações podem sair sem custo para clientes que usam o mesmo provedor do serviço ou para pessoas que utilizam os programas de computadores para fazer suas ligações, como por exemplo, o skype;

- Utilização de uma única infra-estrutura para prover serviços de link de dados e telefonia;

- Eficiência em comunicação com custo acessível;

- Integração com o PABX da empresa: Através de um adaptador você pode conectar a rede voip ao PABX, possibilitando seu uso em telefones convencionais;

- Fácil Implantação dos equipamentos VoIP;

8. Desvantagens

Assim como em todas as tecnologias, o voip também possui as suas fragilidades:

- Dependência da Internet**:** O voip necessita da existência de uma conexão de internet. Caso ela esteja com problemas, passando por manutenção ou até mesmo indisponível, não há a possibilidade comunicação. Esta dependência é um dos principais motivos para que o VoIP não substitua a telefonia convencional, pois nenhuma empresa vai mudar todo seu sistema de telefonia completamente para ficar na dependência de um link que não tem a disponibilidade e confiabilidade que a rede de telefonia convencional tem.

- Qualidade das Chamadas**:** As ligaçõesVoIP possuem um qualidade muito boa, mas essa qualidade depende da banda de internet contratada. Quando não temos um link bom o suficiente, ouvimos o eco da nossa voz, as ligações ficam cortadas e temos uma queda considerável na qualidade das ligações.

- Identificação das Chamadas: Como as ligações VoIP não tem origem de um telefone convencional, elas não podem ser identificadas por um número telefônico.Um questão que exemplifica está ausência de numero de identificação é impossibilidade de autoridades identificarem um infrator que planeja e comete crimes usando voip.

- Quando falta luz o voip não funciona

- A maioria dos sistemas VoIP não faz chamada para bombeiro, polícia e números 0800.

9 Conclusão

Voip pode ser considerado um exemplo de como a internet está mudando as comunicações, onde diversos meios são utilizados para troca de informações. Voip é uma tecnologia que permite ligações semelhantes ao sistema de telefonia convencional, possibilitando reduzir os custos das ligações. Uma realidade é que o voip está ocupando seu espaço no mercado, onde cada vez mais as empresas estão adotando este serviço para comunicação ou até mesmo usuários domésticos que queiram usufruir dos benefícios que ela oferece.

A grande maioria das empresas que implantam a tecnologia de Voz sobre IP alcançam a principal vantagem dessa tecnologia que é a redução com o custo de telefonia e outras às vezes por não usufruir de um setor de TI na empresa, acabam não se interessando, deixando de usufruir dos benefícios que ela proporciona.

Hoje não existem tecnologias totalmente seguras, sendo o voip incluído nesta lista, pois também possui riscos e vulnerabilidades que podem comprometer a segurança e a estabilidade do serviço. Caso voip seja implementado sem uma atenção especial com as questões de segurança, estes riscos e vulnerabilidades podem se tornar cada vez maiores.

O Intuito deste trabalho foi apresentar informações sobre voip, tanto do seu funcionamento, vantagens, desvantagens e em especial dar um enfoque sobre a segurança desta tecnologia, apresentando as formas de ataques que são utilizadas para prejudicar o seu funcionamento e também mecanismos e boas práticas que devem sem adotados para melhorar a segurança, impedindo estes ataques. Visto que não há como garantir a segurança na sua totalidade, mas sim reduzir as possibilidades de que pessoas coloquem em riscos a rede voip.

A segurança das informações é hoje uma das grandes preocupações de uma empresa, independente de seu ramo de atuação e de seu porte.

Bibliografia

[1] SOUZA, WENDLEY. BRASIL ESCOLA. Voip. Disponível em: http://www.brasilescola.com/informatica/voip.htm. Acesso em: 3 de Out. 2010.

[2] SOUTO, ANDRÉ RIBEIRO. UFRGS. A Importância da Segurança Aplicada à Tecnologia Voip. Disponível em: http://www.lume.ufrgs.br/bitstream/handle/10183/15990/000695229.pdf?sequence=1. Acesso em: 3 de Out. 2010.

[3] CUNHA, JEAN CARLOS. WORDPRESS. O que é Telefonia IP. Disponível em: http://jeancarloscunha.wordpress.com/2008/11/15/o-que-e-telefonia-ip/. Acesso em: 3 de Out. 2010.

[4] RAMIRES, ANDERSON. MALIMA. Voip- Mais uma Moda ou Revolução na Comunicação. Disponível em: http://www.malima.com.br/article_read.asp?id=239. Acesso em: 5 de Out. 2010.

[5] ALECRIM, EMERSON. INFOWESTER. Tecnologia Voip. Disponível em: http://www.infowester.com/voip.php. Acesso em: 5 de Out. 2010.

[6] SYMANTEC CORPORATION. SYMANTEC. Voip é o Recurso Certo para Sua Empresa? Disponível em: http://www.symantec.com/pt/br/business/library/article.jsp?aid=voip_for_your_business. Acesso em: 5 de Out. 2010.

[7] REGISTRO. Introdução ao Protocolo SIP. Disponível em: http://eng.registro.br/inoc/SIP_iNOC.pdf. Acesso em: 5 de Out. 2010.

[8] CARDOSO, RÔMULO MENDES. UFRJ. Voz sobre IP (Voip). Disponível em: http://www.gta.ufrj.br/grad/04_2/VoIP/CaptuloVIIProtocolodeSinalizaoH323.html. Acesso em: 5 de Out. 2010.

[9] VOLTAN JUNIOR, GUILHERME. PORTALGEOBRASIL. Voz Sobre IP Segurança de Transmissões. Disponível em: http://www.portalgeobrasil.org/info/material/voip.pdf. Acesso em: 9 de Out. 2010.

[10] BERNAL FILHO, HUNBER. TELECO. Telefonia IP. Disponível em: http://www.teleco.com.br/tutoriais/tutorialtelip/pagina_3.asp. Acesso em: 9 de Out. 2010.

[11] PAGANUCHI, ALESSANDRO. IPNEWS. Segurança em Voip. Disponível em: http://www.ipnews.com.br/voip/fique-por-dentro/artigos/seguranca-em-voip.html. Acesso em: 19 de Out. 2010.

[12] OLCHIK, ALEJANDRO. TELECO. Segurança em Voz Sobre IP. Disponível em: http://www.teleco.com.br/tutoriais/tutorialsegvoip/pagina_5.asp. Acesso em: 19 de Out. 2010.

[13] PINHEIRO, JOSE MAURICIO SANTOS. MALIMA. Aspectos de Segurança em Voz Sobre IP. Disponível em: http://www.malima.com.br/article_read.asp?id=379. Acesso em: 26 de Out. 2010.

[14] TENTEC. O que é Voip. Disponível em: http://www.tentec.com.br/voip.php. Acesso em: 26 de Out. 2010.

[15] INPHONEX. Equipamentos Voip. Disponível em: http://www.inphonex.com.br/equipamentos/equipamentos-voip.php. Acesso em: 12 de Nov. 2010.

[16] VAZ, IGOR; DINAU, PRISCILLA. UFRJ. Sip. Disponível em: http://www.gta.ufrj.br/grad/06_1/sip/Definindooqueumprotocolodesinalizao.html. Acesso em: 14 de Nov. 2010.

[17] CASTRO, RENATO GOMES. UCB. Disponível em: http://www.ucb.br/prg/professores/maurot/RA/RA_arqs/conteudo_web/SIP/SIP.htm. Acesso em: 14 de Nov. 2010.

[18] ALMEIDA, MARCIO NOGUEIRA DE. UNB. Video-Aula em Ambientes de Educação a Distância. Disponível em: http://monografias.cic.unb.br/dspace/bitstream/123456789/92/1/monografia%20marciocarlos.pdf .Acesso em: 14 de Nov. 2010.