Alan Diego Martins
Amir Hamad
Bruno Jesus
Carlos Henrique C. Costa
Ivo Roberto de Mello Junior

Segurança aplicada à VoIP sobre o protocolo SIP: Estudo das vulnerabilidades e suas soluções.

Monografia apresentada a FIAP, para obtenção do título de Tecnólogo em Redes de Computadores

São Paulo
2006

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

ATA	Analog Telephony Adapter
VoIP	Voice over Internet Protocol
SIP	Session Initiation Protocol
IP	Internet Protocol
ROI	Return of Investment
PSTN	Public Switched Telephony Network
CODEC	Compression / Decompression
ITU-T	International Telecommunication Union - Telecommunication
UDP	User Datagram Protocol
TCP	Transmission Control Protocol
IETF	Internet Engineering Task Force
RTP	Realtime Transport Protocol
RTCP	Realtime Control Transport Protocol
TFTP	Trivial File Transfer Protocol
DHCP	Dynamic Host Configuration Protcol
DNS	Domain Name System
VPN	Virtual Private Networks
HTTP	Hyper Text Transfer Protocol
ARP	Address Resolution Protocol
PBX	Private Branch eXchange
SPIT	Spam over Internet Telephony
LAN	Local Area Network
VLAN	Virtual Local Area Network
SRTP	Secure Real-time Transport Protocol
SRTCP	Secure Real-time Transport Control Protocol
IPsec	Internet Protocol Security
IDS	Intrusion Detection System

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, 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 público atual. Este artigo trata da aplicabilidade da segurança da informação ao sistema de Voz sobre IP baseado no protocolo SIP.

Palavras-chave: VoIP. Segurança da Informação. SIP.

Abstract

Many new technologies are coming on the market to optimize enterprise's operations and to make easier people's life. One of the technology that most have been evolving is the Telecommunications. There is a revolution on the telephone system used today, which bases were created more than 100 years ago. The present switched circuit network is being gradually substituted for the packet switched network, which originally was used only for data traffic. This change favors all, because it reduces costs and adds new features to the public telephony system, but it needs attention to the many challenges this new technology brings. Among these, the challenge to enforce at least the same security that exists on the present public telephony system. This article discusses the applicability of information security on the Voice over IP system using the SIP protocol.

Keywords: VoIP. Information Security. SIP.

Capitulo 1

1 Introdução

O mercado de telecomunicações está passando por um período de inovação tecnológica muito importante. Há mais de 100 anos o sistema de telefonia pública não sofreu uma grande alteração, sendo apenas melhorado com o advento de novas tecnologias. Este sistema é baseado em redes de circuitos comutados, uma rede que opera separadamente da rede de pacotes comutados, que é utilizada para o tráfego de dados.

Este sistema clássico está sendo gradativamente alterado, para que o tráfego de voz possa ser encaminhado juntamente com o tráfego de dados. Esta convergência entre as redes de dados e de voz é possível graças à tecnologia de Voz sobre IP.

A convergência entre o sistema de telefonia e de dados por si só já é benéfica, pois diminui os custos com a infra-estrutura de telecomunicações das empresas. Com um sistema convergente, é preciso manter apenas um time para cuidar da rede, não sendo mais necessário ter uma equipe para cuidar da rede de dados e uma outra equipe para cuidar da rede de voz.

Além disso, a utilização da tecnologia de telefonia IP traz uma série de novas funcionalidades, o que, aliado à redução de custos, torna a migração para os novos sistemas cada vez mais comum.

Porém, novas tecnologias trazem novos desafios, e a utilização da rede de dados para carregar o tráfego de voz não poderia ser diferente. Dentre estes novos desafios, a segurança é um dos que mais se destaca. A segurança da informação já é uma área muito desenvolvida em diversas empresas, e os dados que trafegam em suas redes já possuem um nível considerável de proteção. Como o sistema de telefonia tradicional reside em uma rede separada, com um acesso mais restrito, o nível de segurança deste sistema é considerado adequado, pois pouca gente tem acesso a esta rede senão por aparelhos telefônicos tradicionais, assim, pouca gente se preocupa com a segurança de um sistema de telefonia tradicional.

Com a crescente popularização da tecnologia de Voz sobre IP, seja ela entre usuários domésticos ou usuários corporativos, os incidentes de segurança começam a se destacar, pois com mais gente usando, o VoIP passa a ser alvo de ataques, assim como já são as redes de dados tradicionais.

A imprensa especializada já está repleta de notícias e artigos sobre o assunto, e o número de associações e grupos de especialistas se reunindo para discutir as vulnerabilidades e contramedidas para a tecnologia crescem a cada dia.

Este artigo tem como objetivo explorar a tecnologia de VoIP baseada no protocolo de sinalização SIP (Session Initiation Protocol), bem como analisar algumas vulnerabilidades da tecnologia e a aplicabilidade de contra-medidas de segurança para mitigar os riscos relacionados.

Capitulo 2 - Segurança

2 Segurança – Definição acadêmica

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 dano 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 consequentemente 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. Este texto será focado no estudo Segurança da Informação.

2.1 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.

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.

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.

Em tempos de economia nervosa, como o que estamos vivendo, a racionalização dos investimentos nas empresas é fundamental. É preciso focar a utilização dos recursos naquilo que mais agrega valor ao negócio. Os acionistas querem resultados. É preciso priorizar. Como se sabe, as empresas estão constantemente expostas à ameaças. Diversos tipos de incidentes podem ocorrer a qualquer momento. Independentemente de qual seja o tipo, podemos agrupá-los de acordo com a propriedade da informação que eles atingem: confidencialidade (sigilo

da informação), integridade (informações íntegras - corretas), disponibilidade (informação disponível quando você precisar dela – por Exemplo, o site deve estar no ar). Problemas de quebra de confidencialidade (causados, por exemplo, por vazamento ou roubo de informações sigilosas) podem expor para o mercado ou para a concorrência as estratégias ou tecnologias da empresa.

Nesse caso, se deixarem de ser segredo de negócio, podem comprometer a vantagem competitiva no mercado. As empresas concorrentes podem então descobrir alguns segredos e até mesmo oferecer produtos e serviços compatíveis. O marketing será ameaçado. Há o grande risco de a concorrência passar para o campo dos preços. Em última análise, a margem de lucro será comprometida. Os acionistas perderão dinheiro.

Problemas de disponibilidade (exemplo: um ataque ao site, em que ele fique fora do ar por algum tempo), pode causar impacto direto no faturamento, se foi realizada algum tipo de venda on-line. Isso é muito claro. Mas outros tipos de conseqüência podem ser notadas. Por exemplo, se a Internet é usada para fazer compras de suprimentos e/ou matérias-primas de fornecedores, um problema no sistema pode provocar ausência / insuficiência de matéria prima ou suprimentos importantes. Isto pode comprometer os compromissos de entrega de produtos ou serviços para os clientes. Poderá ter problemas de custos, prazos ou qualidade dos produtos. Isso causa impacto na imagem da empresa perante os clientes; pode causar o pagamento de multas contratuais. No caso do uso de mecanismos de contingência (utilizar sistema manual para fazer as compras), o processo se tornará mais caro. Vai impactar diretamente no custo. Novamente: a margem de lucro será comprometida e os acionistas perderão dinheiro. Problemas de integridade causados, por exemplo, por uma invasão ou problema técnico que altere o valor de dados importantes, sem que se perceba, trazem impactos. Os dados armazenados, em algum momento, são usados para tomadas de decisões. Um dado errado leva à decisões erradas. Decisões erradas fatalmente reduzirão faturamento ou aumentarão custos. A margem de lucro será comprometida. Um ataque ao site, com modificação de conteúdo, tornará visível ao mercado que a empresa negligenciou aspectos de Segurança da Informação. Para investidores, pode ser um sinal de que a empresa está vulnerável à perda de rentabilidade devido aos fatores expostos logo acima. Os papéis da empresa serão rejeitados, o que refletirá imediatamente na avaliação. As ações perderão valor, ou seja: os acionistas, mais uma vez, perderão dinheiro. Após esta análise, podemos concluir que elementos

fundamentais para a sobrevivência das empresas - como a busca contínua do aumento do faturamento e da redução de custos e a avaliação que o mercado faz dos papéis - estão relacionados com Segurança da Informação. O valor dos papéis de uma companhia no mercado está associado com a confiança que investidores e agências de classificação de risco depositam nela. A confiança que uma empresa é saudável financeiramente está pouco exposta a riscos de naturezas diversas e vai manter boas margens de lucro (isto é, dividendos para os acionistas) é um elemento-chave para assegurar a valorização de papéis no mercado. Sendo assim, a segurança da informação, permeada por toda a organização, contribui grandemente para lucratividade e avaliação da empresa.

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

Capitulo 3 - Voz sobre IP

3.1 Introdução

Voice over Internet Protocol, ou 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.

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.

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.

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 audio (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.

3.2 Como Funciona

Embora a tecnologia de VoIP seja complexa o suficiente para ser abordada por um livro inteiro, o conceito é relativamente simples e fácil de se entender. Basicamente, utilizar VoIP significa utilizar a rede de dados para transmitir voz.

Um telefone IP (ou um *softphone* instalado em um computador) capta 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.

Esta voz comprimida é dividida em pequenas amostras, geralmente variando entre 10 e 40 milisegundos, 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 audio dos pacotes IP e remonta a mensagem de voz original.

A figura abaixo ilustra uma situação simples onde temos uma ligação entre dois telefones IP pela Internet. Nesta figura não é considerado o tráfego de sinalização.

Figura 1 – Funcionamento do VoIP

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

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.

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.

Abaixo segue uma tabela retirada do documento Avaya IP Voice Quality Network Requirements versão 3.0. Esta tabela mostra o consumo de cada chamada VoIP utilizando-se o CODEC G.711 no meio ethernet.

LAN Bandwidth using G.711 codec in kbps				
Ethernet Type		EV2 with trailer but no preamble	EV2 with trailer and preamble	EV2 with trailer and and preamble and 802.1Q
G.711 Voice Payload Size	10 ms	110.4	116.8	120.0
	20 ms	87.2	90.4	92.0
	30 ms	79.5	81.6	82.7
	40 ms	75.6	77.2	78.0
	50 ms	73.3	74.6	75.2
	60 ms	71.7	72.8	73.3

Tabela 1 – Utilização de banda na LAN

Nesta outra tabela temos a comparação da utilização de banda na WAN utilizando-se os diversos CODECs disponíveis:

WAN Bandwidth (using Frame Relay or PPP L2 Protocol) in Kbps							
Codec Type		G.711m and G.711A	G.711m/A with cRTP	G.729 and G.729A	G.729A with cRTP	G.723 6.3kbps	G.723 5.3kbps
Voice Payload Size	10 ms	102.4	~73.6	46.4	~17.6	N/A	N/A
	20 ms	83.2	~73.6	27.2	~12.8	N/A	N/A
	30 ms	76.8	~67.2	20.8	~11.2	19.1	18.1
	40 ms	73.6	~66.4	17.6	~10.4	N/A	N/A
	50 ms	71.7	~65.9	15.7	~9.9	N/A	N/A
	60 ms	70.4	~65.6	14.4	~9.6	12.7	11.7

Tabela 2 – Utilização de banda na WAN

3.3 Qualidade de Serviço

O fato de as ligações VoIP não precisarem de circuitos dedicados como no caso da PSTN permite uma melhor utilização dos links de comunicação disponíveis nas empresas, porém, como as ligações dividem o mesmo meio com diversas outras aplicações, é preciso tomar alguns cuidados para que não se tenha uma degradação na qualidade das chamadas.

O tráfego de voz é considerado um tráfego em tempo real, diferentemente do tráfego de dados comum, pois é muito sensível à atrasos. Aplicações multimedia, como o VoIP, são muito sensíveis à atrasos, mas toleram uma certa perda de pacotes. Já aplicações de dados, como transferências de arquivos, toleram o atraso, mas são sensíveis à perda de pacotes. Por isso, o tráfego de audio é feito sobre o protocolo UDP (User Datagram Protocol, que é um protocolo não orientado à conexão, ou seja, não oferece nenhuma garantia de entrega, mas é mais rápido do que o TCP (Transmission Control Protocol), que é orientado à conexão e oferece a garantia de entrega.

Por causa desta característica do VoIP, é preciso dar prioridade ao tráfego de voz em uma rede congestionada, pois se houver atraso ou muita perda de pacotes, a qualidade da ligação vai cair até um ponto onde não é possível mais manter uma conversa telefônica. Para isto, existem várias tecnologias que buscam garantir uma Qualidade de Serviço, priorizando o tráfego de voz sobre outros tráfegos que dividem a mesma banda.

3.4 Protocolos

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. Este artigo tem como assunto o protocolo SIP.

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

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 a configurações de telefones IP, o DHCP (Dynamic Host Configuration Protcol), utilizado para entregar as configurações de IP dos telefones e o DNS (Domain Name System), utilizado principalmente pelo SIP para encontrar os usuários na rede.

3.5 Vantagens

Uma das maiores vantagens de se adotar a tecnologia de Voz sobre IP é a redução nos custos de ligações de longa distância. Empresas ou pessoas que ligam frequentemente para outros estados e principalmente outros paises podem usufruir de uma redução muito significativa em suas contas telefonicas. Isto acontece pois, como a ligação utiliza a Internet como meio de transporte, não é preciso pagar as altas taxas que as operadoras de telefonia cobram para efetuar estas ligações. A ligação pode sair totalmente sem custo, no caso de uma ligação de *softphone* para *softphone*, ou custar menos do que uma ligação local no caso de uma ligação através de um provedor VoIP.

Existem diversos programas para se fazer ligações pela Internet, como o Skype. No caso de ligações feitas de Skype para Skype, não há custo nenhum. Caso o usuário queira utilizar o Skype para fazer ligações para telefones convencionais, ele pode contratar o serviço SkypeOut, um sistema pré pago que faz a interligação entre o Skype e a PSTN.

O VoIP também permite a redução de custos com a infra-estrutura de telecomunicações das empresas. No sistema atual, o sistema de telefonia é separado do sistema de dados, e equipes diferentes cuidam de seus respectivos sistemas. Ao implantar o VoIP, as empresas podem juntar os dois sistemas em apenas um, o que é chamado de convergência. Uma rede convergente é uma rede capaz de realizar a transmissão de dados, voz e video através de um mesmo meio físico. Mantendo apenas um tipo de rede, é possível diminuir os custos de manutenção, bem como diminuir o número de pessoas responsáveis pelo suporte à rede, já que será preciso apenas uma equipe com conhecimento em redes convergentes.

Além da redução de custos, o VoIP traz uma série de novas funcionalidades, como a utilização de ramais virtuais. Um ramal virtual pode ser utilizado em qualquer lugar do mundo com acesso à Internet. Uma empresa pode aliar um sistema de telefonia IP com um sistema de VPN (Virtual Private Networks) para permitir que seus colaboradores utilizem seu ramal em qualquer lugar do planeta, em suas casas ou em quartos de hotel, por exemplo.

3.6 Segurança em VoIP

O VoIP veio para ficar, cada vez mais empresas e pessoas utilizam esta nova tecnologia. Com o aumento na utilização, os problemas relacionados à segurança da solução começam a chamar mais atenção.

A PSTN oferece um nível de segurança e confiabilidade adequado para a maioria dos usuários, pois é um sistema de difícil acesso, para capturar uma ligação, por exemplo, o atacante precisa ter acesso físico ao sistema. Além disso, a arquitetura utilizada na PSTN a torna uma rede estável e com uma qualidade praticamente garantida, pois cada ligação tem o seu circuito próprio alocado para ela do início ao fim da chamada.

A utilização da rede IP para o tráfego de voz expôe o sistema de telefonia aos mesmo riscos que a rede de dados já sofre, além de trazer novos desafios para os engenheiros de segurança e rede das empresas. Com uma rede bem projetada para a utilização do VoIP, estes riscos são minimizados.

Existem diversos tipos de ataques aos sistemas VoIP. Este artigo visa abordar os principais tipos de ataques bem as soluções disponíveis. Embora existam diversos protocolos de sinalização para o VoIP, abordaremos aqui o protocolo SIP, pois a tendência é que as futuras implantações de VoIP sejam todas baseadas em SIP.

Capitulo 4 Protocolo SIP

4.1 O SIP

Para se proteger ou atacar um sistema, é preciso conhecer muito bem o seu funcionamento. Os sistemas VoIP são complexos, baseados em uma série de protocolos, sendo eles classificados como protocolos de sinalização (SIP, H.323), protocolos de transporte (RTP, RTCP) e protocolos de suporte (DNS, DHCP, TFTP). Um problema relacionado à qualquer um destes protocolos pode afetar o sistema como um todo, por isso é importante que um enegenheiro de segurança conheça toda a estrutura envolvida, para garantir o maior nível de segurança possível.

O SIP é um protocolo criado pelo IETF (Internet Engineering Task Force) para a sinalização de sistemas multimedia, e é responsável por estabelecer, localizar, configurar, modificar e finalizar sessões. Este protocolo é parecido com o HTTP (Hyper Text Transfer Protocol), também do IETF, pois é baseado em mensagens de texto.

4.1 Componentes do SIP

A estrutura do SIP é formada por dois elementos principais, o agentes de usuário (User Agents) e os servidores SIP (SIP Servers). Para os usuários, temos o agente de usuário cliente (User Agent Client) e o agente de usuário servidor (User Agent Server), o cliente envia as requisições e receber as respostas para estas requisições, o servidor responde às requisições. Em uma comunicação, todos os agentes envolvidos realizam o papel de clientes e servidores uns dos outros. Para os servidores, existem três tipos:

Servidor Proxy – são responsáveis por encaminhar as requisições dos usuários para outros servidores ou usuários, estabelecendo assim a comunicação entre as partes.

Servidor de Registro – é o servidor onde os usuários devem se registrar de modo a serem localizados por outros usuários na rede.

Servidor de Redirecionamento – são responsáveis por redirecionar os usuários para outros usuários.

É importante notar que todas estas funções podem ser realizadas por um mesmo servidor SIP, ou podem ser configuradas em máquinas diferentes para uma maior escalabilidade da solução.

4.2 Mensagens do SIP

O funcionamento do SIP é baseado em mensagens de texto, o que simplifica bastante a implementação, desenvolvimento e soluções de problemas relacionados ao protocolo.

Existem dois métodos de comunicação no SIP, as requisições e as respostas. Algumas das requisições que fazem parte da comunicação do SIP são:

Register – Utilizado pelo agente de usuário para registrar seu endereço SIP e o endereço IP no servidor de registro.

Invite – Utilizado para convidar um outro agente de usuário a iniciar uma sessão.

Ack – Utilizado para o agente aceitar uma sessão.

Bye – utilizado para se terminar uma sessão.

As respostas que são enviadas pelos agentes de servidores SIP são divididas em três categorias principais, formadas por um número de três dígitos, com o primeiro dos dígitos identificando a categoria da mensagem. As categorias são:

Informational (1xx) – A requisição foi recebida e está sendo processada.

Success (2xx) – A requisição foi confirmada e aceita.

Redirection (3xx) – A requisição não pôde ser completada e foi redirecionada para outro endereço.

Client error (4xx) – A requisição contém erros, por isso o servidor não pôde processá-la.

Server error (5xx) – A requisição foi recebida, mas o servidor em questão não pôde processar a requisição. Outro servidor poderá fazê-lo.

Global failure (6xx) – A requisição foi recebida e servidor não pôde processa-la. Outros servidores também não conseguirão processar mensagens com este erro.

4.3 Arquitetura

O SIP mistura a arquitetura cliente/servidor com a arquitetura ponto a ponto. A comunicação em uma rede SIP começa com o modelo cliente/servidor, com os agentes de usuários se registrando no servidor de registro. A figura abaixo mostra este processo:

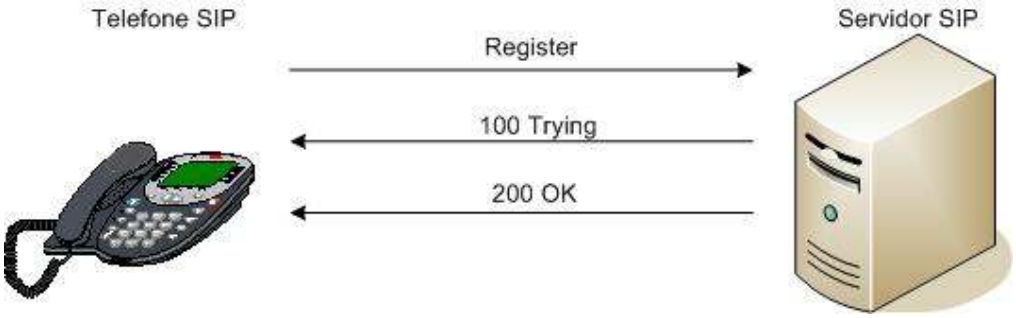


Figura 2 – Arquitetura cliente/servidor

Depois de registrados, os agentes ainda utilizam o modelo cliente/servidor para iniciarem as ligações. Se o usuário A quer falar com o usuário B, o mesmo deve enviar uma mensagem INVITE para um servidor proxy ou de redirecionamento. O servidor Proxy reencaminha este INVITE para o usuário B, que então inicia uma comunicação ponto a ponto com o usuário A.

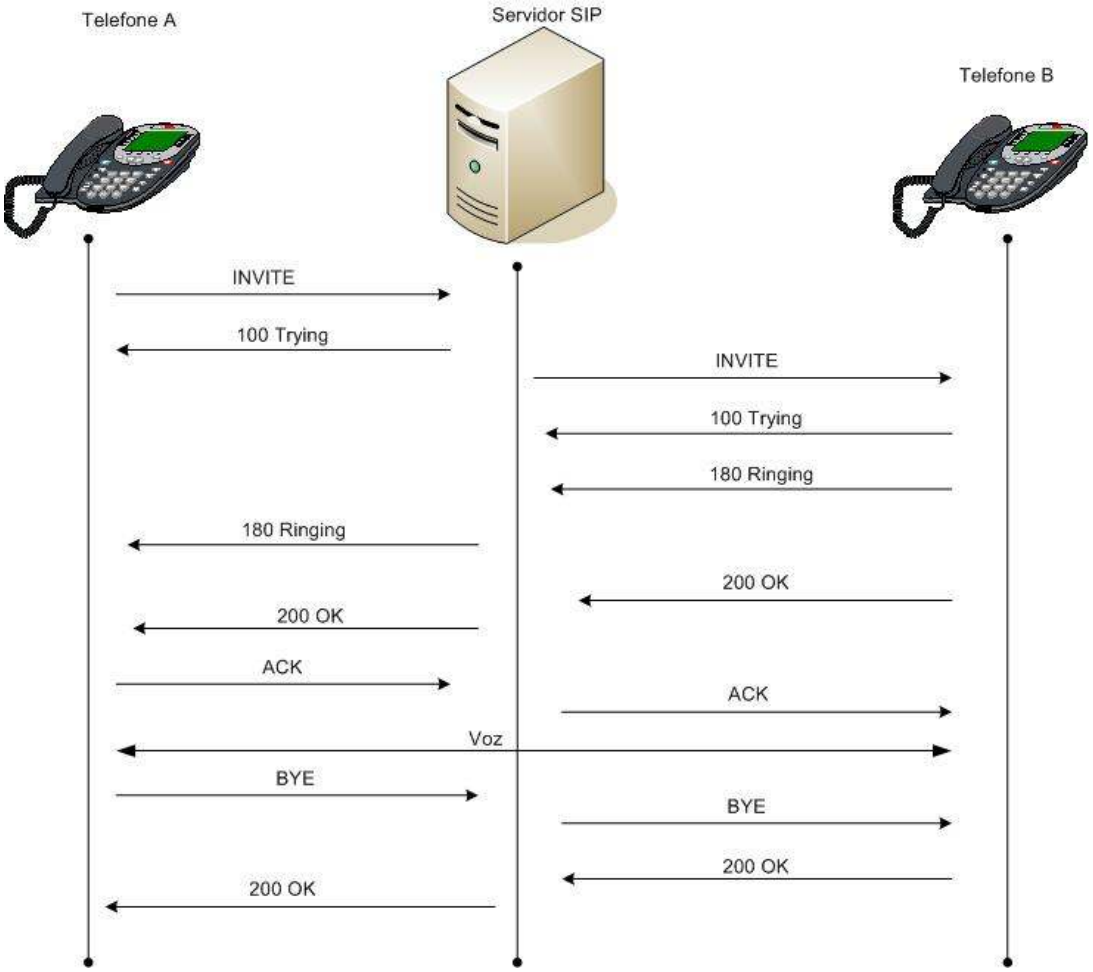


Figura 3 – Sinalização de dois usuários SIP

Já o servidor de redirecionamento recebe o INVITE, checa o endereço do usuário B, e informa o mesmo para o usuário A, que então envia o INVITE direto para o usuário B, e ambos iniciam então uma comunicação ponto a ponto.

Capitulo 5 – Riscos de Segurança em uma Rede VoIP

5 Introdução

A utilização da rede IP para o tráfego de voz faz com os riscos de segurança que já existem na rede IP afetem também o sistema de telefonia. Existem alguns riscos que devem ser considerados ao se implantar uma sistema VoIP. Neste artigo citaremos alguns dos principais.

5.1 Negação de Serviço

O risco que talvez seja o mais preocupante para a maioria das empresas é a negação de serviço. Este tipo de ataque é comum nos sistemas de dados. Para realizar este ataque, o atacante pode explorar falhas nos equipamentos e sistemas ou simplesmente esgotar os recursos dos sistemas, como memória, processamento e banda de rede.

O ataque de negação de serviço a um sistema VoIP é fácil de ser realizado em redes que não são bem preparadas, pois por ser um tipo de aplicação em tempo real, o VoIP é particularmente sensível ao excesso de trafego gerado por um vírus por exemplo.

5.2 Captura de Chamadas

Outro tipo comum de risco é a captura de chamadas. Para algumas empresas, as ligações telefônicas carregam dados sensíveis e confidenciais. Um atacante pode ter acesso à algum ponto da rede, e instalar ali um software capaz de capturar os pacotes RTP e montá-los em um arquivo de áudio que pode ser ouvido posteriormente. Este tipo de ataque é mais difícil em redes que utilizam switches, pois estes equipamentos segregam os dados, porém, existem ataques que fazem com que seja possível a captura do tráfego, como o ARP spoofing.

5.3 Manipulação do Protocolo de Sinalização

O protocolo de sinalização SIP utiliza mensagens de texto para iniciar, configurar e finalizar as chamadas. Um usuário mal intencionado poderia manipular estas mensagens de forma a direcionar as chamadas para onde quisesse, sem que o usuário que está ligando perceba.

Este tipo de ataque pode ajudar muito um outro tipo de ataque muito utilizado, a engenharia social.

5.4 Ligações Fraudulentas

Este tipo de ataque é muito perigoso para todas as empresas. Um atacante poderia se utilizar de falhas de sistema ou mesmo configurações inadequadas no sistema de PBX das empresas para efetuar ligações fraudulentas.

Este tipo de ataque se torna mais perigoso ainda quando o atacante divulga esta falha para um grande número de pessoas, como com a publicação do fato pela Internet.

O resultado deste tipo de ataque é que, até que a empresa perceba o problema, diversas ligações fraudulentas serão feitas, e a empresa receberá uma conta telefônica exorbitante.

5.5 SPIT (Spam over Internet Telephony)

O SPIT traz para a telefonia um problema que todo usuário de e-mail conhece muito bem, o SPAM, ou seja, mensagens em massa não solicitadas. Todos os usuários de e-mail estão cansados de receber e-mails vendendo todo o tipo de coisa, e o problema se tornou tão crítico que existem diversas ferramentas para combater o SPAM hoje em dia.

Apesar de parecer apenas um inconveniente, o SPAM é realmente um problema sério para as empresas, pois consome muitos recursos da infra-estrutura (servidores de e-mail, tráfego de rede, espaço de armazenamento nas caixas de e-mail), consome tempo dos funcionários que são obrigados a perder sempre algum

tempo apagando este tipo de e-mail e podem trazer diversos riscos à segurança da empresa, como vírus e engenharia social.

Este problema se torna pior ainda quando é transferido para a telefonia. Os Spammers, como são conhecidas as pessoas que enviam estes e-mails em massa, também podem enviar mensagens de voz em massa pela rede VoIP.

Este tipo de SPAM também consome muitos recursos, pois mensagens de voz costumam precisar de maior capacidade de armazenamento, e pior, consomem muito mais tempo dos usuários. Identificar e apagar mensagens de email é realmente muito mais rápido do que identificar e apagar mensagens de voice mail.

5.6 Servidores Controladores de Chamada

Os servidores que controlam todo o processamento de chamadas, os PBXs, são instalados em servidores de mercado, com sistemas operacionais de mercado. Temos soluções baseadas em servidores Windows e em servidores Linux.

Todas as vulnerabilidades presentes nestes sistemas operacionais acabam por afetar o serviço de processamento de chamadas, resultando principalmente em negação de serviço.

5.7 Riscos Relacionados aos Protocolos de Suporte

Um sistema de telefonia IP depende muito de outros serviços de rede para operar. Servidores DHCP são utilizados para enviar as configurações de rede para telefones IP, servidores de TFTP e HTTP são utilizados para guardar e enviar configurações para os telefones IP, servidores DNS são utilizados para fornecer a resolução de nomes para telefones e servidores, principalmente em um sistema baseado em SIP.

Um problema de segurança em algum destes serviços com certeza afetará a rede de telefonia IP. Se um atacante consegue tirar do ar o servidor de DHCP, novos telefones IP não conseguirão entrar na rede, causando assim uma negação de serviço.

Um atacante que consegue acesso à um servidor de TFTP ou HTTP, pode modificar as configurações de todos os telefones IP de uma vez, o que pode facilitar

o roubo de informações ou simplesmente causa uma negação de serviço em todos os telefones.

O DNS é uma aplicação crítica principalmente para o SIP. Um atacante pode modificar as entradas do servidor de DNS, e assim redirecionar as chamadas para onde quiser, ou simplesmente pode tirar o serviço de DNS do ar e causar uma negação de serviço aos usuários.

Capitulo 6 - Soluções de Segurança em uma Rede VoIP

6 Soluções de Segurança em uma Rede VoIP

Embora a quantidade de riscos relacionados à utilização da telefonia IP seja grande, é fato que esta tecnologia veio para ficar, e cada vez mais empresas e usuários domésticos estão aderindo a alguma forma de comunicação em VoIP.

Mesmo que os riscos relacionados à utilização do VoIP devam ser considerados antes da implantação de um sistema de telefonia IP, os mesmos não devem ser considerados um fator limitante para a nova tecnologia. Todos os sistemas tecnológicos possuem riscos relacionados, e graças à criticidade destes sistemas para as empresas, a grande maioria delas já possui um sistema de segurança efetivo implantado.

Muitas empresas já possuem uma cultura de segurança da informação bem madura, e já implementam diversos mecanismos de segurança que podem ser aplicados também para a segurança do novo sistema de telefonia. Para as empresas que ainda não possuem uma cultura de segurança da informação desenvolvida, a implantação do sistema de telefonia IP é uma boa hora para se iniciar o processo.

O primeiro passo para se garantir a segurança de um sistema é criar uma política de segurança da informação, com a política pronta, deve-se conscientizar todos os envolvidos, e então implementar ferramentas tecnológicas que auxiliam a aplicação das políticas criadas.

6.1 A Política de Segurança

A política de segurança deve definir de forma clara o que pode e o que não pode ser feito com as informações da empresa, bem como definir as regras de utilização dos seus sistemas.

Esta política deve ter o apoio da alta administração da empresa, e deve envolver os principais representantes de cada área da empresa na sua criação. A política deve ter foco nos processos críticos de negócio da empresa, as regras definidas devem ter como objetivo garantir a proteção destes processos críticos.

Com a política definida, deve-se partir para o processo de conscientização de todos os envolvidos nos processos de negócio da empresa sobre a existência e a importância desta política. Uma política de segurança não vale nada se não for seguida pelas pessoas.

A política define as regras de utilização dos sistemas, as pessoas que utilizam os sistemas seguem as regras, e ferramentas tecnológicas são utilizadas para efetivamente implantar os controles que estão definidos na política.

6.2 Conscientização dos Usuários

Os usuários do sistema devem ser conscientizados sobre a importância da segurança da informação, e devem ser treinados para que possam seguir com sucesso as regras impostas pela política de segurança.

Este trabalho é muito importante, os usuários precisam conhecer as regras, e devem saber como segui-las. Devem ser realizadas campanhas junto ao setor de marketing da empresa para que se tenha um grande impacto, e devem ser oferecidos treinamentos presenciais ou mesmo por meio eletrônico, para se garantir que os usuários realmente estão aptos a seguir o que foi definido na política.

Com o trabalho de conscientização feito, é preciso definir prêmios e punições. Os usuários que seguirem à risca a política, e ajudarem a área de segurança da informação, devem ser recompensados por isto. Já os usuários que não seguirem as regras devem ser advertidos e punidos.

6.3 Implementação de VLANs

Uma Virtual LAN, como o nome diz, é uma rede virtual. A maioria dos switches atualmente é capaz de suportar a utilização de VLANs. Um VLAN segrega um mesmo switch em diversas redes distintas, como se fossem redes físicas diferentes. Esta VLAN pode se estender pos diversos switches diferentes, não precisando assim ficar isolada em cada switch. A comunicação entre as VLANs deve ser feita por um dispositivo de camada 3, seja ele um roteador ou um switch com suporte à roteamento.

O tráfego de voz deve ser separado do tráfego de dados através de VLANs, e a comunicação entre as duas redes deve ser restrita e controlada. Esta abordagem evita que problemas na rede de dados afetem o tráfego de voz. Neste cenário, caso um vírus comece a se disseminar entre os computadores da rede, o alto tráfego gerado por ele não afetará muito o tráfego de voz que está em uma rede separada.

Além de evitar que problemas na rede de dados afetem o tráfego de voz, a utilização de VLAN ajuda na implantação de mecanismos de qualidade de serviço, garantindo assim o desempenho necessário para as aplicações VoIP.

A separação das rede através de VLANs também dificulta a captura do tráfego de áudio ou de sinalização por parte dos atacantes.

6.4 Criptografia

Além de separar o tráfego de voz, é possível também criptografar o seu conteúdo, e assim, mesmo que um atacante consiga capturar os pacotes, o conteúdo dos pacotes continuará protegido.

Alguns equipamentos VoIP suportam a encriptação das mensagens utilizando o SRTP (Secure Real-time Transport Protocol) e o SRTCP (Secure Real-time Transport Control Protocol), outros não.

No caso dos equipamentos que não suportam o SRTP, pode-se encriptar o tráfego através da utilização do IPsec (Internet Protocol Security). Neste caso, a

encriptação ocorre nos gateways com suporte a IPsec, como os concentradores de VPN (Virtual Private Networks).

6.4.1 Métodos de Criptografia para o SIP

Como mencionado anteriormente, para se ter mais confidencialidade nas chamadas VoIP, é possível criptografar o seu conteúdo, de forma que mesmo que um atacante consiga capturar o tráfego, o mesmo seja ilegível para terceiros.

O SIP pode utilizar três soluções de criptografia, sendo elas: Secure/Multipurpose Internet Mail Extensions (S/MIME), Transport Layer Security (TLS) e o Secure RealTime Transport Protocol (SRTP).

6.4.2 S/MIME

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.

6.4.3 Transport Layer Security

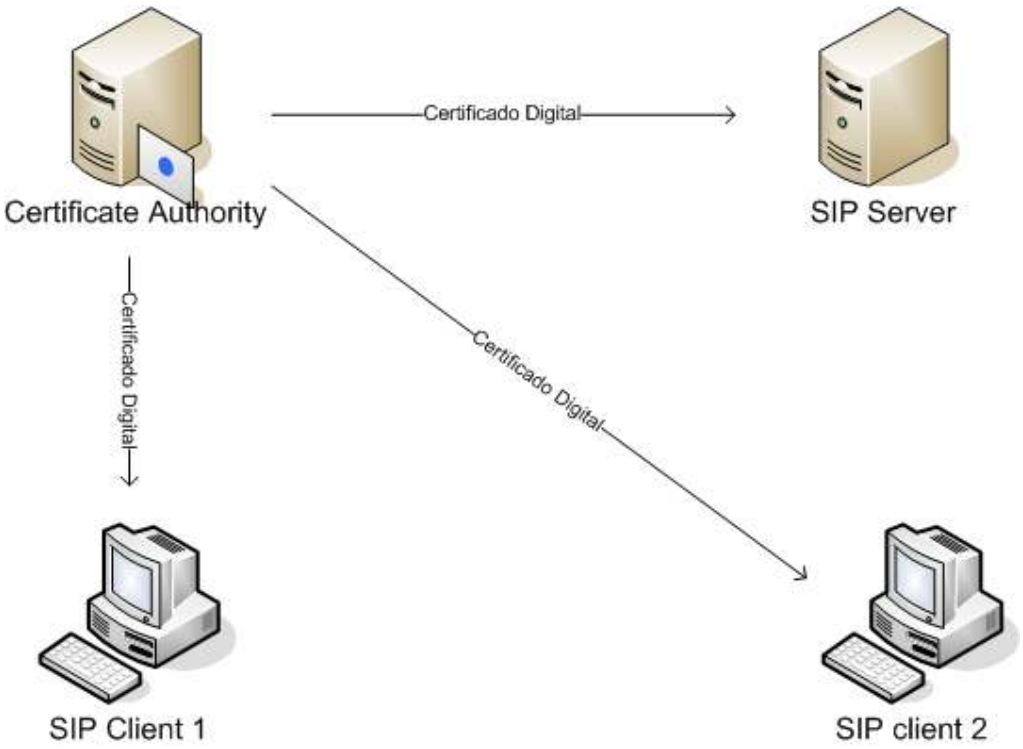
O TLS é a evolução do protocolo Secure Socket Layer versão 3 (SSLv3), apesar de os mesmos serem incompatíveis. A utilização do TLS estabelece um canal seguro criptografado entre dois participantes de uma comunicação em rede.

A utilização do TLS é transparente para a aplicação, o que permite que diversas aplicações possam utilizar este protocolo para realizar transações em um meio seguro, sem muitas modificações no software.

Como o TLS depende de certificados digitais X.509, uma infra-estrutura de chave pública e privada deve ser utilizada. Esta estrutura deve possuir um servidor de certificados, chamado Certificate Authority. Este servidor será o responsável por distribuir os certificados digitais para os demais computadores da rede, e assim todos os participantes da estrutura terão um servidor em comum, que todos confiam. É possível que uma empresa monte seu próprio servidor Certificate

Authority, mas desta forma somente os usuários internos que confiam neste servidor poderão efetuar comunicações seguras via TLS. Se for preciso realizar transações seguras com sistemas externos, de outras empresas por exemplo, é preciso contratar serviços de CA de empresas especializadas, os quais outras empresas também podem confiar.

Em uma infra-estrutura de chave pública, uma CA é responsável por emitir os certificados para todos os participantes, bem como revogar certificados que por ventura devem perder a sua validade.



De posse de um certificado digital, as partes envolvidas na comunicação poderão realizar suas transações de forma encriptada através do TLS. Para fechar uma comunicação segura.

O TLS é utilizado para criptografadas as mensagens de sinalização SIP, como INVITE, REGISTER e BYE.

6.4.4 Secure Realtime Transport Protocol

O SRTP é um padrão criado pelo IETF para garantir a confidencialidade e a integridade do áudio transportado pelo RTP, de modo que mesmo que o tráfego de áudio seja capturado por um terceiro, os dados sejam inúteis, pois não será possível remontar o áudio e ouvir a conversa sem a chave de criptografia.

Para o gerenciamento das chaves de criptografia, o SRTP utiliza o protocolo Multimedia Internet Keying (MIKEY), que utiliza o sistema de chaves pré-compartilhdas (pre-shared keys), infra-estrutura de chave pública e o algoritmo Diffie-Hellman para trocar as chaves.

Como o tráfego de áudio pode ser criptografado de ponta a ponta, ou seja, de um telefone para o outro, o SRTP foi projetado para utilizar poucos recursos computacionais, já que geralmente um telefone IP possui um hardware simples.

Assim como o RTP, o SRTP possui um protocolo irmão, o SRTCP (Secure Real-Time Transport Control Protocol), utilizado para proteger o tráfego do RTCP (Real-Time Transport Control Protocol).

O algoritmo de criptografia utilizado pelo SRTP é o Advanced Encryption Standard (AES) de 128 bits, o que proporciona um nível de segurança elevado para o tráfego de áudio.

Para se evitar que o tráfego de voz seja capturado e utilizado por terceiros, devemos utilizar a criptografia no tráfego de áudio, ou seja, nos pacotes RTP e RTCP. Já para evitarmos a manipulação dos protocolos de sinalização, devemos também criptografar o tráfego de sinalização, impedindo assim a captura e modificação das mensagens de configuração de chamadas. Assim evitamos que um atacante engane os usuários enviando as chamadas feitas pelo mesmo para o lugar errado.

6.5 Segurança dos Servidores

Como sabemos, os sistemas VoIP utilizam servidores e sistemas operacionais de mercado. Estes servidores precisam dos mesmos cuidados que os demais servidores da empresa. Isto inclui a segurança física, os servidores de processamento de chamadas, DHCP, DNS e HTTP devem ficar em um datacenter apropriado, com os devidos controles de acesso aplicados.

Os sistemas operacionais dos servidores devem sempre estar atualizados com as ultimas correções de segurança lançadas pelos fabricantes, possuir

softwares antivírus, IDS (Intrusion Detection System), e controles lógicos de acesso rígidos.

O sistema de alimentação elétrica deve ser redundante, garantindo assim uma alta disponibilidade aos servidores.

6.6 Sistema de Alimentação (Rede Elétrica)

Ao se adotar um sistema de telefonia IP, os telefones comuns são substituídos por telefones IP, ou mesmo *softphones* instalados nos computadores dos usuários. Os telefones comuns são alimentados através da própria linha telefônica, o que garante que mesmo que falte energia para o computador do usuário, o mesmo ainda será capaz de fazer ligações telefônicas, visto que os sistemas de PBX devem possuir sistemas de alimentação elétrica redundantes.

É fato que computadores precisam de energia elétrica para funcionar, portanto, se o usuário utilizar um *softphone*, estará vulnerável à quedas de energia, no caso de a empresa não possuir um sistema de alimentação elétrica emergencial que contemple também os computadores dos usuários.

No caso dos telefones IP, o cenário se torna um pouco menos critico, pois os mesmos podem ser alimentados pelo cabo de rede, da mesma forma que os telefones comuns são alimentados pelo cabo telefônico. Para isso, a empresa deve dispor de switches que suportem o padrão 802.3af, ou, no caso de possuir switches e telefones de um mesmo fabricante, utilizar-se de algum protocolo proprietário para o fornecimento de energia através da rede.

6.7 Sobre o SPIT

O SPAM sobre a telefonia IP ainda não é um problema, já que hoje em dia não é muito fácil enviar ligações em massa, pois, diferentemente do envio de e-mails, isto ainda envolve um custo. Porém, o rápido desenvolvimento da tecnologia VoIP e sua maior adoção tornará o SPIT possível em breve, e medidas de prevenção estão sendo estudadas atualmente pelos fabricantes de equipamentos e softwares VoIP.

7 Conclusão

A utilização das redes de pacotes comutados para o tráfego de áudio é uma tendência que está cada vez mais se afirmando no mundo corporativo, bem como está chegando cada vez mais às residências de usuários domésticos, seja através de simples programas de computador como o Skype ou até equipamentos mais especializados para o VoIP como o ATA (Analog Telephony Adapter), que permite a utilização de um telefone comum para as ligações via internet. Importante ressaltarmos também a fundamental necessidade da aplicação da segurança para a utilização do VoIP, tendo em vista que a expansão freqüente desta tecnologia trás consigo ameaças, que devem ser combatidas com o máximo de eficácia.

Desta forma concluímos que a segurança sobre sistemas VoIP será cada vez mais requisitada conforme o seu crescimento e expansão e o protocolo SIP conforme tema base de nosso trabalho atualmente é um dos mais aptos para atingis todas estas expectativas, sejam elas corporativas, domesticas ou em qualquer outra área onde aplicações VoIP estiverem rodando.

Bibliografia

ISSAC S. Debra; ISSAC J. Michael **The SSCP® Prep Guide** Mastering the Seven Key Areas of System Security. Estados Unidos Wiley 2003

KRUTZ L. Ronald; VINES D. Russel **The CISSP® Prep Guide** Mastering the CISSP and ISSEP™ Exams Segunda Edição. Estados Unidos Wiley 2004

HARRIS Shon **CISSP All-in-One Exam Guide** Terceira Edição. Estados Unidos McGraw-Hill Osborne Media 2005

DAVISON Jonathan. et al **Voice over IP Fundamentals** Segunda Edição. Estados Unidos Cisco Press 2006

PORTER Thomas **Practical VoIP Security.** Canada Syngress 2006

AVAYA, Inc., **Avaya IP Telephony Implementation Guide,** www.avaya.com 2005