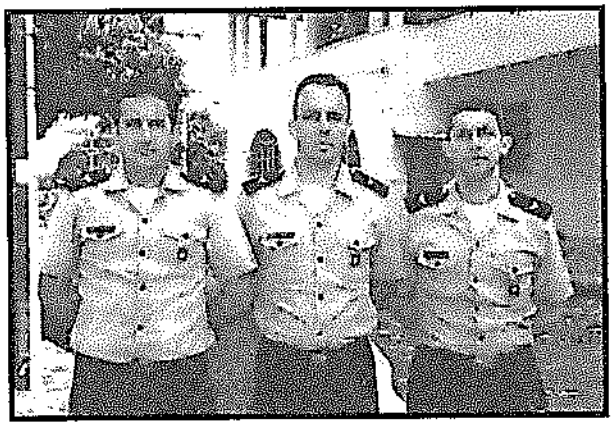

Reduzindo os riscos em redes Voz sobre IP (VOIP)

JOSOÉ Moreira[1]
Wagner WALTER de Souza Fialho[2]
Wanderlei SANDIM Borges[3]

Cap Esp Com Francisco ALMEIDA da Silva*
Cap Esp Com Marcelo de Souza FREITAS**

RESUMO

Este artigo discorre acerca da tecnologia Voz Sobre IP, ao mesmo tempo em que explora alguns aspectos de risco à segurança neste tipo de comunicação, aborda as situações em que eles podem ocorrer, mostra os pontos vulneráveis e sugere algumas soluções para reduzir os riscos. Longe de solucionar todos os problemas, pretende divulgar as implicações do uso deste tipo de tecnologia e expor algumas particularidades, de modo a disseminar este conhecimento entre os militares do Comando da Aeronáutica.

Palavras-chave: segurança, riscos, tecnologia.

---

1 - CFOECOM. Serviu até 2004 no DTCEACY, como sargento BCO; Engenheiro Eletricista.
2 - CFOECOM. Serviu até 2004 no CLBI, como sargento BEI; Físico.
3 - CFOECOM. Serviu até 2004 na CIAer, agência São José dos Campos, como sargento BCO; Analista de Sistemas.

** Leitor Técnico - Cap Esp Com Francisco Almeida da Silva - Engenheiro Eletricista*
** Leitor Técnico - Cap Esp Com Marcelo de Souza Freitas - Engenheiro Eletricista*

Reduzindo os riscos em redes Voz sobre IP (VOIP)

Um breve histórico

O Comando da Aeronáutica possui uma rede de comunicações estruturada que atende a sua função, mas que necessita de melhorias, principalmente quanto à diminuição de custos, à segurança no tráfego das informações e à confiabilidade no sistema. O uso de redes públicas de comunicações implica uma possível falha de segurança e vazamento de informações, o que é indesejável; não se pode, entretanto, tê-la como uma rede totalmente insegura, mas como uma rede suscetível a violações por parte de qualquer pessoa ou instituição com tecnologia e intenções afins. A segurança nas informações deve existir até mesmo em uma mesa de escritório, quando papéis e meios eletrônicos estão expostos, ao alcance de qualquer pessoa, bem intencionada ou não, que possa divulgar ou até mesmo vender estas informações.

A tecnologia Voz sobre IP transforma sinais de voz em pacotes de informação, que trafegam nas redes internas ou via internet, e assim ficam suscetíveis aos mesmos ataques de vírus e quebras de sigilo a que estão sujeitos os dados comuns que trafegam nestas redes. As soluções podem ser simples para alguns tipos de vulnerabilidades, como instalação de firewalls e restrição aos pontos físicos onde podem ocorrer acessos ilegais, reduzindo os riscos.

O desenvolvimento da tecnologia no campo das comunicações propiciou o desenvolvimento de processadores de sinais digitais (DPS), que convertem os sinais de voz e fax em sinais digitais como pacotes de dados, podendo ser transmitidos em redes de dados. Evoluindo a tecnologia de redes, objetivando sempre a maior integração, surgem as redes de alta velocidade, possibilitando trafegar em conjunto com os dados "tradicionais" os sinais de voz como pacotes digitalizados.

O Voz sobre IP (VoIP- Voice over Internet Protocol)

Existem várias tecnologias de redes de dados que permitem o tráfego de voz e dados, como as redes baseadas em ATM, Frame Relay e TCP/IP. Embora apenas o ATM tenha sido idealizado para o tráfego conjunto de dados e voz, o Frame Relay e o TCP/IP são os mais utilizados.

A diferença básica entre as tecnologias de Voz sobre IP (VoIP) e Voz sobre Frame Relay (VoFR) está no fato de que o VoIP está associado à camada 3 no modelo OSI (roteamento) e, portanto, com características de baixo custo e a capacidade de operação em redes heterogêneas. No entanto, tem seu preço: baixa qualidade de serviço (QoS limitado) e questões relacionadas com a segurança. O VoFR e VoATM estão associados à camada 2 do modelo OSI (data link), de custo mais

elevado, requerendo redes homogêneas ou gateways Layer 2 especializados.

O VoIP utiliza protocolos para transporte (RTP, RTCP, SCTP) e para sinalização (SIP, H.323, MGCP, etc.). O baixo custo de implantação da tecnologia VoIP é acompanhada de problemas de falta de padrão e de segurança, que agora são abordados, iniciando-se pelas ameaças a que estão sujeitos esses sistemas.

Identificando as ameaças

A primeira ameaça a esses sistemas é a sua própria divulgação. Como os protocolos de VoIP são relativamente novos, não há interesse e conhecimento profundo por parte dos hackers, mas com a divulgação da tecnologia, a tendência é que comecem a ser veiculadas, na internet, matérias sobre a vulnerabilidade da tecnologia e métodos de exploração para acesso indevido, fraudes e negação de serviços. A informação que está sendo veiculada, mesmo sendo voz em pacotes, é valiosa e pode trazer prejuízos. Por exemplo, o voice-mail de um executivo ou comandante de uma unidade das forças armadas pode permitir acesso indevido a informações confidenciais. Mais ainda, a captura de pacotes de informação através de programas de captura é um fato real. Se a informação é voz, basta convertê-la em formato de áudio. Aí está o grampo digital!

Fica claro que a convergência das redes de voz com as redes de dados baseadas em TCP/IP beneficia-se das vantagens que ela oferece, mas também sofre as suas vulnerabilidades.

A proteção contra as ameaças, exigida pelo computador, deve também ser dirigida ao telefone IP-compatível que estiver instalado nele, uma vez que tanto o telefone IP quanto o computador estarão suscetíveis às vulnerabilidades. Portanto, a vulnerabilidade é diretamente relacionada com a tecnologia que suporta o telefone IP.

A captura de tráfego e o acesso indevido a informações é a primeira vulnerabilidade abordada. O conteúdo das conversas telefônicas, quando no VoIP, trafega na rede de dados com encapsulamento em pacotes IP e a captura de pacotes de dados em uma rede IP através de técnicas de "Sniffing" é relativamente simples. O VOMIT (Voice Over Misconfigured Internet Telephones) é um aplicativo que utiliza a ferramenta tcpdump do Unix para capturar pacotes de uma conversa telefônica e consegue remontá-los e convertê-los em um formato de áudio (*.wav). Os pacotes de voz não utilizam criptografia, o que torna mais fácil ainda sua captura. O VOMIT é compatível apenas com o CODEC G.711, um padrão livre, bastante utilizado pela Cisco, mas logo outros aplicativos compatíveis com outros padrões podem surgir.

Outra técnica é o ataque de "Caller Identify Spoofing" (pode ser traduzido como falsificação da identidade do usuário que iniciou a chamada), pela qual o invasor induz o usuário remoto a pensar que está

conversando com outra pessoa. O processo é o seguinte: o invasor, após obter acesso à rede física, instala um telefone IP não autorizado e, utilizando outra técnica (MAC Spoofing), procura obter e assumir a identidade de um telefone IP válido da rede invadida. O resto é habilidade estelionatária do invasor.

Nesse ponto, vê-se que o acesso à rede física é um ponto importantíssimo para garantir a integridade da rede. Pontos de rede ativos, como hubs e switchers, e pontos terminais abandonados devido ao remanejamento de máquinas são portas abertas para ataques e fraudes diversas.

Os códigos nocivos, como vírus, trojan horses e outros, podem infectar os sistemas de telefonia IP de maneira análoga às redes de dados. A interferência em componentes críticos da infra-estrutura da rede VoIP e nos gateways podem paralisar o serviço de VoIP.

O uso indevido de recursos corporativos, fraudes financeiras (toll fraud) e desvios são ataques que visam ao uso não autorizado de serviços de telefonia IP ou à fraude dos mecanismos de bilhetagem e cobrança de ligações realizadas. As possibilidades são variadas, como por exemplo, utilizar indevidamente um telefone IP para realização de chamadas que sejam contabilizadas como originadas pelo telefone IP de algum funcionário (o qual responderia pelos custos). Outra possibilidade é instalar um voice gateway falsificado pelo atacante. Basicamente, este host é o ponto de convergência entre a rede de telefonia pública com a rede de dados, ou ainda com a Internet ou Intraer. Todas as ligações efetuadas passam por esse dispositivo, o que faz com que ele seja um dos alvos mais críticos em um ambiente de TI (tecnologia da informação) e, portanto, um dos principais alvos dos hackers. Quando o voice gateway oficial não é comprometido diretamente, o atacante tenta instalar na rede um segundo gateway e tenta redirecionar para ele o tráfego destinado ao host original, conseguindo bloquear, desviar e, até mesmo, escutar ligações.

Uma falha no sistema VoIP consiste no fato de que, a menos que se tenha um mecanismo eficiente para autenticação, não será possível identificar os usuários dos serviços, discriminando quem executou quais chamadas e a partir de qual telefone IP, se for negada a autoria da ligação. Alguns sistemas atuais possuem diretivas de seguranças como senhas pessoais de acesso e login para início do serviço, o que deve ser considerado quando da implantação do VoIP.

Todos os ataques de DoS, Denial of Service, capazes de paralisar os serviços de redes TCP/IP irão afetar também os serviços de voz, fax e vídeo.

Reduzindo os riscos

A implantação de uma rede VoIP segura depende de algumas práticas que consistem em:

1. Segmentar tráfego de voz e dados. Se possível, convém segmentar as redes de voz e dados, utilizando switchers e, caso necessite de mais segurança, pode-se usar uma VLAN (Rede Virtual). Isso contribui para uma melhor gestão do QoS e facilita a gerência da rede de voz e simplifica a sua manutenção. Tal procedimento também reduz os riscos de ataques de eavesdropping (captura não autorizada de tráfego de conversas telefônicas que trafegam na rede encapsuladas em pacotes IP) realizados com o VOMIT e outras ferramentas semelhantes.

A segmentação também protege a rede de voz de alguns ataques baseados em TCP/IP que, mesmo destinados a outros alvos, podem indisponibilizar o VoIP, se todo o tráfego estiver no mesmo segmento. Uma boa prática é que os segmentos de voz e dados sejam separados em VLANs distintas. Uma VLAN para o tráfego de voz, onde seriam instalados o call manager e os telefones IP, e outra para os dados.

2. Controlar o acesso ao segmento de voz com um firewall especializado. Convém que o acesso ao segmento de rede em que está instalado o call manager seja protegido por um firewall especializado, com o objetivo de filtrar todo o tipo de tráfego que seja endereçado à rede de voz e que não seja necessário para o funcionamento desses serviços. O firewall protegerá o call manager de acessos indevidos por parte de telefones IP não autorizados instalados em outros segmentos. O firewall deve ser compatível com o protocolo H.323, utilizado em telefonia IP, devendo ser capaz de lidar com o tráfego H.323, ou através de um proxy, ou utilizando algum método para determinar que portas estão sendo alocadas para as seções H.323.

3. Evitar o uso de aplicações de telefones para microcomputadores (PC- Based IP Phones), utilizando preferencialmente telefones IP que suportem VLAN. Tal medida é aconselhável, já que aquelas estão sujeitas a um número maior de ataques que os aparelhos baseados em hardware. Além do risco de falhas em seu próprio código, as aplicações de telefone IP para PC estão sujeitas às vulnerabilidades do sistema operacional e também de outras aplicações que residem no computador em que estão instaladas, bem como vírus, worms e outros códigos maliciosos. Os telefones IP executam sistemas operacionais proprietários com serviços limitados (menos vulneráveis).

4. Usar, nos telefones IP, endereços IP privativos e não válidos na Internet. Não é necessário utilizar endereço IP válido em telefones IP. Isso reduz a

possibilidade de que o tráfego de voz possa ser monitorado de fora da rede interna e para evitar que hackers consigam mapear o segmento de voz em busca de vulnerabilidades. As conexões com redes externas devem utilizar endereços IP válidos fornecidos por um firewall, através do serviço NAT (Network Address Translation).

5. Configurar os telefones IP com endereços IP estáticos, associados ao MAC address, que é um parâmetro importante para permitir a autenticação dos telefones IP. Quando um telefone IP tenta obter configurações da rede do call manager, seu MAC address pode ser verificado em uma lista de controle de acesso. Se o endereço for desconhecido, o dispositivo não receberá a configuração, desde que o recurso de registro automático não esteja habilitado.

6. Utilizar servidores DHCP separados para voz e dados. Com esse procedimento, os ataques de negação de serviços e outros, lançados contra o servidor DHCP no segmento de dados, não vão interferir com a alocação de endereços IP para os telefones no segmento de voz e vice-versa.

7. Monitorar os endereços de MAC no segmento de voz. Isso pode ser feito com o ARPWATCH, uma ferramenta que registra as alterações não autorizadas na associação entre endereço IP e endereço MAC.

8. Implementar mecanismos que permitam autenticar os usuários dos telefones IP. Alguns telefones IP exigem que o usuário faça um login informando uma senha ou número de identificação (PIN), válidos para que possam utilizar o dispositivo.

9. Implementar um sistema IDS, Sistemas de Detecção de Intrusos. Esse procedimento pode ser útil para monitorar ataques baseados em UDP e http; recomenda-se instalar no mesmo segmento em que estiver o call manager.

10. Criptografar o tráfego de VoIP. Quando possível, entre o telefone IP e o call manager, evitando o uso do VOMIT por invasores.

Conclusão

Nas redes em que há convergência de voz e dados, há muitos alvos potenciais em risco, como telefones IP, roteadores, switchers, gateways, sistemas de voice/mail, firewall e outros. O VoIP herda da rede de dados todas as suas ameaças (mapeamento, TCP/IP, denial of service, exploração das vulnerabilidades dos sistemas operacionais, engenharia social, roubo de identidade e spoofing, etc). Ao mesmo tempo, também é sujeito às ameaças e problemas inerentes aos

serviços de voz (delay, jitter, perda de pacotes, toll fraud, IP phone spoofing, etc).

Em muitos projetos, os mecanismos de autenticação ainda são deficientes, permitindo apenas a identificação do telefone, e não do usuário. Ferramentas como o VOMIT podem comprometer a confidencialidade das conversas telefônicas, permitindo ao hacker acesso indevido a informações sigilosas. Nos ataques de negação de serviços, é preciso considerar que o impacto do downtime do sistema de telefonia, uma vez integrado à rede de dados, pode ser extremamente incômodo.

Não há uma solução única que ofereça proteção para todas essas falhas. O conhecimento delas e as opções expostas minimizam bastante o risco em redes de Voz sobre IP. Finalmente, destaca-se como ponto fulcral que a definição de uma política de segurança é muito importante e constitui-se no ponto inicial para a segurança das Redes de Voz sobre IP.

Glossário de Termos Técnicos

VOIP - Sigla de Voice over Internet Protocol, técnica que transforma voz em pacotes de dados e a transmite como informação comum na rede internet.

IP Internet Protocol. Protocolo de internet.

FIREWALL - Componente de uma rede, geralmente software, que tem a função de rastrear e controlar o fluxo das comunicações que passam por ele, bloqueando, desviando ou autorizando o fluxo de informações, segundo uma definição especificada pelo gerenciador da rede.

GATEWAY - Porta de acesso, equipamento que tem a função de prover acesso a outra rede.

UDP - User Datagram Protocol. Protocolo de transporte sem conexão da pilha de protocolos TCP/IP.

HUB - Equipamento de uma rede que converge os hosts em um único ponto e todos se comunicam com todos na rede.

SWITCHER - Equipamento de uma rede que converge os hosts, mas identifica quem quer falar com quem e direciona o tráfego. Desse modo apenas o destinatário recebe a informação.

ROTEADOR - Equipamento de uma rede que converge os hosts, redes e sub-redes, gerenciando o tráfego das comunicações.

HOST - Qualquer equipamento que utiliza uma rede para uma função. Pode ser um terminal de computador, servidor, etc.

Bibliografia

GALVÃO, Marcio.ZATTAR, Alexandre. Aspectos de Segurança em Redes Voz sobre IP. São Paulo. Módulo Security Lab, 2003.

DAMASCENO, Rodney. Abordagem sobre Tecnologias para Segurança de Perímetro São Paulo, Trabalho de Pesquisa da Unicamp. Unicamp, 2004.

TOLEDO, Adalton P. Redes de Acesso em Telecomunicações. São Paulo, Makron Books, 2001.

MEDOE, Pedro A. Cabeamento de Redes na Prática!. São Paulo, 1ª Edição, Editora Saber Ltda, 2002.