

Voz sobre IP: A nova telefonia e a segurança

Por André Fucs de Miranda, CISSP <afucs@uol.com.br>

Introdução

Como já dizia o compositor Chico Science, "Um passo à frente e você não está mais no mesmo lugar". Infelizmente nem sempre o novo lugar é o mundo ideal no qual desejamos estar. Essa é a realidade que muitas empresas que vêm se enveredando pelo mundo da Voz sobre IP têm encontrado. Os problemas com segurança são muitos e mais uma vez impulsionados pela rotineira expectativa por remédios universais, as empresas vem tomando decisões que no mínimo serão fonte de muita dor de cabeça no futuro.

O problema é o mesmo ocorrido na relação entre instituições financeiras, internet banking, emails e cavalos de tróia. Seduzidas pelos benefícios de novas tecnologias, muitas empresas vêm-se prejudicadas por não terem adotado mecanismos eficientes que lhes protejam das ameaças presentes no novo cenário. Ao mesmo tempo, ainda é comum observar que os profissionais de segurança ainda ignoram a análise de risco, preferindo adotar uma estratégia de obstrução as novas tecnologias. Portanto, caberá aos gestores de produtos em conjunto com os de segurança arquitetar soluções compatíveis com as prioridades da empresa.

Antes de aprofundar sobre o aspecto da segurança em VoIP, é interessante fazer uma retrospectiva sobre algumas características dessa tecnologia. Entende-se por VoIP não apenas o tráfego de voz através de pacotes IP, mas também a oferta de serviços de comunicação assim como fax, voicemail, UMS, etc. É importante notar, que apesar do mercado de voz sobre IP no Brasil ainda estar pouco avançado, não devemos ignorar que a transmissão de voz é apenas um dos primeiros passos rumo ao IP Multimedia Subsystem.

Observe também que apesar de comumente associado a Internet, o uso da tecnologia não está restrito a esse universo visto que cresce mundo afora o número de operadoras de telefonia sobre IP com foco no mercado corporativo.

Outra forte característica da tecnologia é o fato de que por ser um movimento de convergência, tecnologias VoIP frequentemente baseiam-se em protocolos de diferentes origens. Exemplo disso é o extenso uso de protocolo SS7 e SIP em soft-switches. Além do forte impacto no *peopleware*, essa convergência leva também ao confronto de diferentes formas de encarar a segurança. Culturalmente as redes globais de telefonia são vistas como ambientes restritos com mínima interação entre diferentes empresas, redes IP por sua vez, tendem a possuir enorme interação de dados.

É igualmente significativo o fato de que nas tecnologias VoIP a segregação entre voz e dados é relativamente inferior a dos ambientes PSTN. Ainda que SIP, MGCP e NCS possuam essa preocupação, as empresas aproximam-se novamente do cenário de *in-band signaling* presente no SS5.

Ainda no que tange as diferenças culturais de ambos os ambientes, é interessante relatar um recente experiência com profissionais europeus durante um projeto no oriente médio. Esses profissionais, todos com enorme experiência em sistemas de telefonia mas pouca familiaridade com tecnologias IP, apelidaram os profissionais com *background* de transmissão de dados por IP de *data cowboys* em virtude da forma menos metódica com que o segundo grupo de profissionais trabalhava. Essa diferença deriva-se do fato de que o sistema telefônico é historicamente regado e especificado por normas locais ou internacionais que chegam ao nível de especificar métodos de operação dos ambientes. Já a tecnologia IP, originalmente concebida para resistir a uma guerra nuclear é significativamente mais flexível.

Aspectos da segurança

No que tange a segurança, um enorme esforço vem sendo efetuado por desenvolvedores e padronizadores na criação de mecanismos que garantam a segurança operacional do novo modelo, caso por exemplo do CableLabs, que lista em um de seus padrões os seguintes riscos:

- Roubo de Serviço;
- Violação da privacidade;
- Manipulação do protocolo de sinalização e;
- Interrupção de serviço;

A mesma especificação descreve de forma objetiva como tentar proteger dessas ameaças, especialmente no que tange ao serviço em si. A especificação descreve também uma série de mecanismos tecnológicos responsáveis por proteger os canais de comunicação contra essas fraudes. Note portanto que a tecnologia em si não é intrinsecamente insegura.

Em geral os modelos de segurança aplicados em ambientes VoIP não diferem significativamente dos modelos utilizados em ambientes Internet seguros. Um ou mais dispositivos de segurança são responsáveis por definir os limites da comunicação entre clientes e os *Call Management Server*. Em geral, ao invés de firewalls de uso genérico são utilizados firewalls de uso específico, conhecidos como *Session Border Controllers*, cujo funcionamento é idêntico ao de um firewall de aplicação. Cabe ao SBC aplicar grande parte das políticas de segurança e controle de acesso, oferecendo acesso aos clientes legítimos e bloqueando o tráfego restante. O mesmo modelo pode ser aplicado na comunicação entre uma empresa e outra.

Apesar de eficiente e funcional, o modelo ainda apresenta alguns pontos nebulosos. São eles:

- Ataques de Denial of Service;
- Análise de tráfego, e;
- Delegação de privilégios;

Conforme veremos a seguir, esses pontos, apesar de abordados pela maior parte dos modelos de segurança para ambiente VoIP, são em geral abordados de forma genérica, sem se preocupar com características do serviço.

Ataques de Denial of Service;

A negação de um serviço em geral se dá através de duas formas, a exaustão de recursos utilizados no transporte ou processamento do serviço, ou o comprometimento direto do provedor do serviço. Ataques de SYN Flood e WinNuke são respectivamente exemplos desses dois tipos de ataques. Atualmente, praticamente todo dispositivo de segurança é capaz de minimizar os riscos de ataques de exaustão, os Session Border Controllers não são exceção. Já o comprometimento direto, depende em geral da maturidade dos equipamentos responsáveis pelo serviço oferecido, incluindo aí o próprio Session Border Controller.

Em uma conversa uma das maiores autoridades sobre o assunto afirmava diversas soluções, de *switches* telefônicos a *media gateways*, apresentavam baixíssima maturidade de código, podendo ser vítimas de ataques diretos tão simples quanto o famigerado Ping Of Death. Longe de mero alarmismo, trata-se de uma ameaça real como mostram dois alertas do Centro de Resposta a Incidente da Carnegie Mellon University (CERT/CC). Consequência do trabalho de acadêmicos finlandeses, os alertas do CERT listam inconsistências em diversas soluções VoIP, entre elas um softswitch capaz de atender 250 mil linhas telefônicas. É também fato conhecido que alguns dos principais fornecedores de SBCs eram vulneráveis a ataques remotos em suas plataformas de gerenciamento.

Não se trata de dizer que há ataques e técnicas contra essas plataformas sendo amplamente disponibilizadas na Internet, mas de que o problema existe e é necessário tomar algumas providências. Porém é preocupante o fato de que parte dos mecanismos de proteção em uso hoje em dia são de pouca utilidade contra essas ameaças. Isso devido ao fato de que exceto os Session Border Controllers, firewalls tem pouca integração com protocolos VoIP, e aqueles que tem, preocupam-se mais em manter controle da sessão do que inspecionar o conteúdo das mesmas em busca de dados perigosos. Mas com produtos relativamente imaturos na linha de frente da proteção surge uma pergunta: Como proteger os produtos que nos protegem?

Usando novamente o padrão Voice over PacketCable, é interessante ver como a segurança é item preocupante. Na especificação do protocolo MGCP, encontra-se um item de nome "*Fighting the Restart Avalanche*", essa situação, característica do protocolo, tende a ocorrer quando inúmeros gateways são iniciados ao mesmo tempo e pode entre outras coisas causar congestionamento da rede, instabilidades dos servidores e até mesmo um denial of service. Ainda que muito similar a um SYN Flood, a vulnerabilidade chama a atenção por constar da especificação do próprio protocolo ao invés de fazer parte do documento específico sobre segurança.

Resta porém lembrar que o fato que o problema exista, isso não elimina a necessidade de utilização de dispositivos como os SBCs por exemplo. Na verdade, em decorrência da capacidade de lidar diretamente com os protocolos de sinalização e transmissão de voz, os Session Border Controllers inserem significativa proteção nesses ambientes mas para que isso seja eficiente, é fundamental que SBCs sejam vistos como mais do que dispositivos de *NAT Transversal* pois essa é de longe uma das menos importantes funcionalidades de um SBC.

Análise de tráfego

Outro importante ponto a ser observado quando o assunto é a segurança de ambientes VoIP de grande porte é a análise de tráfego em grandes velocidades. Ainda que inúmeras soluções de analisadores de protocolo estejam hoje disponíveis no mercado, nenhuma delas é capaz de garantir captura não amostral de dados em links de alta velocidade. Ou seja, dentre o enorme fluxo de informações, dados aparentemente não importantes podem passar despercebidos, isso obviamente inclui soluções de detecção de intrusos, ou IDS, que uma vez afrontados com enormes quantidades de dados, tende a ter problemas de performance e perda de pacotes. Some a esses problemas, o fato de que não há no mercado solução plena para monitorar incidentes de segurança em plataformas VoIP e um cenário bem perigoso se forma.

Apesar disso, saídas podem ser tomadas para reduzir o impacto desses problemas, ainda que a solução do problema ainda não exista. Uma das melhores formas de se fazer isso é separando o tráfego de acordo com sua característica. Ou seja, pacotes IP contendo dados da conversa telefônica são enviados através de um canal, enquanto dados contendo sinalização são enviados por outro caminho. Há inúmeras formas de fazê-lo, como por exemplo o uso de Policy-Based Routing e Network-Based Application Recognition em plataformas Cisco.

A idéia por trás da separação do tráfego, é simples, em geral redes VoIP geram enorme massa de pacotes, porém se comparados os volumes de pacotes contendo voz e pacotes contendo sinalização, o primeiro gera um maior volume de dados, sendo esse significativamente menos complexo que os pacotes de sinalização. Essa separação pode ser usada por exemplo para prover maior granularidade a um Sistema de Detecção de Intrusos ou algum sistema passivo de combate a fraudes.

Essa grande preocupação em torno da análise de tráfego decorre da importância de processos de monitoramento, tema que embora não seja totalmente ignorado, costuma ser identificado de forma muito tímida nas empresas, a exemplo dos IDSs.

O fato é que com o crescimento de soluções VoIP sem fio, como Voice over WiMax, ou até mesmo o crescimento do *voice-peering* a atenção com monitoramento deve ser redobrada, pois é incerto

se a relação entre alta-velocidade e monitoramento, será alterada. Provavelmente como acontece hoje, as tecnologias de transmissão de dados evoluirão mais rapidamente do que as tecnologias de monitoramento.

Delegação de Privilégios

O ITU, órgão da Organização das Nações Unidas responsável por padronizar sistemas internacionais de telecomunicações publicou em 2004 um documento denominado *Telecommunication networks security requirements, ou E.408*.

Ainda que seja mais focado em operadoras de telefonia, o documento pode ser interpretado de forma flexível, sendo aplicado por exemplo a ambientes de VoIP de menor porte, como um PABX por exemplo. Conforme outras recomendações do ITU, o documento constitui uma recomendação de práticas a serem adotadas por operadoras de serviços de telecomunicações. Dentre as inúmeras práticas recomendadas, uma consiste na necessidade de se especificar os “atores e personagens” da operação do sistema. Segundo o ITU são considerados atores pessoas ou processos responsáveis pela operação de uma rede de telecomunicações. Cada vez que um ator atua junto a rede, ele assume o papel de um personagem, seja o de assinante de serviços, fornecedor de software e hardware, operador, etc.

Ainda segundo o documento, entre os objetivos da segurança em sistemas de telecomunicações encontramos:

- Apenas atores autorizados deveriam ser capazes de acessar e fazer uso de redes de telecomunicações;
- Atores legítimos, deveriam ser capazes de acessar e operar os ativos aos quais estão autorizados a acessar;
- Uma rede de telecomunicações deve prover mecanismos que garantam que os atores sejam impedidos de obter acesso a recursos aos quais não tenham direito de acesso.

Essas objetivos expressam claramente a preocupação dos reguladores com um controle de acesso granular mas eficiente.

Diante dessa preocupação, é natural que um sistema de convergente de telecomunicações, deveria apresentar uma alta granularidade de direitos de acesso e grande capacidade de contabilidade sobre as operações realizadas. Porém nem sempre esse é o caso muitas soluções VoIP concentram quase todos seus esforços na proteção da conversa telefônica, ignorando totalmente a operação do sistema.

É importante que respeitadas as limitações de cada sistema, esforços em torno de um sistema de controle de acesso eficiente sejam fundamentais. De pouco adianta segmentar completamente um rede utilizando firewalls, criptografia e outros mecanismos se a segurança da aplicação de gerenciamento é simplesmente ignorada. Não se trata de mero alarmismo, é possível encontrar softswitches no mercado cujo gerenciamento deve ser todo feito com apenas um login, criando um cenário terrível onde à revelia de todas as boas práticas de segurança, o sistema praticamente força os operadores a utilizar um login único para administrar o sistema. Tente responder em um ambiente como esse à pergunta “quem modificou esse parâmetro do sistema?”

Atente também para o fato de que muitas vezes em uma solução VoIP, não apenas o Call Management System é crítico ao funcionamento do ambiente mas também servidores DHCP, DNS, switches, roteadores e uma série de outros componentes. As soluções devem portanto levar em consideração o sistema como um todo.

Conclusão e outras considerações

Ainda que a telefonia sobre IP seja grande novidade, é fundamental enxergá-la como mais um mecanismo de prover telecomunicações. Problemas já conhecidos como fraudes em sistemas de PABX, Voicemail e comunicações de longa distância continuam merecendo atenção e nesse sentido a recomendação E.408 do ITU-T possui uma abordagem muito interessante e merece ser utilizado junto com o padrão X.805 como guia para os responsáveis pelos processos de segurança em ambientes VoIP. Fato interessante de ambos os documentos é a forma com que lidam com a segurança de soluções de transmissão de dados e voz. Ao invés de especificar os mecanismos e algoritmos de proteção de dados, ambos documentos preocupam-se em modelos de alto nível baseados em classes e requerimentos que sirvam como base para os mecanismos de segurança, sendo esses extremamente flexíveis.

O fato é que pouco a pouco a voz sobre IP aproxima-se do ambiente corporativo e doméstico, e por se tratar de uma tecnologia emergente e em fase de fortes mudanças, é extremamente importante que os gestores e profissionais de tecnologia envolvidos com essa nova tentãdia evitem focar-se excessivamente em mecanismos de segurança.

Muita coisa ainda deve acontecer no mercado de VoIP e o grau de maturação das tecnologias ainda precisa crescer, mas o mercado sinaliza claramente que soluções de mídia em IP serão realidade nos próximos anos e devem elevar significativamente o nível de competitividade entre as empresas prestadoras de serviços de telecomunicação e a forma com que esses sistemas cuja essência é a troca de dados irão se comportar no futuro depende de decisões tomadas hoje.

Sobre o Autor:

André Fucs de Miranda é Certified Information Systems Security Professional com cerca de uma década de atuação no mercado internacional de segurança da informação e participou de alguns dos mais importantes projetos de VoIP do Oriente Médio, e em sua carreira registra passagem em empresas como Lucent Technologies, Unibanco e CFSEC Security Architects.