Segurança Aplicada a VoIP: Aspectos e Soluções

Ellen da Silva Alencar, Wendell Rodrigues
Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE
Departamento de Tecnologia em Telemática
Av. Treze de maio, 2081 – Fortaleza – CE - Brasil
ellenalencar88@gmail.com, Wendell@ifce.edu.br

Abstract. *Currently, the Voice over IP technology in the corporate networks is a common practice and allows valuable advantages. The IP protocol became a "de facto" standard even in local networks. Moreover, more and more conventional PBX solutions are replaced by IP PBX. However, integrating telephone systems in communication networks is a complex concern in relation to quality of service and information security. In this context, this paper addresses the main issues about security on VoIP as well as the ways to assure the quality of service maintenance.*

Resumo. *Atualmente, o uso de tecnologias Voz sobre IP em redes corporativas é uma prática comum e traz grandes benefícios. O protocolo IP tornou-se um padrão de fato mesmo em redes locais e percebe-se uma gradativa substituição de soluções baseadas em PABX convencionais por PABX IP. Entretanto, a inserção do sistema de telefonia nas redes de comunicação de dados traz uma preocupação constante com relação a garantias de qualidade de serviço e segurança da informação. Neste contexto, este artigo aborda os principais questionamentos relacionados à segurança de VoIP e de que formas podemos garantir o convívio com a manutenção da qualidade do serviço.*

Palavras chaves: VoIP; SIP; RTP; RTCP; IPsec; IPS; IDS; Gateway SIP

1. INTRODUÇÃO

A tecnologia que vem crescendo no mundo da telefonia é o VoIP (*voice over IP*), voz sobre uma rede baseada em IP. O VoIP de acordo com [6] é um protocolo que implementa meios de trafegar voz na rede IP. Para se estabelecer uma sessão VoIP é necessário usar juntamente com o protocolo SIP (*Session Initiation Protocol*) que é responsável em gerenciar as chamadas, estabelecendo, registrando e finalizando.

O VoIP junto com o SIP obteve grandes avanços ao longo dos anos, porém a implementação destes protocolos deixaram brechas no quesito segurança da informação, atraindo a atenção de hackers. Para a telefonia IP ser amplamente adotada é necessário fornecer as devidas instalações de segurança. Além da autenticação inicial dos usuários é necessário ter uma chave de sessão para ser usada na proteção do fluxo de dados da voz.

Neste trabalho aborda-se a segurança das ligações VoIP utilizando o SIP, como também uma proposta de solução baseada no estudo de opções existentes para empresas. Neste caso, prioriza-se o protocolo IPSec (*IP Security Protocol*) para prover segurança das ligações dentro do ambiente empresarial e o servidor gateway SIP com IPS para controlar a autenticação dos usuários externos, identificando quem pode se registrar ou não no servidor SIP da empresa.

Este artigo está organizado em seis seções, contando com a introdução. A segunda seção explica o funcionamento de chamadas SIP como também o conceito de segurança em VoIP, seguindo por trabalhos relacionados, explanado na seção três. Na seção quatro, é definido as tecnologias utilizadas neste artigo como o IPsec e sistemas de prevenção contra intrusos, seguido pela proposta de topologia para um ambiente corporativo mais seguro, explanado na seção cinco. Na seção seis, mostramos as considerações finais.

2. SEGURANÇA NO PROTOCOLO SIP

Para falarmos das questões de segurança VoIP, em primeiro lugar temos que considerar uma chamada SIP. A Figura 1 mostra as mensagens trocadas pelo usuário Alice (alice@minisip.com) entre seu amigo Bob (bob@ifce.edu.br).

Segundo [8], Alice envia a mensagem "INVITE" (mensagem para iniciar uma chamada) através do seu Proxy SIP, que por sua vez usa o DNS para localizar o Proxy SIP do Bob (ifce.edu.br). O servidor encaminha a requisição de sessão ao Bob com a mensagem "INVITE" que tem a resposta "200 OK", onde indica que a requisição foi recebida com sucesso e automaticamente o servidor SIP também encaminha a resposta para Alice, indicando que a requisição também foi recebida com sucesso. Em seguida o cliente Alice envia uma mensagem "ACK" para o cliente Bob e a conexão entre os dois é estabelecida, tornando assim uma arquitetura ponto a ponto.

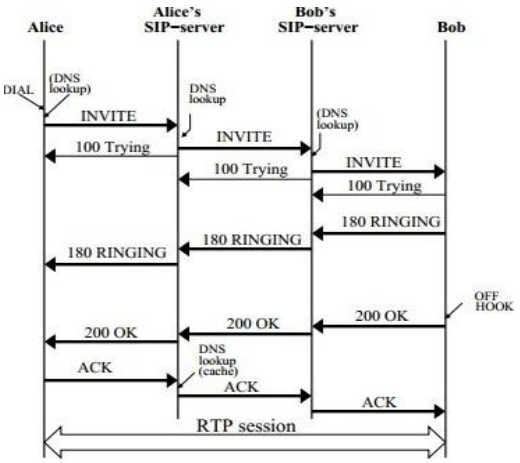

Fig. 1. Estabelecendo uma sessão VoIP utilizando SIP. (BILIEN, 2005).

A arquitetura SIP é composta por diversos elementos funcionais, que são:

- Agentes dos usuários ou clientes do agente usuário (UAC): são capazes de iniciar ou terminar sessões, pode ser telefones IP, SoftPhones, gateways de interconexão com outras redes, servidores de mídia entre outros.
- Servidores de agente de usuário (UAS): organizam as conexões e também são responsáveis em localizar o servidor destino UAC ou um servidor intermediário UAS. [2].

Como dito antes, o protocolo SIP estabelece um conjunto de mensagens que permite estabelecer, modificar e terminar vários tipos de sessões, depois que a sessão é estabelecida a voz é digitalizada utilizando um codificador/decodificador (CODEC). Segundo [7] a voz que é digitalizada trafega na rede através do protocolo UDP com auxilio do protocolo RTP (Real Time Protocol) e RTCP (Real Time Control Protocol) que compensam os requisitos de transporte que não podem ser satisfeito pelo UDP.

Após uma breve explicação do funcionamento do SIP é importante tratar de conceitos de segurança da informação para ter uma chamada VoIP segura, que são:

- Confidencialidade: Protege a informação ou parte dela contra a leitura ou cópia por pessoas não autorizadas. [4].
- Integridade: Consiste em garantir que o conteúdo de um documento se mantenha inalterado. A integridade pode ser verificada através de assinaturas digitais. [8].
- Autenticação: Requer que a origem de uma mensagem seja corretamente identificada. Protegendo os sistemas VoIP baseados no SIP contra ataques de manipulação de protocolos de sinalização, evitando fraudes e garantindo a integridade das partes envolvidas na comunicação. [4].
- Disponibilidade: Protege os serviços prestados pelo sistema de forma que eles não sejam degradados ou paralisados. [4].
- Controle de acesso: Permite ou nega acesso aos serviços e recursos do sistema. [4].
- Auditoria: Capacidade de verificar as atividades do sistema e determinar o que foi feito, por quem e quando foi afetado. [4].

Então com estes conceitos podemos concluir que para estabelecer uma chamada VoIP segura, teremos que ter um sistema que apenas permite que uma chamada seja estabelecida com o receptor que a espera, onde este deverá estar devidamente registrado no servidor SIP. Chamadas VoIP indesejadas serão bloqueadas para evitar spam VoIP (*SPIT – Spam Over Internet Telephony*), e os dados de voz como também as informações trafegadas e a identidade dos usuários terão que ser protegidas contra espionagem, utilizando criptografia entre outras ferramentas.

3. TRABALHOS RELACIONADOS

Alguns trabalhos disponíveis no mundo acadêmico ou comercial abordam este tema. Descrevemos a seguir alguns que julgamos mais próximos dos objetivos de nossa abordagem.

Em [1] são apresentados resultados sobre estudos relacionados com o uso do IPsec sobre o VoIP, concluindo que com o uso do IPsec a largura de banda cai 50% em relação ao VoIP. Além disso, mostra que a criptografia pode prejudicar o desempenho do tráfego de voz, devido ao tempo que leva para criptografar a carga, acrescentar um novo cabeçalho e criar um novo pacote. Porém neste mesmo artigo é abordado uma solução para o cabeçalho do pacote de compressão, propondo o cIPsec que reduz significativamente a sobrecarga dos pacotes na rede. Entretanto, há dificuldades de implementar tal solução, pois implicaria em alteração dos algoritmos em todos os equipamentos envolvidos.

O artigo de [3] sugere que a comunicação VoIP use efetivamente soluções baseadas em IPsec ou SRTP para garantir proteção dos dados. Concluindo que tais soluções não são impactantes no estabelecimento de chamadas. Entretanto, a conclusão apresentada se baseou em um cenário real, porém em uma rede local controlada. Tal cenário não demonstra como a solução apresentada se comportaria em um cenário real de comunicação em roteadores da Internet.

O trabalho de [9] mostra resultados a favor do IPsec, concluindo que apesar do impacto negativo na qualidade da fala, é possível selecionar algoritmos otimizados para ter o melhor desempenho na rede. Porém, mais uma vez vemos um cenário limitado, implementado em laboratório que ao passar para um cenário empresarial teria resultados impactantes.

4. TECNOLOGIAS UTILIZADAS

Para prover segurança aos pacotes que trafegam na camada de rede IP podemos utilizar o protocolo IPsec que segundo [7] consiste em uma coleção de protocolos projetados pela IETF (*Internet Engineering Task Force*).

O IPsec pode operar em dois modos: modo de transporte e modo túnel. No modo de transporte, o IPsec protege a carga útil a ser encapsulada na camada de rede, não protegendo o cabeçalho IP. Normalmente esse modo é utilizado quando precisamos de proteção de dados fim a fim, pois o host emissor utiliza o IPsec para autenticar ou cifrar a carga útil entregue pela camada de transporte e o receptor usa o IPsec para verificar a autenticidade do pacote IP antes de entregá-lo a camada de transporte. [7].

No modo túnel o IPsec protege o pacote IP inteiro, adicionando um novo cabeçalho IP. O modo túnel é normalmente usado entre dois roteadores ou entre uma estação e roteador, protegendo todo o pacote original no caminho como se ele passasse por um túnel. [7].

Em [7] define os dois protocolos utilizados pelo IPsec da seguinte forma: o protocolo AH (Authentication header – cabeçalho de autenticação) que fornece autenticação dos pacotes no nível IP sem confiabilidade e o protocolo ESP (Encapsulating Security Payload – Encapsulamento de dados de segurança) responsável por fornece os serviços de

autenticação de origem, integridade e confiabilidade que aos poucos irá substituir o AH.

Para tratarmos da prevenção do sistema contra invasões, podemos utilizar as tecnologias IPS (Intrusion Prevention System) e IDS (Intrusion Detection System). Que são comumente utilizadas para monitorar atividades em computadores, redes e analisar eventos na busca por sinais de invasão. Tendo o objetivo de alertar ou interromper os acessos não autorizados.

O IDS é uma solução passiva podendo ser reativa ou não, pois quando ele detecta uma eventual violação de segurança, registra no log do sistema e envia um alerta, sendo assim uma solução não reativa, mas quando ele responde a atividade suspeita finalizando a sessão do usuário ou reprogramando o firewall ele é considerado uma solução reativa. [10].

Já o IPS é considerado ativo, pois promove segurança em todos os níveis do sistema, desde o núcleo operacional até os pacotes de dados da rede. Definido políticas e regras para o tráfego na rede. O IDS e IPS podem trabalhar juntos um emitindo alertas e o outro definindo as regras de segurança para a rede [10]. O software SNORT é um exemplo da aplicação IDS/IPS em uma rede IP. Trata-se de um software livre de detecção de intrusão para a rede que analisa o trafego da rede e os pacotes IP em tempo real, prevenindo-os contra ataques.

5. PROPOSTA DE TOPOLOGIA

Como visto nas seções anteriores, há um misto de soluções que implementam diversos níveis de segurança em aplicações de rede. Especificamente em aplicações de VoIP com protocolo de gerenciamento de sessão SIP, as recomendações acadêmicas e comerciais apontam para o uso de criptografia na comunicação com o objetivo de impedir o acesso direto às informações trocadas.

Entretanto, apesar dessas tecnologias oferecerem um alto nível de confidencialidade, elas pecam pela complexidade e overhead imposto aos protocolos originais. Isto afeta diretamente a latência da comunicação e diminuição da largura de banda e, desta forma, diminuindo o número de canais de voz.

O que propomos aqui é uma alternativa mista baseando-se no princípio que o impacto da adoção de criptografia como as implementadas pelo uso de IPSec em redes locais é muito menos percebida que em comunicações remotas sobre os roteadores da Internet. A razão é simples, redes locais são localmente gerenciadas e possuem soluções de comunicação de dados mais sofisticadas com tráfego mais facilmente controlado. A Figura 2 apresenta o esboço dos elementos propostos nesta abordagem mista. A principal ideia é manter um gateway SIP com canais de voz com funcionalidades previstas em sistemas de detecção e prevenção de intrusos. Este equipamento oferece, dentre outras funcionalidades:

- Gateway de Autenticação SIP;
- *Honeypot* para detecção de intrusos;
- Autenticação baseada em chaves assimétricas com suporte a certificador digital;
- Bloqueio automático para intrusos;

Este equipamento é implementado através de um IPS Snort reconfigurado especificamente para controle de aplicações VoIP conforme é descrito em [5].

Não se intenciona abandonar o IPSec no contexto local. O objetivo é, sobretudo manter a qualidade de serviço na comunicação de voz sem negligenciar a segurança e confidencialidade da aplicação.

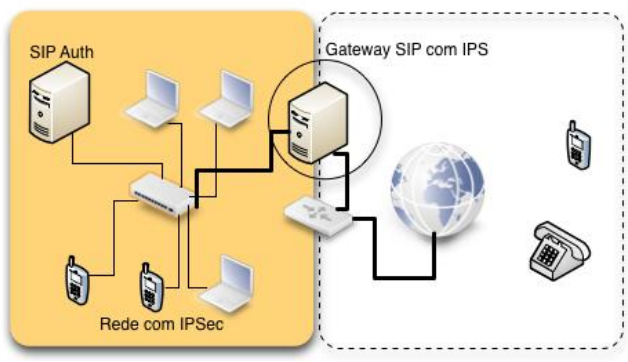

Fig. 2. Elaborado pelo autor (2013)

6. CONSIDERAÇÕES FINAIS

Neste artigo apresentamos um estudo experimental de uma rede VoIP. Utilizando o IPsec para a comunicação LAN, onde criptografa o tráfego de pacotes IP, e gateway SIP para prevenção contra invasões na comunicação WAN. Propomos esta alternativa mista para manter a rede baseada na arquitetura SIP confiável e íntegra, impedindo o acesso não autorizado às informações trocadas pela rede. Vimos que apesar do alto nível de confidencialidade da nossa proposta, ela peca no quesito de complexidade e ovehead que são impostos aos protocolos originais, ocasionando a diminuição da largura de banda utilizada. Concluímos que é possível mantermos o sistema VoIP seguro, prevenindo ataques que visam comprometer a confidencialidade e a integridade das ligações mantendo a qualidade de serviço. Porém temos que usar uma largura de banda maior que aquela utilizada em sistemas que não provêem segurança em suas ligações.

AGRADECIMENTOS

Este trabalho foi de muita importância para o aprofundamento dos meus conhecimentos dentro enquanto estudante da área de redes, mas especificamente em segurança da informação e telefonia IP. Tendo como motivação a conclusão do curso de tecnologia em telemática, como também a colaboração no âmbito acadêmico. Gostaria de agradecer aos laboratórios do IFCE que propiciaram um ambiente para realização deste trabalho.

REFERÊNCIAS

[1] BARBIERI, R; BRUSCHI, D; ROSTI, E. “Voice over IPsec: Analysis and Solutions”. 18th Annual Computer Security Applications Conference, Dec. 2002, pp. 261-270.

[2] BERNAL, P. S. M. “Voz sobre protocolo IP: A nova realidade da telefonia”. São Paulo: Érica, 2007.I.S. Jacobs and C.P. Bean, “Fine

particles, thin films and exchange anisotropy," in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[3] BILIEN, J; ELIASSON, E; ORRBLAND, J; VATN, J. O. "Secure VoIP: call establishment". Second Workshop on Securing Voice over IP, Stockholm - Sweden, 2005.

[4] BRITO S. H. B. "Aspectos de Segurança e Sigilo em Comunicações VoIP". São Paulo, p. 13. 2011.

[5] CIZ, P.; LABAJ, O.; PODHRADSKY, P.; LONDAK, J., "VoIP Intrusion Detection System with Snort", ELMAR, 2012 Proceedings , vol., no., pp.137,140, 12-14 Sept. 2012.

[6] COLCHER, S. ;GOMES, A. T. A. ; SILVA, A. O. ; SOUZA FILHO, G. L.; SOARES, L. F. G.. "VoIP: Voz sobre IP" 3. ed. Rio de Janeiro: Elsevier, 2005.

[7] FOROUZAN, B. A. e MOSHARRAF, F. "Redes de Computadores: uma abordagem Top-Down". 1. ed. Porto Alegre: AMG Editora, 2013.

[8] KUROSE, J. F.; ROSS, K. W. "Redes de computadores e a Internet: Uma abordagem Top-Down". 3. ed. São Paulo: Person Addison Wesley, 2006.

[9] MOTA, E. S. ; NASCIMENTO, A. G. O. ; JESUS, L.M.V. ; QUEIROZ, A. P. ; SILVA, E. N. J. ; CARVALHO, L. S. G. "Utilizando o IPSec em chamadas VoIP para a comunicação segura sem fio". In: SSI 2006, 2006, São José dos Campos. Proc. of the 8th International Symposium on Systems and Information Security, 2006.

[10] UFES, Universidade Federal do Espírito Santo. "O que significam as siglas IPS e IDS, no contexto de redes de computadores?", Núcleo de Processamentos de Dados, 2010. Disponível em: http://www.npd.ufes.br/faq/52#faq-expand-all. Acesso em 24 de Set. de 2013.