Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Felipe do Nascimento Machado

SEGURANÇA EM VOIP: Ameaças aos Sistemas VoIP

Rio de Janeiro

2007

Felipe do Nascimento Machado

SEGURANÇA EM VOIP: Ameaças aos Sistemas VoIP

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Paulo Henrique de Aguiar Rodrigues, UFRJ, Brasil

Rio de Janeiro

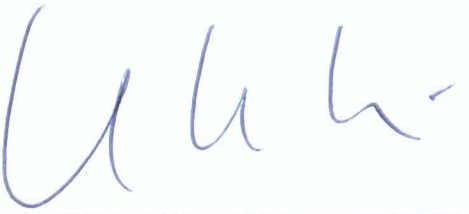
2007

Felipe do Nascimento Machado

SEGURANÇA EM VOIP: Ameaças aos Sistemas VoIP

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Novembro de 2007.



Prof. Paulo Henrique de Aguiar Rodrigues, UFRJ, Brasil

Para meus pais e meu irmão pelo apoio em todas as fases da minha vida.

AGRADECIMENTOS

Aos meus pais e meu irmão pelo carinho e compreensão.

Aos mestres, pelo conhecimento passado durante todo o curso e pela dedicação nas aulas, principalmente ao meu orientador, Paulo Aguiar.

RESUMO

MACHADO, Felipe do Nascimento. **SEGURANÇA EM VOIP: Ameaças aos Sistemas VoIP**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

A comunicação de voz sobre redes IP, conhecida como VoIP, vem crescendo muito. E com esse crescimento surgem novos negócios, novos produtos, fornecedores e também novos tipos de ataque. Como toda aplicação, VoIP se torna também vulnerável a ataques no mundo IP. O objetivo deste trabalho é identificar essas ameaças e estabelecer recomendações para diminuir a vulnerabilidade do VoIP.

ABSTRACT

MACHADO, Felipe do Nascimento. **SEGURANÇA EM VOIP: Ameaças aos Sistemas VoIP**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

Voice communication over IP networks, known as VoIP, is being increasingly adopted. With this growth new businesses new products, suppliers and also new types of network attacks. As any application, VoIP is also very vulnerable to these threats. This work enumerates these threats and establishes recommendations to minimize VoIP vulnerability.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AES	Advanced Encryption Standard
ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
EAP	Extensible Authentication Protocol
FDDI	Fiber-Distributed Data Interface
FIREWALL	Dispositivo de segurança de redes
HIDS	Host-based intrusion detection systems
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol
ITU-T	International Telecommunications Union
LAN	Local Area Network
MAC	Media Access Control
NAT	Network Address Translation
NIDS	Network intrusion detection systems
NTP	Network Time Protocol
QoS	Quality of Service
RADIUS	Remote Authentication Dial in
RFC	Request for Comment
RTCP	Real-Time Control Protocol
RTP	Real-Time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
SKEME	Secure Key Exchange Mechanism
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOFTPHONE	Telefone IP disponibilizado em software
SPIT	Spam over Internet Telephony
SRTP	Secure Real-Time Transport Protocol
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLAN	Virtual LAN
VoIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wide Area Network

SUMÁRIO

1 **INTRODUÇÃO**

Voz sobre IP (VoIP) é o termo utilizado para caracterizar o serviço que consiste em transmitir voz através do protocolo IP (Internet Protocol). De uma forma geral, isto significa enviar voz em formato digital dentro de pacotes de dados ao invés da utilização do tradicional protocolo de comutação de circuitos utilizado há décadas pelas companhias telefônicas.

O uso de voz sobre IP (VoIP) vem sendo uma das grandes metas de investimentos de fornecedores de soluções e usuários de telecomunicações nos últimos anos. Esta tecnologia abre um novo horizonte para as possíveis aplicações integrando-se voz e dados num mesmo equipamento terminal de usuário, aproximando pessoas geograficamente distantes, aumentando a interatividade de aplicativos e diminuindo os custos de comunicação, quando comparada às convencionais ligações telefônicas interurbanas.

A comunicação telefônica através de VoIP apresenta grandes vantagens sobre a telefonia convencional, sendo que a principal delas tem sido a redução de despesas que proporciona, visto que a rede de dados (e conseqüentemente VoIP) não está sujeita à mesma tarifação das ligações telefônicas convencionais, que é calculada em função de distâncias geodésicas e horárias de utilização estabelecidos pelas operadoras de telefonia. Outra grande vantagem de VoIP em relação à telefonia convencional para as operadoras é que a telefonia convencional está baseada em comutação de circuitos, que podem ou não estar sendo utilizados, enquanto VoIP utiliza comutação por pacotes, que possibilita um melhor aproveitamento dos recursos existentes (circuitos físicos e largura de banda).

Para se implantar uma solução VoIP em uma empresa é necessário fazer um projeto para identificar qual é a real necessidade da empresa, determinar qual

solução será utilizada, verificar se a empresa possui IP fixo ou IP dinâmico, o tamanho da banda de acesso, e determinar as características do tráfego de dados que possam vir a prejudicar a geração de VoIP.

Como muitas novas tecnologias, VOIP introduz riscos de segurança e oportunidades de ataques. VOIP tem uma arquitetura muito diferente dos tradicionais circuitos dedicados de telefonia, e estas diferenças resultam em questões de seguranças significativas. Baixo custo e uma maior flexibilidade estão entre algumas promessas de VOIP para as empresas, mas VOIP não pode ser implementado sem cuidadosas considerações de segurança. Administradores podem equivocadamente supor que como a voz digitalizada viaja em pacotes, eles podem simplesmente plugar componentes VOIP em suas redes já seguras e permanecerem seguros. Entretanto o processo não é tão simples.

Os principais protocolos VoIP são SIP – Session Initiation Protocol e o H.323. SIP é um protocolo da camada de aplicação baseado em texto, que utiliza o modelo “requisição-resposta”, similar ao HTTP, para iniciar sessões de comunicação interativa entre usuários. Já o padrão H.323 é parte da família de recomendações ITU-T (International Telecommunication Union) H.32x, que pertence à série H da ITU-T, e que trata de "Sistemas Audiovisuais e Multimídia". A recomendação H.323 tem o objetivo de especificar sistemas de comunicação multimídia em redes baseadas em pacotes e que não provêem uma Qualidade de Serviço (QoS) garantida. Além disso, estabelece padrões para codificação e decodificação de fluxos de dados de áudio e vídeo, garantindo que produtos baseados no padrão H.323 de um fabricante interopere com produtos H.323 de outros fabricantes [2]. Tanto SIP como H.323 utilizam o RTP para transporte de mídia [1].

Neste trabalho os conceitos, vulnerabilidades e recomendações apresentados estão relacionados ao protocolo SIP. A escolha desse protocolo foi devido a sua maior utilização em VoIP atualmente.

Embora sua implementação seja difundida, a tecnologia ainda está em desenvolvimento e está crescendo rapidamente, mas na maioria das vezes é implementado desajeitadamente oferecendo riscos de segurança.

A proposta deste trabalho é analisar os impactos das vulnerabilidades e como elas podem ser eliminadas em um ambiente VoIP, reduzindo ao máximo os riscos de segurança.

2 **Arquitetura SIP**

Uma rede SIP é composta por clientes, proxy e/ou servidor de redirecionamento, location server e um servidor de registro. No modelo SIP um usuário não está limitado a operar em um único host. O usuário informa sua posição a um servidor de registro que pode ser integrado com um proxy server ou servidor de redirecionamento.

Mensagens dos clientes devem ser roteadas por um proxy ou servidor de redirecionamento. O proxy server intercepta as mensagens dos clientes, contata o servidor local para resolver o nome em um endereço e encaminhar a mensagem para o cliente apropriado ou outro servidor. O servidor de redirecionamento tem a mesma funcionalidade de resolução, mas a responsabilidade da transmissão real é dos clientes. O servidor de redirecionamento obtém o atual endereço do destinatário no servidor local e retorna essa informação para o remetente original, que então envia sua mensagem diretamente para o endereço resolvido.

A Figura 1 descreve os procedimentos de mensagens para o estabelecimento de uma sessão SIP.

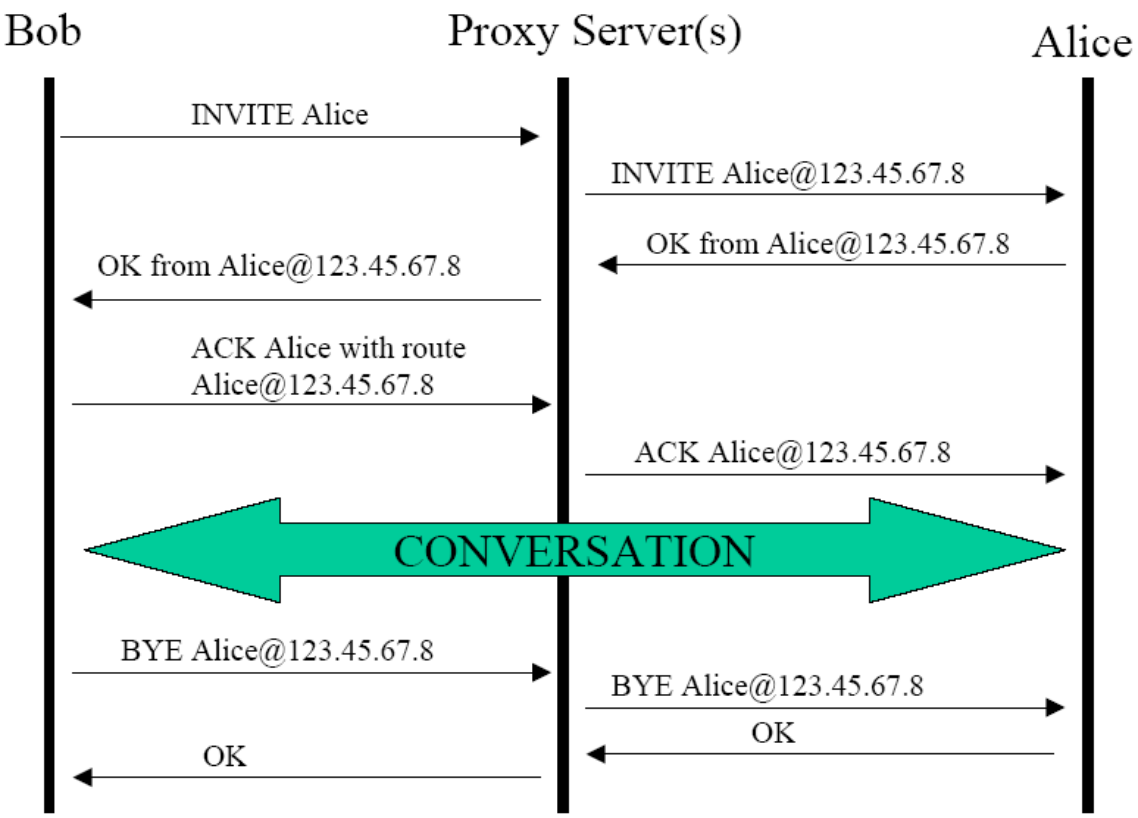


Figura 1 - Three-Way Handshake SIP / TCP [5]

Durante o processo de estabelecimento da sessão os detalhes da comunicação são negociados entre os clientes usando o Session Description Protocol (SDP), que contém os campos do codec usado, nome do chamador e etc.

Se Bob quer fazer uma chamada para Alice ele envia um INVITE para o proxy server que contém a informação SDP para a sessão, que é encaminhada então para Alice pelo proxy de Bob, possivelmente através do seu proxy server. Supondo que Alice quer falar com Bob, ela enviará um “OK” contendo as suas preferências da chamada no formato SDP. Então Bob responderá com um “ACK”. No SIP o SDP pode estar no ACK, de modo que o INVITE pode ser visto sem um protocolo específico. Depois que o “ACK” é recebido à conversação pode começar nas portas RTP / RTCP previamente acordadas [5].

3 **Características Gerais de Ataques**

Segurança em comunicações, principalmente de voz, é uma preocupação constante de corporações, empresários, políticos e diversos outros usuários de serviços públicos. Apesar de chamadas VoIP não utilizarem redes tradicionais de telefonia e, conseqüentemente não serem suscetíveis a ataques comuns como escutas telefônicas tradicionais, diversas outras vulnerabilidades existem e representam riscos não antes enfrentados. Por utilizar muitas vezes redes geograficamente dispersas, a disponibilidade do serviço muitas vezes não depende de uma única estrutura ou está abaixo de um único responsável. Ataques de negação de serviço, com o objetivo único de causar indisponibilidade podem ser executados de diversas formas e direcionados a diversos alvos. A confidencialidade das comunicações pode ser comprometida através da captura e análise do tráfego IP, transmitido na maioria das vezes sem qualquer criptografia ou proteção. Ataques de repetição, onde parte de uma chamada é capturada na rede e retransmitida ou ataques do tipo man-in-the-middle, onde um terceiro usuário ofensor se coloca entre o usuário legítimo e o serviço, se fazendo passar por ele, são apenas algumas possibilidades existentes.

Devido à convergência de voz e dados um ataque à rede principal de uma empresa pode prejudicar toda a infra de telecomunicação. A segurança na infra-estrutura de VoIP requer planejamento, análise e conhecimento detalhado sobre sua implementação.

Nem todas as ameaças estão presentes em todas as organizações, ou seja, isto vai depender dos equipamentos utilizados, das configurações existentes nesses

equipamentos, da informação trafegada na rede e como essa informação é tratada pelas aplicações, se são criptografadas.

A tabela abaixo descreve em níveis gerais que podem ser alvos de ataques em uma infra-estrutura VoIP:

Tabela 1 – Níveis Gerais de Ataque [3]

Vulnerabilidade	Descrição
Infra-estrutura IP	Vulnerabilidades em sistemas relacionados com VoIP podem comprometer toda a infra-estrutura IP.
Sistema operacional subjacente	Dispositivos VoIP herdam as mesmas vulnerabilidades que os sistemas operacionais ou firmware que rodam eles. Os sistemas operacionais são Windows e Linux.
Configuração	Na maioria dos dispositivos VoIP a configuração default vem com os serviços abertos. Esses serviços abrem portas e podem estar vulneráveis a ataques DoS, buffer overflows ou autenticações fracas.
Nível de Aplicação	Tecnologias imaturas podem ser atacadas para destruir o serviço ou para manipular. Um legado de aplicação tem problemas conhecidos.

Abaixo são listados alguns ataques direcionados a redes VoIP.

Denial of Service/Distributed Denial of Service (DoS/DDoS) - Esse tipo de ataque pode afetar qualquer rede baseada em IP. O impacto de um ataque DoS pode variar da degradação do serviço até a parada total do mesmo. Há várias classes de ataque DoS. Um tipo de ataque é quando simplesmente inundam a rede de múltiplas fontes

externas que é chamado de Distributed Denial of Service (DDoS) [3]. Esse tipo de ataque pode prejudicar muito o tráfego de voz que é extremamente sensível ao tempo e demora dos pacotes.

Ataques DoS são difíceis de serem defendidos, e como VoIP é um serviço baseado em IP esta suscetível a ataques DoS como qualquer outro serviço IP. Ataques DoS são particularmente efetivos contra serviços VoIP e outros serviços em tempo-real, porque esses serviços são muito sensíveis a variações na rede. Vírus e worms causam freqüentemente ataques DoS/DDoS devido ao grande poder que eles têm de gerar um grande número de pacotes e de se reproduzir e propagar rapidamente pela rede [3].

Um exemplo de um ataque de DoS [3] ocorre quando telefones IP deixam de funcionar ao receber pacotes UDP maiores que 65534 bytes na porta 5060.

Registration Hijacking - Esse ataque ocorre quando o atacante se faz passar por um usuário válido, alterando o cadastro para o seu próprio endereço.

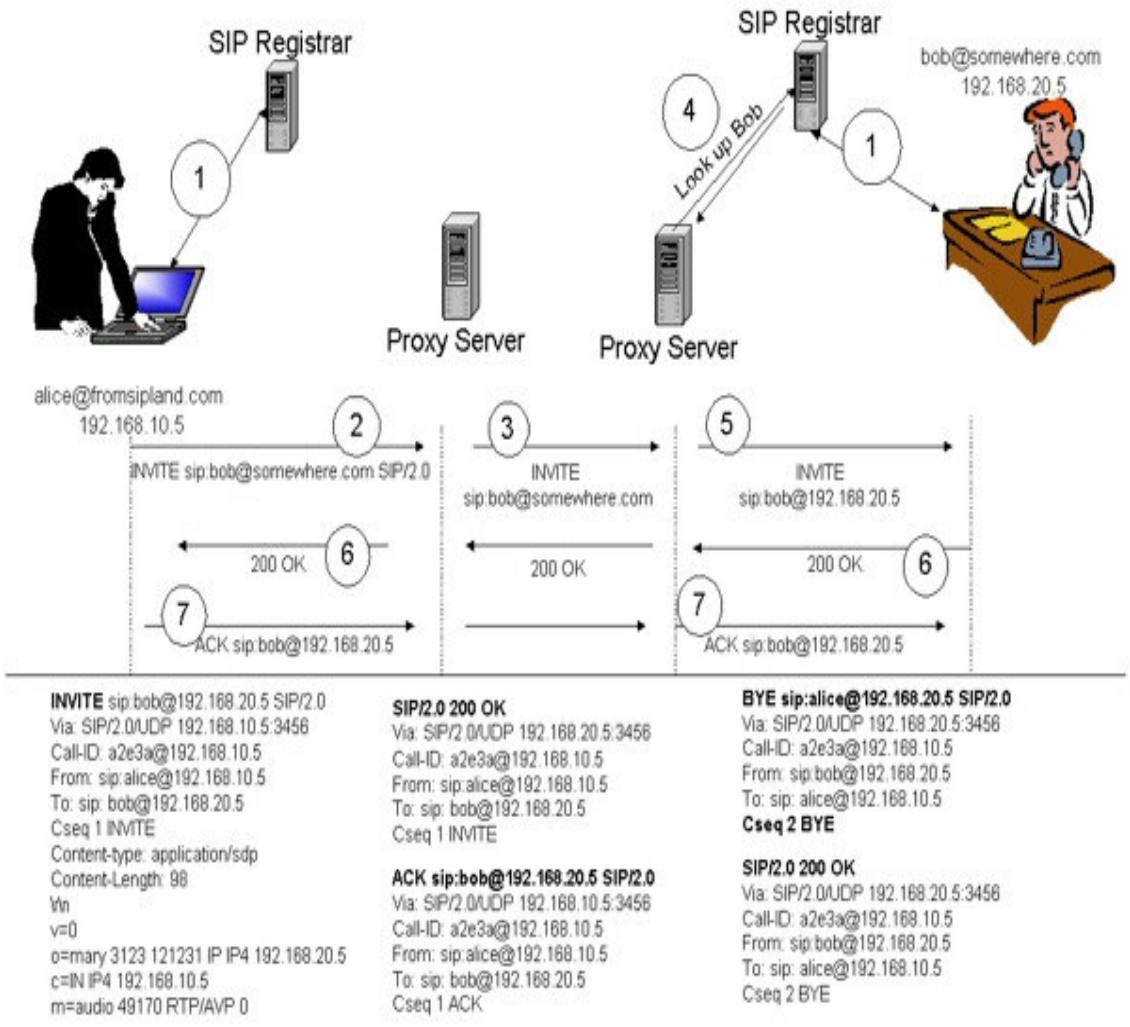


Figura 2 – Mensagens SIP [4]

No primeiro passo (1), o dispositivo do usuário (chamado de User Agent na terminologia SIP) se registra com o servidor de registro do domínio que é responsável por manter um banco de dados de todos os registros para o respectivo domínio. O registro é necessário para localizar e contatar o usuário. Quando Alice quiser falar com Bob, ela enviará um INVITE para o seu servidor proxy (2), que encaminham ao Servidor Proxy responsável pelo destino somewhere.com (3), que procura no servidor de registro a presença de Bob (4). Descoberto o IP onde Bob

está, o invite é encaminhado a este destino final (5). Quando Bob atende é retornado a confirmação (6) e Alice envia um ACK ao Bob.

A figura abaixo descreve a uma mensagem de registro válida e a resposta do servidor SIP, que é responsável por anunciar o ponto de contato do usuário. Isto indica que o dispositivo do usuário aceita chamadas [4].

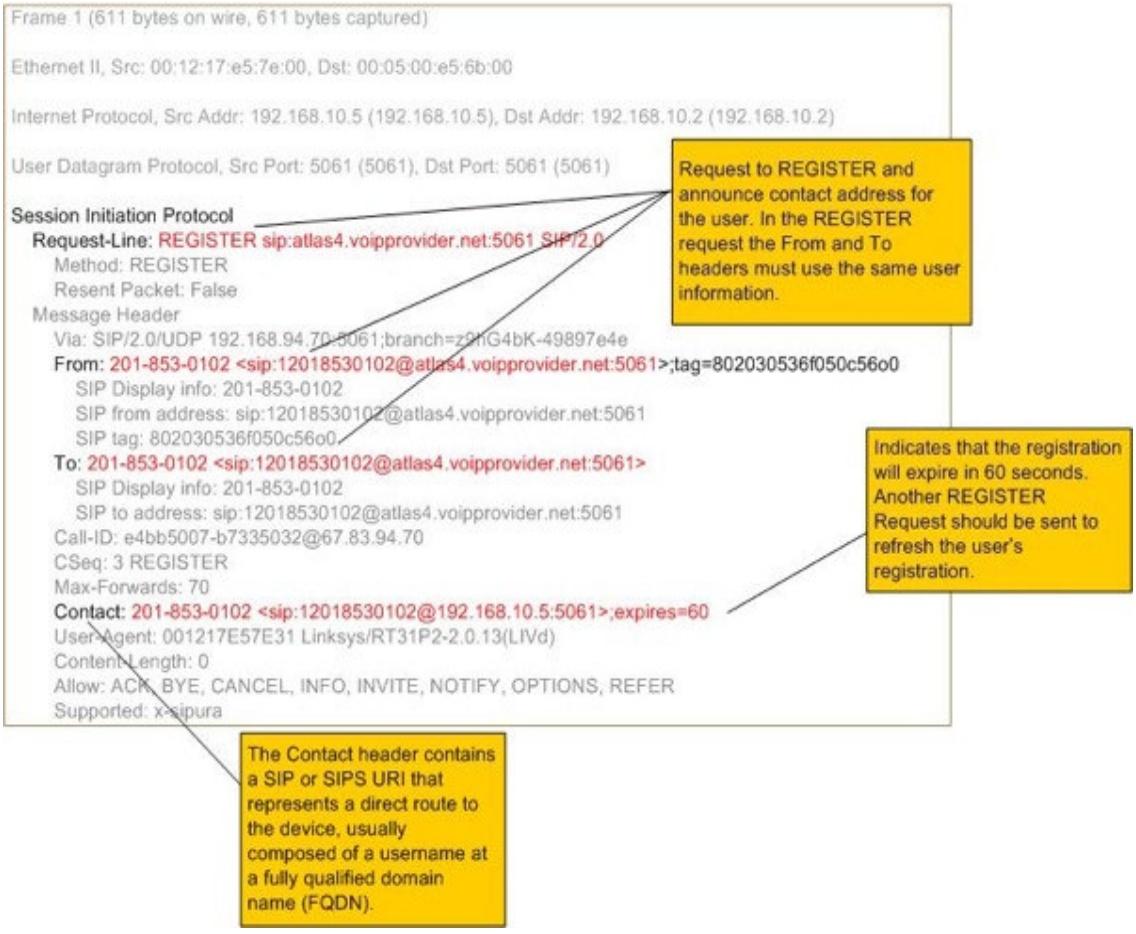


Figura 3 – Mensagem de registro SIP [4]

O REGISTER contém um cabeçalho que indica o endereço IP do dispositivo do usuário (para um VoIP soft ou hardphone). Quando um proxy recebe um pedido para processar uma chamada (INVITE), executará um lookup para identificar onde o respectivo usuário pode ser contatado. Neste caso, o usuário com o número de

telefone 201-853-0102 pode ser localizado no IP 192.168.94.70, logo, o proxy remeterá o INVITE para o endereço IP 192.168.94.70 [4].

A figura abaixo mostra uma versão modificada do REGISTER que é enviado pelo atacante:

Figura 4 - Mensagem de registro SIP modificada [4]

Neste pedido, todos os cabeçalhos e parâmetros da mensagem permanecem os mesmos exceto no cabeçalho do Contact. A informação alterada foi o endereço IP (192.168.1.3) que é o endereço do dispositivo do atacante [4].

A ferramenta usada para gerar este pedido foi o SiVuS como podemos ver abaixo:

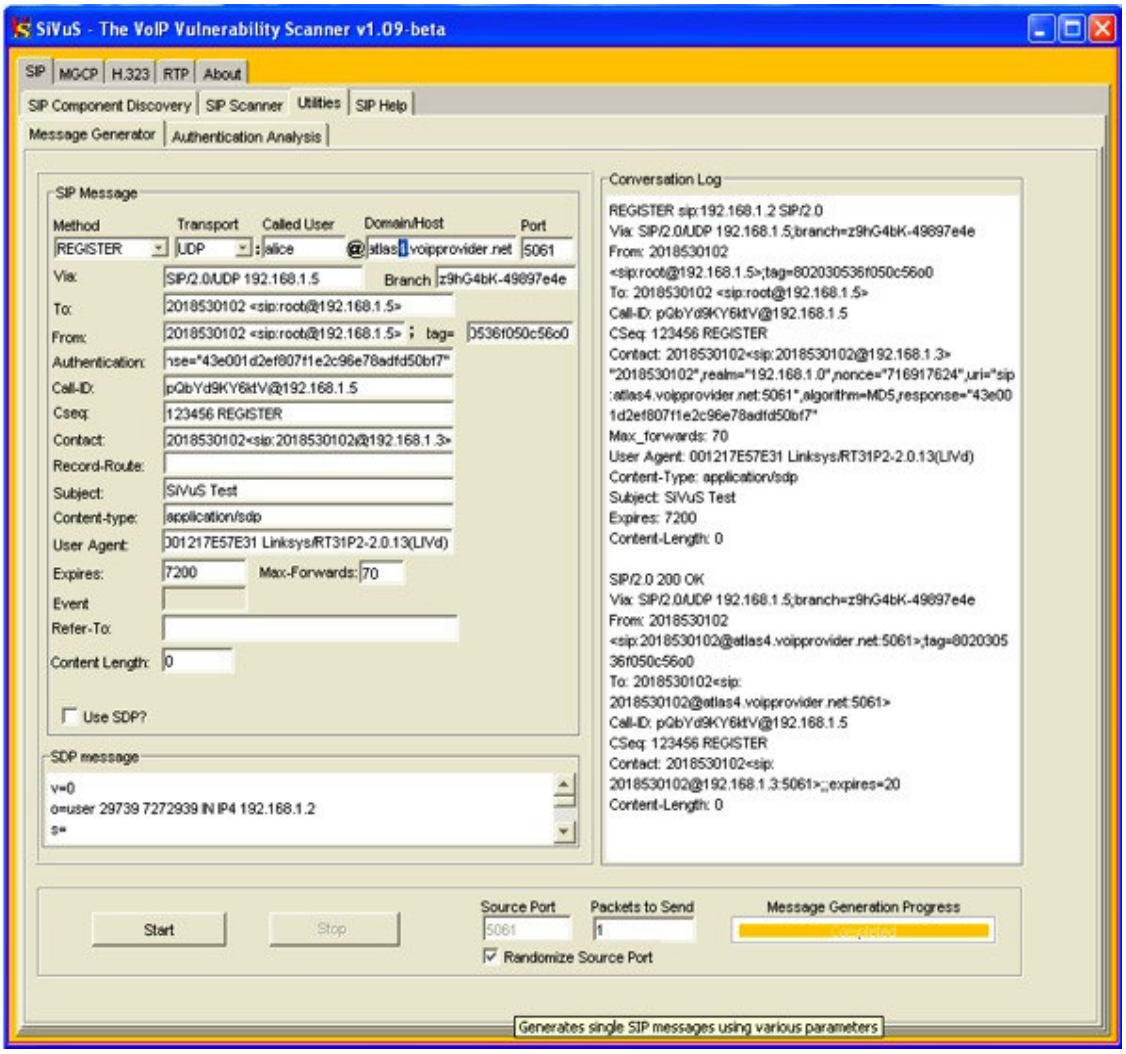


Figura 5 - Ferramenta Sivus [4]

Abaixo os passos do ataque:

- Desabilitar o registro do usuário legítimo.

- Executando um ataque DoS contra o dispositivo do usuário

  - Desregistrando o usuário (outro tipo de ataque), enviando repetidamente REGISTER num período mais curto de tempo (15 segundos) para anular o pedido do usuário legítimo.

- Enviar um REGISTER com o IP do atacante se passando como um usuário legítimo.

A figura abaixo demonstra o ataque:

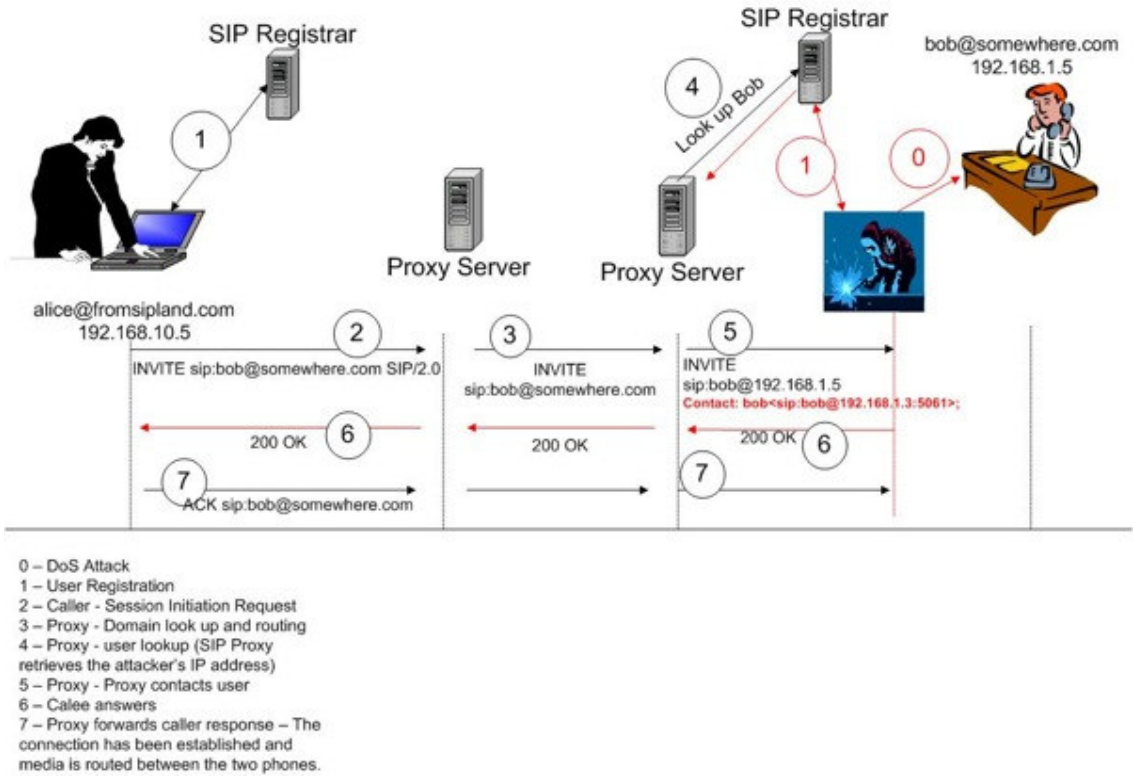


Figura 6 – Passos do ataque [4]

O atacante executa um ataque de DoS no equipamento de Bob não deixando ele se registrar e faz o registro se passando por Bob (0 e 1). A sessão continua normalmente até o passo 4 onde o servidor de registro retorna com o IP do atacante que está registrado como Bob no servidor de registro, o atacante então continua a sessão como se fosse o Bob respondendo com ACK (6). A conexão é estabelecida com o ACK de Alice para Bob (7) e o atacante consegue ter acesso à comunicação.

Call interception and Eavesdropping - *Call interception e Eavesdropping* são outras ameaças a redes VoIP. *Eavesdropping* é o método pelo qual um atacante pode monitorar uma chamada, mas não pode alterar o conteúdo da chamada. Já no ataque *Call interception,* o atacante além de monitorar pode alterar os dados e, em ambos os ataques, sem o conhecimento dos usuários. Um atacante que intercepta e armazena dados de chamadas VoIP pode fazer uso dos mesmos de modo malicioso [3].

Esses ataques são bem sucedidos na ausência de criptografia. Ataques nessa categoria buscam comprometer a integridade da mensagem em uma conversação. Estas ameaças demonstram a necessidade de autenticação do originador da chamada e verificar se o conteúdo da mensagem não foi alterado no caminho [3].

Abaixo um exemplo de Eavesdropping em 3 passos usando o ethereal, atualmente se utiliza o wireshark:

- Capturar e decodificar pacotes RTP.

- Analisar a Sessão

- Salvar e ouvir

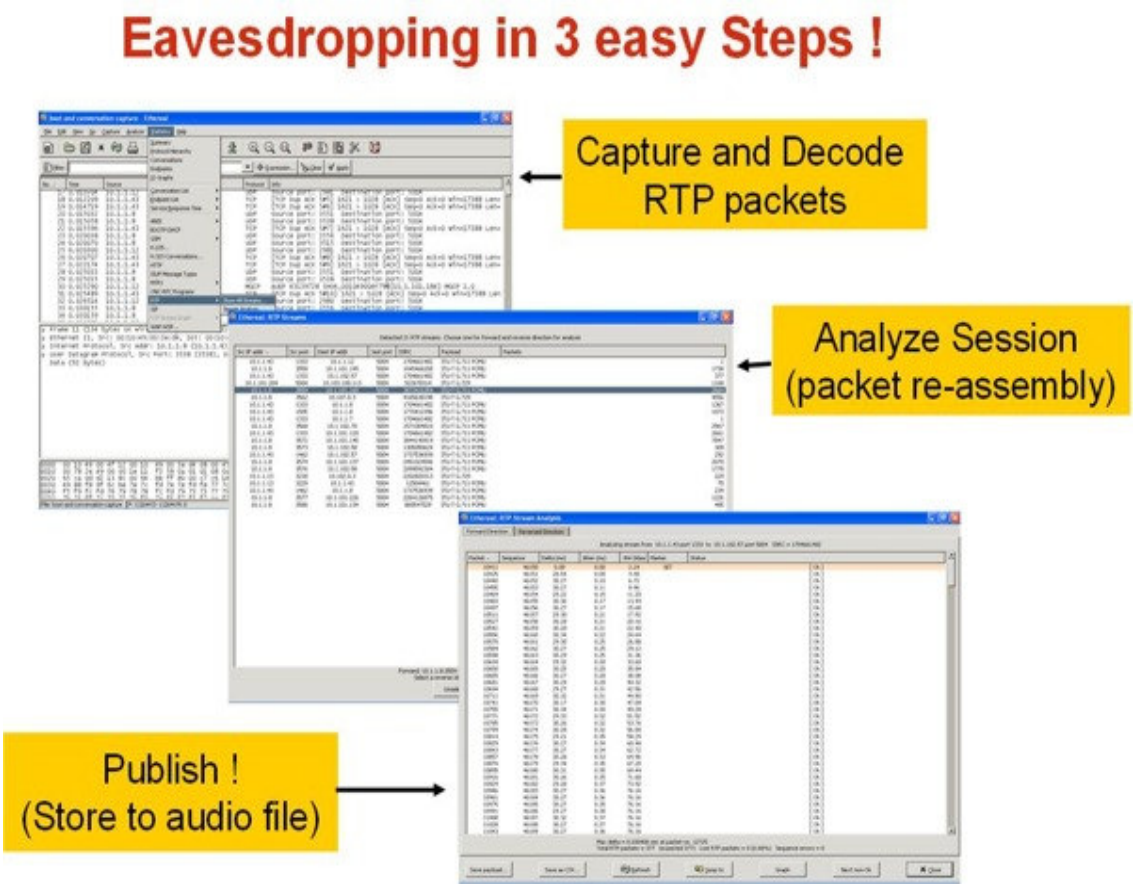


Figura 7 – Eavesdropping em 3 passos [4]

Algumas pessoas afirmam que esse ataque pode ser eliminado com o uso de switches que restringem o tráfico de broadcast para toda a rede, limitando quem pode acessar essas informações [4].

Este argumento pode ser descartado quando um ARP Spoofing é introduzido para lançar um ataque man-in-the-middle. O objetivo do ARP Spoofing é enganar os dispositivos da rede se fazendo passar por um deles [4].

A figura abaixo demonstra o uso da ferramenta Cain que tem a habilidade de executar um ataque man-in-the-middle e capturar o tráfico VoIP:

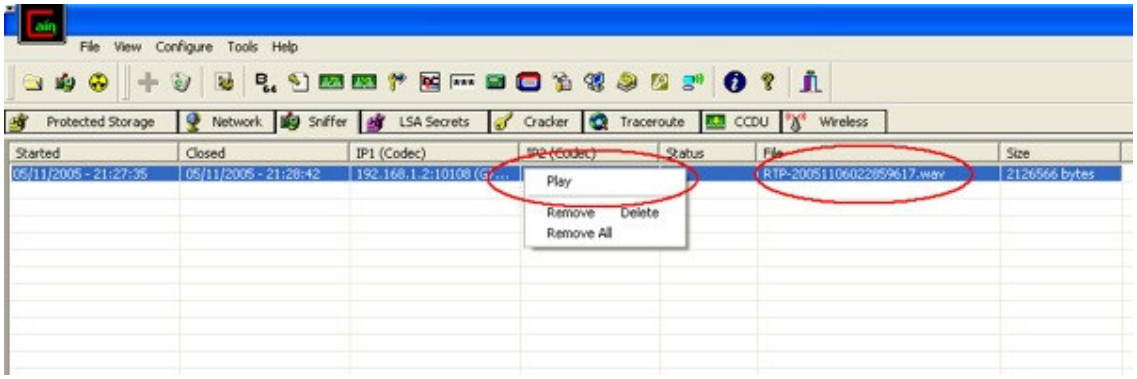


Figura 8 – Ferramenta Cain [4]

TFTP Server Insertion Attack - Este ataque também permite que um atacante mude a configuração de um telefone IP. É o mesmo princípio do ataque **DHCP Server Insertion Attack,** explorando a resposta do Trivial File Transfer Protocol Trivial File Transfer Protocol (TFTP) [5].

O uso de um Intrusion Detection System (IDS) pode filtrar esses pacotes maliciosos [5].

Switch Default Password Vulnerability - É comum em switches deixar usuários e senhas padrões como: admin/admin ou root/root. Se essa senha não for alterada isso se torna uma vulnerabilidade que permite a um atacante ter acessos administrativos e interceptar todo o tráfego das comunicações que estão sendo feitas. O atacante pode então monitorar não só chamadas VoIP como também descobrir outras informações como usuários e senhas de outras aplicações [5].

Essa vulnerabilidade pode parecer simples de se resolver, mas esse é um dos erros mais comuns feitos por usuários inexperientes [5].

Web Server interfaces - Tanto switches VoIP como terminais de voz provavelmente tem uma interface web para administração local ou remota. Um atacante pode

monitorar a rede por onde passam esses pacotes e se esses pacotes passam em claro usando http, ele pode conseguir informações confidenciais como usuário e senha para administração [5].

Para explorar essa vulnerabilidade o atacante requer acesso à rede local, se possível não utilizar HTTP para administração. Se for necessário o uso de um acesso web para administração remota, usar protocolo HTTPS (HTTP sobre SSL ou TLS), nesse tipo de conexão os dados são passados criptografados [5].

4 **Mecanismos de Segurança**

Das ameaças descritas acima, lembrando que são apenas algumas, percebemos que os serviços de segurança fundamentais para o protocolo SIP são: preservar a confidencialidade e integridade das mensagens, prevenir replay attacks ou spoofing, fornecer autenticação e privacidade para os participantes da sessão, e prevenir ataques DoS. O corpo das mensagens SIP requer separadamente serviços de segurança de confidencialidade, integridade e autenticação [1].

Melhor que definir novos mecanismos de segurança específicos para SIP, ele reusa modelos de segurança já existentes derivados do HTTP e SMTP.

A encriptação oferece os melhores meios de preservar a confidencialidade da sinalização - e pode também garantir que as mensagens não serão modificadas por nenhum intermediário malicioso. Entretanto, SIP request e response não podem ser encriptados fim-a-fim em sua totalidade por que os campos Request-URI, Route e VIA precisam ser visíveis aos proxies para que os SIP request e response sejam roteados corretamente.

As entidades SIP também têm a necessidade de identificar um ao outro de uma forma segura. Quando um cliente SIP confirmar a identidade do usuário a um UA ou um Proxy server, essa identidade deve de alguma maneira ser identificada. Procedimentos de autenticação e criptografia são fornecidos no SIP para cumprir essa exigência.

4.1 **Transport and Network Layer Security**

Segurança na camada de rede ou transporte encripta o tráfego de sinalização, garantindo confidencialidade e integridade da mensagem [1].

Muitas vezes certificados são usados no estabelecimento da segurança para camadas mais baixas, e estes certificados podem fornecer meios de autenticação em muitas arquiteturas [1].

Duas alternativas populares para fornecer segurança na camada de transporte e rede são, respectivamente TLS (RFC 2246) e IPSec (RFC 2401) [1].

IPSec é uma extensão do protocolo IP que visa ser o método padrão para o fornecimento de privacidade do usuário (aumentando a confiabilidade das informações fornecidas pelo usuário para uma localidade da internet, como bancos), integridade dos dados (garantindo que o mesmo conteúdo que chegou ao seu destino seja a mesma da origem) e autenticidade das informações ou *identity spoofing* (garantia de que uma pessoa é quem diz ser), quando se transferem informações através de redes IP pela internet. IPSec combina diferentes e diversas tecnologias para prover uma melhor segurança, como um mecanismo de troca de chaves de *Diffie-Hellman*; criptografia de chave pública para assinar as trocas de chave de *Diffie-Hellman*, garantindo assim a identidade das duas partes e evitando ataques do tipo *man-in-the-middle* (onde o atacante se faz passar pela outra parte em cada um dos sentidos da comunicação); algoritmos de encriptação para grandes volumes de dados, como o DES (*Data Encryption Standard*); algoritmos para cálculo de hash (resto de uma divisão, de tamanho fixo) com utilização de chaves, com o HMAC, combinado com os algoritmos de hash tradicionais como o MD5 ou SHA, autenticando os pacotes e certificados digitais assinados por uma autoridade certificadora, que agem como identidades digitais. IPSec é usado geralmente em arquiteturas em que um host ou um domínio tem uma relação de confiança com outro. IPSec normalmente é implementado no sistema operacional de um host ou em um Security Gateway que prove confidencialidade e integridade para todo o

tráfego recebido em uma determinada interface (Como em uma arquitetura de VPN) [1].

Em algumas arquiteturas IPSec não requer integração com aplicações SIP. IPSec é melhor utilizado quando adicionar segurança diretamente nos hosts SIP é mais complicado [1].

IPSec geralmente é usado em um cenário de VPN ou entre domínios SIP.

IPSec pode ser usado para fornecer autenticação, integridade e confidencialidade nas transmissões fim-a-fim e também hop-by-hop.

Um protocolo usado e recomendado para a gerência de chaves é o Internet *Key Exchange* (IKE), um protocolo híbrido baseado nos protocolos *Internet Security Association and Key Management Protocol* (ISAKMP), *Oakley Key Determination Protocol* (RFC 2412) e no *Secure Key Exchange Mechanism* for the Internet (SKEME). O Protocolo IKE fornece mecanismos automatizados para troca e gerência das chaves para IPSec. IKE é usado para negociar as Security Associations (SAs) para uso com sua própria troca de chaves (Fase 1) e para outros serviços como IPSec (Fase 2). IKE é particularmente usado no estabelecimento de VPNs [5].

TLS fornece segurança na camada de transporte. TLS é mais usado em arquiteturas nas quais a segurança hop-by-hop é requerida entre hosts sem nenhuma associação de segurança. Por exemplo, Alice confia no seu proxy server local que depois de uma troca de certificados decide confiar no proxy server local de Bob, e que confia em Bob, então Bob e Alice podem se comunicar seguramente [1].

TLS deve ser acoplado com uma aplicação SIP. Mecanismos de transporte são específicos passo-a-passo, onde cada passo se refere a uma interação UA-Proxy ou entre Proxies, assim um UA que envie requests sobre TLS para um Proxy server não tem nenhuma garantia que TLS será usado end-to-end [1].

RFC 3261 recomenda o uso de TLS para Proxies, Servidor de redirecionamento, Servidor de registro para proteger a sinalização SIP. O uso de TLS pelos UAs também é recomendado.

4.2 **HTTP Authentication**

SIP fornece um mecanismo de desafio que é baseado na autenticação http. Toda vez que um *Proxy Server* ou UA recebe um *request*, ele pode desafiar o originador do *request* que forneça a garantia de sua identidade [1].

Esse mecanismo não fornece integridade da mensagem ou confidencialidade, apenas autenticação [1]. Outras medidas descritas neste documento previnem atacantes ativos de modificarem SIP requests e responses.

4.3 **S/MIME**

Como foi visto mais acima, a criptografia de mensagens SIP fim-a-fim para manter a confidencialidade não é apropriado porque intermediários na rede (como Proxy servers) necessitam ver determinados campos no cabeçalho para rotear corretamente as mensagens e se esses intermediários são excluídos da associação de segurança, então as mensagens SIP serão essencialmente não roteáveis. Entretanto, S/MIME permite que SIP UAs encriptem MIME dentro de SIP, assegurando as mensagens fim-a-fim sem afetar o cabeçalho. S/MIME pode fornecer confidencialidade e integridade fim-a-fim para as mensagens bem como

autenticação mútua. Também é possível usar S/MIME para fornecer uma forma de integridade e confidencialidade para os campos do cabeçalho SIP com tunelamento da mensagem SIP [1], mas isso pode gerar um overhead adicional. O tunelamento das requisições e respostas não constituem um diálogo ou uma transação separada, eles são uma cópia da mensagem “externa” que é usada para verificar a integridade ou para fornecer informação adicional. Se um UA recebe um pedido que contém o tunelamento S/MIME no corpo da mensagem, ele deve incluir o mesmo tipo do S/MIME na resposta.

O SIP pode usar S/MIME para permitir mecanismos como distribuição de chave pública, autenticação e proteção da integridade ou confidencialidade na sinalização SIP.

A RFC 3261 recomenda que S/MIME seja usado pelos UAs. Além disso, se S/MIME for usado para “túnel” das mensagens é recomendado o uso de TCP por causa das mensagens maiores. Isto é para evitar problemas que podem ter com a fragmentação UDP.

4.4 **Confidencialidade da Mídia**

SIP por si só não considera a encriptação da mídia. O uso da encriptação RTP definida na RFC 3550 pode fornecer confidencialidade para a mídia. Outra opção para a segurança da mídia é o uso do SRTP (RFC 3711) descrito mais abaixo. Para o gerenciamento de chaves o SDP pode ser utilizado (RFC 2327).

4.5 **Secure Real-Time Transport Protocol (SRTP)**

RTP é usado geralmente para transmissão de áudio/vídeos em tempo real nas aplicações de telefonia na Internet. RTP é considerado inseguro quando não é utilizado nenhum tipo de proteção com ele [7].

O SRTP é um perfil do RTP oferecendo não somente confidencialidade, mas também autenticação da mensagem para o tráfego RTP bem como RTCP. SRTP era um padrão IETF, foi liberado como RFC 3711 em Março de 2004 [7].

SRTP fornece uma estrutura para encriptar e autenticar mensagens de RTP e RTCP [7].

AES é o algoritmo padrão, se for utilizada a encriptação. O tamanho padrão da chave de autenticação se sessão é de 160 bits [7].

SRTP fornece um aumento na segurança:

- Confidencialidade para RTP bem como para o RTCP encriptando os respectivos payloads.
- Integridade para os pacotes RTP e RTCP.
- Possibilidade de atualização das chaves de sessão periodicamente.
- Uma estrutura que permite atualizações com novos algoritmos de criptografia.
- Segurança para aplicações unicast e multicast.

5 **Exemplo do Funcionamento dos Mecanismos de Segurança**

Tradicionalmente, protocolos de segurança incluem facilidades para aceitar os mecanismos usados, algoritmos, e outros parâmetros de segurança. Isto é feito para adicionar flexibilidade, desde que diferentes mecanismos são usados em diferentes cenários. Também, a evolução dos mecanismos de segurança introduzem freqüentemente novos algoritmos, ou descobrem problemas em mecanismos já existentes, fazendo da negociação dos mecanismos uma necessidade.

De acordo com a RFC 3329 [6] a figura abaixo ilustra como um mecanismo de segurança trabalha.

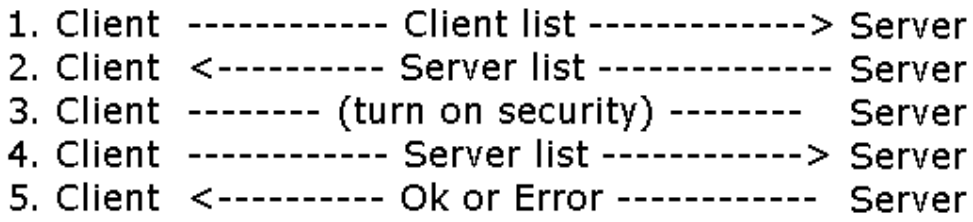


Figura 9 Passos do Mecanismo de Segurança [6]

Passo 1 – Os clientes que desejam usar esta especificação podem enviar uma lista dos mecanismos de segurança suportados no primeiro request para o servidor.

Passo 2 – Os servidores que desejam usar esta especificação podem desafiar o cliente a executar um procedimento. Os mecanismos e os parâmetros de segurança suportados pelo servidor são enviados durante esse desafio.

Passo 3 – O cliente então procede para selecionar o mecanismo de segurança de sua preferência e que eles tem em comum e então esse mecanismo é ativado.

Passo 4 – O cliente contata o servidor outra vez, mas agora usando o mecanismo de segurança. A lista de mecanismos suportados pelo servidor é enviada com uma resposta para o desafio.

Passo 5 – O servidor verifica a sua própria lista de mecanismos de segurança para se assegurar que a lista original não esteja modificada.

Este procedimento é "*stateless*" para os servidores (a menos que o mecanismo de segurança tenha que manter algum estado).

As listas dos clientes e servidores são estáticas, mas podem ser mantidas diversas listas estáticas, uma para cada interface, por exemplo.

6 **Recomendações**

Para combater as ameaças aos sistemas VoIP algumas recomendações devem ser seguidas. Sua organização pode já ter muita das ferramentas e da infra-estrutura necessária para fornecer soluções adequadas de segurança em VoIP, logo não tente reinventar a roda.

Elementos SIP podem e devem também implementar IPSec ou outros protocolos de segurança [3].

Quando um UA tenta contactar um Proxy server ou Servidor de redirecionamento, o UA deve iniciar uma conexão TLS que enviará as mensagens SIP. Em algumas arquiteturas UAs também podem receber requests sobre uma conexão TLS [3].

Abaixo serão apresentadas as melhores práticas para segurança em VoIP.

6.1 **Segurança Física**

A Segurança Física é parte essencial de todo ambiente de segurança. A Segurança Física se refere à proteção dos locais e dos equipamentos (e toda informação e softwares que estão dentro deles) contra roubos, invasões, vandalismo, desastres naturais e danos acidentais (por exemplo, panes elétricas, altas temperaturas e derramamento de café) [3].

A menos que o tráfego de VoIP seja criptografado, qualquer um com acesso físico na LAN de uma organização pode conectar a rede e utilizar ferramentas de monitoração e seqüestrar chamadas VoIP. Embora as linhas telefônicas convencionais também podem ser monitoradas quando se tem acesso físico, a

maioria das empresas tem mais pontos de rede e podem ser conectados mais facilmente sem despertar suspeita [3].

Mesmo que seja feita a encriptação dos dados, o acesso físico aos servidores e gateways VoIP permite a um atacante fazer análise do tráfego (isto é, quem esta se comunicando e com que freqüência se comunica). O controle físico deve ser feito para restringir o acesso aos componentes de rede VoIP. As medidas de Segurança Física incluem sistemas de controle de acesso, travas, “barreiras” e guardas são a primeira linha de defesa [3].

6.2 **Auditagem de Segurança**

Todos os ativos em uma rede VoIP devem seguir um procedimento padrão de configuração e serem sujeitados a um Hardening antes de serem conectados à rede. Uma equipe dentro da empresa deve ser responsável por fazer esse Hardening em Windows, Linux, AIX, Unix e outros sistemas operacionais ou dispositivos VoIP. Esse grupo deve definir este procedimento e assegurar que os ativos estão seguros e com as últimas atualizações aplicadas e fazer essa verificação periodicamente [3].

6.3 **Ferramentas de Gerenciamento de Rede**

As ferramentas que são usadas na gerência de redes de dados também devem ser usadas em redes convergidas de dados e VoIP. Essa é uma das vantagens de uma rede convergida. Essas ferramentas podem necessitar de algum tipo de atualização para trabalhar com redes VoIP. Se possível o tráfego de gerência deve estar em uma rede à parte. Algumas ferramentas são recomendadas para o gerenciamento. MRTG é uma ferramenta baseada em SNMP para visualizar o tráfego e as tendências da rede. Também pode ser usado para monitorar outros

dispositivos baseados em SNMP. Big Brother é outra boa ferramenta e “livre” que permite gerenciar rapidamente o estado de aplicações e serviços remotos [3].

6.4 **Confirmação do Usuário**

Um atacante pode comprometer uma rede e seqüestrar chamadas VoIP podendo escutar e alterar a conversação que trafega na chamada. Ele pode se fazer passar por uma outra pessoa, fazendo com que o usuário que esteja do outro lado da ligação passe informações confidenciais e até mesmo fazer com que ele execute arquivos maliciosos permitindo ao atacante obter controle do computador remotamente [3].

A maneira de impedir esse ataque é identificando as pessoas ou dispositivos que estão nos dois lados da conversação. O nome disso é autenticação [3].

Autenticação é uma medida de confiança. A Autenticação em rede geralmente é baseada em algum segredo compartilhado (se você sabe o segredo é autenticado) ou por métodos de certificados com chaves públicas (você prova sua identidade possuindo a chave privada) [3].

A figura abaixo mostra que usuários e dispositivos devem ser autenticados. Eles são freqüentemente relacionados, mas são processos diferentes. Autenticação pode ser separada da autorização:

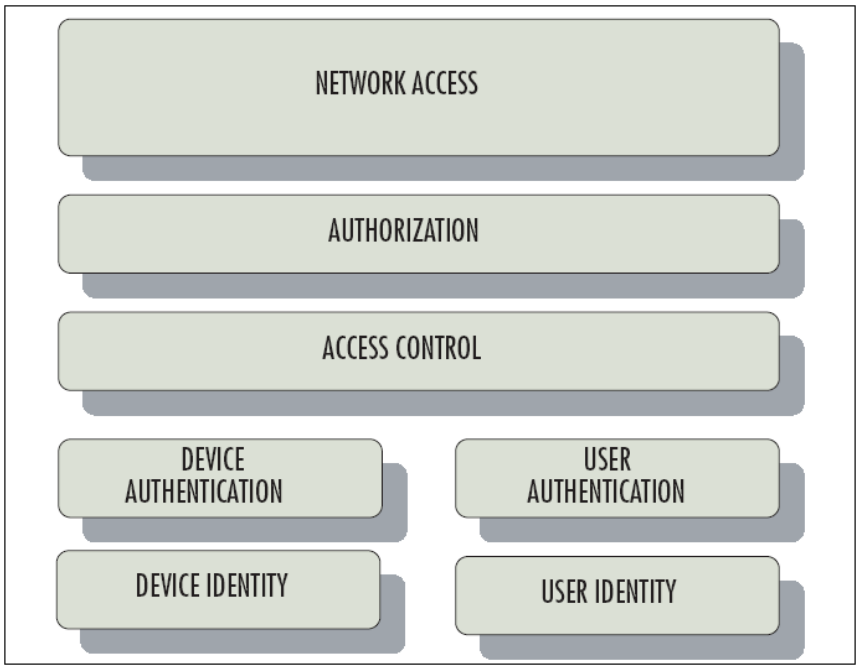


Figura 10 – Autenticação de usuários e dispositivos [3]

802.1x restringe clientes desautorizados de se conectar na LAN. O cliente deve primeiro se autenticar em um servidor de autenticação, tipicamente um servidor RADIUS, antes que a porta do switch esteja disponível e o cliente possa acessar a rede. EAP (Extensible Authentication Protocol) é um protocolo de autenticação que fornece uma infra-estrutura de múltiplos métodos de autenticação [3].

A recomendação é que 802.1x seja utilizado para autenticação em dispositivos e usuários. EAP-TLS deve ser usado se uma Public Key Infrastructure (PKI) existir; se não, a recomendação é EAP-PEAP para os ambientes baseados em clientes Windows, e EAP-PEAP ou EAP-TTLS para os outros [3].

6.5 **Network intrusion detection systems (NIDS) e Host-based intrusion detection systems (HIDS)**

Os NIDS são projetados para alertar administradores quando tráfego ilegítimo ou malicioso é detectado. O tráfego malicioso pode consistir em um Worm ou um código de um exploit que esteja sendo executado, quanto ao ilegítimo pode ser uma navegação em sites pornos ou conexões peer-to-peer (P2P) que não são permitidas pela política de segurança atual. Os HIDS operam com informações coletadas de computadores individuais, eles são IDS de host. Isso permite que o HIDS analise as atividades de um host e monitore em um nível mais detalhado, podendo, por exemplo, determinar que processos e/ou usuários estão envolvidos em atividades maliciosas [3].

O uso de ambos é recomendado. O NIDS deve ser distribuído para monitorar o tráfego de rede, geralmente em pontos onde passa a maior parte do tráfego interligando diferentes redes. É preciso também definir um processo de escalonamento quando um evento de segurança for detectado [3].

HIDSs devem ser instalados em todos serviços/host classificados como críticos na infra-estrutura de VoIP. Estes incluem servidores (DNS, DHCP, RADIUS, NTP, etc...), gateways, proxies, servidores de banco de dados, servidores de diretórios e firewalls. Relatórios dos HIDS devem ser monitorados regularmente e se possível em tempo real [3].

6.6 **Log e SNMP**

O Syslog (system logger) fornece a opção de se enviar eventos dos logs através da rede para um servidor Syslog, podendo armazenar os logs de diversas

máquina em um único lugar. As mensagens nativas do Syslog não são encriptadas, logo, esse sistema deve ser utilizado apenas em redes internas. Algumas soluções oferecem criptografia no serviço Syslog, é altamente recomendável o seu uso [3].

Os telefones IP podem ser reconfigurados e reiniciados através de comandos SNMP. SNMP trabalha com comunidades e essas comunidades são como senhas para acesso aos dispositivos através de SNMP. Nas versões 1 e 2 do SNMP as comunidades são simples de serem descobertas e na maioria das vezes os administradores deixam a comunidade padrão chamada public. Mensagens SNMP e de Syslog podem ser “seqüestradas” e oferecer a um atacante informações preciosas como configurações dos dispositivos e informações de usuários conectados podendo fazer com que o atacante eleve seus privilégios na rede usando essas informações [3].

Recomenda-se o uso da versão 3 do SNMP para monitoração e configuração das redes VoIP. Se não for possível o uso da versão 3 é essencial restringir o acesso ao SNMP apenas para os endereços realmente necessários (Uso de ACLs) e a mudança do nome padrão public para outro qualquer. Evitar também o uso de comunidades com permissões de leitura e escrita [3].

6.7 **Testes de Invasão e Vulnerabilidade**

Estes testes são conduzidos por uma equipe que emula e analisa um ataque real em sistemas para descobrir maneiras de burlar a segurança implementada obtendo acesso a serviços não autorizados, descobrir informações sensíveis e/ou simular danos aos sistemas negando serviços [3].

Testes de segurança devem ser executados regularmente se possível num período trimestral ou em qualquer mudança feita na infra-estrutura. No geral existem 2 tipos de testes: internos e externos. Os testes podem ser feitos por pessoas internas ou por empresas especializadas. Esses testes têm múltiplas finalidades: “salvar” o dinheiro da empresa, ajuda a aprender mais sobre o ambiente de rede, mantém a equipe sempre atualizada sobre vulnerabilidades e os últimos tipos de ataques lançados na Internet [3].

6.8 **VLANs**

É recomendável a separação das redes de dados das redes de voz para impedir que problemas na rede de dados afetem a rede de voz e vice-versa. VLANs criam uma segmentação lógica na rede e novos domínios de colisão. O uso das VLANs remove a necessidade de se organizar e controlar PCs ou Softphones pela posição física [3].

A segmentação da rede com VLANs, criando domínios de transmissão independentes, reduz o tráfego geral, balanceando a rede e diminuindo o estrago de ataques DoS [3].

6.9 **QoS**

Na ausência de QoS, as redes de dados operam na base de best-effort (melhor-esforço), o que significa que todo tráfego seja ele de dados, voz ou qualquer outro tem a mesma prioridade no momento da entrega. O mesmo ocorre quando temos um congestionamento na rede, tráfego de dados e de voz tem a mesma chance de serem descartados, em uma rede que trafega dados e voz esse procedimentos é prejudicial ao tráfego de voz e a qualquer outro que seja em tempo

real. É preciso dar uma prioridade aos pacotes de voz para que a qualidade não seja afetada [3].

Em redes VoIP é preciso usar QoS para não afetar a qualidade, mas algumas medidas de segurança em VoIP podem prejudicar o desempenho de uma conexão afetando a qualidade do serviço. A maior parte dos atrasos causados pela segurança implementada vem da autenticação na troca de chaves [3].

6.10 **Firewalls**

Firewalls fornecem uma demarcação física e lógica entre a parte interna e externa de uma rede. A maioria dos firewalls tem certas características, como:

1 – É o único ponto entre duas ou mais redes onde todo o tráfego deve passar

2 – Pode ser configurado para permitir ou negar IP ou qualquer outro protocolo

3 – Permite logar regras para posterior auditoria

4 – Fornece função de NAT

5 – O Sistema Operacional é seguro

6 – Fornece opção de uso de VPN

7 – Se por algum motivo o firewall parar nenhum tráfego é permitido

A tabela abaixo fornece uma lista dos serviços e portas mais comuns utilizados em VoIP:

Tabela 2 – Serviços e Portas [3]

Serviços	Portas
Skinny	TCP 2000-2002
TFTP	UDP 69
MGCP	UDP 2427
Backhaul (MGCP)	TCP 2428
Tapi/Jtapi	TCP 2748
HTTP	TCP 8080/80
SSL	TCP 443
SCCP	TCP 3224
Transport traffic	16384-32767
SNMP	UDP 161
SNMPTrap	UDP 162
DNS	UDP 53
NTP	UDP 123
LDAP	TCP 389
H.323RAS	TCP 1719
H.323 H.225	TCP 1720
H.323 H.245	TCP 11000-11999
H.323 Gatekeeper Discovery	TCP 1718
SIP	TCP 5060
SIP/TLS	TCP 5061

Filtragem de firewall é necessária para gerir protocolos de rede eficazmente nos dias de hoje. Os tradicionais filtros de pacotes não conseguem lidar com protocolos de dados complexos tais como streaming IP e videoconferência, que utilizam múltiplas portas UDP e TCP e complicados esquemas de inicialização. Para

ser eficaz, a inspeção de firewall deve ter conhecimento específico dos protocolos que gere [3].

É recomendável que todo o tráfego remoto de voz seja encapsulado em uma VPN.

7 **REFERÊNCIAS**

[1] RFC 3261. **SIP: Session Initiation Protocol**. Disponível em ftp://ftp.rfc-editor.org/in-notes/rfc3261.txt. Acesso em Abril de 2007.

[2] Wikipedia. H.323. Disponível em http://pt.wikipedia.org/wiki/H.323. Acesso em Abril 2007.

[3] PORTE, T.; BASKIN B.; CHAFFIN L.; CROSS M.; KANCLIRZ J.; ROSELA A.; SHIM C.; ZMOLEK A. **Pratical VoIP Security.** Disponível em http://www.syngress.com/catalog/?pid=3725. Acesso em Junho 2006.

[4] THERMOS, P. **EXAMINING TWO WELL-KNOWN ATTACKS ON VOIP**. Disponível em http://www.voiponder.com/posts/examining_two_well_known_attacks_on_voip/. Acesso em Maio 2006.

[5] KUHN R.; WALSH T.; FRIES S. **Security Considerations for Voice Over IP Systems.** Disponível em http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf. Acesso em Maio 2006.

[6] RFC 3329. **Security Mechanism Agreement for the Session Initiation Protocol (SIP)**. Disponível em ftp://ftp.rfc-editor.org/in-notes/rfc3329.txt. Acesso em Abril de 2007

[7] RFC 3711. **The Secure Real-Time Transport Protocol (SRTP)**. Disponível em ftp://ftp.rfc-editor.org/in-notes/rfc3711.txt. Acesso em Abril de 2007

[8] VILLAR, F. **Vulnerabilidades do Windows I: Ataques básicos.** Disponível em http://www.mabsp.com/recursos/ppt/APRES_MABSP_VulWin1_060606.pdf. Acesso em Agosto 2006.

[9] COLLIER, M. D. **Enterprise Telecom Security Threats.** Disponível em http://download.securelogix.com/library/Enterprise_Telecom_Security_Threats_Draft_10-12-04.pdf. Acesso em Setembro 2006.

[10] GLOBAL KNOWLEDGE. **Enterprise VoIP Security: Potential Threats and Best Practices.** Disponível em http://www.globalknowledge.com/training/whitepaperlist.asp?pageid=502&country=United+States&translation=English. Acesso em Maio 2006

[11] KUHN, R. **Voice Over Internet Protocol (VOIP) SECURITY.** Disponível em http://csrc.nist.gov/ispab/2004-06/kuhn_2004_06_ispab.pdf. Acesso em Maio 2006.

[12] MATERNA, B. **A Proactive Approach to VoIP Security: Understanding VoIP security requirements, threats and architectures.** Disponível em http://www.it-observer.com/pdf/dl/proactive_approach_voip_sec.pdf. Acesso em Junho 2006.

[13] NETCLARITY. **Securing Your VoIP.** Disponível em http://www.neisg.org/Archive/2005/10VoIP/SecuringYourVoIP.pdf. Acesso em Outubro 2006.

[14] THALHAMMER, J. **Security inVoIP-Telephony Systems.** Disponível em http://www.iaik.tugraz.at/teaching/11_diplomarbeiten/archive/thalhammer.pdf. Acesso em Maio 2006.

[15] DISA. **VOICE OVER INTERNET PROTOCOL (VOIP) SECURITY TECHNICAL IMPLEMENTATION GUIDE.** Disponível em http://iase.disa.mil/stigs/stig/voip_stig_v1r1.pdf. Acesso em Junho 2006.