Alison da Cruz

Caracterização e Identificação de Chamadas Maliciosas em PABX IP

São José, Julho de 2018

Alison da Cruz

Caracterização e Identificação de Chamadas Maliciosas em PABX IP

Monografia apresentada à Coordenação do Curso Superior de Tecnologia em Sistemas de Telecomunicações do Instituto Federal de Santa Catarina para a obtenção do diploma de Tecnólogo em Sistemas de Telecomunicações.

Orientador:

Prof. Dr. Marcelo Maia Sobral

CURSO SUPERIOR DE TECNOLOGIA EM SISTEMAS DE TELECOMUNICAÇÕES

INSTITUTO FEDERAL DE SANTA CATARINA

São José – SC

Julho de 2018

Resumo

Inúmeros são os benefícios em se utilizar a telefonia IP, comprovado pelo elevado índice de convergência de telefonia digital e analógica para cenários que utilizam o Voip. Em contrapartida é preciso que haja uma preocupação relacionada com a integridade, confiabilidade e segurança dos ambientes que usam essa tecnologia. Tem aumentado consideravelmente as tentativas de ataques e invasões que buscam usar a infraestrutura existente para efetuar chamadas, acarretando assim prejuízos para as empresas e operadoras de telefonia IP.

Sabendo disso justifica-se a proposta desse trabalho que é realizar um estudo de identificações de padrões anômalos e hostis de mensagens do Protocolo SIP (*Session Initiation Protocol*), recebidas de um PABX IP através de uma rede de VoIP. Com isso, busca-se verificar se a identificação dos padrões de tentativas de invasões possibilita reduzir os efeitos dos ataques recebidos nas redes de Telefonia IP. Para isso serão coletados logs reais com equipamentos IP que sofrem tentativas de invasão no dia a dia.

Tendo em mão os logs, será feito a análise de pacotes SIP procurando reconhecer padrões que identifiquem ataques através de informações disponíveis no cabeçalho SIP. A ferramenta utilizada para análise será o software gratuito Wireshark que permite a coleta e especificação de filtros para futura análise de pacotes de tráfego na rede.

1 Introdução

A telefonia tem conectado as pessoas ao redor do mundo por muitos anos, desde a invenção do telefone foi possível a realização da comunicação em tempo real entre duas pessoas que podem estar em cidades ou até mesmo continentes diferentes, isso tudo por meio do tráfego de voz em uma rede de telecomunicações.

Com o avanço exponencial da Internet as inovações relacionadas a comunicação tem se expandido. Com essa evolução foi possível a realização de chamadas telefônicas entre dois ou mais pontos através da internet. A conversação em tempo real pela Internet, também conhecida como VoIP (Voice Over Internet), surgiu na década de 90 e para o usuário final é semelhante ao tradicional serviço telefônico por comutação de circuitos. No entanto, nesse tipo de serviço, os usuários se comunicam por meio do envio de voz codificada em pacotes de dados, que são transportados através de redes IP (Internet Protocol) (Ferdous, 2014).

A telefonia IP oferece diversos benefícios e soluções de baixo custo para os usuários da telefonia, tais como: vicissitude da integração de voz e dados na mesma infraestrutura; chamadas sem custo dentro do meio VoIP; mobilidade com a utilização de softphones em um computador ou até mesmo em um celular, entre outras possibilidades. Por essas razões, no decorrer dos anos, cada vez mais empresas substituem seus antigos sistemas de telefonia analógicos ou digitais por um sistema baseado em voz sobre IP.

Porém, o VoIP é vulnerável a escutas, o que possibilita tentativas de invasões se sua infraestrutura não for bem protegida. Os ataques ocorrem quando pessoas mal-intencionadas buscam o PABX através de ferramentas (softwares) que inicialmente identificam que naquele endereço IP ou FQDN (Fully Qualified Domain), existe um PABX IP na rede. Posteriormente, procuram descobrir por usernames/hosts e senhas para então usufruir dos recursos disponíveis no PABX, geralmente realizando chamadas para outras cidades ou até mesmo outros países. Atualmente as próprias operadoras buscam orientar os clientes a reforçar a segurança da rede a fim de evitar ou minimizar essas invasões.

1.1 Objetivo geral

O objetivo geral deste trabalho de conclusão de curso é realizar um estudo de padrões anômalos e hostis de mensagens do Protocolo SIP (*Session Initiation Protocol*), recebidas por um PABX IP.

1.2 Objetivos específicos

Para a realização deste projeto tem-se como seguintes objetivos específicos:

- Classificar padrões de chamadas anômalas ou maliciosas
- Verificar a possibilidade de minimizar tentativas de ataques tendo reconhecido os padrões utilizados

1.3 Proposta de trabalho

Não há dúvidas de que é preciso reforçar segurança dos sistemas de telefonia VOIP para minimizar e prevenir as tentativas de invasão e ataques. Ações eficazes devem ser tomadas pois caso contrários, essas incursões maliciosas podem acarretar enormes prejuízos para as empresas. Para agir na causa e propor soluções que impeçam os ataques é preciso identificar os padrões utilizados por esses servidores mal-intencionados.

A proposta do trabalho em questão é realizar um estudo de identificações de padrões anômalos e hostis de mensagens do Protocolo SIP (*Session Initiation Protocol*), recebidas de um PABX IP através de uma rede de VoIP. Para isso serão coletados arquivos de captura com o fluxo de dados (pcap) reais com equipamentos IP que sofrem tentativas de invasão no dia a dia. Serão capturados os pacotes que chegam na interface de rede do PABX/Terminal IP que possui acesso à internet.

Tendo em mão os logs, será feito a análise de pacotes SIP procurando reconhecer padrões que identifiquem ataques através de informações disponíveis no cabeçalho SIP. A ferramenta utilizada para análise será o software gratuito Wireshark que permite a coleta e especificação de filtros para futura análise de pacotes de tráfego na rede.

Por fim, a finalidade desse estudo é reconhecer se com padrões de tentativas de invasões identificados, será possível minimizar os ataques recebidos nas redes de Telefonia IP.

2 FUNDAMENTAÇÃO TEÓRICA

Esse capítulo tem por objetivo prover o embasamento teórico e dar subsídios para o desenvolvimento do estudo proposto.

2.1 PROTOCOLO SIP

O SIP (*Session Initiation Protocol*) é um protocolo que controla a criação, estabelecimento e término de sessões, dessa forma esse protocolo trata-se apenas de tráfego de sinalização. Esse protocolo foi desenvolvido pelo IETF em 1997, como diversas mudanças tiveram de ser feitas em 2002 foi submetida a versão 2.0 que é a utilizada nos dias atuais.

De acordo com Kurose (2013), o protocolo SIP, definido pela RFC 3261 é um protocolo que possui a finalidade de:

- Prover mecanismos para estabelecer chamadas entre dois interlocutores por uma rede IP, permitindo que a chamada seja encerrada por um destes interlocutores e que os participantes concordem com a codificação da mídia.

Oferecer mecanismos que permite a quem chama determinar o endereço IP atual de quem é chamado, já que os usuários não possuem um endereço IP único, pois podem receber endereços dinamicamente da rede, além da possibilidade de ter vários equipamentos IP, cada um com um endereço IP diferente.

Prover dispositivos de gerenciamento de chamadas, tais como adicionar novos fluxos de mídia, mudar a codificação, convidar mais interlocutores para participar da chamada, além de realizações de transferências.

Junior e Júnior (2017) listam 5 funcionalidades básicas oferecidas pelo protocolo SIP: localização de usuário; verificação de disponibilidade de usuário; descoberta das capacidades ou recursos de um usuário; estabelecimento de parâmetros de uma sessão; e por fim, gerenciamento de uma sessão. Concordando com a afirmativa acima Porter(2006) cita que além de além de configurar e gerenciar as sessões, o SIP tem a função de determinar a localização, disponibilidade e compatibilidade entre os agentes usuários envolvidos na comunicação.

Os principais componentes da arquitetura SIP são:

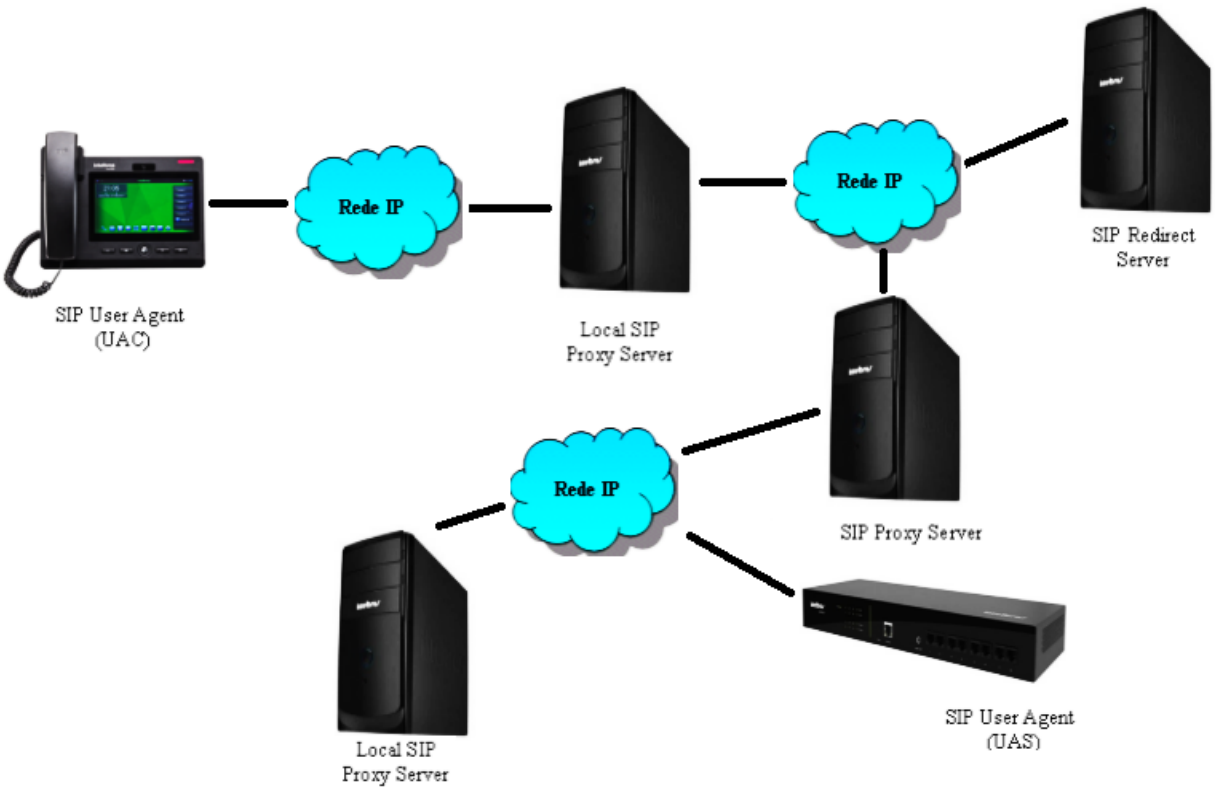
Agente usuário (*User Agent*): UAC são os clientes que originam pedidos de conexão e UAS são servidores que recebem e respondem os pedidos de conexão. Pode-se citar como agentes usuários equipamentos terminais como atas, telefones IP, *softphones* e servidores de registro.

Servidor proxy (*Proxy Server*): atua de forma intermediária, passando adiante requisições para o próximo servidor SIP como se fosse o originador da chamada, e quando a resposta é recebida este redireciona para quem de fato originou a requisição. .

Servidor de redirecionamento (*Redirect Server*): a função do *Redirect Server* é fornecer informações sobre a localização do servidor para que o cliente possa entrar em contato diretamente.

Servidor de registro (*SIP Registrar):* é um tipo especial de UAS responsável por receber e aceitar pedidos apenas solicitações do tipo REGISTER, além disso armazena informações (como a localização) dos agentes usuários.

Esses componentes descritos acima são apresentados na figura a seguir:



2.1.1 Métodos SIP

O SIP se baseia no formato de requisições de texto, semelhante ao HTTP (*Hiper Text Protocol*), segundo a RFC3261 foram definidos 6 métodos que serão apresentados e descritos resumidamente no quadro a seguir. Existem outros métodos definidos em outras RFC's que não serão detalhados nesse documento.

Método SIP	**Descrição**
REGISTER	Usado por um agente para notificar a rede SIP (outros agentes) sobre sua URI de contato
INVITE	Usado para estabelecer sessões entre dois agentes
ACK	Confirma respostas finais a requisições INVITE
BYE	Termina uma sessão previamente estabelecida
CANCEL	Encerra tentativas de chamadas
OPTIONS	Consulta um agente sobre suas capacidades

Fonte: https://wiki.sj.ifsc.edu.br/wiki/index.php/RMU-2015-1

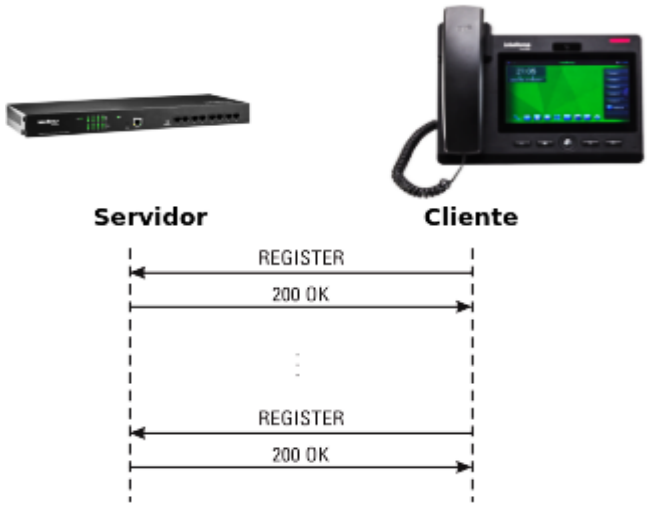
Cada método apresenta uma ação requerida, como será apresentado mais detalhadamente abaixo.

REGISTER

Tem o papel de informar a localização do usuário com as informações que o identificam. De acordo com Johnston (2009), a informação relacionada a localização está contida no campo *Contact* do cabeçalho. O servidor compara o SIP URI do campo *To* com o SIP URI do campo *Contact,* que revela a localização do UAC. É esse serviço de localização que é utilizado pelo *proxy* para rotear as chamadas para os usuários. Dependendo do uso dos campos *Contact* e Expires, o servidor tomará medidas diferentes. Se o campo *Expires* não for utilizado, o registro do SIP será cancelado em uma hora, se o *Expires* estiver igual a zero o registro será cancelado imediatamente. O *RequestURI* contém apenas o domínio do servidor registrar (não possui o usuário). O REGISTER pode ser encaminhado por um proxy até chegar ao servidor registrar responsável pelo domínio. O campo *To* contém o SIP URI que será registrada no servidor. O campo *From* contém o SIP URI do originador da requisição, recomenda-se que o mesmo Call-ID seja usado para todos os registros de um usuário agente.

Na figura abaixo, adaptada de Johnston (2009), mostra uma troca de mensagem SIP entre Cliente e Servidor, na qual o cliente faz uma requisição de registro para o Servidor, este por sua vez aceita e o registro é estabelecido.

No período de tempo de registro configurado no UAC, este enviará novamente uma



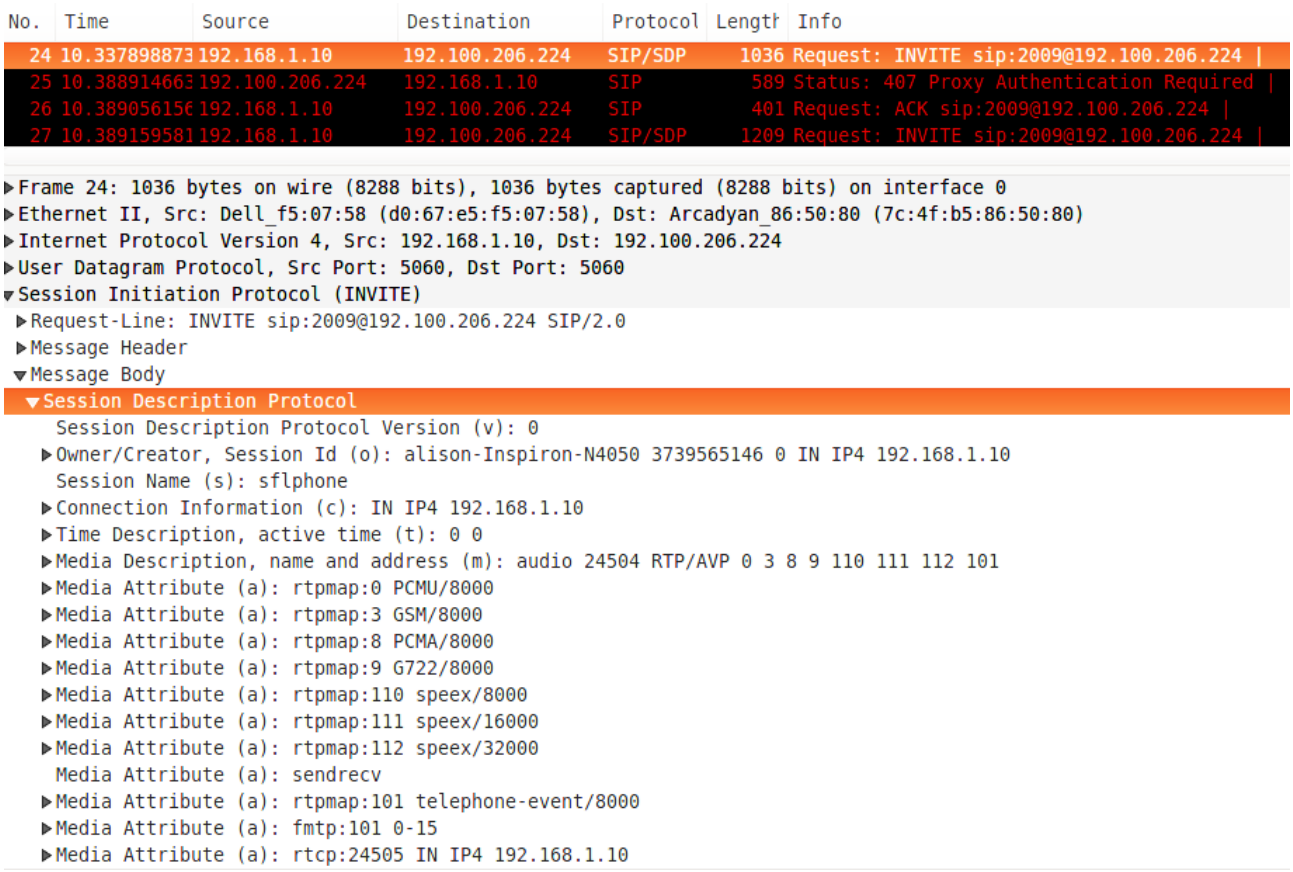
mensagem REGISTER ao servidor para que essa sessão não seja encerrada e o cliente permaneça registrado. Alguns campos são obrigatórios no cabeçalho REGISTER: Call-ID, Cseq, From, To, Via e Max-forwards, que podem ser vistos na figura abaixo.

```
▼Session Initiation Protocol (REGISTER)
 ▶Request-Line: REGISTER sip:192.100.206.225 SIP/2.0
 ▼Message Header
  ▶Via: SIP/2.0/UDP 192.168.1.10:5060;rport;branch=z9hG4bKPj6fad59a7-1b46-4ef8-806c-a123d615ba43
   Max-Forwards: 70
  ▶From: <sip:2005@192.100.206.225>;tag=7220d2c8-e907-4944-8d8a-4e4f99a108ab
  ▶To: <sip:2005@192.100.206.225>
   Call-ID: afd767ad-9ec0-4c33-8995-7436750f4663
  ▶CSeq: 7707 REGISTER
   User-Agent: SFLphone/1.3.0
  ▶Contact: <sip:2005@192.168.1.10:5060>
   Expires: 60
   Allow: PRACK, SUBSCRIBE, NOTIFY, REFER, INVITE, ACK, BYE, CANCEL, UPDATE, INFO, OPTIONS, MESSAGE, PUBLISH
   Content-Length:  0
```

INVITE

O método INVITE é usado para estabelecer uma sessão de mídia entre dois agentes usuários. O INVITE sempre deve ser confirmado através de uma mensagem ACK. O INVITE possui um cabeçalho com a descrição da sessão (via protocolo SDP). Caso o INVITE não possua a descrição da sessão, a mensagem ACK deverá possuí-la. Caso a descrição da sessão não seja aceita pelo agente servidor, este deverá enviar um BYE para terminar a sessão (JOHNSTON, 2009).

Um exemplo do fluxo do método INVITE é apresentado na figura a seguir.

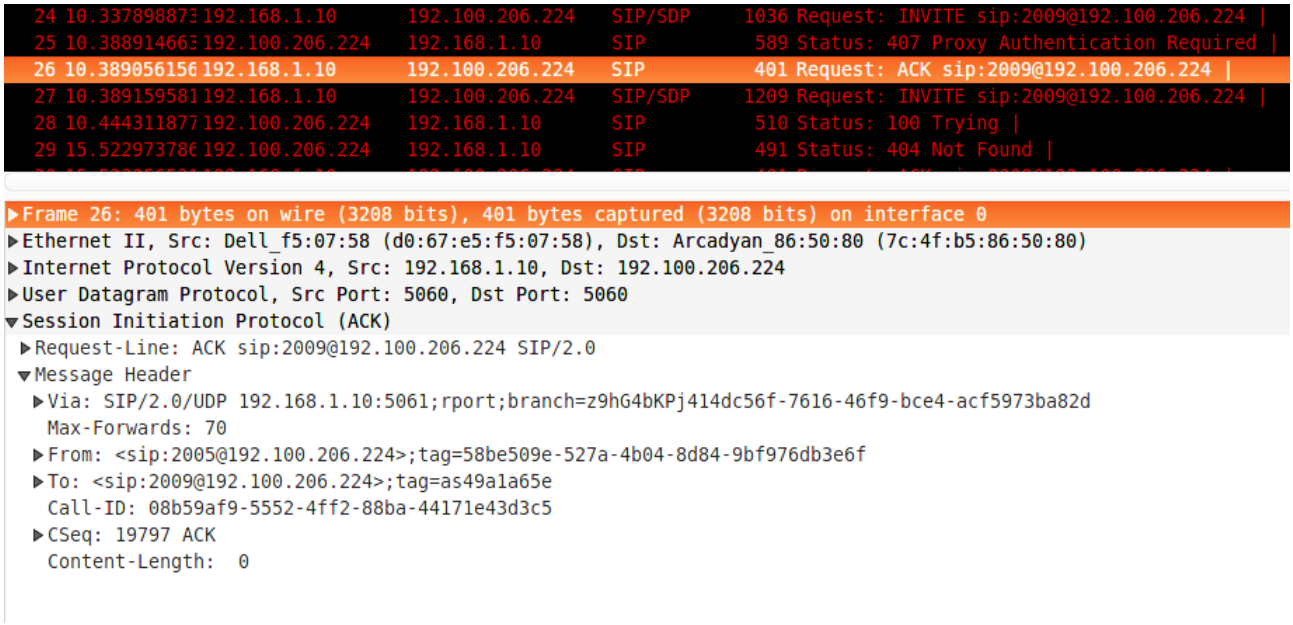


Ainda segundo Johnston (2009), o usuário cliente (UAC) que gera o INVITE para estabelecer um diálogo, gera juntamente um identificador chamado de Call-ID que é usado durante toda a sessão. O campo CSeq do cabeçalho é usado para numerar em ordem das mensagens. Os campos From e To servem para identificar o usuário chamador e usuário chamado. No campo From do INVITE é adicionado um parâmetro tag pelo UAC e no campo To das respostas é adicionado um parâmetro tag pelo agente servidor (UAS). A tag do campo To da mensagem 200 OK em resposta ao INVITE, é usada no cabeçalho To da mensagem ACK e em todas as mensagens seguintes do diálogo. A combinação das

tags do To e From e Call-ID formam um identificador único para esse diálogo. O campo Via é usado para gravar o caminho da requisição. Depois ele é usado para rotear as respostas exatamente pelo mesmo caminho no sentido inverso. Uma mensagem INVITE enviada em um diálogo já existente é chamado de re-INVITE e é usado para mudar alguma característica da mídia utilizada naquela sessão. Caso o re-INVITE não seja aceito, a sessão continua como antes.

ACK

Segundo a RFC2543 a requisição ACK confirma que o cliente recebeu uma resposta final para uma requisição de INVITE. O método ACK funciona como a confirmação de um INVITE, se o INVITE não tiver a descrição da sessão, o ACK deverá possuir. O CSeq nunca é incrementado quando se envia um ACK, de modo que o usuário servidor possa relacionar com o INVITE correspondente. A figura abaixo mostra um exemplo de uma mensagem ACK.

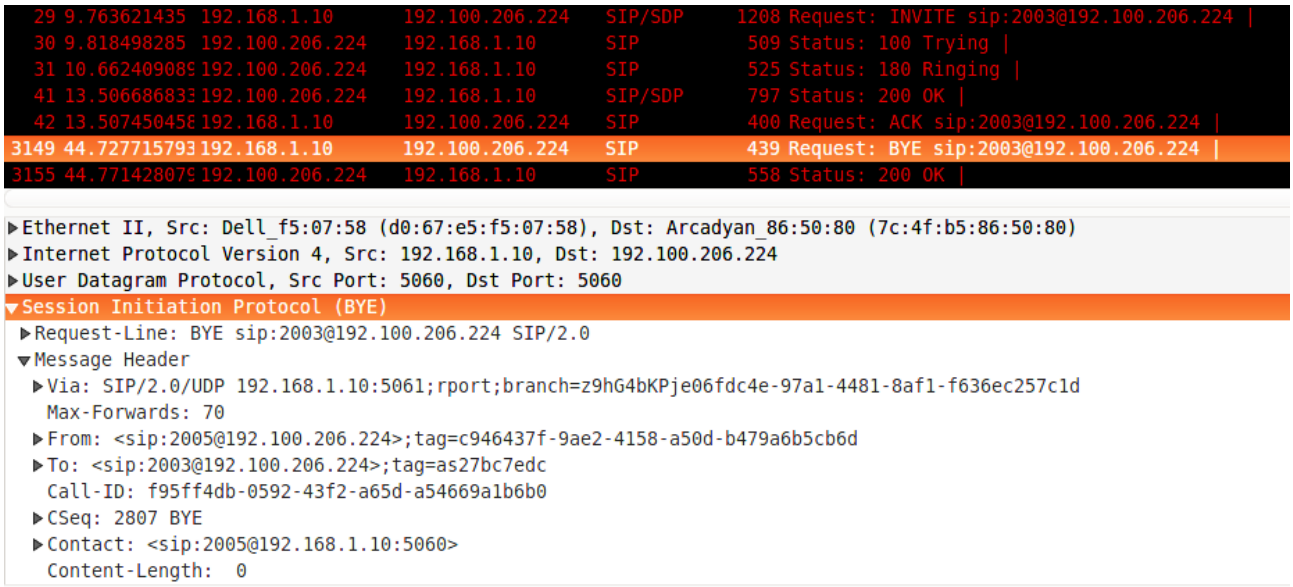


Os campos de cabeçalho obrigatórios do método ACK são os mesmos da requisição REGISTER.

BYE

Conforme descrito na RFC 3261, o método específico para a finalização de um diálogo é o método BYE. Um usuário agente (UA) não deve enviar um BYE fora de um diálogo e quando o BYE é recebido dentro de uma sessão, esta deve ser encerrada.

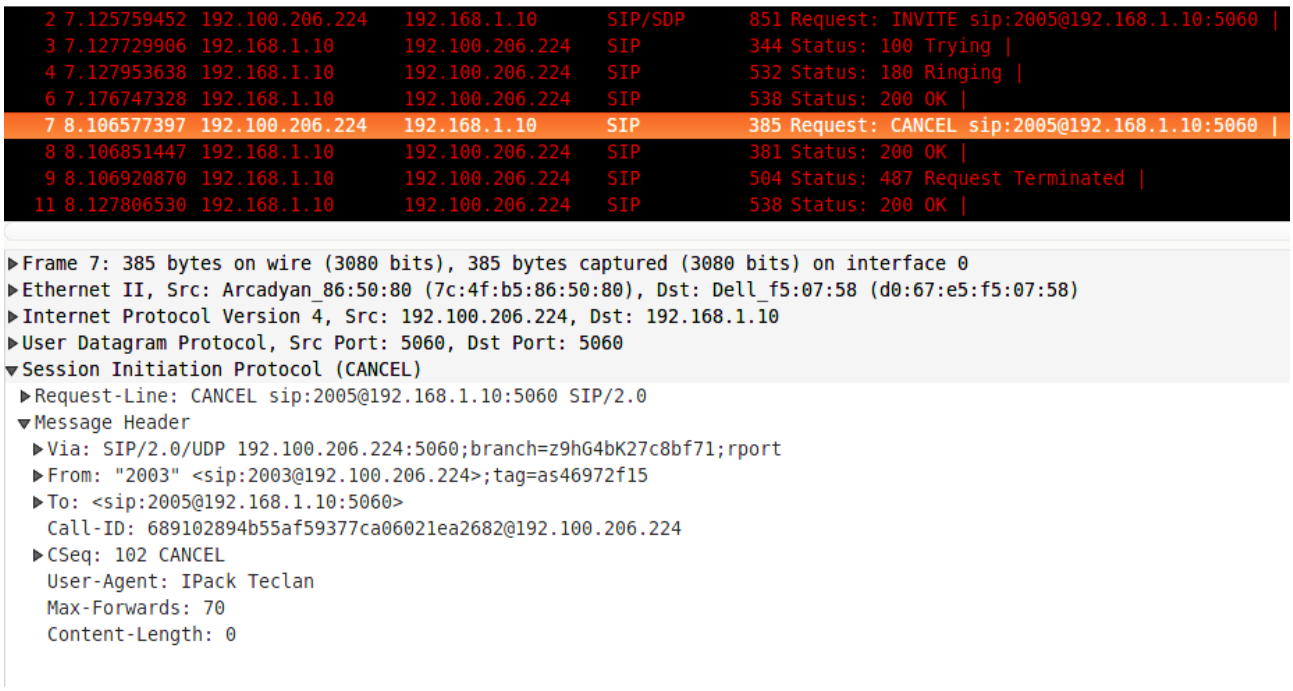
Ainda segundo a RFC3261, quando um dos pontos envia um BYE essa sessão não deverá ser finalizada até que o outro ponto confirme com um ACK.



A requisição BYE só pode ser enviada por UA's que participam da sessão e nunca por servidores proxies, ou seja, é um método fim-a-fim (JOHNSTON, 2009).

CANCEL

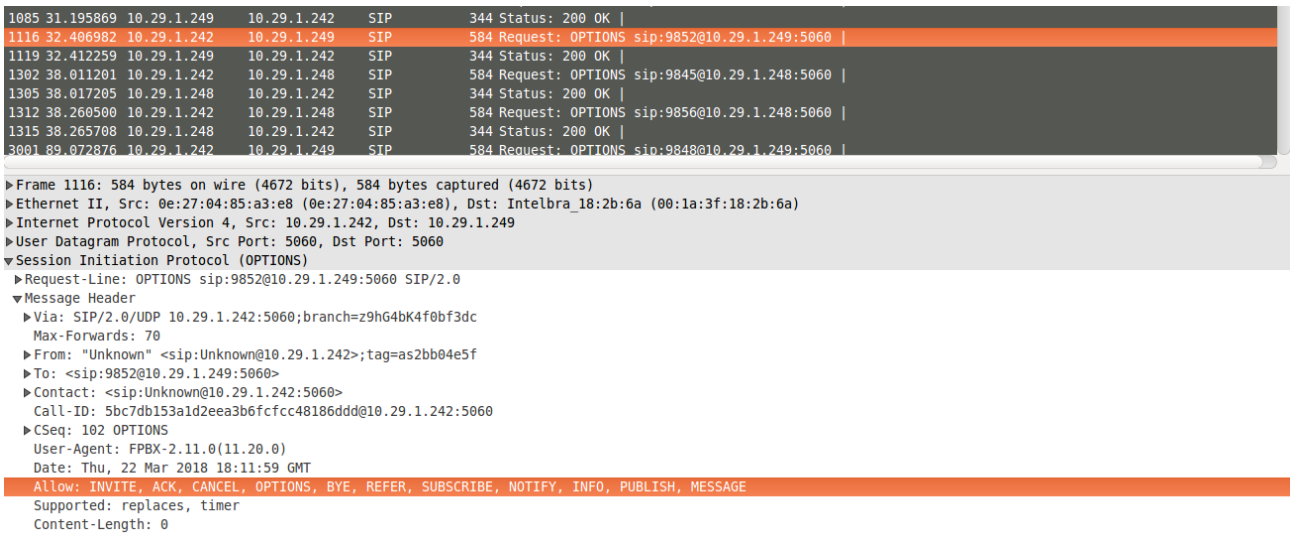
O método CANCEL é usado para encerrar sessões que ainda não foram estabelecidas ou, conforme a RFC3261, cancela pedidos enviados que não obtiveram respostas dentro do tempo estabelecido. Um cliente ou servidor confirma o cancelamento através de uma mensagem 200 OK e responde com uma mensagem 487 *Request Terminated*, conforme figura a seguir.



Diferentemente do método BYE, o método CANCEL pode ser enviado tanto por UA's quanto por servidores proxies. Quando um proxy recebe uma mensagem CANCEL repassa essa para os mesmos *hops* de onde as mensagens INVITE pendentes foram encaminhadas.

OPTIONS

Segundo Johnston (2009), o método OPTIONS é usado para questionar um usuário cliente ou servidor sobre sua disponibilidade ou capacidades. Faz uma pergunta sobre quais métodos e extensões são suportados pelo servidor e pelo usuário descrito no campo de cabeçalho. Tanenbaum (2003) descreve que geralmente o OPTIONS é usado antes da sessão ser iniciada, com o intuito de descobrir se a máquina suporta os recursos solicitados, a resposta contém uma listagem com métodos, extensões e codecs suportados. A figura abaixo exemplifica esse método.



Os campos de cabeçalho *Allow, Accept, Accept-Encoding, AcceptLanguage* e *Supported* devem estar na mensagem 200 OK em resposta ao OPTIONS.

2.1.2 RESPOSTAS SIP

De acordo com Johnston (2009), as respostas SIP geralmente são geradas por um UAS que responde a uma requisição feita por um AUC. Existem seis classes de respostas SIP que são descritas na tabela a seguir, junto de alguns exemplos de respostas.

Classe	**Descrição**	**Ação**
1xx	Informativo	Indica que a requisição foi recebida e que o estabelecimento da sessão está em curso. Este tipo de mensagem é fim-a-fim. 100 – Tentando 180 – Ringando 182 – Chamada colocada na fila
2xx	Bem-sucedido	Indica que a requisição foi recebida, processada e bem-sucedida. 200 – OK
3xx	Redirecionado	Indica que uma ação mais adiante precisa ser tomada para que a requisição possa ser completada, isto é, uma nova requisição deve ser gerada pelo UAC ou proxy para o(s) endereço(s) contido(s) no cabeçalho Contact da resposta.

		300 – Múltiplas escolhas 301 – Movido temporariamente 380 – Serviço alternativo
4xx	Erro do Cliente	Indica que não foi possível executar a requisição pelo servidor do modo que foi recebida. A resposta específica do erro do cliente ou a presença de certo tipo de campo de cabeçalho deve indicar ao UAC a razão do erro e como a requisição deve ser corrigida antes de ser enviada novamente. 400 – Pedido inválido 401 – Não autorizado 403 – Proibido 404 – Não encontrado 407 – Necessária autenticação de proxy 408 – Tempo de pedido esgotado 480 – Temporariamente indisponível
5xx	Erro do Servidor	Indicam a incapacidade do servidor em executar uma requisição. 500 – Erro interno no servidor 502 – Gateway inválido 505 – Versão SIP não suportada
6xx	Falha Global	Indica que a requisição falhou. A requisição não pode ser atendida por este ou outro servidor. 603 – Declínio 604 – Não existe em nenhum lugar 606 – Não aceitável

Fonte: adaptado de Johnston (2009)

2.2 ATAQUES MALICIOSOS EM REDES VOIP

Os ataques têm por objetivo comprometer, de forma unitária ou conjunta, os três aspectos relacionados à segurança da informação: confiabilidade; integridade; e disponibilidade. A confiabilidade está relacionada com a privacidade, se dá garantindo que

apenas a origem e o destino tenham conhecimento do conteúdo da mensagem, ou seja, que essa informação não possa ser interceptada por partes não autorizadas. A integridade garante que as mensagens não sofreram alterações ao longo do caminho, ou seja, que foi preservada em sua íntegra. E por fim, a disponibilidade deve garantir que as informações e recursos estejam disponíveis para os legítimos usuários.

Da mesma forma que já acontecia nas redes de computadores, com o surgimento do VoIP surgiram também ameaças que que tem como intuito comprometer a integridade, a confiabilidade ou a disponibilidade das redes baseadas em SIP. No que se refere a riscos, a própria RFC do SIP (3261) o descreve como um protocolo que não é fácil implementar segurança. Segundo matéria publicada no site *Network World*, os ataques cibernéticos que utilizam o protocolo VoIP têm crescido e representam mais de 51% das falhas de segurança analisadas no ano de 2016.

A seguir serão apresentadas as formas mais comuns de tentativas de ataques a redes VoIP.

Denial of Service (DoS) (Negação de Serviço)

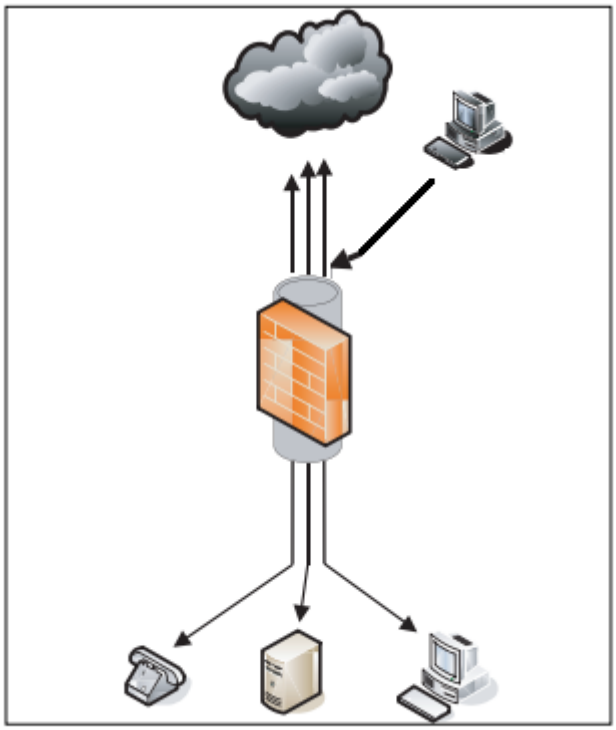
O ataque do tipo negação de serviço tem por objetivo esgotar os recursos disponíveis de determinado servidor, para que os verdadeiros usuários não possam utiliza-los. Não se trata de uma invasão propriamente dita, mas sim de provocar uma indisponibilidade do serviço prestado. De acordo com Thermos e Takanen (2007), no cenário do VoIP o ataque pode ser direcionado tanto para os servidores quanto para a rede em si.

Para exemplificar esse tipo de ataque pode-se citar um servidor que consiga processar 10 requisições por segundo, mas está chegando 30 requisições por segundo. Esse servidor pode parar de responder pelo fato de estar sobrecarregado os limites disponíveis. Dessa forma esse tipo de ataque objetiva comprometer a disponibilidade do serviço prestado.

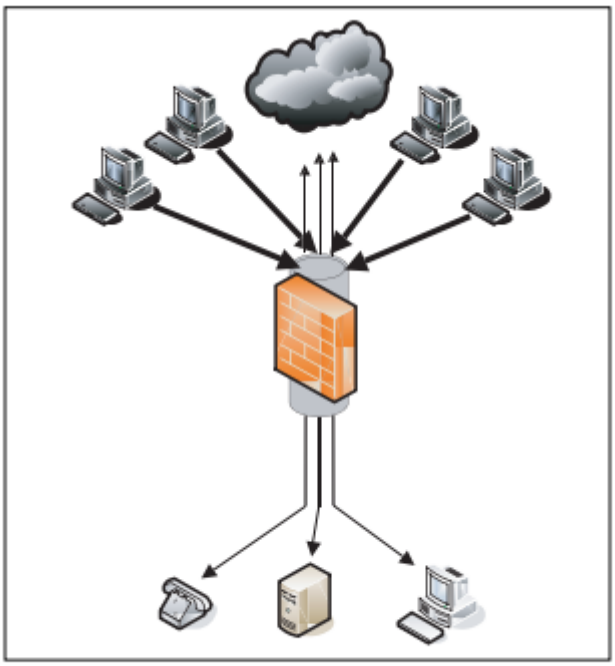
O ataque de negação de serviço distribuído (DDoS) opera semelhante ao DoS e o que difere é que a origem dos ataques não é um único ponto, a origem podem ser dezenas, ou até centenas de computadores conectados com a internet, com o intuito de alcançar o mesmo alvo e afetar sua disponibilidade. Furlan e Santos (2017) ressaltam que o impacto causado por estes ataques na maior parte das vezes se traduz em perda financeira, pois os serviços prestados pela instituição atingida não poderão ser acessados

por seus usuários, podendo vir até mesmo prejudicar a imagem e a credibilidade desta instituição, uma vez que os reflexos do ataque na sua operação serão a lentidão de acesso aos recursos ou até mesmo a indisponibilidade total da infraestrutura.

Nas imagens abaixo adaptadas de Porter (2006), são ilustrados os ataques DoS e DDoS, respectivamente.



Fonte: Adaptado de Porter (2006)



Fonte: Adaptado de Porter (2006)

***SIP Flood* (Inundação SIP)**

De acordo com Furlan e Santos (2017) em um ataque SIP *Flood* o atacante sobrecarrega o *proxy* SIP com inúmeros pacotes *invites*. O grande volume de requisições a esse *proxy* causará a deterioração da rede, impossibilitando o atendimento de requisições válidas e, consequentemente, tornando o serviço indisponível. A grande maioria dos ataques é utilizado a técnica de IP *Spoofing*, onde o endereço de origem das conexões é alterado por endereços inválidos fazendo com que as respostas nunca alcancem seus destinos.

***VoIP Packet Replay Attack* (Ataque de Resposta de Pacotes VoIP)**

Consiste na captura e reenvio pacotes VoIP fora de ordem para os equipamentos finais gerando assim atraso nas chamadas em curso e degradando a qualidade das ligações Porter (2006).

***SIP Sinalling Loop* (Repetição de Sinalizações SIP)**

Segundo Thermos (2007, *apud* Antoniazzi, 2008, p.28) esse tipo de ataque afeta cenários que não possuem mecanismos de detecção de looping. Esse ataque resume-se a registrar dois usuários em domínios diferentes, de forma que quando o servidor proxy receber mensagens INVITE provindas desse ataque, acontecerá a duplicidade das mensagens nos domínios. Dentro do contato de cada registro existem dois valores, cada um direcionado para um domínio. Quando o proxy de um domínio recebe o INVITE para um desses usuários, ele irá gerar duas mensagens de INVITE uma para cada usuário no outro domínio. Já o SIP Proxy do outro domínio por sua vez, ao receber esses dois INVITES irá gerar quatro novas mensagens de INVITE para o outro domínio. Assim, as mensagens crescerão em ordem de potência, conforme demonstrado na imagem abaixo, podendo assim comprometer a disponibilidade do sistema SIP.

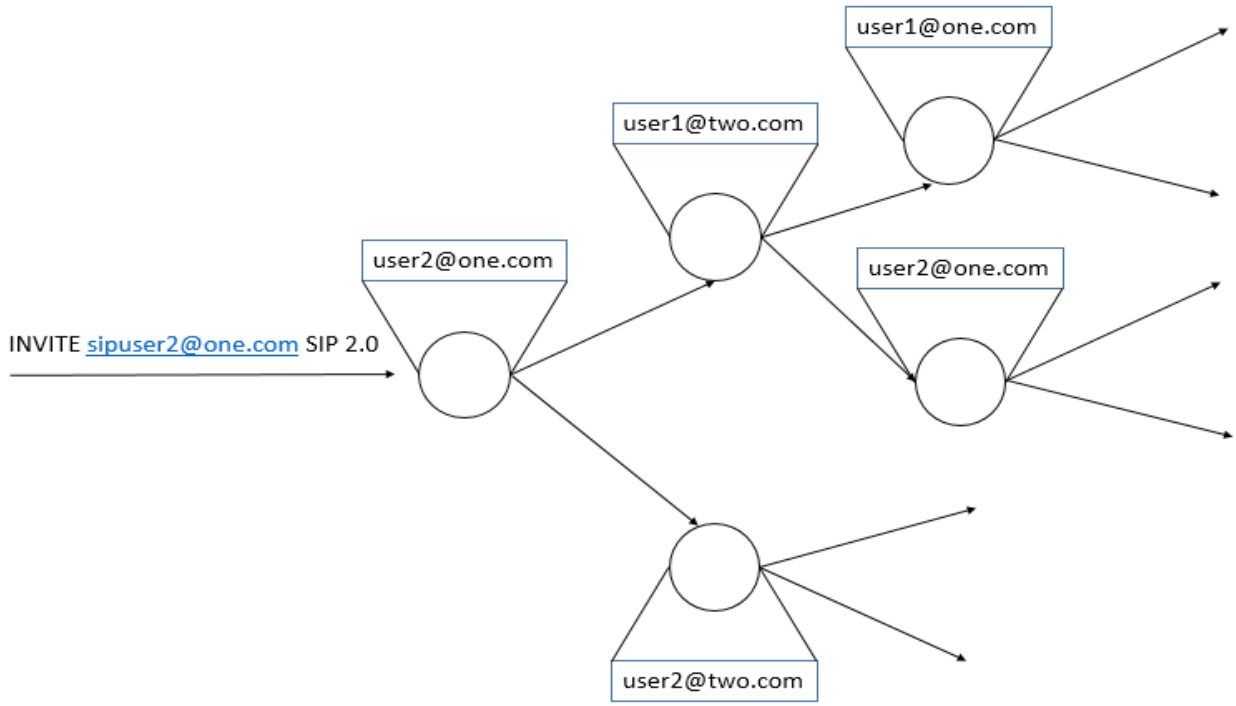


Figura x: adaptado de Thermos (2007)

***Man in the Midlle* (MITM)**

Neste tipo de ataque, o invasor pode utilizar duas técnicas: clonagem do DNS, ou envenenamento da tabela ARP. Qualquer uma delas, obtém-se permissão para estar entre o servidor e o usuário. Nessa maneira descrita, o interceptador não precisa obrigatoriamente conhecer usuários e senhas válidos; basta rotear o tráfego entre

servidor e cliente e agir interceptando os pacotes, impedindo assim de chegar ao seu verdadeiro destino, que é o servidor SIP. Para parecer ao cliente que que a requisição de autenticação foi aceita pelo servidor, o atacante envia mensagens de sucesso a quem originou a requisição (NAKAMURA, 2007).

A figura X abaixo, exemplifica um ataque do tipo MITM.

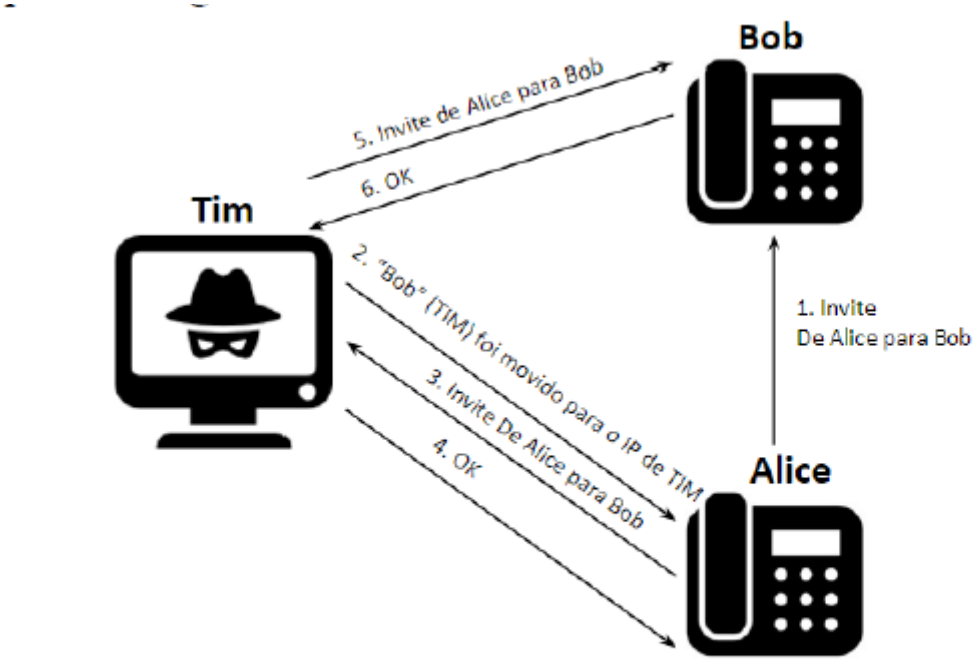


Fig. 5. Ilustração de um ataque *man-in-the-middle*.

Nomoto e Ferreira (2016)

1. Alice envia uma mensagem INVITE para o Bob e esta mensagem é detectada por Tim.
2. Tim envia uma resposta para Alice com a mensagem 301 *Moved Permanently* e informa o seu próprio endereço como sendo o novo endereço IP de Bob.
3. Alice envia uma nova mensagem INVITE acreditando estar enviando para Bob, porém está enviando para Tim.
4. Tim responde com uma mensagem de reconhecimento ACK para estabelecer uma conexão entre ele e Alice.
5. Ao mesmo tempo, Tim envia uma mensagem INVITE para Bob como se fosse Alice.
6. Tim responde com 200 OK e a conexão entre Bob e Tim é estabelecida.

***Registration Hijack* (Sequestro de registro)**

O Sequestro de registro ocorre quando um invasor altera a identidade de um usuário legítimo para o seu próprio endereço, dessa forma as chamadas serão encaminhadas para o atacante ao invés de serem direcionadas para o dispositivo do verdadeiro usuário. De acordo com Porter (2006), a alteração do campo *Contact* no cabeçalho SIP é feita da seguinte forma: o invasor envia uma requisição de registro semelhante à capturada em um pacote do usuário verdadeiro, porém com o campo de *IP address* de origem modificado para o seu próprio IP.

Nomoto e Ferreira (2016) descrevem detalhadamente como acontece esse tipo de ataque. No exemplo dos autores citados, Alice deseja registrar-se no servidor REGISTRAR usando protocolo SIP. A mensagem REGISTER, que é utilizada para este fim, é demonstrada a seguir:

```
REGISTER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@192.168.2.3
CSeq: 314159 INVITE
Contact: Alice <sip:alice@192.168.1.77:5061>;expire=60
Content-Type: application/sdp
Content-Length: 142
```

Nesta mensagem, os campos *To* e *From* possuem a mesma informação que identifica o originador do pedido de registro através de um URI *(Uniform Resource Identifier*), que é um identificador único. O campo *Contact* contém a SIP URI que representa o seu endereço IP associado. O invasor pode construir uma mensagem REGISTER similar modificando o campo *Contact,* conforme exemplo abaixo.

```
REGISTER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@192.168.2.3
CSeq: 314159 INVITE
Contact: Alice <sip:alice@192.168.1.88:5061>;expire=60
Content-Type: application/sdp
Content-Length: 142
```

Neste modelo, o endereço IP é modificado de 192.168.1.77 para 192.168.1.88, sendo assim, o invasor se registrará aparentemente como um usuário válido, qualquer chamada encaminhada para Alice será direcionada para o IP do invasor mal-intencionado, consequentemente Alice ficará impossibilitada de originar ou receber ligações. Souto (2008) afirma que esse tipo de ataque geralmente acaba evoluindo para um ataque do tipo MITM.

Quebra de senha (Ataque por dicionário)

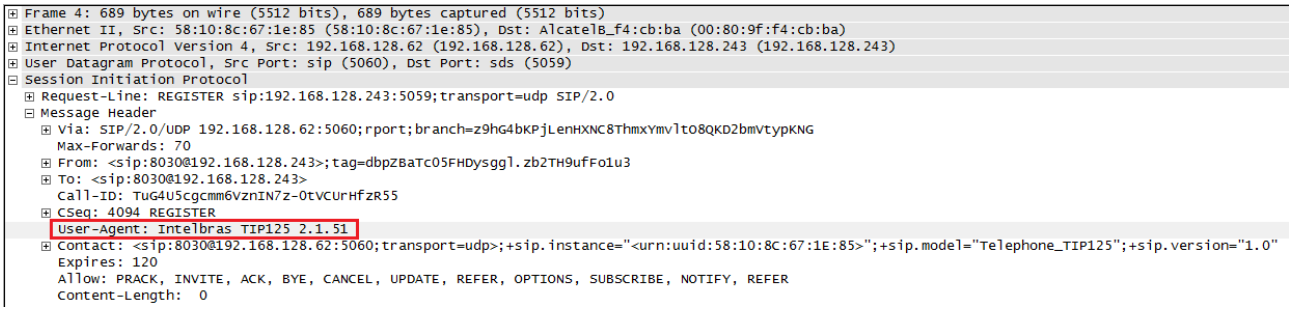
Nesse cenário o interceptador pode, através de captura de pacotes de sinalização SIP, descobrir o usuário SIP e então lista prováveis senhas (baseadas em um dicionário). Em posse dessas informações são disparadas diversas requisições REGISTER (ataque de força bruta) para o servidor com as possíveis senhas, até que uma funcione. Descoberta a senha, o invasor possa usufruir dos recursos disponíveis no sistema, por isso a importância de não utilizar senhas óbvias nos ramais.

Call Eavesdropping **(escuta telefônica)**

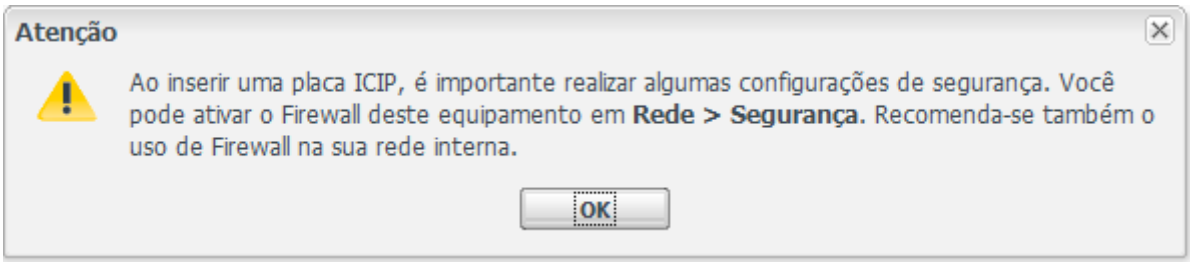
Nesse método de ataque a integridade da confiabilidade é posta em risco pois nesse cenário é monitorado tanto a sinalização SIP quanto o fluxo de mídia (conversação). Através da sinalização o atacante pode descobrir usuários, senhas, contas e através da escuta da conversação pode ter acesso às informações confidenciais. O mecanismo *eavesdropping* é muito eficaz quando os pacotes SIP e RTP trafegam na rede sem nenhum método de proteção das informações. Para capturar a sinalização e a mídia os interceptadores utilizam de softwares snifers de rede, Souto (2008) cita as seguintes ferramentas: WireShark, Cain e Abel, Vomit, Voipong, Oreka e DTMF decoder.

3 CENÁRIO DE DESENVOLVIMENTO DO TRABALHO

Conforme exposto anteriormente, os ataques VoIP acarretam em diversos tipos de prejuízos para o usuário final, empresas, operadoras e o próprio fabricante do equipamento. Através de um scanner de rede um PABX IP pode ser localizado, esse descobrimento busca informar dentro de uma faixa de rede os equipamentos que existem. Assim que é identificado o equipamento é feito a escuta telefônica (*Call Eavesdropping*), durante essa captura o invasor busca primeiramente coletar informações como *hosts*, *usernames* e numeração das extensões. Após descobrir essas informações, o atacante pode monitorar retornos de solicitações SIP como INVITE, REGISTER e OPTIONS. De acordo com as respostas, é sabido o tipo de equipamento que existe naquele endereço IP através das informações fornecidas no campo User-Agent.



Para reproduzir esse tipo de situação foram realizadas capturas de pacotes com o software Wireshark em um cenário real com a central telefônica impacta 140, da fabricante Intelbras. Este modelo de central é considerado híbrido, devido a possibilidade de utilizar tecnologia digitais, analógicas e IP. Nesse modelo de PABX ao inserir uma placa que possibilita a central ter ramais IP / Troncos IP é apresentada uma imagem alertando sobre a necessidade de configuração de segurança.



O fato de não configurar esses parâmetros de segurança pode gerar diversos transtornos para o usuário final ou até mesmo para o responsável pela infraestrutura. Um exemplo muito comum é o ring falso recebido pelo PABX IP, o atacante envia inundações de INVITES (*SIP Flood*) para o IP do PABX, caso não exista nenhum tipo de firewall na infraestrutura ou os próprios parâmetros de segurança da central não forem configurados, essas chamadas falsas podem vir com identificações aleatórias e no momento que o usuário atende a chamada, fica totalmente mudo, dando a impressão que se trata de um trote. Esse ataque também prejudica a disponibilidade dos recursos da central telefônica, pois no momento que essa chamada entrou pela central e está ringando em um ramal, um canal SIP foi ocupado, algo que pode impedir que outras pessoas originem ou recebem chamadas se todos os canais estiverem ocupados.

Plano de trabalho

O trabalho se propõe a identificar e caracterizar padrões de ataques a que estão sujeitas centrais telefônicas IP, e propor contramedidas em cada caso.

Pretendem-se identificar os padrões de ataques através de coletas de pacotes em cenários reais, além de cenários simulados em bancada onde um PABX ficou exposto sem nenhuma proteção em uma rede interna ou externa. A ferramenta utilizada para procurar identificar os padrões será o software Wireshark. Essa ferramenta gratuita, permite visualizar toda a sinalização SIP entre o servidor e o agente mal-intencionado, além da possibilidade de ouvir a mídia das chamadas.

Para caracterização do tipo de ataque que está sendo recebido pelo PABX, serão analisados os métodos SIP recebidos durante essa invasão que são: REGISTER, INVITE e OPTIONS. Dentro do REGISTER será analisado as informações referente ao registro, já que durante o pedido de registro de um terminal IP ou softphone, o servidor responde com um desafio para aceitar a autenticação. Dentro dessas informações estão os campos localizados no *authorization*: realm, nonce, *uri*, *response*, *algorithm* e *user-agent*. Todos esses campos encontrados no *Header* serão analisados, além do intervalo de tempo que os pacotes são recebidos, horários, os campos From e TO que indicam a origem e destino daquele pacote, respectivamente. Em relação ao INVITE serão analisados os campos que são comuns ao caso anterior, além de verificar informações do SDP, que encontrasse dentro do corpo (*Message Body*) da mensagem SIP como *owner/creator*, *conection*

information, e codecs utilizados. As mesmas informações que são comuns aos casos anteriores serão analisadas nos pacotes OPTIONS. Com essas informações, poderemos descrever que tipo de ataque está sendo recebido pelo PABX.

Durante um ataque de negação de serviço (DoS) o invasor procura descobrir uma falha ou fragilidade do PABX IP para indisponibilizar seus serviços. Esse tipo de ataque pode fazer com que o PABX receba diversas chamadas (INVITES entrantes) e fique gerando um ring falso para o usuário, dando a falsa impressão que se trata de um trote, pois no momento que a chamada foi atendida não há áudio. Isso pode ficar ocorrendo até que essas chamadas consumam muito processamento ao ponto de reiniciar ou até mesmo de travar o PABX, dependendo do pacote recebido e da falha/fragilidade identificada pelo atacante. Ao conseguir indisponibilizar o serviço, o usuário ficará impossibilitado de originar/receber chamadas.

Um outro de ataque muito comum é o ataque por dicionário (quebra de senha), nesse cenário o interceptador pode, através de captura de pacotes de sinalização SIP, descobrir o usuário SIP e então lista prováveis senhas (baseadas em um dicionário). Tendo essas informações são disparadas diversas requisições REGISTER para o servidor com as possíveis senhas, até que uma funcione. Assim que a senha for descoberta, o atacante pode utilizar os recursos disponíveis no sistema, geralmente realizando chamadas internacionais, fato que causaria um grande prejuízo para a empresa que adquiriu o PABX.

Em relação ao ataque DoS recebido pelo PABX no cenário estudo, seria importante que esse PABX IP pudesse informar se irá permitir ou não a possibilidade de originar/receber chamadas via ponto a ponto. Caso permitisse o ponto a ponto, ter um campo onde se possa informar os endereços IP de onde será possível receber esses INVITES. Chamadas direcionadas via ponto a ponto fora dessa faixa de endereço IP seriam inclusos em uma blacklist. Já em relação a autenticação por dicionário, seria importante o PABX exigir que as senhas contenham caracteres especiais além de letras e números. Dessa forma, impossibilitaria que usuários configurem senhas óbvias como o próprio número do ramal.

Cronograma

Etapas	fev/ 2018	mar/ 2018	abr/ 2018	mai/ 2018	jun/ 2018	jul/ 2018	ago/ 2018
Pesquisa Bibliográfica	X	X	X	X			
Escrita do TCC				X	X	X	X
Entrega e defesa do TCC I							X

Etapas	Ago/2018	Set/2018	Out/2018	Nov/2018	Dez/2018
Apresentação do Seminário do TCC I	X				
Testes e análises dos Ataques VoIP	X	X			
Identificação do tipo de padrão da Invasão		X	X		
Propor formas de minimizar os ataques sofridos			X		
Preparação do documento final				X	X
Apresentação final					X

REFERÊNCIAS

RFC3261

ANTONIAZZI, André Scomazzon. **Segurança em VoIP: Ameaças, Vulnerabilidade e as Melhores Práticas de Segurança**. 2008. 55 f. TCC (Graduação) - Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, UFRGS, Porto Alegre, 2008.

FURLAN, Káren Bartholo; SANTOS, Guilherme Rezende dos. **Ataques DDoS.** 5. ed. Santa Rita do Sapucaí: Inatel, 2017.

JOHNSTON, Alan B.. **SIP: Understanding the Session Initiation Protocol.** 3. ed. Norwood: Artech House, 2009.

JUNIOR, Márcio de Salles Paiva; JÚNIOR, Mário Ferreira Silva. **Abordagem de segurança em VoIP - SIP.** Santa Rita do Sapucaí: Inatel, 2017.

NAKAMURA, Emílio T.; GEUS, Paulo Lício de. **Segurança de rede em ambientes corporativos**. São Paulo: Novatec Editora, 2007.

NOMOTO, Leonardo Juniti; FERREIRA, Mário. **Segurança e Privacidade em redes VoIP.** Santa Rita do Sapucaí: Inatel, 2016.

PORTER, T., GOUGH, M. *How to Cheat at VoIP Secutity*. Rockland: Syngress Publishing, 2006.

ROSENBERG et al (Org.). RFC 3261 **SIP: Session Initiation Protocol.** 2002. Disponível em: <https://www.ietf.org/rfc/rfc3261.txt>. Acesso em: 08 jul. 2018.

SOUTO, André Ribeiro**. A Importância da Segurança Aplicada à Tecnologia VOIP.** 2008. 34 f. TCC (Graduação) - Curso de Especialização em Tecnologias, Gerência e Segurança de Redes de Computadores, UFRGS, Porto Alegre, 2008.

TANENBAUM, Andrew S. **Redes de Computadores.** Rio de Janeiro: Elsevier, 2003

THERMOS, Peter; TAKANEN, Ari. **Securing VoIP Networks:** Threats, Vulnerabilities, and Countermeasures. Boston: Pearson Education, 2007.