Criptografia Baseada em Identidade para Confidencialidade das Comunicações VOIP

Paulo Renato de Moraes Vieira, Luciano Ignaczak, Jéferson Campos Nobre

[1]Escola Politécnica – Universidade do Vale do Rio dos Sinos (UNISINOS)
São Leopoldo, RS – Brasil

paulo.renato@terra.com.br, lignaczak@unisinos.br, jcnobre@unisinos.br

Abstract. *VOIP technology has introduced support for creating and expanding collabration environments at a low cost of operation, based on values if in a Public Telephony Network. However, the related technologies do not meet the basic security needs, requiring attention to this subject to avoid any impact due to information exposure on VOIP calls to unauthorized users. In order to attend to this requirement in such scenario, this paper come up with a draft on a security model using the identity-based cryptographic schema on VOIP calls, as well as introduce a pilot project and a discussion on authentication importance using other cryptographic scheme.*

Resumo. *A praticidade gerada pela tecnologia VOIP permite a criação ou expansão de ambientes colaborativos, a um custo reduzido de operação frente à opção em Rede Pública de Telefonia. No entanto, por definição as tecnologias envolvidas não apresentam suporte aos requisitos básicos de segurança, exigindo atenção a esse fator para evitar impactos causados pelo acesso indevido às informações trafegadas em ligações VOIP. Para atender aos critérios de segurança desse ambiente, este artigo apresenta um modelo conceitual de proteção utilizando criptografia com base na identidade para garantir o sigilo das comunicações, além de um protótipo de implementação e debate à importância de autenticação utilizando outros esquemas de criptográficos.*

1. INTRODUÇÃO

A capacidade e acessibilidade das infraestruturas de rede tem evoluído de forma considerável nos últimos anos. Infelizmente, muitas vezes essa evolução não se traduz diretamente em melhores mecanismos de segurança para todas as aplicações e usuários. Normalmente, tais mecanismos implementam as propriedades conhecidas como CID: Confidencialidade, Integridade e Disponibilidade. Problemas em tais propriedades causam perdas financeiras para provedores e consumidores de serviços.

Nesse contexto, serviços executados em Redes Nacionais de Pesquisa e Ensino (*National Research and Education Network* - NREN) como, por exemplo, a Rede Nacional de Pesquisa (RNP) também necessitam apresentar CID. Em muitas desses serviços, mecanismos de segurança são implementados tanto para tarefas operacionais, quanto para a investigação de novas técnicas e metodologias de redes e sistema distribuídos.

Serviços Voz sobre IP (VoIP) são costumeiramente utilizados para a possibiliar a execução de chamada de voz através de redes de dados. Esses serviços também possibilitam que as chamadas VoIP sejam interconectadas à Rede Pública de Telefonia Comutada

(*Public Switched Telephone Network* - PSTN). Tais ligações podem ser encaminhadas para rede IP de forma transparente para quem está realizando as chamadas através da PSTN. No contexto da RNP, o fone@RNP[1] oferece serviços de VoIP de forma alternativa e colaborativa, proporcionando economia em telefonia para os participantes. O fone@RNP encaminha chamadas telefônicas pela rede Ipê, o backbone de alto desempenho da RNP. Por meio de um acordo entre os participantes, o fone@RNP permite ligações de longa distância para telefones fixos na rede pública e para algumas universidades ao redor do mundo, também a custo zero. No entanto, as instituições que fazem parte desta rede devem entregar as ligações para fixos destinadas à sua cidade.

O serviço fone@RNP possibilita que os usuários realizem chamadas telefônicas para outros membros sem custo por chamada, assim como não há custos para adesão ou mensalidades para participar do serviço. Além disso, o sistema permite que usuários realizem chamadas sem necessidade de treinamentos adicionais. No entanto, tal gratuidade não exime o serviço de oferecer funcionalidades de segurança. Notadamente, muitos mecanismos de proteção, como por exemplo, autenticação e autorização, e firewall, já são utilizados no fone@RNP. Entretanto, com relação ao sigilo das chamadas, o fone@RNP não oferece suporte à criptografia. Dessa forma, a confidencialidade das chamadas é equivalente à PSTN, mas inferior a aplicações como Whatsapp e Signal, as quais utilizam a *Signal Protocol library*[2]. Diante disso, a publicação do Decreto-Lei 8135 (4 de novembro de 2013) exige medidas de instituições nacionais para manter o sigilo das informações, o que não é compatível com o atual estado do fone@RNP.

Novas técnicas na área de criptografia tem sido propostas para lidar com características diversas dos sistemas e ambientes. Tais técnicas podem ser utilizadas considerando estudos realizados em universidades e unidades de pesquisa. Uma das técnicas propostas é a Criptografia Baseada em Identidade (*Identity-Based Encryption* - IBE). O IBE é um tipo de criptografia assimétrica na qual uma *string* conhecida publicamente que representa um indivíduo ou organização é utilizada como chave pública. Essa *string* pode ser composta por informações como endereço IP, número telefônico ou endereço de *email*. Soluções de infraestrutura de chave pública (*Public-Key Infrastructure*- PKI) que utilizam IBE já são conhecidas há bastante tempo SHAMIR(1984). Em tais soluções, usuários podem verificar assinaturas digitais usando apenas informações disponíveis publicamente (e.g., endereço de email). Um exemplo de implantação de tais soluções reside na utilização de IBE para comunicações restritas no Reino Unido, conforme descrição realizada pelo *National Cyber Security Center*[3] .

O presente trabalho descreve um modelo de proteção para garantir sigilo das ligações VOIP, convergindo as tecnologias envolvidas nesta estrutura de comunicação com o esquema criptográfico IBE. Com o objetivo de proporcionar mais detalhes acerca da proposta, é apresentado um protótipo com base na organização do serviço fone@RNP, que ao incorporar soluções de criptografia para chamadas, permite que a RNP se adeque ao Decreto-Lei 8135 e também aos anseios da comunidade formada para instituições de ensino e pesquisa brasileira. Além disso, questões práticas relativas à implementação de uma PKI utilizando informações de identidade para um serviço VoIP são apresentadas.

[1] foneRNP-https://www.rnp.br/servicos/servicos-avancados/fonernp

[2] Signal Protocol library-https://github.com/whispersystems/libsignal-protocol-java/

[3] https://www.ncsc.gov.uk/guidance/secure-voice-official

O trabalho está organizado da seguinte forma: na Seção 2, é descrita a fundamentação teórica referente ao esquema IBE e o protocolo SIP. Em seguida, são apresentados, na Seção 3, alguns trabalhos relacionados ao assunto, proporcionando base de comparação. Na seção 4 é descrito o modelo conceitual que integra IBE e SIP em comunicação VOIP. A proposta de implementação de IBE no fone@RNP e resultados esperados são discutidos nas Seções 5 e 6, respectivamente. Finalmente, comentários finais são apresentados na Seção 7.

2. FUDAMENTACAO TEÓRICA

A seguir são apresentados detalhes do esquema criptográfico e protocolo relacionado à comunicação presentes nesta proposta. O objetivo é permitir a compreensão das tecnologias envolvidas na formatação da estrutura sugerida para promover a confidencialidade das ligações VOIP.

2.1. IBE

Idealizado em [Shamir 1985], a origem do esquema IBE está na busca por um sistema criptográfico mais simples frente a outras opções, no qual não houvesse a necessidade de troca de chaves ou repositórios públicos de distribuição. O objetivo era apresentar um esquema criptográfico em que os usuários pudessem utilizar uma informação de domínio público, como a identidade do destinatário para estabelecer a troca de mensagens seguras, mesmo que os envolvidos nunca tenham estabelecido qualquer canal de comunicação antes.

Esquema assimétrico de criptografia, no IBE, as chaves estão associadas a uma central confiável de geração de cifras, denominada *Private Key Generator* (PKG). A base de cálculo da chave pública está na associação dos valores pseudorrandômicos, sendo estes conceitualmente ligados à identidade do destinatário e aos parâmetros obtidos junto à PKG, fornecendo assim a chave para cifragem dos dados. A recuperação da chave privada ocorre com uso de uma chave mestra presente na PKG associado à identidade do usuário.

Segundo o modelo conceitual de Shamir, de posse da mensagem ”m”, o usuário executa o cálculo necessário para obter a chave pública ”ke”do destinatário, utilizando a identidade ”i”como fator randômico. Após, o texto cifrado “c” é enviado em canal seguro para o destinatário, que recupera a chave privada “kd” calculando sua identidade “i”, mais um valor denominado chave mestra, recuperando a mensagem “m”, conforme ilustrado na Figura 1 (fonte: [Shamir 1985]). O estudo de Shamir ficou somente no campo das ideias, uma vez que o autor não encontrou métodos e tão pouco a tecnologia necessária para colocar o esquema em prática, conforme [Schneier 1996].

Com base no modelo de Shamir e estudos posteriores no campo da matemática, no estudo apresentado por [Boneh and Franklin 2003] descreveram o primeiro protocolo considerado seguro e eficiente, do ponto de vista computacional, que torna viável a aplicabilidade do sistema, utilizando técnicas de emparelhamento bilinear sobre grupos criptográficos gerados em curvas elípticas. Os três valores que estruturam o esquema de proteção do sistema IBE proposto pelos autores são, além da chave mestra, o valor pseudorrandômico gerado pelo usuário (ID) e outro que nunca é conhecido, mas sabe-se que é logaritmo discreto da identidade do destinatário. Estes dois últimos utilizam um

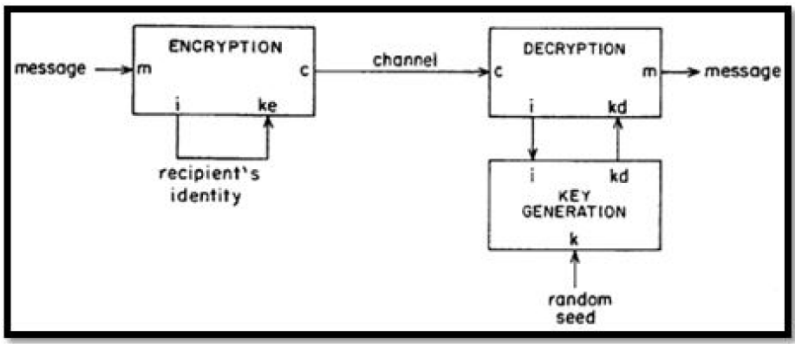

Figura 1. Processo de Criptografia e decriptografia de mensagem no esquema IBE

parâmetro público que direciona para um ponto em uma curva elíptica, enquanto a chave mestra é de domínio único da PKG e é utilizada para geração dos fatores privados do ambiente, sendo que a perda ou comprometimento desta seria desastroso para o sistema. A RFC5091[4] publicada por [Boyen and Martin 2007] descreve detalhes desse protocolo, cuja estrutura está dividida na operação de 4 algoritmos:

- *Setup* (inicialização): Esse é o algoritmo que descreve a etapa de inicialização dos parâmetros básicos para o funcionamento do sistema, incluindo a chave mestra utilizada pelo IBE para cálculo da chave privada dos usuários. O algoritmo recebe dois valores, um deles indicando a versão do protocolo e o outro está relacionado ao tamanho da chave, sendo o retorno, os valores de parâmetros e da chave mestra, codificados separadamente. A separação é necessária pois os parâmetros devem ser de domínio público, enquanto a chave mestra será de acesso exclusivo da PKG;
- *Extraction* (extração): O algoritmo de extração é responsável por executar os cálculos que irão recuperar a chave privada do usuário. As informações envolvidas no processo são: o valor aleatório referente à identidade do usuário, também utilizada para cálculo da chave pública; as propriedades do sistema e a chave mestra da PKG. O retorno do algoritmo será um valor único, referente à chave privada;
- *Encrypt* (criptografia): Algoritmo responsável pelo processo de transposição ou codificação dos dados, disponível a qualquer uma das partes envolvidas na comunicação, pode ser acionado utilizando um texto claro, parâmetros do sistema e o valor de identificação do outro ponto da comunicação. O retorno do algoritmo será o texto protegido.
- *Decrypt* (decifragem): Este algoritmo está relacionado à etapa de recuperação da informação protegida pelo algoritmo de criptografia. Ele pode ser executado por qualquer uma das partes da comunicação e necessita de três fatores para executar as operações: os parâmetros do sistema, texto cifrado e a chave privada do usuário. O retorno será o texto aberto.

A Figura 2 (fonte:elaboração própia com base em [Martin 2008]) apresenta o processo de decifragem de mensagem com base na RFC5091, que envolve o funcionamento dos algoritmos Decrypto e Extraction, sendo o último relacionado à recuperação da chave privada do usuário. Após receber a informação cifrada ”c”, a solicitação de chave privada é enviada para a PKG, representado pela etapa 1. Os dados enviados são as informações

[4]https://tools.ietf.org/html/rfc5091

da identidade do usuário e a propriedade do sistema. Na etapa 2, aqueles dados enviados são somados à chave mestra, fornecendo informações para recuperação da chave privada ”Pr”e envio ao usuário, permitindo assim que este decifre o conteúdo de ”c”e recupere a mensagem ”m”em texto claro.

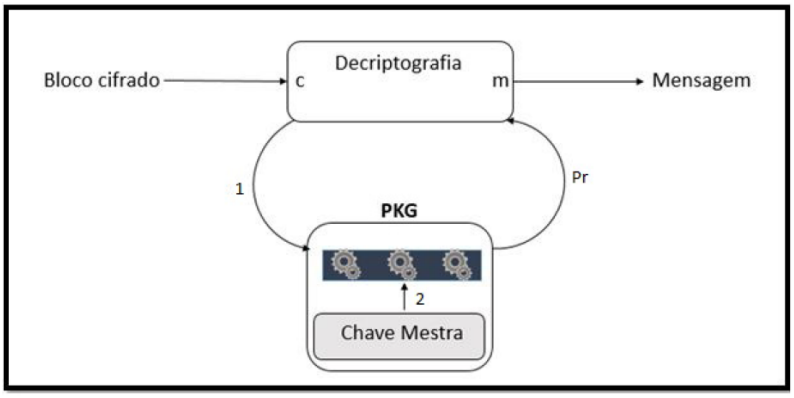

Figura 2. Decifragem de mensagem com base na RFC5091

Em determinados cenários, a custódia da chave privada permite a geração de soluções interessantes frente àquelas promovidas por soluções voltadas ao uso de certificados digitais, por exemplo, no que tange à confidencialidade dos dados. Com base no cálculo da identidade do ator, é possível estabelecer sistemas de proteção transparentes, em que a interação do usuário é indireta, ao apenas indicar o destino.

Considerando as três propriedades básicas de segurança da informação, conforme a norma ISO 27001, o esquema IBE é capaz de garantir a confidencialidade dos dados, exigindo convergência com soluções paralelas em busca de respostas aos outros fatores, em especial àquelas que promovem assinatura digital. Uma solução híbrida pode fornecer a estrutura robusta necessária para atender a todos os requisitos de segurança do ambiente.

Dos esquemas de assinatura digital, o *Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption* - ECCSI proporciona uma estrutura de validação similar aos modelos, com base em certificados digitais, no que tange a capacidade de garantir a autenticidade e integridade da informação, porém a um custo operacional reduzido. Assim como no IBE, o ECCSI introduz um método que utiliza a identidade dos usuários na geração das chaves, contando com uma entidade externa, denominada *Key Management System* - KMS, para manutenção e fornecimento das mesmas. O processo de validação ocorre localmente com base em um artefato de conhecimento prévio. Detalhes do modelo ECCSI proposto estão publicados na RFC6507[5] por [Groves 2012].

2.2. SIP

O Protocolo de Iniciação de Sessão (*Session Initiation Protocol* - SIP) foi inicialmente projetado pelo grupo de trabalho denominado *MMUSIC* do *Internet Engineering Task Force* (IETF) e definido na RFC2543[6]. Atualmente o grupo *SIPCORE* é o responsável pela manutenção dos requisitos e desenvolvimento contínuo das extensões do protocolo,

[5]https://tools.ietf.org/html/rfc6507
[6]https://www.ietf.org/rfc/rfc2543.txt

tal como a revisão das definições (RFC 3261[7]) e publicação de outras RFCs como 3262[8], 3263[9], 3264[10], e 6665[11].

SIP é um protocolo de sinalização, presença e mensagens instantâneas da camada de aplicação da pilha TCP/IP, desenvolvido para criação, alteração dos parâmetros e finalização de sessões multimídia, podendo estas serem do tipo *unicast* (ponto a ponto) ou *multicast* (conferência), como uma ligação VOIP. Conforme [Johnston 2015] o protocolo está baseado na troca de mensagens de texto em pacotes UDP (preferencialmente), utilizando a arquitetura 'cliente-servidor' importada do Protocolo de Hiper Texto (*Hyper Text Protocol* - HTTP) e endereçamento do Protocolo Simples de Transferência de Correio (*Simple Mail Transfer Protocol* - SMTP).

Conforme as definições, o SIP é capaz de estabelecer ou finalizar uma sessão, com controle dinâmico do número de usuários, devido ao suporte de 5 funcionalidades básicas: determinação do destino, identificação da disponibilidade do usuário, detalhes da mídia e parâmetros, definição dos parâmetros no ambiente e gerenciamento da sessão. Essas funcionalidades são estabelecidas através de uma lista de métodos, que indicam diferentes ações ao longo do processo de inicialização, alteração ou encerramento das sessões. Abaixo são listados os 6 métodos básicos, conforme RFC3261:

- *INVITE*: utilizado para convidar um sistema remoto a participar de uma sessão;
- *REGISTER*: método utilizado para registrar o endereço do contato em um servidor SIP;
- *BYE*: indica o pedido de encerramento da sessão e pode ser enviado por qualquer participante;
- *ACK*: método utilizado para confirmação do recebimento do aceite ao convite pelo sistema remoto;
- *CANCEL*: cancela requisições pendentes;
- *OPTIONS*: utilizado para detectar os detalhes de um servidor SIP.

Importante ressaltar a presença de outros 8 métodos, segundo [Johnston 2015], definidos em RFCs separadas como *NOTIFY* (RFC2848[12]), *UPDATE* (RFC3311[13]) e *INFO* (RFC6086[14]). Muitos desses métodos estão ligados principalmente às características de presença e mensagens instantâneas do protocolo, fugindo do escopo desse trabalho que está ligado à comunicação VOIP.

Segundo as definições do protocolo, os principais elementos presentes na arquitetura SIP são:

- Usuário Agente (*User Agent* - UA): pode atuar como cliente (*User Agent Client* - UAC) ou servidor (*User Agent Server* - UAS), iniciando ou respondendo à requisição, respectivamente.

[7] https://www.ietf.org/rfc/rfc3261.txt
[8] https://www.ietf.org/rfc/rfc3262.txt
[9] https://www.ietf.org/rfc/rfc3263.txt
[10] https://www.ietf.org/rfc/rfc3264.txt
[11] https://www.ietf.org/rfc/rfc6665.txt
[12] https://tools.ietf.org/html/rfc2848
[13] https://tools.ietf.org/html/rfc3311
[14] https://tools.ietf.org/html/rfc6086

- Servidor Proxy: entidade intermediária responsável por encaminhar as requisições dos usuários, atuando como UAC e UAS, com base em regras previamente estipuladas. O servidor Proxy não inicializa ou finaliza uma sessão, fornece suporte para estabelecê-la.
- Servidor Registrar: aceita as requisições de registro, guardando essas informações em base de dados para posterior consulta dos servidores do mesmo domínio.
- Servidor de Redirecionamento: responsável por retornar às requisições, quando necessário, indicando o endereço atualizado do UAS com base nas informações guardadas no Registrar.
- Servidor Gateway: é uma aplicação que faz interface de uma rede SIP com outra rede utilizando um protocolo de sinalização distinto, como PSTN.

Conforme descrito na Figura 3 (fonte: elaboração própria), são apresentados detalhes da mensagem *INVITE* enviada por Alice (UAC) a Bob (UAS), que está operando no endereço "bob.avaya.unisinos.br", convidando-o a participar de uma sessão. Ao receber a mensagem, o UAS irá responder conforme uma numerosa lista padrão de possíveis respostas, divididas em categorias: 1xx (*Information*), indicativo de que uma requisição está em processamento, mas ainda não foi aceita ou finalizada; 2xx (*Success*), requisição aceita; 3xx (*Redirection*), encaminhamento da requisição para outro endereço; 4xx (*Client Error*), erro no cliente devido a falha na requisição; 5xx (*Server Error*), requisição não finalizada devido falha de servidor causado por erro no receptor; 6xx (*Global Failure*), requisição falhou.

```
INVITE sip:bob@unisinos.br SIP/2.0
Via: SIP/2.0/UDP bob.avaya.unisinos.br;branch=z9hG99sa0xkdyfy
To: Bob <sip:bob@unisinos.br>
From: Alice <sip:alice@unisinos.br>;tag=00x99
Max-Forwards: 10
Call-ID: 887yyyj78y2htg
CSeq: 1 INVITE
```

Figura 3. Exemplo de mensagem de convite do SIP

A Figura 4 (fonte: elaboração própria com base em [Johnston 2015]) descreve os passos necessários para estabelecer uma ligação VOIP entre membros de uma mesma instituição. Como Alice não sabe em qual dispositivo telefônico Bob está registrado, ela inicia o processo enviando um convite (*INVITE*) através de um servidor Proxy, facilitando na identificação do endereço de destino. Ao receber a mensagem, o servidor atualiza o cabeçalho da mensagem e encaminha para o destino, que confirma o recebimento (*180 Ringing*). Após a confirmação, Bob envia uma mensagem aceitando o convite (*200 OK*), que é novamente manipulada pelo servidor proxy antes de ser enviada para Alice. Após esse último ajuste do servidor, Alice terá as informações necessárias para enviar o conhecimento (*ACK*) do aceite direto para Bob, permitindo que então seja estabelecida a sessão multimídia. Para finalizar a sessão, Bob envia a mensagem de encerramento, lembrando que a mensagem *BYE* poderá ser enviada por qualquer um dos participantes a qualquer momento.

Como é possível detectar, o tráfego de dados do SIP é restrito à troca de mensagens para identificação do endereço do sistema remoto, inicialização, alteração e encerramento da sessão, ficando a cargo de outros protocolos, como Protocolo de Tempo Real (*Real*

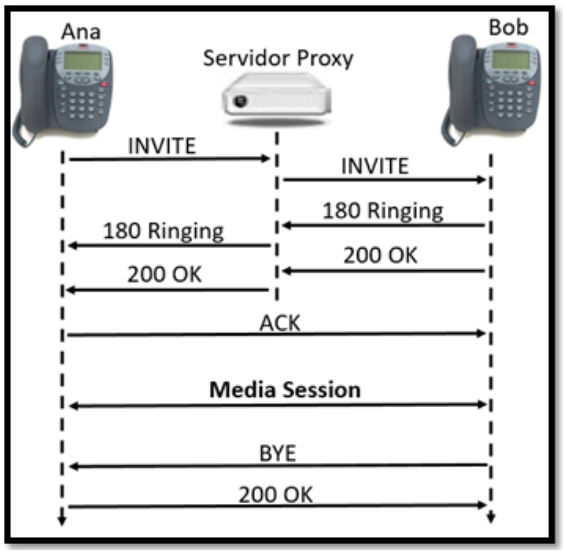

Figura 4. Exemplo de chamada SIP com servidor Proxy

Time Protocol - RTP) e Protocolo de Descrição da Sessão (*Session Description Protocol* - SDP), a sincronização de pacotes de comunicação e detalhes da sessão. Dessa forma, a busca por sigilo às ligações demanda uma solução capaz de convergir a estrutura do SIP com outros protocolos e modelos criptográficos, resultando em uma organização de segurança capaz de promover a confidencialidade dos dados trafegados em VOIP.

3. TRABALHOS RELACIONADOS

Associando as características do IBE com o padrão criptográfico EECMO, [Deusajute] propõe o sigilo às comunicações VOIP através de um método em que a troca de chaves de proteção pelos usuários ocorre após três rodadas iniciais, permitindo a criptografia e assinatura dos dados antes de estabelecer a conexão multimídia. A solução descrita pelo autor apresenta um processo de criptografia de ponta a ponta, associando a funcionalidade da PKG aos servidores proxy do SIP, iniciando a troca das chaves junto com o processo de registro e troca de mensagens de convite.

Na RFC4474[15] publicada por [Elwell 2007], é apresentado um método para assinar digitalmente as mensagens SIP, introduzindo dois novos campos à estrutura inicial das mensagens SIP, incluindo a assinatura digital do remetente no campo *Indentity* e informações do algoritmo utilizado no campo *Identity-Info*. Com essas informações o destinatário será capaz de validar a autenticidade da origem da requisição ou resposta SIP. A manipulação desses campos pode fornecer suporte a outras soluções, elevando a capacidade de associação do SIP a protocolos e esquemas de segurança.

Através do modelo IBE e método específico de distribuição de chaves, o trabalho apresentado por [Bo and Shu 2011] descreve a viabilidade de utilização do protocolo SIP com padrões assimétricos de criptografia, criando estrutura matemática capaz de suportar os requisitos do ambiente em que há troca de chaves entre os envolvidos. A PKG nesse ambiente é responsável por fornecer os dados iniciais, sem alternância dos fatores geradores dos grupos criptográficos que são raiz para geração das chaves privadas.

[15]https://tools.ietf.org/html/rfc4474

4. IBE e SIP

A busca por uma solução alternativa de proteção idealizada por [Shamir 1985] parece adaptar-se ao cenário de comunicação VOIP, no qual o perímetro de conexão é normalmente amplo e os usuários habitualmente não possuem canal privado de comunicação, tão pouco notam a necessidade prévia de interlocução com outros participantes, o que permitiria a antecipação de troca de chaves criptográficas, por exemplo. Dessa forma, há espaço para desenvolvimento de soluções que agreguem a estrutura do esquema criptográfico IBE à organização do protocolo SIP, propondo a confidencialidade das comunicações VOIP.

Utilizando como referência o exemplo anterior da Figura 4, o ambiente se mostra propício à solução apresentada por [Deusajute], uma vez que a estrutura de comunicação está ligada à organização de rede da instituição em que Alice e Bob trabalham, promovendo uma visão mais clara dos limites de conexão e permitindo associação da PKG no servidor Proxy. No entanto, a proposta carece de resposta para os ambientes nos quais a conectividade está sob gerenciamento descentralizado.

Na busca por respostas a essa necessidade, é crucial a formatação de estratégia que permita ampliar a capacidade de distribuição das chaves criptográficas, mesmo nos cenários em que os usuários estejam conectados a estruturas desconhecidas de rede, como a Internet. Dessa forma, o modelo de segurança proposto neste documento utiliza o método de criptografia IBE associado a um sistema de distribuição de chaves capaz de adaptar-se aos diversos cenários, manipulando o conteúdo das mensagens SIP permitindo a identificação dos usuários, auxiliar na troca de chaves e garantir acesso às informações necessárias para criptografia dos dados em comunicação VOIP.

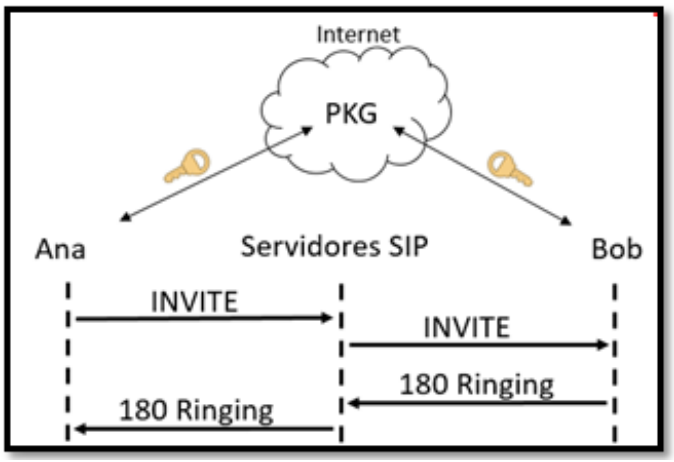

Figura 5. Modelo conceitual de criptografia VOIP utilizando IBE

Ponto crucial para construção do modelo conceitual descrito na Figura 5 (fonte: elaboração própria), a disposição da PKG na Internet, associada à extensão das características básicas propostas na RFC4474, tornam viável a criação de soluções capazes de assinar digitalmente e criptografar o conteúdo de sessões multimídia. A PKG será consultada nas rodadas iniciais, fornecendo acesso ao fator público e a chave privado aos usuários, permitindo que os mesmos possam gerar e trocar a chave de segurança de forma segura antes do envio das mensagens *Invite* e *180 Ringing*.

Após a distribuição da chave de segurança, os participantes da ligação passarão a

utilizá-la para criptografia dos dados ao longo da sessão multimídia, como uma ligação VOIP. Para adicionar novos participantes, basta que estes estabeleçam as etapas iniciais com um UAS já presente na sessão, o qual irá fornecer acesso à respectiva chave de segurança para acesso ao conteúdo e permitir envio de dados criptografados à sessão.

5. PROTÓTIPO DE IMPLEMENTAÇÃO

Através do projeto fone@RNP, a Rede Nacional de Pesquisa (RNP) oferece serviços de VoIP de forma alternativa e colaborativa aos usuários, permitindo a realização de chamadas telefônicas para outros membros sem custo por ligação. No entanto, tal gratuidade não exime o serviço de oferecer funcionalidades de segurança, sendo relevante o desenvolvimento de estudos para aplicação de métodos de sigilo às chamadas. Nesse contexto, a solução proposta a seguir visa garantir o requisito de confidencialidade através do modelo IBE de proteção, o qual permite usar uma informação de domínio público no processo de criptografia. Foi elencado nesta proposta o endereço eletrônico, pois o mesmo é utilizado pelo SIP na localização do destinatário, podendo também ser considerado o uso do endereço telefônico.

Para viabilizar o uso do modelo IBE é necessária a inclusão da PKG na arquitetura do fone@RNP, pois ela necessitará ser acessada pelas duas partes envolvidas em uma comunicação, o agente chamador (UAC) e o agente chamado (UAS). Durante o estabelecimento da comunicação, o agente chamador deverá acessar a PKG para obtenção dos elementos públicos, já o agente chamado também necessitará acessar a PKG para recuperação da chave privada. A obtenção dos valores pelas duas partes é exigida para a negociação da chave criptográfica compartilhada. A Figura 6 (fonte: elaboração própria) apresenta a arquitetura do fone@RNP com a inclusão da PKG no mesmo nível do SIP Router Central (SRC), localização proposta para que ela seja gerenciada de forma centralizada e acessada por qualquer instituição cliente. Importante destacar que a arquitetura do fone@RNP menciona a possibilidade de isolamento lógico das instituições clientes através do uso de vários SIP Router Local hierarquizados.

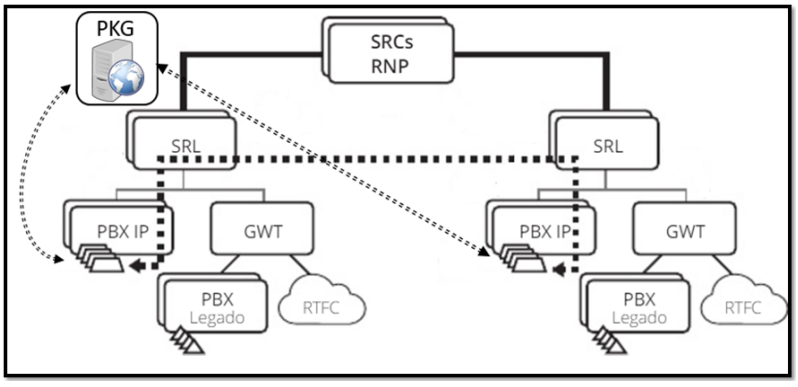

Figura 6. Abstração da estrutura fone@RNP com IBE.

Embora a confidencialidade seja garantida com a implementação da PKG é importante a elaboração de um protocolo que assegure que os elementos públicos e a chave privada estejam sendo distribuídos por ela. Caso contrário, uma entidade, passando-se pela PKG, pode encaminhar os elementos públicos de uma parte maliciosa ao agente chamador forjando ser os elementos públicos do destinatário da comunicação. Caso este

cenário seja concretizado, a comunicação poderia ser interceptada e o requisito de confidencialidade não seria garantido. Uma alternativa para isso é que os elementos públicos e chave privada sejam distribuídos assinados digitalmente pela PKG, possibilitando que as partes possam verificar a origem da mensagem. Uma alternativa para possibilitar que as partes autentiquem a PKG durante a distribuição dos elementos públicos e privados pode ser implementado o esquema de assinatura digital ECCSI, permitindo às partes envolvidas na comunicação verificarem o identificador da PKG. Este esquema é especialmente interessante em cenários compostos por equipamentos com algum tipo de restrição de recursos.

A autenticação da PKG também pode ser assegurada através do uso de uma Infraestrutura de Chaves Públicas - ICP, nesse caso é atribuido à PKG um certificado digital no formato X.509 e pode fazer uso dele para assinar digitalmente as informações enviadas aos agentes. Da mesma forma que é importante para a segurança das comunicações garantir que os agentes confirmem a origem dos elementos criptográficos recebidos, também é fundamental que a PKG consiga verificar a identidade dos agentes que estão solicitando algum elemento, principalmente, o agente chamado em uma comunicação que receberá a chave privada. Caso a PKG envie a chave privada a um agente malicioso, a segurança da comunicação está comprometida. O uso de uma ICP permite mitigar este risco, pois os agentes podem ser obrigados a comprovar a sua identidade à PKG para iniciar uma comunicação. Independente do uso do esquema ECCSI ou de uma ICP é importante que o requisito de autenticação seja implementado para que o modelo IBE possa cumprir o seu papel e garantir a confidencialidade das comunicações.

6. RESULTADOS ESPERADOS

A implementação de IBE no serviço fone@RNP possibilitará a organização de um ecossistema de comunicação usando formas mais simples para a distribuição das chaves criptográficas que asseguram a confidencialidade das chamadas. Enquanto a maioria dos criptossistemas apresenta dificuldades na garantia das identidades dos usuários associados às chaves criptográficas e necessita assegurar que as partes envolvidas possuam conhecimentos técnicos para gerenciamento das chaves, no modelo modelo IBE a chave é uma informação pública do usuário, por exemplo o endereço eletrônico, permitindo que as partes conheçam a identidade dos seus interlocutores. Além disso, no modelo IBE o gerenciamento das chaves é responsabilidade da PKG, a qual centralizará as funções de geração e armazenamento das chaves utilizadas nas comunicações, possibilitando aos usuários uma comunicação segura de maneira transparente. Outro ponto que deve ser destacado na implementação do modelo IBE é que, em consequência do armazenamento centralizado das chaves, ligações sigilosas podem ser recuperadas caso ocorra algum tipo especial de demanda, por exemplo, aquelas envolvendo questões jurídicas. Em um ambiente governamental podem ocorrer situações que conversas realizadas através do serviço fone@RNP necessitam ter a sua classificação de segurança removida, algo tecnicamente possível com o uso do modelo IBE e que pode ser dificultado com o uso de outros criptossistemas. O modelo IBE ainda é pouco estudado pela comunidade científica brasileira, enquanto que a comunidade internacional vem realizando inúmeras pesquisas e determinando padronizações para esse tipo de criptografia, como é o caso da RFC5091[16] e

[16]Identity-Based Cryptography Standard.

RFC6507[17] . A implementação deste modelo no fone@RNP pode despertar o interesse da comunidade científica e produzir a expansão da pesquisa do tema no Brasil, permitindo análises mais detalhadas sobre a possibilidade de utilização de IBE para garantir os requisitos de segurança em outras aplicações. A utilização de IBE no fone@RNP viabiliza que as instituições participantes se comuniquem por VoIP e se conectem com as saídas para a PSTN de forma confidencial. Atualmente, o fone@RNP dispõe de um sistema de monitoramento da infraestrutura central do serviço e dos servidores que ficam nas instituições participantes. De forma análoga, se pretende que as informações relativas ao IBE sejam integradas ao sistema de estatísticas do fone@RNP. Assim, será possível a geração de relatórios contendo dados sobre diferentes aspectos do esquema. Tais dados permitirão a realização de pesquisas em Segurança da Informação pela comunidade acadêmica brasileira em tópicos, como por exemplo, criptoanálise, eficiência de utilização, entre outros.

7. COMENTÁRIOS FINAIS

A implementação de um protocolo que garanta a confidencialidade das comunicações telefônicas no sistema fone@RNP é necessário para proteger a soberania nacional e assegurar que toda a sorte de informações sigilosas trocadas entre as diferentes instituições que utilizam o sistema sejam preservadas. No entanto a definição do criptossistema que garantirá tal requisito não impacte na usabilidade do serviço fornecido pela RNP. Neste sentido, o modelo IBE apresenta-se como uma alternativa para proteger as comunicações nacionais, pois atenua o impacto aos usuários a partir da centralização dos serviços na PKG.

É importante ressaltar que a presença da PKG é um ponto crítico à segurança das comunicações, da mesma forma que qualquer componente que concentre a confiança em um sistema. Por isso,é mandatório a implementação de controles que garantam a segurança da PKG, evitando o seu comprometimento e consequentemente o vazamento das chaves criptográficas utilizadas para garantir a confidencialidade das comunicações. Da mesma forma, devem ser definidos processos rigorosos para a recuperação das chaves criptográficas das comunicações, pois a credibilidade do criptossistema é importante para a sua adoção.

Por fim, embora existam implementações de IBE para a proteção de conversas telefônicas, este artigo apresenta uma proposta para uso do modelo na arquitetura do fone@RNP. Até o presente momento, os autores não realizaram implementações deste modelo para criptografia de comunicações no serviço da RNP, etapa esta que deverá ser conduzida para conhecer a viabilidade do uso de IBE no fone@RNP.

Referências

Bo, W. S. and Shu, L. C. (2011). Identity-based sip authentication and key agreement. In *2011 Seventh International Conference on Computational Intelligence and Security*, pages 808–811.

Boneh, D. and Franklin, M. (2003). Identity-based encryption from the weil pairing. *SIAM J. of Computing.*, 32(3):586–615.

Boyen, X. and Martin, L. (2007). Identity-based cryptography standard (ibcs)(version 1), request for comments (rfc) 5091.

[17]Elliptic Curve-Based Certificateless Signatures for Identity-Based Encryption.

Deusajute, A. M. *Proposta de um mecanismo de segurança alternativo para o SIP utilizando o protocolo Massey-Omura aperfeiçoado com o uso de emparelhamentos bilineares.* PhD thesis, Universidade de São Paulo.

Elwell, J. (2007). Connected identity in the session initiation protocol (sip).

Groves, M. (2012). Elliptic curve-based certificateless signatures for identity-based encryption (eccsi).

Johnston, A. B. (2015). *SIP: understanding the session initiation protocol*. Artech House.

Martin, L. (2008). *Introduction to Identity-Based Encryption*. Artech HouseIT, Norwood, Massachusetts - EUA.

Schneier, B. (1996). *Applied Cryptograpy*. John Wiley and Sons, Inc, Minneapolis-MI, EUA.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. *Advances in Cryptology - 1984.*, LNCS(196):47–53.