Introduzindo Segurança no Correio Eletrônico Internet

Edjozane Campos Cavalcanti
Walfredo da Costa Cirne Filho[1]
Francisco Vilar Brasileiro

{zane, walfredo, fubica}@dsc.ufpb.br

Universidade Federal da Paraíba
Centro de Ciências e Tecnologia
Departamento de Sistemas e Computação
Laboratório de Sistemas Distribuídos
Aprígio Veloso, s/n - Bodocongó
CEP: 58.109-970 - Campina Grande - PB - Brasil

Resumo

O Simple Mail Transfer Protocol (SMTP) é o padrão TCP/IP que especifica como o serviço de correio eletrônico transmite uma mensagem na Internet. Ele não trata aspectos como a possibilidade de interceptação da mensagem e falsificação do remetente. Várias tentativas tem sido feitas para remediar este problema, mas todas elas têm limitações, seja porque são ferramentas externas ao sistema de e-mail, ou porque dependem de uma complexa infra-estrutura global de distribuição de chaves de criptografia, ou ainda porque ignoram a necessidade de garantir localmente a segurança das mensagens armazenadas. Este trabalho propõe um protocolo com recursos de segurança, que denominamos Secure Simple Mail Transfer Protocol (SSMTP), que pode ser facilmente integrado na aplicação de e-mail e que não depende de nenhum serviço de suporte. Além do SSMTP, definimos o Local Mail Security Procedures (LMSP), que se constitue de um conjunto de procedimentos para a garantia da privacidade e segurança locais. Em conjunto, o SSMTP e o LMSP provêm segurança ao serviço de correio eletrônico Internet, sem apresentar nenhum dos problemas acima listados.

Abstract

The Simple Mail Transfer Protocol (SMTP) is the TCP/IP standard for electronic mail transfer from one computer to another. It does not address security aspects, like catching the message and faking the sender. There are a number of solutions to this, but they either require the use of an external cryptography application, or the availability of a global cryptographic key distribution infrastructure, or because they do not provide any kind of mechanism to avoid local attacks to the stored mails. This work specifies the Secure Simple Mail Transfer Protocol (SSMTP), which is a SMTP secure extension. It was designed to be easily integrated within the e-mail software and to run independently of any distribution key supporting service. Besides SSMTP, this work defines the Local Mail Security Procedures (LMSP) to assure local security for e-mail servers. Together, SSMTP and LMSP provide a safe Internet e-mail service and do not have any of the problems listed above.

1. Introdução

O problema de segurança em sistemas de computação é um tópico bastante abrangente, envolvendo desde aspectos como o acesso e manipulação, intencional ou não, de informações confidenciais por usuários não autorizados, até a utilização não autorizada de um computador ou de seus dispositivos periféricos [Soares 95].

As técnicas de proteção especificam mecanismos para segurança da informação (dados armazenados), para segurança física (intrusos e desastres) e segurança da comunicação (dados que trafegam numa rede) [Russel 92]. Com a crescente utilização de redes de computadores, a segurança da comunicação assume uma importância cada vez maior.

---

[1] Atualmente em doutoramento na UCSD (University of California San Diego), com suporte da CAPES (processo BEX2428/95-4).

A criptografia é o recurso utilizado para garantir a segurança de dados que trafegam numa rede. A criptografia é a ciência de escrever a informação em cifras, de forma que somente as pessoas autorizadas possam compreendê-la. O objetivo da criptografia é a construção de cifras invioláveis que garantam a privacidade e a autenticação das mensagens transmitidas.

Existem duas abordagens básicas para a criptografia: a simétrica e a assimétrica. Na criptografia simétrica (ou criptografia de chave única) a mesma chave é utilizada para cifrar e decifrar a informação. Na criptografia assimétrica (ou criptografia de chave pública) são geradas duas chaves, uma pública e outra privada, em que uma decriptografa o que a outra criptografou.

O sistema de criptografia simétrica apresenta dois grandes problemas. Primeiro, cada par de usuários que estabelece comunicação precisa escolher uma chave. Assim, se um dado usuário comunica-se com outros n usuários, ele precisa conhecer n chaves distintas. Em um ambiente onde n usuários comunicam-se dois a dois, há necessidade de $(n^2 - n)/2$ chaves. Segundo, existe o problema do destinatário da mensagem precisar utilizar a mesma chave que o remetente utilizou, levando à questão de como distribuir a chave de maneira segura.

Na criptografia assimétrica só existe a necessidade da existência de duas chaves por usuário: a chave privada, que não é conhecida por nenhum outro participante do sistema, e a chave pública, que é distribuída sem restrições.

O correio eletrônico (ou e-mail - Eletronic Mail) Internet, embora seja o maior sistema existente para troca de mensagens eletrônicas [Burns 95] [Garfinkel 95], não oferece recursos de segurança, sendo necessário ao usuário implementar o seu próprio plano de prevenção de acessos indesejados aos seus e-mails. Neste trabalho, propomos um ambiente que possibilita a troca segura de e-mails na Internet, de forma transparente para o usuário. A nossa solução é composta de um protocolo de transferência de e-mails (SSMTP) e de procedimentos locais (LMSP).

O restante deste artigo é composto de quatro seções. Na seção 2 descrevemos a arquitetura do correio eletrônico Internet e apresentamos soluções existentes para a privacidade e autenticação em e-mail Internet. Na seção 3 mostramos a nossa especificação do Secure Simple Mail Transfer Protocol e do Local Mail Security Procedures. Na seção 4 apresentamos aspectos da implementação de um programa de transferência de mensagens e de um ambiente de correio eletrônico que implementam o SSMTP e o LMSP. Na seção 5 fazemos a conclusão do nosso trabalho.

2. Arquitetura do Correio Eletrônico Internet

A Internet é notoriamente conhecida como a maior rede de computadores do mundo [Comer 95]. Ela fornece uma variada gama de serviços a seus usuários, sendo que o correio eletrônico é um dos mais antigos e também dos mais populares.

A Internet está baseada no conjunto de protocolos TCP/IP. No TCP/IP, a transferência de correio eletrônico entre máquinas distintas se dá através do protocolo Simple Mail Transfer Protocol (SMTP).

2.1. Componentes Básicos

A estrutura de uma máquina que implementa o SMTP inclui as caixas-postais dos usuários, uma ou mais áreas para enfileiramento de mensagens em trânsito e um ou mais processos rodando em *background* (*daemons*) para entrega e recebimento dos e-mails [RFC 1123] (veja a figura 1). Abaixo, segue a descrição de cada um destes componentes:

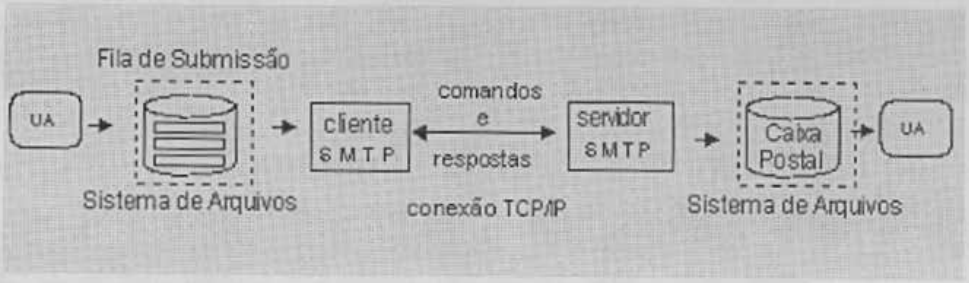

Figura 1: Modelo Funcional SMTP

- Caixa Postal - É uma área de armazenamento, na qual as mensagens permanecem até que o usuário as elimine ou as transfira para outra área. É a versão eletrônica da caixa postal do sistema de correios tradicional.

- Área de Enfileiramento das Mensagens - É uma área onde as mensagens são armazenadas para futura transmissão.
- Agente Usuário - O UA[2] é o software de correio eletrônico que permite ao usuário confeccionar, enviar, receber e ler mensagens, bem como manipular a caixa postal.
- Agente de Transferência de Mensagens - O MTA[1] é o programa que coloca a mensagem diretamente na caixa postal, quando o UA de destino está ligado a ele, ou a encaminha para a máquina de destino, usando o SMTP. Durante o diálogo entre duas máquinas que implementam SMTP, a máquina de origem age como cliente SMTP, e a máquina de destino age como servidor SMTP aceitando as mensagens e as colocando na caixa postal do destinatário. As máquinas que rodam MTAs são conhecidas como servidores de e-mail.

2.2. Procedimentos do SMTP

Um usuário utiliza um UA para confeccionar a mensagem e solicita ao sistema de correio eletrônico que encaminhe o e-mail ao destinatário. O processo de transferência de mensagens é executado em *background*. O cliente SMTP abre uma conexão de transporte com o servidor de correio eletrônico da máquina destino e espera por uma mensagem 220 (Ready for mail). Em seguida, o cliente envia uma mensagem HELO e recebe do servidor a sua identificação. Estabelecida a comunicação, a transação para a transmissão dos e-mails é iniciada com o comando MAIL. O receptor prepara-se para receber os novos e-mails e responde com uma mensagem 250 (Ok). O cliente envia uma série de comandos RCPT, tantos quantos forem os destinatários, que são respondidos com 250 (Ok) ou 550 (No such user here).

Após um ou mais comandos RCPT, o cliente envia o comando DATA. O comando DATA informa ao destinatário que o cliente está preparado para transferir o conteúdo do e-mail. O servidor responde com uma mensagem 354. Para encerrar é enviado um comando QUIT, que é respondido com um 221, concordando com o término. Veja na figura 2, a comunicação entre dois sistemas de e-mail Internet, utilizando SMTP (as linhas iniciadas por S são geradas pelo servidor e as começadas por C, pelo cliente).

```
S: 220 fenix.cgsoft.softex.br Simple Mail Transfer Service Ready
C: HELO dsc.ufpb.br
S: 250 fenix.cgsoft.softex.br
C: MAIL From: <maria@dsc.ufpb.br>
S: 250 ok
C: RCPT To: <joao@cgsoft.softex.br>
S: 250 ok
C: DATA
S: 354 Enter mail, end with .
C: Date: Sun, 28 Jan 1996 23:05:00 -0200 (EDT)
C: From: Maria Silva <maria@dsc.ufpb.br>
C: To: joao@cgsoft.softex.br
C: Subject: Reuniao
C:
C: Nossa reuniao esta confirmada para hoje (28/01), as 15:00.
C: Maria
C: .
S: 250 ok
C: QUIT
S: 221 fenix.cgsoft.softex.br Service closing transmission channel
```

Figura 2: Exemplo de diálogo cliente/servidor SMTP

Os procedimentos para transferências de e-mails, comandos e respostas, são definidos no RFC 821, que especifica o SMTP. Como demonstrado no exemplo, a comunicação entre o cliente e o servidor é um diálogo, controlado pelo cliente. O cliente envia um comando e recebe uma resposta.

2.3. Segurança em Correio Eletrônico Internet

No ambiente de correio eletrônico Internet não há nenhum tratamento para segurança da mensagem, nem na transmissão, pois o SMTP não trata a possibilidade de interceptação da mensagem e falsificação do remetente, nem na máquina servidora, pois as mensagens ficam armazenadas desprotegidas nas caixas-postais dos usuários e na fila de transmissão.

---

[2] Não traduzimos as siglas UA (User Agent) e MTA (Message Transfer Agent), para evitarmos confusões com ATM (Asynchrnous Transfer Mode), que normalmente não é traduzida.

O RFC 1421 define procedimentos para criptografia e autenticação de e-mails Internet, chamados de serviços Privacy Enhanced Mail (PEM), utilizando criptografia simétrica e assimétrica. O RFC 1422 especifica suporte a mecanismos de gerenciamento de chaves baseado em criptografia de chave pública. O RFC 1423 provê os algoritmos de criptografia usados nos RFC 1421 e 1422 e o RFC 1424 detalha os procedimentos para o gerenciamento de chaves e infra-estrutura para o suporte a esses serviços [RFC 1421].

No PEM, as chaves públicas devem ser assinadas por uma Autoridade Central e apenas as chaves oficialmente assinadas podem ser usadas. O processo de assinatura de chaves é denominado certificação. Um certificado é uma estrutura de dados que contém o nome do usuário, a chave pública e o nome da entidade organizacional a qual o usuário pertence.

A Autoridade Central agindo como a raiz da hierarquia de certificados para a comunidade Internet, com a necessidade de pagamento de uma taxa para o seu funcionamento e necessidade de que todas as chaves sejam certificadas, demanda suporte e custo adicionais. A complexidade imposta pela certificação de chaves, sem dúvida, torna a possibilidade de acesso ao sistema por usuários não autorizados mais difícil. Entretanto, é também mais difícil de implementar e de utilizar: o esquema de distribuição de chaves do PEM é tão complexo e demanda tanto esforço para ser instalado, que até o presente momento não está operacional.

Além disso, o PEM não provê nenhum mecanismo para evitar o acesso indevido as mensagens armazenadas nos servidores de e-mail (sejam elas mensagens recebidas ou por enviar).

Assim, a criptografia de e-mails Internet é hoje feita quase que exclusivamente através do Pretty Good Privacy (PGP), software de criptografia disponível gratuitamente, que é utilizado para a criptografia da mensagem antes da transmissão, como também para criptografia dos arquivos, garantindo a segurança local.

O PGP não especifica uma política para distribuição das chaves: os usuários assinam as chaves uns dos outros e criam uma comunidade interconectada de usuários de chaves públicas [Stallings 95], diferentemente do enfoque do PEM, o qual depende de uma Autoridade Central para certificação das chaves. Entretanto, o PGP apresenta uma grande limitação: é um software totalmente independente do ambiente de correio eletrônico. Isto significa que o usuário precisa escrever a mensagem fora do ambiente de e-mail, criptografá-la com o PGP, importar o arquivo cifrado para o ambiente de correio eletrônico e, finalmente, enviar a mensagem. De maneira análoga, na recepção de uma mensagem cifrada pelo PGP, é necessário exportá-la e decriptografá-la com o PGP, antes de lê-la, já fora do ambiente de e-mail. O fato do PGP ser uma solução externa ao software de correio eletrônico implica em grande perda de produtividade no seu uso. Além do mais, demanda a aprendizagem de comandos, que muitas vezes, não são amigáveis para o usuário final. Hoje, para obter a segurança desejada, além do software de correio eletrônico o usuário deve aprender a manipular um software de criptografia.

Recentemente, foi proposto o MOSS como uma substituição ao PEM [RFC 1847] [RFC 1848]. O MOSS é uma extensão do MIME[3] e não do SMTP. Portanto, ele está baseado nas regras de codificação e confecção de mensagens multi-parte do MIME. O maior mérito do MOSS em relação ao PEM é a flexibilidade no que diz respeito a distribuição de chaves.

Embora um serviço global de obtenção de chaves possa ser usado (quando estiver um dia disponível), o MOSS define como chaves podem ser obtidas diretamente, pela simples troca de e-mails internos (i. e., e-mails cujo destinários não são usuários finais, mas sim a implementação do MOSS). Esta abordagem propicia um bom grau de segurança, mas é vulnerável a ataques onde uma máquina intermediária comprometida se passa por destino, ao invés de rotear os pacotes (veja seção 3.3 para uma discussão mais detalhada sobre este problema). De qualquer forma, este nível de segurança deve ser suficiente para a grande maioria dos usuários Internet.

Todavia, apesar da evolução que o MOSS representa em relação ao PEM, ele não discute nada a respeito de como a segurança local dos e-mails armazenados nos servidores deve ser garantida.

3. Um Ambiente Seguro para E-Mail Internet

Em nossa solução para um ambiente com recursos de segurança na troca de e-mails Internet, procuramos deixar a segurança o mais transparente possível para o usuário. Assim, ao invés de termos o software de correio eletrônico e um software de criptografia, optamos por incluir os recursos de criptografia do PGP no MTA e UA. O PGP usa os principais algoritmos de criptografia para garantir a

[3] O MIME é um protocolo usado para especificar e descrever o formato do conteúdo de mensagens na Internet.

privacidade na troca de e-mails e para proteger arquivos. Ele é reconhecidamente um ótimo programa para proteger a privacidade e autenticação da correspondência eletrônica Internet, mas faz isto externamente ao programa de e-mail. Isso demanda do usuário a necessidade de aprender a usar o software corretamente, pois seu uso inapropriado pode levar à perda de informações ou não utilização dos recursos de sigilo e integridade necessários a uma determinada informação.

Assim, a nossa solução está baseada na extensão do SMTP para o Secure Simple Mail Transfer Protocol (SSMTP). O SSMTP possibilita a transmissão segura de mensagens eletrônicas em uma rede TCP/IP. Note que, ao contrário do MOSS, o SSMTP introduz segurança estendendo o próprio SMTP e não o MIME. Isto permite resolver a limitação do SMTP de que as mensagens contenham apenas caracteres de 7 bits [RFC 821], tornando desnecessária a codificação MIME, e, assim, reduzindo a largura de banda necessária para a transmissão dos e-mails.

Uma característica fundamental do SSMTP é sua não dependência de um serviço hierárquica de distribuição de chaves, como o requerido pelo PEM. Esta foi uma decisão de projeto, pois a experiência mostra que tal serviço é extremamente difícil de ser implementado [RFC 1636].

Entretanto, garantir apenas a transmissão segura não basta. É necessário ter certeza que a segurança não seja violada localmente. Dessa forma, a nossa proposta inclui ainda a especificação de procedimentos que garantem o sigilo local da informação. Ao conjunto desses procedimentos denominamos Local Mail Security Procedures (LMSP). O LMSP é composto de regras a serem utilizadas em um ambiente para e-mail Internet, na implementação de MTAs e UAs seguros.

Para incluir o sigilo e autenticação, o SSMTP adiciona comandos e respostas ao SMTP. Ele incorpora recursos de segurança através do uso de criptografia (simétrica e assimétrica) e para isso utiliza-se de um MTA seguro (Secure MTA - SMTA), implementado de acordo com o SSMTP e os procedimentos LMSP. Caso não tivéssemos o LMSP, um intruso ou mesmo o administrador do sistema poderia ler as caixas postais de outros usuários. Uma máquina que implementa o SSMTP é também servidora de chaves públicas.

O UA seguro (Secure UA - SUA), também implementado seguindo procedimentos LMSP, permite ao usuário utilizar ou não os recursos de segurança. É através do SUA que o usuário poderá ter o acesso aos e-mails criptografados, armazenados na caixa postal.

3.1. O SSMTP

O protocolo SMTP é constituído de um conjunto de itens básicos para a troca de e-mails e tem provado ser notavelmente robusto. Todavia, a necessidade de extensões ao protocolo tem se tornado evidente [RFC 1869].

O RFC 1869 provê uma estrutura na qual extensões podem ser especificadas de forma consistente, definindo meios através dos quais uma extensão ao diálogo SMTP pode ser reconhecida e possibilitando a um servidor informar quais as extensões que suporta. O SSMTP foi definido com base no RFC 1869, sendo uma extensão que acrescenta ao SMTP recursos de segurança. Um e-mail criptografado, em ambiente que implementa SSMTP, possui o campo de cabeçalho "Encrypted:", preenchido com o valor "SSMTP 1.0".

O objetivo do SSMTP é transferir de forma segura e-mails entre máquinas na Internet, através do uso de criptografia assimétrica e simétrica. Utiliza-se a criptografia simétrica para cifrar a mensagem, pois na criptografia assimétrica os algoritmos são lentos, o que torna muito vagarosa a cifragem e decifragem de uma grande quantidade de dados. Uma vez cifrada a mensagem, utiliza-se a criptografia assimétrica para cifrar a chave única (que representa muito menos informação que a mensagem propriamente dita) usada na criptografia da mensagem, garantindo a privacidade no seu envio pela rede. Esse é o mesmo método utilizado pelo PGP, no qual nos baseamos.

Para cifragem do e-mail será utilizado o algoritmo IDEA (International Data Encryption Algorithm). O IDEA é um algoritmo de chave única, que trabalha com chave de 128 bits. Ele usa soma em módulo de 2^{16}, ou-exclusivo e multiplicação em módulo de $2^{16} + 1$. Desenvolvido em 1990, o IDEA tem resistido a métodos aplicados com sucesso contra outros algoritmos. Não existe ainda um método de ataque efetivo contra o mesmo [Schneier 93].

A chave IDEA usada na criptografia do e-mail é chamada de chave de sessão. Ela será cifrada utilizando algoritmo RSA de criptografia de chave pública e será enviada com o e-mail para o destinatário, como valor de preenchimento do campo de cabeçalho "Key-Info:" (definido no RFC 1421). O método RSA [Rivest 78] de criptografia assimétrica é uma das mais poderosas formas de criptografia de chave pública conhecida até o momento. Ele se baseia na dificuldade de se fatorar o produto de dois números primos muito grandes.

A criptografia do e-mail torna a mensagem secreta. Para torná-la também autenticada (assinada), calcula-se a função MD5 do texto da mensagem e depois criptografa-se o resultado com a chave privada do remetente. O UA do destinatário decriptografa a informação recebida com a chave pública do remetente e também calcula a função sobre a mensagem recebida, comparando os resultados. Desta forma é possível detectar se houve ou não adulteração da informação. Caso tenha havido violação da informação, o usuário será devidamente informado.

A garantia de que não houve alterações se baseia nas caracteristicas da função MD5 (Message Digest 5) [RFC 1321]. Esta função, a partir de uma entrada de tamanho arbitrário, produz um número de 128 bits. Conjectura-se que é computacionalmente impossível produzir um texto a partir de um resultado MD5 [RFC 1321]. Assim, um eventual intruso não consegue adulterar a mensagem mantendo o mesmo resultado MD5, nem mesmo através da inclusão de um *dumb string*.

Note que com a assinatura digital é possível comprovar a origem de uma mensagem, pois somente o usuário remetente conhece a sua chave privada e portanto somente ele poderia tê-la cifrado. Um e-mail assinado possui o campo "MIC-Info:" [RFC 1421] preenchido com o valor produzido pelo cálculo da função MD5 do e-mail, criptografado com a chave privada do remetente.

A chave privada do usuário precisa permanecer secreta. Porém, tal chave é um número muito grande (da ordem de dezenas de dígitos) e o usuário não pode escolhê-lo. Isto torna sua memorização praticamente impossível. Dessa forma, optamos, baseados no PGP, por armazená-la criptografada com uma senha de acesso[4]. A senha de acesso pode ser uma frase contendo espaços, pontos, letras maiúsculas e minúsculas, caracteres especiais e pode ter qualquer tamanho. Como é escolhida pelo usuário, é muito mais fácil de ser decorada. Usamos a senha de acesso para obter, através da MD5, a chave IDEA que, de fato, criptografa (e decriptografa) a chave privada.

3.1.1. Procedimentos do SSMTP

O Modelo SSMTP utiliza o mesmo modelo SMTP (figura 1), definido nos RFC 821 e 1123, onde o UA e MTA foram substituídos pelo SUA e SMTA, respectivamente. O usuário utiliza um SUA para confeccionar a mensagem e solicita ao SMTA que encaminhe o seu e-mail ao destinatário. O processo de transferência de mensagem é executado em *background*.

Estabelecida a conexão de transporte com o servidor de correio eletrônico da máquina destino, o cliente espera por uma mensagem 220 (Ready for mail). Dando prosseguimento à inicialização da transferência, o cliente envia um comando EHLO[5] e deve receber as extensões que o servidor suporta. Em nosso caso, a extensão SSMTP indica que o servidor está apto a receber e-mails criptografados.

Caso o servidor não reconheça o EHLO ou não suporte SSMTP, o MTA continuará ou não a transferência da mensagem usando o SMTP, dependendo da escolha do usuário no momento do envio do e-mail. Caso o usuário tenha solicitado o envio obrigatoriamente com recursos de segurança, a transferência será abortada. Caso contrário, continuará sem os recursos de segurança.

O campo de cabeçalho "Security-Level:" denota o nível de segurança requerido para transmissão de um determinado e-mail. Os valores possíveis para este campo são *None*, *Optional* e *Mandatory*. É importante ressaltar que o valor *none* implica no fato de que o e-mail será enviado via SMTP.

Assim, a comunicação será estabelecida de acordo com o valor Security-Level e do suporte a SSMTP na máquina receptora da mensagem. A transação para a transmissão dos e-mails é iniciada com o comando MAIL. O comando MAIL envia a identificação do usuário remetente para a máquina destino. O receptor prepara-se para receber o novo e-mail e responde com uma mensagem 250 (Ok).

Após o a identificação do usuário, o enviador informa qual o destinatário do e-mail. Neste momento, há duas alternativas possíveis para o funcionamento do SSMTP. Caso o enviador já conheça a chave pública do destinatário, ele utiliza o comando RCPT. Caso contrário, envia um comando RCPT com o parâmetro PKEY (o parâmetro PKEY[6] indica a solicitação da chave pública do usuário destinatário). Em ambos os casos, o destinatário é especificado, embora no segundo, também esteja sendo solicitada sua chave pública.

O enviador já conhece a chave pública quando está configurado para usar uma infra-estrutura segura de distribuição de chaves. Neste caso, antes de iniciar a conexão de transferência de e-mail, o enviador faz uma consulta ao servidor de chaves solicitando a chave pública do destinatário.

---

[4] *Pass phrase*, no PGP.

[5] Conforme especificado no RFC 1869, um cliente que suporta extensões SMTP, inicia uma sessão usando o comando EHLO.

[6] Foi previsto na RFC 1869 que extensões ao SMTP poderiam utilizar parâmetros adicionais associados aos comandos MAIL e RCPT.

Quando o enviador solicita a chave pública do destinatário durante a transferência do e-mail, o receptor age também como o servidor de chaves. Um comando RCPT com parâmetro PKEY deve ser respondido com a chave pública do destinatário, com uma mensagem de usuário não tem chave pública ou com a mensagem de usuário inválido. Embora este procedimento não seja tão seguro quanto a obtenção da chave de um serviço especialmente projetado para este fim (veja seção 6.3), ele garante a independência de tais serviços. Este é um ponto fundamental no SSMTP, pois a dependência de um serviço externo para obtenção de chaves tem inviabilizado o uso de outras soluções (tal como o PEM), exatamente porque estes serviços implicam na criação de uma hierarquia segura de certificação de chaves que abranja toda a Internet, o que representa um enorme esforço administrativo e de suporte.

Após um comando RCPT bem sucedido, o cliente envia o comando DATA, que informa ao servidor que o conteúdo de um e-mail será transferido. O comando DATA negocia com a máquina destino o inicio do envio do e-mail criptografado. Se aceito, transmitir-se-á o e-mail. O servidor deverá responder com uma mensagem 250 (Ok).

Para encerrar, é enviado um comando QUIT. O comando QUIT deve receber uma resposta 221 concordando com o encerramento da conexão, ou uma resposta 500 se houver algum erro. Após isso, a conexão TCP/IP é encerrada.

Na figura 3, que segue abaixo, temos um exemplo de uma transferência de e-mail via SSMTP.

```
Solicitação de conexão TCP
S: 220 fenix.cgsoft.softex.br Ready
C: EHLO anjinho.dsc.ufpb.br
S: 250-fenix.cgsoft.softex.br
S: 250-SSMTP
S: 250 8BITMIME
C: MAIL From: <maria@dsc.ufpb.br>
S: 250 ok
C: RCPT To: <joao@cgsoft.softex.br> PKEY
S: 250-ok
S: 250 I3rRIGXUGWAF8js5wCzRTkdhO34PTHdRZY9Tuvm03M+NM7fx6qc5udixps2
   Lng0+wGrtiUm/ovtK
S: dinz6ZQ/aQ==
C: DATA
S: 354 Enter mail, end with .
C: Date: Sun, 28 Jan 1996 23:05:00 -0200 (EDT)
C: From: Maria Silva <maria@dsc.ufpb.br>
C: To: joao@cgsoft.softex.br
C: Encrypted: SSMTP 1.0
C: Security-Level: Mandatory
C: Key-Info: I3rRIGXUGWAF8js5wCzRTkdhO34PTHdRZY9Tuvm03M+NM7fx6qc5
   udixps2Lng0+ wGrtiUm/ovtKdinz6ZQ/aQ==w78xodj
C: MIC-Info: UdFJR8u/TIGhfH65ieewe2lOW4tooa3vZCvVNGBZirf/7nrgzWDAB
   z8w9NsXSexvAjRFbH oNPzBuxwmOAFeA0HJszL4yBvhG
C: Subject: Informacoes
C:
C: HB0eJzyhP+/fSStdW8okeEnv47jxe7SJ/iN72ohNcUk2jHEUSoH1nvNSIWL9MxD
C: tEjmF/zxB+bATMtPjCUWbz8Lr9wloXIkjHUlBLpvXR0UrUzYbkNpk0agV2IzUpk
C: 6UiRRGcDSvzrsoK+oNvqu6z7Xs5Xfz5rDqUcMlK1Z6720dcBWGGsDLpTpSCnpot
C: dXd/H5LMDWnonNvPCwQUHt==
C: .
S: 250 ok
C: QUIT
S: 221 fenix.cgsoft.softex.br Service closing transmission channel
Liberação da conexão TCP
```

Figura 3: Exemplo de Transmissão de E-Mail via SSMTP

Além dos procedimentos de uma transação para o envio de um e-mail, temos um comando adicional, o PKEY (note que existe também o parâmetro PKEY do comando RCPT). O PKEY é usado em uma nova conexão SSMTP, estabelecida apenas com o propósito de pegar a chave pública do usuário remetente, necessária para que se proceda a verificação de assinatura de um e-mail. Com uma nova conexão pretendemos obter mais segurança, dificultando a falsificação do remetente.

3.2. O LMSP

O LMSP constitue-se de um conjunto de regras que visam garantir a segurança local em uma máquina que implementa o SSMTP.

A primeira regra refere-se ao grau de segurança que o usuário estabelece para transmissão. Um e-mail pode ser enviado com três graus de segurança: obrigatória, opcional e nenhuma. A opção segurança obrigatória significa que o usuário estabeleceu que o e-mail só deve ser transmitido se a

máquina destino também implementa recursos de segurança, i.e., utiliza SSMTP. A opção de segurança opcional indica que o e-mail deve ser enviado preferencialmente de forma segura, mas que o usuário permite que o e-mail seja enviado caso a máquina destino não implemente recursos de segurança, ou seja, use apenas SMTP. Obviamente, quando nenhuma segurança é especificada para um determinado e-mail, ele é transferido usando apenas SMTP.

Note que, de acordo com o SSMTP, a definição do nível de segurança deve constar no campo "Security-Level:" do cabeçalho da mensagem. Quando a segurança for obrigatória, este campo é preenchido com o valor *Mandatory*. Para segurança opcional, o valor usado é *Optional* e, por fim, um e-mail sem segurança tem o valor *None* neste campo.

A segunda regra diz respeito a segurança do conteúdo dos e-mails. Os conteúdos dos e-mails recebidos devem ser armazenados criptografados. Se os e-mails forem recebidos já criptografados, são simplesmente armazenados pelo SMTA. Senão, são criptografados[7] e armazenados pelo SMTA.

A terceira regra estabelece que o SUA deve arquivar os e-mails nos *folders* devidamente criptografados.

A quarta regra especifica que os e-mails devem ser armazenados na área de enfileiramento de mensagens já cifrados pela chave de sessão. A chave de sessão é uma chave IDEA, utilizada para criptografia do e-mail. Ela é criptografada com a chave pública do usuário destinatário e enviada com o e-mail.

Se o usuário tiver determinado segurança *Mandatory* (de acordo com a regra número um), a chave de sessão deve ficar armazenada apenas na memória do SMTA, até a obtenção da chave pública do destinatário e seu encaminhamento. Isto implica que se o SMTA ou a máquina falharem, os e-mails enfileirados que solicitaram segurança obrigatória serão devolvidos ao remetente. Caso tenha sido solicitado segurança opcional, a chave de sessão pode também ser guardada em um arquivo, o que possibilita a recuperação de uma falha do servidor.

A quinta regra diz respeito à segurança do SUA e SMTA: como forma de garantir que o SUA e o SMTA não sejam modificados sem que essas alterações possam ser detectadas, devem existir disponíveis os programas fontes que testam a integridade de ambos, podendo o próprio usuário compilá-los em caso de suspeita de adulteração. Em posse do código fonte, o usuário pode, em última instância, procurar por trechos de códido que propositalmente introduzam falhas de segurança. Além disso, o resultado MD5 destes programas também deve estar amplamente disponível, facilitando sua verificação.

Dessa forma, objetivamos proteger as informações do usuário também localmente e não apenas durante a comunicação com outras máquinas.

3.3. Análise da Segurança

A nossa solução oferece um forma mais segura para troca de e-mails na Internet. Mas, na alternativa em que utilizamos a máquina servidora SSMTP também como servidora de chaves públicas, há, ainda, um problema de segurança nas transmissões: um impostor, num roteador, pode se fingir de destino, via a alteração do transporte TCP/IP deste roteador. Ao se fingir de destino, o impostor pode fornecer uma chave pública falsa para o destinatário. Isso possibilita o acesso à mensagem cifrada, uma vez que ele possui a chave privada do par pública/privada que forjou.

Todavia, grande parte dos problemas é resolvida, mesmo porque a maior parte deles é local, provocados por acessos indevidos ao sistema. Assim, a implementação dos procedimentos descritos no LMSP torna a quebra da segurança do sistema de e-mail muito mais difícil.

Além do mais, interceptar mensagens num roteador é difícil, pois há roteamento dinâmico[8] no *backbone* Internet, ou seja, existe mais de uma rota possível para um mesmo destino, e as mensagens podem ser divididas em pacotes que seguem caminhos diferentes. É também muito difícil comprometer a segurança de roteadores dedicados e, mais ainda, alterar a implementação TCP/IP destes roteadores.

Para se ter mais segurança exclusivamente através da rede, há um alto preço a pagar: é necessário mais suporte técnico, mais *overhead* e, claramente, isso pode demandar recursos vultosos[9].

---

[7] Neste caso, o e-mail foi enviado sem segurança, mas a máquina destino implementa SSMTP e, portanto, dispõe da chave pública do usuário destinatário.

[8] No roteamento dinâmico as tabelas de rotas são construídas automaticamente por protocolos projetados para este fim. Os protocolos ajustam dinamicamente as rotas, refletindo mudanças nas condições da rede.

[9] Pode-se optar, por exemplo, por utilizar uma hierarquia de certificação como a do PEM, que demanda de custos adicionais.

A opção por um canal seguro para transmissão da chave, i.e., fora da rede, também traz problemas: sempre que se imagine que esta chave esteja comprometida ou, ainda, se os requisitos de segurança determinarem a alteração periódica das chaves, uma nova chave terá que ser gerada e, novamente, transportada. O pior é que não há como fazer com que duas pessoas estabeleçam uma chave de forma completamente segura, exceto se elas se encontrarem pessoalmente.

Assim, a nossa solução oferece um esquema alternativo, onde ao se utilizar o servidor de e-mail como servidor de chaves públicas, não temos um sistema completamente seguro. Por outro lado, oferecemos um custo/benefício muito bom, onde se tem o melhor possível em segurança para troca de e-mails Internet, sem demandar suporte especial para a distribuição de chaves. Esta abordagem atende grande parte dos usuários, pois a maioria das mensagens que trafegam na Internet não justificam o esforço de quebrar o esquema de segurança que propomos, e se o custo requerido para quebrar um sistema ou decifrar uma mensagem é maior que o valor da informação que poderá ser obtida, então, para todos os fins práticos, o sistema é seguro [Weber 95].

Para os casos em que é necessário mais segurança, existe a flexibilidade de se trabalhar com servidores de chaves, onde as chaves armazenadas são certificadas.

4. Implementando Software Seguro para Uso de Correio Eletrônico Internet

Embora o SSMTP defina de forma clara quais mecanismos garantem a segurança do envio de correio eletrônico em redes TCP/IP e o LMSP assegure que a privacidade dos e-mails não será violada localmente, ainda há algumas decisões que precisam ser tomadas no momento da implementação destas especificações. Apresentamos aqui o SMTA ssmtpd e o SUA spine, projetados em conformidade com o SSMTP e o LMSP. O objetivo é mostrar como alguns detalhes de implementação podem ser bem resolvidos no momento de tirar do papel as idéias até aqui apresentadas e colocá-las para funcionar. O ssmtpd e o spine estão atualmente em desenvolvimento (em C).

4.1. O ssmtpd

O ssmtpd é um MTA de configuração muito mais simples que o sendmail, substituindo-o sempre que toda a troca de correio eletrônico for feita através de redes TCP/IP. Caso seja necessário utilizar outros protocolos para troca de e-mail (como o X.400 e UUCP), utilizar-se-á o sendmail para escolher entre os diversos MTAs instalados no servidor. Ressalvamos, entretanto, que a grande maioria dos servidores de e-mail conectados à Internet utilizam apenas o TCP/IP como mecanismo de troca de correio. Assim sendo, o ssmtpd resolverá o conhecido problema de configuração do sendmail [Avolio 94] na maior parte dos casos.

O ssmtpd é capaz de receber e enviar e-mails via SSMTP, tendo também suporte ao SMTP tradicional. Além disso, ele entrega e-mails locais. O ssmtpd roda em *background* e, para processar os e-mails que estão chegando, fica "ouvindo" na porta TCP 25, a mesma utilizada pelo SMTP.

O ssmtpd tem suporte a transferência de mensagens no formato 8bit MIME. Ou seja, não estabelece restrições aos caracteres que compõem a mensagem. Essa é uma característica importante, pois também representa uma extensão ao SMTP, que suporta apenas o transporte de dados que estejam representados em caracteres ASCII imprimíveis de 7 bits. Por isso, quando o SMTP "puro" é usado para o transporte de outros tipos de dados via e-mail, é necessário compatibilizar o formato dos dados através das codificações MIME base64 ou quoted-printable.

No ssmtpd encontramos as seguintes operações básicas:

- Criptografia do e-mail usando o algoritmo IDEA e criptografia da chave de sessão usando RSA.
- Assinatura do e-mail, usando RSA para criptografar, com a chave privada do remetente, o resultado MD5 da mensagem.
- Envio e recepção do e-mail sobre um suporte TCP/IP.
- Envio de e-mails locais.
- Fornecimento de chaves públicas.

No momento da transação SSMTP, ao receber a chave pública do usuário destinatário, o ssmtpd criptografa a chave de sessão randomicamente gerada para o e-mail, que é cifrado com o algoritmo IDEA. A chave de sessão é criptografada com o algoritmo RSA. Como já foi explicado antes, os

algoritmos de criptografia de chave pública são muito lentos, por isso opta-se por criptografar o conteúdo da mensagem com algoritmos de chave única.

A assinatura do e-mail é feita aplicando-se a MD5 sobre o texto do e-mail. Ao aplicar MD5 é produzido um número de 128 bits que é criptografado com a chave privada do remetente.

Os arquivos de chaves públicas e privadas (public.key e secret.key, respectivamente), contendo as chaves de todos os usuários do servidor ficam disponíveis em área do sistema. O public.key será consultado para fornecer as chaves públicas no momento de uma transação SSMTP de envio de e-mails e o secret.key é consultado para assinatura de e-mails e para decriptografia das mensagens, no momento que o usuário tem acesso à sua caixa postal.

É importante ressaltar que cada chave contida no secret.key é criptografada através do IDEA com o resultado MD5 da senha de acesso de seu dono. Além da chave, é criptografado também uma constante arbitrária (*magic number*) de 128 bits. Esta constante permite ao SUA descobrir se a senha de acesso fornecida por um usuário é a correta.

O ssmtpd provê a chave pública do usuário remetente, para o caso em que os e-mails são também assinados. Para isso, é verificado o preenchimento ou não do campo de cabeçalho "MIC-Info:". Caso esteja preenchido, uma nova conexão é estabelecida pelo SMTA para solicitar a chave pública do usuário remetente, após o recebimento da mensagem. Como discutido anteriormente, o objetivo de utilizarmos uma nova conexão é o de obtermos mais segurança.

O ssmtpd só reconhece endereçamento padrão Internet (usuário@domínio) ou local (usuário). Uma máquina que tenha mais de um MTA para transferência de e-mails terá que, obrigatoriamente, usar o sendmail, que age como despachador para os diversos MTAs que compõem um sistema de correio eletrônico. Nesta situação, o sendmail deve ser configurado para passar o processamento para o ssmtpd todas as vezes que o endereço do destinatário for Internet ou local.

No ssmtpd existem duas formas básicas de como o e-mail será encaminhado, uma localmente (figura 3.a) e a outra remotamente, via SSMTP (figura 3.b).

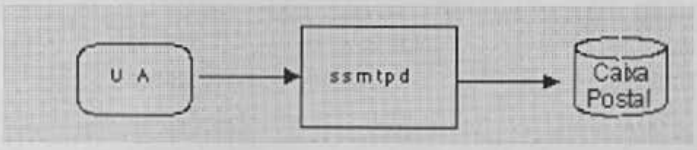

Figura 3.a: Mensagem local

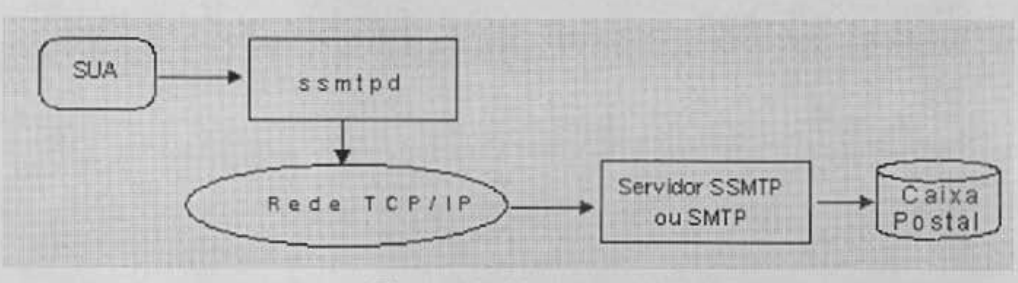

Figura 3.b: Mensagem SSMTP

O ssmtpd, por só encaminhar e-mails locais e SSMTP, é muito mais fácil de configurar que o sendmail (citado na seção 2), como o MTA mais utilizado em máquinas Unix). A maioria das máquinas utilizam apenas estas formas de encaminhar e-mails, não tendo suporte a vários MTAs em um único servidor. Dessa forma, estaremos facilitando a configuração para a maior parte dos casos. Pois, a flexibilidade que o sendmail oferece para atender as necessidades dos diferentes MTAs usados num sistema de e-mail, tornam a sua configuração uma tarefa complicada.

4.2. O spine

O Program for Internet News and Email (pine) é um ambiente de manipulação de e-mails (i.e. um UA) desenvolvido pela Universidade de Washington, em Seattle, para usuários finais. O pine utiliza protocolos padrões de mensagens na Internet, como o SMTP, MIME, IMAP e NNTP e está disponível para Unix, DOS/Windows e Macintosh.

O pine permite a manipulação da caixa postal de correio eletrônico padrão e também de folders criados pelo usuário. A edição de mensagens é em "tela cheia". É um agente usuário bastante poderoso

e de fácil utilização, com menus disponíveis em todos os seus estados[10]. A interface com o usuário é bastante amigável, com menus de comandos sempre presentes e alta tolerância aos erros dos usuários. Devido a esses fatores, escolhemos o pine como referência para o desenvolvimento do nosso agente usuário seguro (SUA), o spine.

O spine solicita a senha de acesso do usuário ao ser executado. Uma vez que a senha de acesso tenha sido fornecida corretamente (o que pode ser verificado graças a constante arbitrária criptografada junto com a chave privada), os e-mails do usuário que estiverem com o campo de cabeçalho "Encrypted:" preenchido com o valor "SSMTP 1.0" poderão ser decriptografados para leitura no momento de sua exibição.

Assim como no pine, o spine apresenta um menu principal ao usuário, que é identificado por MAIN MENU e pela versão do spine, na parte superior da tela. No menu principal estão exibidas claramente as opções do spine. O arquivo de mensagens recebidas é denominado INBOX e o arquivo de mensagens enviadas sent-mail. A diferença em relação ao pine é que estes arquivos guardam as mensagens criptografadas.

O arquivo .spinerc contém a configuração do spine, inclusive as opções de segurança. Por *default*, estas opções colocam o nível de segurança em obrigatório e assinam todos os e-mails. Tais opções podem ser alteradas pelo usuário, via o comando **S** (Setup) do menu principal do spine, que permite o acesso ao sub-comando **S** (Security).

O usuário pode modificar as opções de segurança apenas para o e-mail que está confeccionando através do comando **^S** (control-S). Isto permite alterar o nível de segurança e também habilitar/desabilitar a assinatura digital somente para uma determinada mensagem.

Quanto a assinatura, há três possibilidades para os e-mails recebidos: não foram assinados, foram assinados e foram falsificados (i. e., foram assinados, mas a assinatura não confere). Quando o spine está mostrando a lista de e-mails (também conhecido como índice) de um *folder*, a primeira coluna denota o *status* de cada e-mail: **N** mostra que o e-mail não foi assinado, **S**, que foi e **F**, que foi forjado (veja a figura 4). Esta informação também está disponível no momento de exibição do e-mail. Neste caso, as quatro posições mais a direita da primeira linha conterão **NSIG**, **SIGN** ou **FAKE** para denotar, respectivamente, que o e-mail não foi assinado, foi assinado ou foi falsificado.

```
SPINE 1.00   FOLDER INDEX                Folder: INBOX  Message 58 of 88

S      58  Jun 24 Jacques Philippe S  (3,049) Re: Artigo
S + A  59  Jun 24 Monica Fernandes    (1,861) Favorzinho
N      60  Jun 25 Jose E M de S Bran  (2,487) DNS fantasma?
F + A  61  Jun 25 mmelo@redebrasil.c  (1,860) Re: Noticias
N      62  Jun 25 Associacao dos Pro (10,986) [CNPQ-L] SOS UNIVERSIDADE
S + A  63  Jun 25 Walfredo Cirne Fil  (1,104) Re: Ser ou nao ser...
S      64  Jun 25 Walfredo Cirne Fil  (1,719) Re: Correio seguro
S      65  Jun 25 Walfredo Cirne Fil  (2,331) Re: Artigo
N      67  Jun 26 CERT Advisory      (14,759) CERT Advisory CA-96.12 -
F      68  Jun 26 Stephen Kent       (10,570) draft meeting minutes
S    A 69  Jun 27 Ernandes Lopes Bez  (2,542) News
N      70  Jun 27 VICENTE DE PAULO A  (1,306) CURSO DE ESPECIALIZACAO E
N      71  Jun 27 lucas_avila@easyli  (1,197) Security
N      72  Jun 27 Coordenacao da Bib  (4,752) Informativo Miniblio
N + A  73  Jun 28 Ismenia Mangueira     (741) UNIX
N +    74  Jul  1 Ismenia Mangueira     (582) Obrigada
S      75  Jul  1 Walfredo Cirne Fil  (1,283) Banca de Zane
F + A  76  Jul  1 Acesso aa estacao     (818) Sinais de vida!!!

? Help       M Main Menu  P PrevMsg   - PrevPage  D Delete   R Reply
O OTHER CMDS V [ViewMsg]  N NextMsg Spc NextPage  U Undelete F Forward
```

Figura 4: Tela do spine mostrando a lista de e-mails no INBOX

[10] No pine os estados são as opções do menu principal, ou seja, as diversas funcinalidades que o pine oferece.

5. Conclusão

O correio eletrônico é uma das principais razões para o crescimento fantástico da Internet e a sua segurança tem sido um problema desde a primeira vez em que o e-mail foi utilizado. A correspondência eletrônica pode ser interceptada e copiada sem o conhecimento do remetente e do destinatário e, mais, na maioria dos UAs utilizados, o simples ato de enviar o e-mail envolve fazer uma cópia dessa mensagem. Uma cópia fica armazenada em um *folder* de e-mails enviados, podendo vir a ser lido pelo administrador do sistema, ou até, por falta de conhecimento do usuário, acessível a todo um grupo, devido às permissões estabelecidas para o arquivo. Como se não bastasse, é muito fácil enviar um e-mail falsificando o remetente.

O PEM é uma solução muito complexa no que se refere a infra-estrutura necessária para certificação de chaves (além de ser muito pesada e trazer custos adicionais) e não fornece nenhuma segurança local. O PGP, que é a solução que de fato tem sido utilizada, tem os inconvenientes de ser externo ao software de correio eletrônico e não especificar uma política para a distribuição segura de chaves. O MOSS não tem os problemas de distribuição de chave do PEM, mas também não apresenta nenhuma solução para segurança local e requer a utilização da codificação MIME, o que aumenta o tamanho dos e-mails, gerando, assim, mais tráfego na rede.

Assim sendo, o uso de um protocolo que oferece ao usuário segurança na troca de e-mail Internet de forma intrínseca e sem depender de um complexo serviço de distribuição de chaves nem tampouco de codificação MIME, e de procedimentos que garantem a segurança local representam uma solução vantajosa para o usuário, garantindo a reserva em sua comunicação via correio eletrônico.

A solução aqui proposta atende a estes requisitos. O LMSP garante a segurança local, enquanto o SSMTP possibilita a transmissão segura de e-mail pela Internet, sem requerer nenhum serviço centralizado nem utilizar nenhuma forma de codificação que expande o tamanho das mensagens. Embora exista a possibilidade de interceptação das mensagens por intrusos em roteadores, temos uma solução satisfatória para a maioria dos usuários Internet (devido ao valor das informações que são transmitidas). Além do mais, caso esta abordagem não seja suficiente, pode-se utilizar uma hierarquia de distribuição de chaves (incorrendo em todo o custo associado a sua implantação e operação), única forma de obter mais segurança.

A especificação do protocolo SSMTP e do LMSP, para garantia da integridade local, bem como o desenvolvimento do SMTA ssmtpd e do SUA spine, contribuem com um aspecto relevante que é a segurança na troca de e-mails em redes TCP/IP, em particular na Internet.

Referências Bibliográficas

[Avolio 94] AVOLIO, Frederick M.; VIXIE, Paul A. **Sendmail Theory and Practice**, Digital Press, California, 1994.

[Burns 95] BURNS, Nina. **O Correio Eletrônico Vai Além da Rede Local**. PC Magazine Brasil, Julho, 1995.

[Comer 95] COMER, Douglas E. **Internetworking with TCP/IP**. Prentice Hall, New Jersey, 1995.

[Garfinkel 95] GARFINKEL, Simson. **PGP Pretty Good Privacy**. O'Reilly & Associates Inc., 1995.

[Hunt 92] HUNT, Craig. **TCP/IP Network Administration**. O'Reilly & Associates Inc., 1992.

[Malamud 92] MALAMUD, Carl. **Analyzing SUN Networks**. VNR Computer Library, New York, 1992.

[RFC 821] POSTEL, Jonathan B. **Simple Mail Transfer Protocol**. 1982.

[RFC 822] CROKER, David H. **Standard for the Format of ARPA Internet Text Messages**.1982.

[RFC 1123] BRADEN, Robert. **Requirements for Internet Hosts - Application and Suport**. 1989.

[RFC 1321] RIVEST, Ronald L. **The MD5 Message-Digest Algorithm**. 1992.

[RFC 1421] LINN, J. **Privacy Enhancement for Internet Eletronic Mail: Part I: Message Encryption and Authentication Procedures**. 1993.

[RFC 1869] KLESIN et al. **SMTP Service Extensions**, United Nations University, November, 1995.

[RFC 1847] GALVIN, J et al. **Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted**, Trusted Information System and Innosoft, September, 1995.

[RFC 1848] CROCKER, S. et al. **MIME Object Security Services**. Trusted Information System and Innosoft, October, 1995.

[Rivest 78] RIVEST, R. L.; SHAMIR, A.; ADELMAN, L. **A Method for Obtaining Digital Signatures and Public Key Cryptography**. Communications of the ACM, vol 21, no. 2, February, 1978.

[RNP 95] **Guia de Operações Internet Brasil**. Documento RNP/RPU/0015D, Junho, 1995.

[Russel 92] RUSSEL, Deborah; SR. GANGEMIN, G. T. **Computer Security Basics**, O'Reilly & Associates Inc., 1992.

[Schneier 93] SCHNEIER, B. **The IDEA Encryption Algorithm**. Dr. Dobb's Journal, vol. 18, no. 13, 1993.

[Soares 95] SOARES, Luiz Fernando Gomes, LEMOS, Guido e COLCHER, Sérgio. **Redes de Computadores, Das LANs, MANs e WANs às Redes ATM**. Editora Campus, Rio de Janeiro, 1995.

[Weber 95] WEBER, Raul Fernando. **Criptografia Contemporânea**. VI Simpósio de Computadores Tolerantes a Falhas, 1995.