Cartilha de Segurança para Internet
Parte III: Privacidade

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha discute questões relacionadas à privacidade do usuário ao utilizar a Internet. É apresentado o conceito de criptografia, onde são discutidos os métodos de criptografia por chave única, por chaves pública e privada e as assinaturas digitais. Também são abordados temas relacionados à privacidade dos *e-mails*, a privacidade no acesso e disponibilização de páginas *Web*, bem como alguns cuidados que o usuário deve ter com seus dados pessoais e ao armazenar dados em um disco rígido.

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@nic.br.

Nota de *Copyright* e Distribuição

Sumário

1 Criptografia

Criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:

- autenticar a identidade de usuários;
- autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias;
- proteger a integridade de transferências eletrônicas de fundos.

Uma mensagem codificada por um método de criptografia deve ser **privada**, ou seja, somente aquele que enviou e aquele que recebeu devem ter acesso ao conteúdo da mensagem. Além disso, uma mensagem deve poder ser **assinada**, ou seja, a pessoa que a recebeu deve poder verificar se o remetente é mesmo a pessoa que diz ser e ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Os métodos de criptografia atuais são seguros e eficientes e baseiam-se no uso de uma ou mais **chaves**. A chave é uma seqüência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens.

Atualmente, os métodos criptográficos podem sem subdivididos em duas grandes categorias, de acordo com o tipo de chave utilizada: a criptografia de chave única (vide seção 1.1) e a criptografia de chave pública e privada (vide seção 1.2).

1.1 O que é criptografia de chave única?

A criptografia de chave única utiliza a mesma chave tanto para a codificar quanto para decodificar mensagens. Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.

Exemplos de utilização deste método de criptografia e sugestões para o tamanho mínimo da chave única podem ser vistos nas seções 1.4 e 1.5, respectivamente.

1.2 O que é criptografia de chaves pública e privada?

A criptografia de chaves pública e privada utiliza duas chaves distintas, uma para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves: uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em segredo pelo seu dono. As mensagens codificadas com a chave pública só podem ser decodificadas com a chave privada correspondente.

Seja o exemplo, onde José e Maria querem se comunicar de maneira sigilosa. Então, eles terão que realizar os seguintes procedimentos:

1. José codifica uma mensagem utilizando a chave pública de Maria, que está disponível para o uso de qualquer pessoa;
2. Depois de criptografada, José envia a mensagem para Maria, através da Internet;
3. Maria recebe e decodifica a mensagem, utilizando sua chave privada, que é apenas de seu conhecimento;
4. Se Maria quiser responder a mensagem, deverá realizar o mesmo procedimento, mas utilizando a chave pública de José.

Apesar deste método ter o desempenho bem inferior em relação ao tempo de processamento, quando comparado ao método de criptografia de chave única (seção 1.1), apresenta como principal vantagem a livre distribuição de chaves públicas, não necessitando de um meio seguro para que chaves sejam combinadas antecipadamente. Além disso, pode ser utilizado na geração de assinaturas digitais, como mostra a seção 1.3.

Exemplos de utilização deste método de criptografia e sugestões para o tamanho mínimo das chaves pública e privada podem ser vistos nas seções 1.4 e 1.5, respectivamente.

1.3 O que é assinatura digital?

A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

Desta forma, é utilizado o método de criptografia de chaves pública e privada, mas em um processo inverso ao apresentado no exemplo da seção 1.2.

Se José quiser enviar uma mensagem assinada para Maria, ele irá codificar a mensagem com sua chave privada. Neste processo será gerada uma assinatura digital, que será adicionada à mensagem enviada para Maria. Ao receber a mensagem, Maria irá utilizar a chave pública de José para decodificar a mensagem. Neste processo será gerada uma segunda assinatura digital, que será comparada à primeira. Se as assinaturas forem idênticas, Maria terá certeza que o remetente da mensagem foi o José e que a mensagem não foi modificada.

É importante ressaltar que a segurança do método baseia-se no fato de que a chave privada é conhecida apenas pelo seu dono. Também é importante ressaltar que o fato de assinar uma mensagem não significa gerar uma mensagem sigilosa. Para o exemplo anterior, se José quisesse assinar a mensagem e ter certeza de que apenas Maria teria acesso a seu conteúdo, seria preciso codificá-la com a chave pública de Maria, depois de assiná-la.

1.4 Que exemplos podem ser citados sobre o uso de criptografia de chave única e de chaves pública e privada?

Exemplos que combinam a utilização dos métodos de criptografia de chave única e de chaves pública e privada são as conexões seguras, estabelecidas entre o *browser* de um usuário e um *site*, em transações comercias ou bancárias via *Web*.

Estas conexões seguras via *Web* utilizam o método de criptografia de chave única, implementado pelo protocolo SSL (*Secure Socket Layer*). O *browser* do usuário precisa informar ao *site* qual será a chave única utilizada na conexão segura, antes de iniciar a transmissão de dados sigilosos.

Para isto, o *browser* obtém a chave pública do certificado[1] da instituição que mantém o *site*. Então, ele utiliza esta chave pública para codificar e enviar uma mensagem para o *site*, contendo a chave única a ser utilizada na conexão segura. O *site* utiliza sua chave privada para decodificar a mensagem e identificar a chave única que será utilizada.

A partir deste ponto, o *browser* do usuário e o *site* podem transmitir informações, de forma sigilosa e segura, através da utilização do método de criptografia de chave única. A chave única pode ser trocada em intervalos de tempo determinados, através da repetição dos procedimentos descritos anteriormente, aumentando assim o nível de segurança de todo o processo.

1.5 Que tamanho de chave deve ser utilizado?

Os métodos de criptografia atualmente utilizados, e que apresentam bons níveis de segurança, são publicamente conhecidos e são seguros pela robustez de seus algoritmos e pelo tamanho das chaves que utilizam.

Para que um atacante descubra uma chave ele precisa utilizar algum método de força bruta, ou seja, testar combinações de chaves até que a correta seja descoberta. Portanto, quanto maior for a chave, maior será o número de combinações a testar, inviabilizando assim a descoberta de uma chave em tempo hábil. Além disso, chaves podem ser trocadas regularmente, tornando os métodos de criptografia ainda mais seguros.

Atualmente, para se obter um bom nível de segurança na utilização do método de criptografia de chave única, é aconselhável utilizar chaves de no mínimo 128 bits. E para o método de criptografia de chaves pública e privada é aconselhável utilizar chaves de no mínimo 1024 bits. Dependendo dos fins para os quais os métodos criptográficos serão utilizados, deve-se considerar a utilização de chaves maiores: 256 ou 512 bits para chave única e 2048 ou 4096 bits para chaves pública e privada.

2 Privacidade dos *E-Mails*

O serviço de *e-mails* foi projetado para ter como uma de suas principais características a simplicidade. O problema deste serviço é que foi comparado com o correio terrestre, dando a falsa idéia de

[1] Certificados são discutidos nas partes I (Conceitos de Segurança) e IV (Fraudes na Internet) desta Cartilha.

que os *e-mails* são cartas fechadas. Mas eles são, na verdade, como cartões postais, cujo conteúdo pode ser lido por quem tiver acesso a eles.

2.1 É possível alguém ler *e-mails* de outro usuário?

As mensagens que chegam à caixa postal do usuário ficam normalmente armazenadas em um arquivo no servidor de *e-mails* do provedor, até o usuário se conectar na Internet e obter os *e-mails* através do seu programa de *e-mails*.

Portanto, enquanto os *e-mails* estiverem no servidor, poderão ser lidos por pessoas que tenham acesso a este servidor[2]. E enquanto estiverem em trânsito, existe a possibilidade de serem lidos por alguma pessoa conectada à Internet.

2.2 Como é possível assegurar a privacidade dos *e-mails*?

Se a informação que se deseja enviar por *e-mail* for confidencial, a solução é utilizar programas que permitam criptografar o *e-mail* através de chaves (senhas ou frases), de modo que ele possa ser lido apenas por quem possuir a chave certa para decodificar a mensagem.

Alguns *softwares* de criptografia podem estar embutidos nos programas de *e-mail*, outros podem ser adquiridos separadamente e integrados aos programas de *e-mail*.

Devem ser usados, preferencialmente, programas de criptografia que trabalhem com pares de chaves (vide seção 1.2), tais como o PGP ou o GnuPG, que podem ser obtidos no site `http://www.pgpi.org/`.

Estes programas, apesar de serem muito utilizados na criptografia de mensagens de *e-mail*, também podem ser utilizados na criptografia de qualquer tipo de informação, como por exemplo, um arquivo sigiloso a ser armazenado em uma cópia de segurança (parte II desta Cartilha: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção).

2.3 A utilização de programas de criptografia é suficiente para assegurar a privacidade dos *e-mails*?

Os programas de criptografia são utilizados, dentre outras finalidades, para decodificar mensagens criptografadas, recebidas por um usuário, no momento em que este desejar lê-las.

Ao utilizar um programa de criptografia para decodificar uma mensagem, é possível que o programa de *e-mail* permita salvar a mensagem no formato decodificado, ou seja, em texto claro. No caso da utilização de programas de *e-mail* com esta característica, a privacidade do conteúdo da mensagem é garantida durante a transmissão da mensagem, mas não necessariamente no seu armazenamento.

[2] Normalmente existe um consenso ético entre administradores de redes e provedores de nunca lerem a caixa postal de um usuário sem o seu consentimento.

Portanto, é extremamente importante o usuário estar atento para este fato, e também certificar-se sobre o modo como suas mensagens estão sendo armazenadas. Como uma mensagem pode ser decodificada sempre que o usuário desejar lê-la, é aconselhável que ela seja armazenada de forma criptografada e não em texto claro.

3 Privacidade no Acesso e Disponibilização de Páginas *Web*

Existem cuidados que devem ser tomados por um usuário ao acessar ou disponibilizar páginas na Internet. Muitas vezes o usuário pode expor informações pessoais e permitir que seu *browser* receba ou envie dados sobre suas preferências e sobre o seu computador. Isto pode afetar a privacidade de um usuário, a segurança de seu computador e até mesmo sua própria segurança.

3.1 Que cuidados devo ter ao acessar páginas *Web* e ao receber *Cookies*?

Cookies são muito utilizados para rastrear e manter as preferências de um usuário ao navegar pela Internet. Estas preferências podem ser compartilhadas entre diversos *sites* na Internet, afetando assim a privacidade de um usuário. Não é incomum acessar pela primeira vez um *site* de música, por exemplo, e observar que todas as ofertas de CDs para o seu gênero musical preferido já estão disponíveis, sem que você tenha feito qualquer tipo de escolha.

Além disso, ao acessar uma página na Internet, o seu *browser* disponibiliza uma série de informações, de modo que os *cookies* podem ser utilizados para manter referências contendo informações de seu computador, como o *hardware*, o sistema operacional, *softwares* instalados e, em alguns casos, até o seu endereço de *e-mail*.

Estas informações podem ser utilizadas por alguém mal intencionado, por exemplo, para tentar explorar uma possível vulnerabilidade em seu computador, como visto nas partes I (Conceitos de Segurança) e II (Riscos Envolvidos no Uso da Internet e Métodos de Prevenção) desta Cartilha.

Portanto, é aconselhável que você desabilite o recebimento de *cookies*, exceto para *sites* confiáveis, onde sejam realmente necessários.

As versões recentes dos *browsers* normalmente permitem que o usuário desabilite o recebimento, confirme se quer ou não receber e até mesmo visualize o conteúdo dos *cookies*.

Também existem *softwares* que permitem controlar o recebimento e envio de informações entre um *browser* e os *sites* visitados. Dentre outras funções, estes podem permitir que *cookies* sejam recebidos apenas de *sites* específicos[3].

Uma outra forma de manter sua privacidade ao acessar páginas na Internet é utilizar *sites* que permitem que você fique anônimo. Estes são conhecidos como *anonymizers*[4] e intermediam o envio e recebimento de informações entre o seu *browser* e o *site* que se deseja visitar. Desta forma, o seu

[3] Um exemplo deste tipo de *software* pode ser encontrado em http://internet.junkbuster.com/.
[4] Um exemplo desse tipo de *site* pode ser encontrado em http://www.anonymizer.com/.

browser não receberá *cookies* e as informações por ele fornecidas não serão repassadas para o *site* visitado.

Neste caso, é importante ressaltar que você deve certificar-se que o *anonymizer* é confiável. Além disso, você não deve utilizar este serviço para realizar transações via *Web*.

3.2 Que cuidados devo ter ao disponibilizar um página na Internet, como por exemplo um *blog*?

Um usuário, ao disponibilizar uma página na Internet, precisa ter alguns cuidados, visando proteger os dados contidos em sua página.

Um tipo específico de página *Web* que vem sendo muito utilizado por usuários de Internet é o *blog*. Este serviço é usado para manter um registro freqüente de informações, e tem como principal vantagem permitir que o usuário publique seu conteúdo sem necessitar de conhecimento técnico sobre a construção de páginas na Internet.

Apesar de terem diversas finalidades, os *blogs* têm sido muito utilizados como diários pessoais. Em seu *blog*, um usuário poderia disponibilizar informações, tais como:

- seus dados pessoais (*e-mail*, telefone, endereço, etc);
- dados sobre o seu computador (dizendo, por exemplo, "... comprei um computador da marca X e instalei o sistema operacional Y...");
- dados sobre os *softwares* que utiliza (dizendo, por exemplo, "... instalei o programa Z, que acabei de obter do *site* W...");
- informações sobre o seu cotidiano (como, por exemplo, hora que saiu e voltou para casa, data de uma viagem programada, horário que foi ao caixa eletrônico, etc);

É extremamente importante estar atento e avaliar com cuidado que informações serão disponibilizadas em uma página *Web*. Estas informações podem não só ser utilizadas por alguém mal-intencionado, por exemplo, em um ataque de engenharia social (parte I desta Cartilha: Conceitos de Segurança), mas também para atentar contra a segurança de um computador, ou até mesmo contra a segurança física do próprio usuário.

4 Cuidados com seus Dados Pessoais

Procure não fornecer seus dados pessoais (como nome, *e-mail*, endereço e números de documentos) para terceiros. Também **nunca** forneça informações sensíveis (como senhas e números de cartão de crédito), a menos que esteja sendo realizada uma transação (comercial ou financeira) e se tenha certeza da idoneidade da instituição que mantém o *site*.

Estas informações geralmente são armazenadas em servidores das instituições que mantém os *sites*. Com isso, corre-se o risco destas informações serem repassadas sem autorização para outras instituições ou de um atacante comprometer este servidor e ter acesso a todas as informações.

Fique atento aos ataques de engenharia social, vistos na parte I desta Cartilha (Conceitos de Segurança). Ao ter acesso a seus dados pessoais, um atacante poderia, por exemplo, utilizar seu *e-mail* em alguma lista de distribuição de *SPAMs* (vide parte VI desta Cartilha: SPAM) ou se fazer passar por você na Internet (através do uso de uma de suas senhas).

5 Cuidados com os Dados Armazenados em um Disco Rígido

É importante ter certos cuidados no armazenamento de dados em um computador. Caso você mantenha informações sensíveis ou pessoais que você não deseja que sejam vistas por terceiros (como números de cartões de crédito, declaração de imposto de renda, senhas, etc), estas devem ser armazenadas em algum formato criptografado.

Estes cuidados são extremamente importantes no caso de *notebooks*, pois são mais visados e, portanto, mais suscetíveis a roubos, furtos, etc.

Caso as informações não estejam criptografadas, se você necessitar levar o computador a alguma assistência técnica, por exemplo, seus dados poderão ser lidos por algum técnico mal-intencionado.

Para criptografar estes dados, como visto na seção 2.2, existem programas que, além de serem utilizados para a criptografia de *e-mails*, também podem ser utilizados para criptografar arquivos.

Um exemplo seria utilizar um programa que implemente criptografia de chaves pública e privada (seção 1.2), como o PGP. O arquivo sensível seria criptografado com a sua chave pública e, então, decodificado com a sua chave privada, sempre que fosse necessário.

É importante ressaltar que a segurança deste método de criptografia depende do sigilo da chave privada. A idéia, então, é manter a chave privada em um CD ou em outro disco rígido (em uma gaveta removível) e que este não acompanhe o computador, caso seja necessário enviá-lo, por exemplo, para a assistência técnica.

Também deve-se ter um cuidado especial ao trocar ou vender um computador. Apenas apagar ou formatar um disco rígido não é suficiente para evitar que informações antes armazenadas possam ser recuperadas. Portanto, é importante **sobrescrever** todos os dados do disco rígido (vide seção 5.1).

5.1 Como posso sobrescrever todos os dados de um disco rígido?

Para assegurar que informações não possam ser recuperadas de um disco rígido é preciso sobrescrevê-las com outras informações. Um exemplo seria gravar o caracter 0 (zero), ou algum caracter escolhido aleatoriamente, em todos os espaços de armazenamento do disco.

É importante ressaltar que é preciso repetir algumas vezes a operação de sobrescrever os dados de um disco rígido, para assegurar que informações anteriormente armazenadas não possam ser recupe-

radas.

Existem *softwares* gratuitos e comerciais que permitem sobrescrever dados de um disco rígido e que podem ser executados em diversos sistemas operacionais, como o Windows (95/98, 2000, etc), Unix (Linux, FreeBSD, etc) e Mac OS.