Sigilo e segurança a custo zero

Novo PGP democratiza a encriptação de mensagens

Mensagens eletrônicas têm vantagens evidentes sobre documentos em papel, mas também algumas importantes desvantagens. Para começar, é relativamente fácil para um hacker espião interceptar suas mensagens privadas. Também não é difícil alguém enviar uma mensagem forjada como se fosse sua. Documentos eletrônicos sempre podem ser adulterados sem deixar qualquer marca. Para resolver esses três problemas, e mais alguns, existe um freeware que acaba de ganhar uma nova versão: o PGP 6i, da Network Associates Inc. (NAI).

Esse é o homem que inventou o PGP

O PGP e a lei

A sigla PGP significa Pretty Good Privacy, ou seja, Privacidade Bem Boa. A distribuição na forma de freeware e o tom informal do nome do produto não parecem obra de uma sisuda empresa de sistemas de segurança como a NAI.

De fato, não são. O PGP foi inventado pelo programador americano Phil Zimmermann como um gesto na luta em defesa das liberdades individuais nos EUA e no mundo. Phil percebeu que a popularização da informática permitia, pela primeira vez na história, que cidadãos comuns utilizassem técnicas criptográficas para proteger a privacidade de suas comunicações eletrônicas. Ele notou também que a melhor forma de democratizar o acesso à criptografia era desenvolver um freeware e espalhá-lo pela Rede. Foi isso que ele fez, e por pouco não acabou preso por violar uma lei americana que impede a exportação de programas critptográficos sem autorização prévia do Tio Sam (ficou provado que não foi Zimmermann, mas alguém não-identificado, que colocou o PGP na Internet).

Hoje o PGP é exportado legalmente para fora dos EUA através de um método curioso que demonstra a estupidez da legislação: a equipe do PGP produz, a cada nova versão, livros com o código-fonte integral do programa. Esses livros são exportados legalmente, porque a lei proíbe apenas a exportação do software (a listagem impressa não é considerada "software"). Na Noruega, um grupo de voluntários escaneia todas as páginas dos livros e, com o auxílio de um software de OCR (reconhecimento de escrita), gera novamente os arquivos do programa prontos para serem compilados e distribuídos. Todo esse trabalho traz uma vantagem adicional: o código-fonte do PGP também fica disponível para que qualquer programador possa verificar que ele não contém "portas dos fundos" ou bugs que comprometam sua segurança.

O PGP permite que você criptografe textos de email ou arquivos quaisquer de forma que somente você, ou um grupo específico de destinatários, possa abri-los. Para tanto, é preciso que todos os envolvidos sejam usuários do PGP e que tenham trocado anteriormente suas chaves públicas. O PGP utiliza uma técnica revolucionária, chamada criptografia de chave pública, que não é nada intuitiva, mas dá para entender se você dedicar uma ou duas horas lendo e experimentando *(leia o box nesta matéria)*. Usar um programa de criptografia de forma errada é bem pior do que não usar criptografia nenhuma, já que você pode cometer erros muito graves se estiver com uma falsa sensação de segurança.

Com as ferramentas do PGP ninguém vai interceptar suas mensagens

Versão internacional

Em dezembro de 1997, a PGP Inc., empresa que Zimmermann criou para vender versões comerciais do PGP, foi adquirida pela NAI, que continua desenvolvendo o produto em versões comerciais e freeware. A versão do PGP que analisamos é a 6.0.2i. A letra "i" indica "versão internacional". Ela é praticamente idêntica à versão freeware 6.0.2, que é disponível legalmente apenas para cidadãos americanos e canadenses em virtude da tal legislação. Só há duas diferenças:

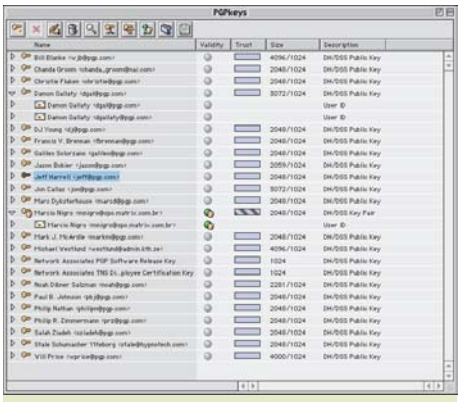
1 A versão internacional suporta um algoritmo criptográfico, chamado RSA, que não existe na versão freeware americana porque o RSA é patenteado nos EUA mas não no resto do mundo. Para evitar incompatibilidades, o freeware suporta o RSA apenas na leitura de chaves, mas não pode gerá-las usando esse algoritmo.

2 O servidor default para armazenagem das chaves dos usuários fica na Holanda, e não nos EUA.

Gerenciamento de chaves

As chaves são peças fundamentais dessa tecnologia. Após instalar o PGP 6, você precisará gerar um par de chaves pessoais ou fornecer o caminho para que o PGP localize seu arquivo de chaves, caso você já seja usuário de uma versão anterior do PGP. Sua chave secreta é protegida por uma *pass-phrase*, ou frase-senha, e sua chave pública é enviada para um servidor de chaves, de onde poderá ser baixada por qualquer pessoa que queira se corresponder com você.

Uma vez criado seu par de chaves pessoais, o PGP exibe a janela do seu principal módulo: o gerenciador de chaves PGP Keys. Com ele você pode enviar e receber chaves de servidores especiais espalhados pela Internet e organizar as chaves daqueles com quem você se corresponde habitualmente. Uma característica muito útil é a possibilidade de criar grupos. Se eu envio com freqüência mensagens cifradas para uma dúzia de colaboradores da Macmania, posso



O PGP Keys gerencia as chaves que serão enviadas e recebidas

Criptografia para as massas

Quando a informação é digital e flui pela Internet, cadeados e cofres não servem mais para protegê-la. Mas uma tecnologia permite que cidadãos comuns mantenham sua privacidade trocando mensagens cifradas. A mesma tecnologia garante a segurança das transações no comércio eletrônico. Seu nome é criptografia de chave pública.

O ato de cifrar ou encriptar consiste em submeter a mensagem original a uma ou mais transformações que a tornem ilegível. Essas transformações são ditadas por um algoritmo, ou seja, uma seqüência de instruções que pode ser repetida com exatidão. O algoritmo pode até ser executado por uma pessoa, mas o mais comum é que ele seja implementado em um chip ou um software. Nos sistemas criptográficos modernos, o segredo não está no algoritmo, e sim na chave. A chave é como uma senha, uma informação secreta que precisa ser fornecida para cifrar e, posteriormente, decifrar a mensagem. A ação de decifrar normalmente utiliza o mesmo algoritmo e a mesma chave.

O grande problema da criptografia convencional é a segurança da chave. Vamos usar dois personagens, Alice e Bruno, para exemplificar a troca de mensagens cifradas. Na criptografia convencional, Alice e Bruno usam a mesma senha para cifrar e decifrar mensagens. Para combinar a senha a ser utilizada, Alice e Bruno precisam se encontrar pessoalmente ao menos uma vez, pois essa é a maneira mais segura de trocar senhas.

A invenção da chave pública

Em 1976, os cientistas americanos Whitfield Diffie e Martin Hellman criaram uma nova modalidade de troca de mensagens cifradas: a criptografia de chave pública, ou "public-key cryptography". A grande inovação foi o uso de duas chaves. Uma delas, chamada chave pública, é usada para cifrar as mensagens, e a outra, a chave privada, serve para decifrá-las. Essa comunicação pode ser esquematizada como na figura.

A característica mais importante desse esquema é que a chave privada dos usuários não precisa circular.

Em um sistema de chave pública, a chave utilizada para cifrar uma mensagem não pode ser usada para decifrá-la. Uma segunda chave é necessária para tanto. Por isso as chaves são sempre criadas em pares. Cada usuário possui seu par de chaves. A chave privada é usada para decifrar mensagens recebidas. Por isso essa chave é protegida por uma senha secreta. A chave pública de outra pessoa é usada quando se enviam mensagens cifradas para ela.

Sem a criptografia de chave pública, o comércio eletrônico seria bem mais complicado. Desde 1995, todos os navegadores Netscape e Internet Explorer utilizam um protocolo chamado SSL para acessar os "servidores seguros" usados no comércio eletrônico. Você pode verificar se uma página está em um servidor seguro se a URL tem o prefixo https://, *em vez de* http://. *Os navegadores também exibem ícones na barra de status indicando quando o SSL está sendo usado. Na prática, ocorre uma troca de chaves públicas quando o navegador solicita uma página de um servidor usando SSL. O servidor usa a chave pública do navegador para cifrar as páginas consultadas, e o navegador usa sua chave privada para decifrá-las e exibi-las. Por outro lado, a chave pública do servidor é usada pelo browser para cifrar os dados enviados pelo usuário.*

É mesmo seguro?

Nada no mundo é totalmente seguro, e nenhum sistema criptográfico é perfeito. Nos últimos anos, têm sido noticiados vários casos de mensagens decifradas por grupos de pesquisadores. Na maioria desses casos, os algoritmos atacados usavam chaves curtas (de até 56 bits) e foram utilizadas técnicas de "força bruta", com dezenas ou mesmo milhares de computadores gerando todas as possíveis combinações de chaves.

O problema é que o governo americano raramente autoriza a exportação de softwares criptográficos capazes de usar chaves maiores do que 56 bits. O motivo, supostamente, é evitar que traficantes e terroristas possam proteger suas mensagens usando chaves longas demais para serem quebradas por força bruta. Pena que terroristas e traficantes não liguem muito para leis e regulamentos.

No caso dos navegadores, o limite para exportação está fixado em 40 bits, o que não se considera suficientemente seguro para aplicações de internet-banking, por exemplo. A segurança das chaves aumenta geometricamente com o número de bits. Por isso, uma chave de 64 bits é milhões de vezes mais segura que uma de 40 bits. Residentes permanentes dos EUA e do Canadá têm acesso a versões do Communicator e do IE com chaves de 128 bits. Tais chaves são consideradas seguras até mesmo para transações financeiras de valores muito altos. No Brasil, alguns sistemas de internet-banking já utilizam chaves de 128 bits, mesmo usando os browsers americanos limitados. Para conseguir isso, os bancos precisaram implementar sistemas de criptografia paralelos usando a linguagem Java ou mesmo plug-ins especiais.

No entanto, na prática, o elo mais fraco de qualquer sistema de segurança geralmente é o usuário. A melhor segurança do mundo é inútil se for usada de forma incorreta, ou se estiver protegida por uma senha tão óbvia quanto sua data de nascimento.

então criar um grupo contendo esses destinatários. A partir daí, poderei incluir suas chaves em qualquer mensagem com apenas um clique.

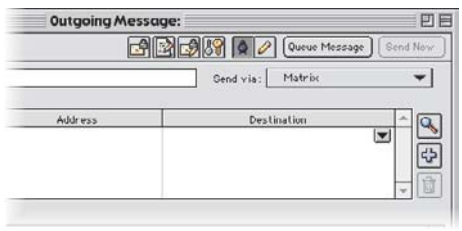
Cifrar, decifrar e assinar

Para cifrar e decifrar mensagens você pode invocar as funções do PGP de dentro de seu programa de email. O PGP 6 acompanha "plug-ins" (módulos de expansão) que suportam os clientes de email Eudora e o Claris Emailer. No Windows, são suportados o Outlook 97/98, Outlook Express 4 e o Eudora 3 e 4. A operação de cifrar é idêntica em todos esses programas. Você escreve sua mensagem normalmente e, logo antes de enviá-la, clica no ícone de "cifrar mensagem" que o PGP coloca na barra de botões do programa de email. O próximo passo é escolher os destinatários a partir da lista de chaves que você possui. Então é só enviar a mensagem cifrada. Ao recebê-la, o destinatário que já instalou o PGP terá

apenas que digitar a frase-senha dele para poder ler seu conteúdo.
Ao cifrar uma mensagem, o PGP oferece a opção *secure viewer*. Se ativada, essa opção fará com que o destinatário seja avisado de que a mensagem só deve ser lida em condições de segurança máxima. Assim ele terá a chance de verificar se ninguém está espiando sobre seus ombros antes de abrir o texto secreto. E para atrapalhar até mesmo os mais sofisticados espiões, o PGP 6 pode exibir o texto utilizando uma fonte especial, resistente à tecnologia Tempest de espionagem eletrônica (com essa técnica, que dizem ter sido usada na captura do famoso espião Aldrich Ames, é possivel captar e reconstruir a imagem gerada pelo monitor do seu micro — mesmo através de paredes).
Outra função do PGP é assinar mensagens. Com isso, os destinatários ganham duas certezas: a de que você é de fato o autor e a de que o texto não foi alterado. A assinatura eletrônica pode ser aplicada sobre mensagens de email de dentro dos próprios aplicativos suportados, também através de um ícone especial. Nesse caso, o procedimento é o seguinte: escreva a mensagem, clique no ícone para assiná-la e então digite sua frase-senha. Um arquivo especial contendo a assinatura digital será anexado à mensagem. Ao abri-la, os destinatários verão um aviso do PGP confirmando a identidade do autor. Caso o texto tenha sido adulterado de qualquer maneira, isso também será sinalizado.

Discos secretos

Se você trabalha diariamente com vários arquivos sigilosos, vai gostar do PGPdisk. Com ele você cria um disco virtual dentro de seu disco rígido. Na verdade, o disco virtual não passa de um arquivo cifrado, de tamanho fixo, que pode conter seus documentos secretos. Ao criar um disco virtual, você associa uma frase-senha e um nome qualquer. Para usá-lo, basta um duplo-clique e o PGPdisk fará com que seu conteúdo apareça associado à letra escolhida, desde que você digite de novo a frase-senha. Para fechá-lo, é só usar o comando unmount PGPdisk, que aparece clicando-se no ícone do disco virtual e pressionando-se Control para acessar o menu contextual. Ele volta a ser um mero arquivo cifrado, que pode ser transportado ou copiado normalmente. Se o conteúdo do disco virtual precisa ser compartilhado por várias pessoas, o PGPdisk permite a criação de múltiplas frases-senha e também a associação das chaves públicas dos indivíduos que precisarão ter acesso.



O PGP tem integração com o Claris Emailer ou com o Eudora

O PGPdisk permite criar uma partição de disco...

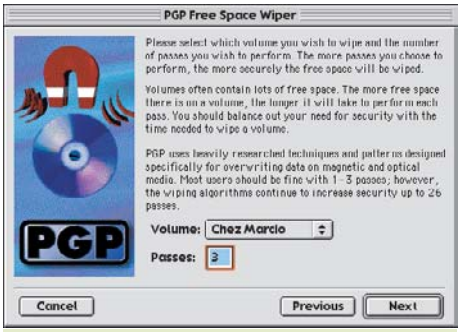
...onde podem ser armazenadas suas informações confidenciais

Arquivos bem apagados

Além dos recursos tradicionais de cifragem e decifragem, o PGP 6 traz também dois utilitários complementares que servem para apagar arquivos sem deixar vestígios. Isso é necessário porque, ao cifrar um documento, o PGP gera uma cópia cifrada do original. Mesmo que você apague do disco o documento original, não é preciso ser um grande perito para recuperá-lo com o auxílio de um programa especial como o Norton Utilities. Para evitar que isso aconteça, você pode usar o comando wipe (limpar), que o PGP coloca no menu contextual ao clicarmos sobre um arquivo pressionando Control. Antes de apagar o arquivo, o wipe o sobrescreve múltiplas vezes com dados aleatórios, impedindo sua reconstituição.
Se você escreveu o documento original em um programa como o Word, é bem provável que o aplicativo tenha gerado cópias temporárias enquanto você trabalhava. Como essas cópias são apagadas pelo aplicativo, o comando wipe não pode ser usado para eliminá-las. Para resolver esse problema, o PGP 6 inclui também o utilitário Free Space Wiper, ou limpador de espaço livre, que realiza a mesma operação em todo o espaço vazio de seu disco rígido, que pode conter fragmentos ou versões antigas de seus dados sigilosos. Apenas por curiosidade, a documentação do Free Space Wipe traz o seguinte aviso: "Sabe-se que empresas comerciais de recuperação de dados podem recuperar arquivos sobrescritos até 9 vezes". O mesmo documento recomenda, então, que para fins "militares" o espaço livre deve ser sobrescrito 18 vezes, ou até 26 vezes para se obter o máximo de segurança!

Conclusão

Quem precisa manter ou trocar dados sigilosos não precisa procurar mais: o PGP 6 é a melhor solução. Diferente de outros programas comerciais que oferecem funções criptográficas, o PGP é o único que coloca seu código-fonte aberto na Internet, para análise de cientistas e hackers de todo o mundo. Ao fazê-lo, o PGP oferece a garantia da transparência. Qualquer criptógrafo concorda que essa é a maior garantia que se pode exigir de um programa baseado em técnicas matemáticas sofisticadas, onde um pequeno bug pode representar uma falha fatal de segurança. A versão freeware pode ser usada por pessoas ou organizações em atividades sem fins lucrativos. Para usar o PGP 6 comercialmente, você precisa adquirir uma licença de uso. A versão paga oferece ainda um recurso, opcional, que garante às empresas a possibilidade de abrir a correspondência comercial de seus funcionários.



O Space Wiper varre qualquer informação de seu HD para sempre

Para encerrar, não podemos simplesmente recomendar o PGP 6 sem repetir o aviso: se suas atividades sigilosas são realmente sérias, não use o PGP antes de estudar cuidadosamente sua documentação. Se você não tem tempo para isso, contrate alguém que possa ajudá-lo a dominar o programa e rever seus procedimentos de segurança. De nada adianta o melhor sistema de criptografia do mundo se, no final, sua frase-senha favorita é "batatinha quando nasce esparrama pelo chão". M

LUCIANO RAMALHO luciano@magnet.com.br
É usuário do PGP desde 1995, tem uma chave pública com ID 0x10473E5E e fingerprint 3B32 6D95 3FDF 271A 8115 8683 6FD0 8C37 1047 3E5E.

Onde oncontrar
PGP: www.pgpi.com
Network Associates: www.nai.com