Developers' Magazine
http://www.developers.com.br

Edição 48, Agosto de 2000

Aspectos de Segurança e Autenticidade na Troca Eletrônica de Mensagens

Francisco Gomes Milagres & Marcio dos Santos Galli

Acompanhando a facilidade da utilização do *e-mail* e o crescimento explosivo do uso da Internet em todos os ramos da indústria, comércio e finanças, as empresas cada vez mais vêm substituindo contatos telefônicos com seus parceiros, clientes, fornecedores e desenvolvedores pelas mensagens eletrônicas. E as vantagens do *e-mail* não se resumem somente a uma quase ausência de custo.

Destaca-se também o curto tempo de entrega, o fato de não ser orientado à conexão (não depende que o destinatário esteja on-line naquele momento) e a cultura flexível em relação ao conteúdo, permitindo muitas vezes uma possibilidade menor de formalismo.

Entretanto, a crescente utilização do *e-mail* em diversas áreas faz com que surja a preocupação em relação aos aspectos de segurança e autenticidade, principalmente quando há o envolvimento de dados como planos de governo, propriedade intelectual ou simplesmente uma correspondência apaixonada.

É natural que o crescimento espantoso da utilização da rede em setores que envolvem troca de dados críticos como comércio eletrônico, *Internet banking* e atividades *business to business* funcionem como um catalisador para o desenvolvimento de uma cultura de segurança. No entanto, grande parte da comunidade na Internet não possui a preocupação necessária com aspectos de segurança até que os problemas apareçam.

Um exemplo pode ocorrer com clientes de provedores de acesso, onde um usuário recebe um *e-mail* com um pedido de recadastramento originado de alguém que se apresenta como um responsável do provedor. Um usuário que não possui conhecimento dos procedimentos de segurança está sujeito a responder tal *e-mail*, disponibilizando para um possível intruso informações como endereço, senhas ou números de cartão de crédito.

Um outro caso surge quando funcionários de uma determinada empresa recebem um *e-mail* forjado de um usuário que se diz membro da empresa (com endereço de *e-mail* igual aos pertencentes à empresa). Uma vez que uma mensagem chega dentro da corporação, muitos funcionários podem lê-la e seguir algum procedimento imaginando que o remetente desta mensagem faz parte da corporação, podendo causar algum dano maior. Especificamente, a execução de um arquivo anexado a esta mensagem pode disparar um software que abre uma brecha possibilitando espionagem ou destruição de dados, afetando a segurança de toda a corporação.

Algumas técnicas de segurança

Para que seja possível uma troca segura de mensagens ou arquivos, criptografia e certificação digital são as técnicas aqui apresentadas para manutenção de privacidade e verificação de autenticidade de mensagens entre o remetente e o destinatário. A seguir será apresentada uma visão geral dessas técnicas.

É importante destacar que elas são específicas aos contexto de segurança e em geral são utilizadas por soluções que provêm as infra-estruturas para troca segura de mensagens e autenticação, tornando a utilização desses processos cada vez mais natural.

Criptografia utilizando par de chaves

Criptografia é uma técnica que permite a codificação e decodificação de dados. A utilização dessa técnica na troca eletrônica de mensagens permite armazenagem e transmissão de forma que somente o remetente e o destinatário da mensagem consigam lê-la.

Basicamente, a técnica de criptografia utilizando-se de chaves pública e privada consiste na utilização desta última para a codificação dos dados e a assinatura de uma mensagem. Já a chave pública correspondente deste par permite a decodificação e verificação da autenticidade da mensagem.

Quando se deseja iniciar uma troca de mensagens criptografadas, inicialmente cada parte (a remetente, "Paula" e o destinatário, "Léo") deve ter criado o seu par de chaves, a pública e a privada, sendo esse par de chaves válido até o dono dele o revogue ou que ele se expire. Como o próprio nome já indica, as chaves públicas devem ser distribuídas a quem você deseja se comunicar, podendo ser diretamente ou através de um servidor de chaves. A chave privada deve ser guardada com cuidado e é somente acessível por uma senha.

Ao codificar uma mensagem a Léo, Paula usa sua chave privada para codificar a mensagem, podendo opcionalmente assiná-la. Ao receber a mensagem, Léo, usando a chave pública de Paula, decodifica a mensagem, podendo também verificar se realmente foi Paula quem a enviou e não um falsário.

Mas como Léo sabe se, desde a primeira mensagem, está ou não trocando mensagens com a verdadeira Paula? O fato de Léo ter recebido com sucesso uma chave pública de Paula não implica que esta seja a chave pública da verdadeira Paula com quem ele deseja se comunicar. Por esta razão existe a *fingerprint*, um conjunto de dados único para o par de chaves que é utilizado para verificação de autenticidade das chaves. É aconselhável que antes de se iniciar uma troca de mensagens utilizando-se chaves, que se faça a verificação de chaves através de um meio seguro conhecido utilizando a *fingerprint*. Um exemplo de *fingerprint* pode ser uma seqüência de

caracteres hexadecimal ou até mesmo uma lista de palavras, facilitando em muito a verificação por telefone.

Certificação digital

Os certificados digitais são *credenciais digitais* e têm a mesma utilidade que um certificado físico. São usados para impedir a substituição ou fraude de uma mensagem e validar seu remetente.

O modelo convencional de certificação de uma mensagem ou documento - em papel - envolve além dos responsáveis por assinar o documento, inclui também a figura de um oficial que reconhece a assinatura em um cartório. O modelo digital é baseado na mesma idéia, porém é mais barato e rápido. No lugar do oficial, há uma entidade certificadora, que pode ser a representada por uma entidade externa de confiança ou até pela própria empresa.

O uso de certificados digitais e de criptografia deixa de ser uma opção e passa a ser uma necessidade em corporações que desejam fazer uso da praticidade da troca eletrônica de mensagens sem estarem expondo sua empresa aos problemas de autenticação e privacidade.

Tendências atuais

Recentemente, o senado norte-americano aprovou um projeto de lei que propõe a validade jurídica de documentos que utilizem assinaturas digitais. Da mesma forma, há leis de mesma natureza em análise do senado brasileiro. Atitudes como essa motivam cada vez mais a utilização de documentos digitais com valor oficial no dia a dia corporativo.

Por exemplo, um funcionário cria um documento e pode enviar ao seu grupo de trabalho para apreciação, inserção de notas, ou uma simples aprovação. Tudo isso com a garantia de que o documento não será adulterado, permitindo somente que notas e assinaturas sejam inseridas.

Em muitos casos, documentos eletrônicos não possuem valor legal se não estiverem acompanhados de uma cópia impressa e assinada, que represente um documento que os valide diante das normas da organização. A utilização de autenticação digital traz a confiabilidade ao processo da utilização da troca de documentos eletrônicos.

Com uma infra-estrutura de confiabilidade e segurança nas mensagens digitais em constante desenvolvimento, a utilização de mensagens eletrônicas pode se tornar cada vez mais natural, eliminando procedimentos adicionais quanto aos aspectos de segurança e autenticidade.

Francisco Gomes Milagres <francisco@milagres.com>, é consultor em segurança computacional, membro pesquisador do Grupo de Segurança da Informação do laboratório Intermídia da USP em São Carlos (http://security.intermidia.icmc.sc.usp.br) e graduando em Ciências da Computação na mesma universidade.

Marcio dos Santos Galli <mgalli@geckonnection.com>, consultor em tecnologias Internet, trabalha para Taboca ArtworK (http://www.taboca.com), é colaborador da comunidade mozilla.org e editor da revista on-line Geckonnection.com, nas quais publica artigos e exemplos utilizando novos padrões WWW.

Links:

Entidades certificadoras:
http://www.certisign.com.br
http://www.verisign.com

Criptografia de chaves pública-privada
http://www.pgp.com
http://www.pgpi.org

Grupo de Segurança da Informação, USP de São Carlos
http://security.intermidia.icmc.sc.usp.br

Outras informações:
http://dmoz.org/Computers/Security/Internet/
http://www.milagres.com
http://www.taboca.com