APLICAÇÕES DA CRIPTOGRAFIA EM AMBIENTES COMPUTACIONAIS

RESUMO

Este artigo demonstra como a criptografia pode ser empregada em transações e protocolos utilizados na Internet, bem como nas redes locais, tendo em vista a integridade e confiabilidade das informações; apresenta alguns exemplos de abrangência desta tecnologia; e também aborda como é estruturado seu funcionamento.

Palavras-Chave: Criptografia, Certificação Digital, Segurança, Algoritmos Criptográficos.

1. INTRODUÇÃO

A Internet tem alterado o modo de nos comunicarmos, fazendo o uso da mesma para vários tipos de serviços como pagamentos de contas, movimentações bancárias, compras, etc. Todas estas atividades, além de muitas vezes serem mais produtivas e ágeis via Web[1], ainda nos possibilitam uma interação maior, seja com pessoas ou estabelecimentos comerciais. E assim, como no dia-a-dia, são necessários vários cuidados com a nossa segurança e de nossos bens para que não sejamos lesados.

Visando este aspecto, a criptografia tem se desenvolvido na busca de soluções cada vez mais seguras. Por exemplo, para que transações comerciais sejam efetuadas sem prejuízos tanto do lado do consumidor quanto para o lado do prestador de serviços, um dos quesitos principais é assegurar que algoritmos cada vez mais complexos e difíceis de serem decifrados por pessoas não autorizadas sejam aplicados.

1 Internet

2. DESENVOLVIMENTO DA CRIPTOGRAFIA, SUAS VANTAGENS E DESVANTAGENS

Um dos sistemas de criptografia mais populares é o RSA. Trata-se de um sistema de criptografia de chave pública que foi inventado em 1977 por Ron Rivest, Adi Shamir e Leonard Adleman, pesquisadores do MIT *(Massachusset Institute of Techonology),* utilizado tanto para cifrar quanto para autenticar dados. O algoritmo[2] RSA faz uso de expressões com exponenciais, onde o texto é cifrado em blocos e cada bloco tem um valor binário menor que um número n, ou seja, o tamanho do bloco tem que ser menor ou igual a $\log_2(n)$.

A principal vantagem do sistema de criptografia baseada em chave pública é a sua maior segurança em relação à criptografia baseada em chave secreta. Isto se deve ao fato que, no sistema baseado em chave pública, as chaves privadas nunca precisam ser transmitidas ou recebidas. No sistema de chave secreta, ao contrário, sempre existe uma chance de que um indivíduo não autorizado possa descobrir a chave secreta enquanto a mesma está sendo transmitida.

Outra vantagem do sistema baseado em chave pública é que este pode fornecer um método seguro para as assinaturas digitais. Em contra partida, apresenta como desvantagem uma velocidade mais baixa, pois o método de chave pública é mais lento na cifragem do que o método de chave secreta.

Para que a criptografia possa se tornar realidade, as aplicações e protocolos necessitam serem criados ou adaptados para trafegar dados seguros. Este processo demanda conhecimento altamente técnico, e muitas vezes, um investimento financeiro elevado de hardware e/ou software. Cada transação ou aplicação seja na Internet, ou em uma rede privada é um caso específico.

2 Conjunto de operações elementares que devem ser efetuadas para se obter um resultado desejado.

3. CERTIFICAÇÃO E AUTENTICAÇÃO DIGITAL

A Certificação digital é uma solução muito utilizada para acessar recursos privados, como por exemplo, a Extranet de uma empresa. O funcionamento da mesma se dá através de uma aplicação na qual uma autoridade de certificação "assina" uma mensagem contendo o nome de um usuário "A" e sua chave pública, de forma que qualquer pessoa possa verificar que a mensagem foi assinada apenas pela autoridade de certificação, e assim, incrementar crédito na chave pública de "A". Com uma assinatura digital comum, qualquer um pode verificar a qualquer momento que a certificação foi assinada pela autoridade de certificação, sem acesso à informação secreta.

A autenticação em um sistema digital é o processo por meio do qual o receptor de uma mensagem digital pode confiar na identidade do remetente e / ou na integridade da mensagem. Os protocolos de autenticação podem ser baseados tanto em sistemas criptográficos convencionais de chave-secreta, como o DES (acrônimo para Data Encryption Standard), ou em sistemas de chave-pública, como o RSA. Neste caso, a autenticação em sistemas de chave pública utiliza assinaturas digitais. A necessidade de assinaturas digitais surgiu justamente desta proliferação de comunicações e transações digitais.

Desta forma, a principal motivação dos sistemas de criptografia é proporcionar segurança a todos usuários e evitar que uma transação possa ser decifrada por pessoas não autorizadas, especialmente em transações bancárias e de compras digitais.

4. REDE PRIVADA VIRTUAL (VPN)

As redes de computadores surgiram com o objetivo de facilitar o compartilhamento mais eficiente de recursos como aplicações, equipamentos e dados, independente da localização física desses recursos ou dos próprios usuários das redes.

Existe um avanço exponencial para que redes de filiais ou empresas parceiras estejam interligadas, facilitando os processos existentes e transmissão de dados. Na maioria dos casos, os administradores e projetistas se vêem frente à necessidade de utilizar linhas dedicadas para conectar redes geograficamente separadas. Contudo, este tipo de solução, oferece dificuldades operacionais que realmente impactam no projeto, tais como: alto custo, dificuldades de escalabilidade e baixa flexibilidade.

Uma solução para este tipo de problema é o uso de uma infra-estrutura aberta e distribuída da Internet para transmissão das informações. Neste caso, os dois principais aspectos da segurança de uma rede - a proteção do acesso à informação e a proteção da transmissão dessa mesma informação - devem ser observados e garantidos através da autenticação dos usuários e da criptografia. A esse tipo de solução chamamos Rede Privada Virtual - VPN (Virtual Private Network).

Uma VPN é uma rede privada criada através da Internet que permite interligar duas ou mais redes de computadores, provendo um mecanismo seguro de comunicação. Nela, criam-se "túneis virtuais" através dos quais a informação é encriptada e transmitida de forma segura. Entretanto, a VPN não deve ser única na rede, pois quanto maior a segurança, maior a dificuldade para acessar as informações.

Como a Internet é uma rede pública, cabe às Redes Privadas Virtuais prover a segurança necessária, através de recursos de criptografia, para se obter a privacidade desejada às redes corporativas. Isto inclui o ciframento, a verificação e a assinatura dos dados que trafegam entre as localidades, protegendo-os contra escuta, alteração e impostura por parte de elementos não autorizados.

Para que isto seja possível, existe um conceito envolvido na definição de VPN que é o túnel, o qual possui relação estreita com o termo "virtual" da VPN. O

tunelamento permite esconder os elementos da rede privada (local ou remota), usando as infra-estruturas do provedor e da própria Internet, criando uma conexão especial entre dois pontos onde a extremidade iniciadora encapsula os pacotes da rede privada para o trânsito através da Internet. Para as VPNs sobre redes IP, este encapsulamento pode significar cifrar o pacote original adicionando um novo cabeçalho IP ao pacote. Na extremidade receptora, um gateway (servidor conectado a extermidade da Internet) remove o cabeçalho IP convencional do pacote usado como meio de transporte na Internet e, se necessário, decifra o pacote repassando o original para o seu destino.

É necessário um planejamento cuidadoso antes de escolher a melhor opção de configuração para um gateway VPN. Qualquer configuração adotada deve ter como objetivo principal atender às necessidades de uma conexão segura.

Como alternativa e seguindo a tendência dos firewalls distribuídos, sugere-se ainda a incorporação de mecanismos que permitam a filtragem pós deciframento no próprio gateway[3] VPN, o que permite uma maior flexibilidade no posicionamento do gateway dentro das configurações possíveis de segmentação da rede.

3 Dispositivo de conexão a rede e software que opera em OSI Camada Sete. Um gateway suporta uma pilha completa de protocolos, como: SNA, DecNet, OSI, TCP/IP

5. SNIFFERS

Os sniffers são programas que, como o próprio nome diz, “farejam” o que se passa pela rede. Eles são utilizados freqüentemente por administradores de rede para identificarem pacotes estranhos “passeando” pela rede ou por pessoas mal intencionadas para tentar descobrir informações importantes, especialmente senhas.

Para utilizar um sniffer é indispensável que você esteja no mesmo segmento de rede que os dados aos quais pretende capturar. Existem muitos sniffers disponíveis na Internet, e sua utilização é bem simples, após um pouco de prática.

Existem várias maneiras de se evitar o uso efetivo de um sniffer por parte de um atacante. Embora não exista uma ``fórmula mágica'' ou método totalmente eficaz, existem várias técnicas que podem ser utilizadas na luta contra tais atacantes.

O uso de canais de comunicação criptografados, embora não evite o uso de sniffers, é a técnica mais eficaz para a proteção de informações na rede, pois torna o tráfego incompreensível a quem não conheça a chave para decifrar. O uso de hardware especializado, técnicas de detecção (remota e local) e intenso trabalho de administração mostram-se efetivos para vários casos, mas nem sempre são confiáveis.

Uma das técnicas mais eficazes para inviabilizar o uso de sniffers é limitar a visibilidade do tráfego evitando que dados não pertinentes a determinada máquina estejam visíveis a outras é uma maneira simples e eficaz para diminuir a eficiência de um sniffer. O modo mais comum de implementar tal técnica é através da utilização de hardware especializado (como switches), configurações de redes onde haja separação entre as partes não relacionadas e utilização de rotas bem implementadas. A tarefa de limitar a visibilidade do tráfego exige planejamento, hardware especializado e intenso trabalho de administração.

6. TÚNEIS CRIPTOGRÁFICOS E SSL

A solução mais eficiente para o problema de acesso indevido a dados é torná-los ilegíveis ou inválidos para o atacante que os consiga capturar. Tal objetivo pode ser alcançado através da utilização de protocolos e canais criptografados (como túneis e VPNs) e outras técnicas de criptografia. É importante lembrar que embora seja um meio eficiente de garantir o sigilo das informações trafegadas, mesmo protocolos considerados seguros, se não bem implementados, podem ser quebrados com pouco ou nenhum esforço. Protocolos como SSL (Secure Socket Layer), utilizado em sites seguros – conhecido como HTTPS; e SSH (Secure SHell) permitem o tunelamento de canais de comunicações de modo que todo o tráfego seja criptografado, e consistem em boas soluções para a implementação de redes seguras.

A utilização de protocolos não criptografados ainda é prática comum. Embora existam alternativas e soluções já há muito tempo disponíveis, o custo de implementação e manutenção adicional que estes acarretam os tornam proibitivos para aplicações em redes simples ou que tenham grande demanda de tráfego. Implementar a utilização de canais criptografados utilizando SSL, pode exigir até o dobro de capacidade de processamento de um servidor ou cliente.

O uso de canais de comunicação criptografados definitivamente se mostra como a melhor solução para o problema da visibilidade dos dados, já que os torna incompreensíveis a terceiros. Com o uso de criptografia, consegue-se anular boa parte da utilidade de um sniffer que esteja à procura de tráfego relevante. Porém a substituição de sistemas funcionais, a necessidade de maior capacidade de processamento e, de um modo geral, a configuração adicional associada à utilização de técnicas de criptografia - como a geração de certificados e chaves por parte do administrador - têm impedido sua ampla utilização.

Mesmo em redes nas quais protocolos criptografados sejam utilizados e o tráfego seja bem delimitado, ainda é grande a quantidade de informações que um atacante munido de um sniffer consegue capturar. A topologia da rede, a versão dos softwares em execução, a carga e o número de usuários, além de diversos outros dados têm um valor substancial na formulação de ataques sofisticados.

A simples existência de um sniffer não autorizado em qualquer ponto da rede é um forte indício de que esta se encontra sob a mira de atacantes ou usuários mal intencionados, independentemente da qualidade e quantidade dos dados que estes possam capturar.

Sendo assim, gera a necessidade da utilização de métodos que detectem a presença de sniffers e a ocorrência de incidentes em geral que sejam suspeitos.

7. CONCLUSÃO

Com base nos tópicos apresentados, podemos concluir que a criptografia está presente em diversos ambientes computacionais. Sendo de grande valor para os administradores de rede e para os usuários em geral, trazendo uma maior segurança nas transações via Internet e em redes locais. Além dos exemplos citados, existe uma gama de aplicações para a criptografia. Neste artigo foram apresentadas algumas mais usuais e práticas para o ambiente de TI.

Pesquisas têm sido realizadas no âmbito da criptografia quântica, para que os algoritmos sejam cada vez mais complexos, dificultando ataques de Criptoanálise. Isso aumentará ainda mais a segurança e confiabilidade das transações.

A criptografia em si, não resolve todos os problemas de segurança de dados; ela é uma das alternativas eficazes para essa finalidade, porém outras ações necessitam serem tomadas para garantir um ambiente confiável e íntegro, tais como: Política de Segurança para os usuários e administração da rede, monitoração dos servidores, ambientes de redundância, dentre outros fatores.

8. REFERÊNCIAS BIBLIOGRÁFICAS

RHEE, MAN YOUNG**, Internet Security: Cryptographic Principles, Algorithms and Protocols**, CRC-PRESS, 1995

REZENDE, PEDRO A. DOURADO, **Criptografia e Segurança na Informática**, 1998, Brasília.

A. MENEZES, P. VAN OORSHOT, F. VANSTONE, **Handbook of Applied Cryptography** CRC Press, 1996

R. T., **Segurança de dados em rede de computadores**, Ed. E. Blucher, 2000

NETO, Criptografia Quântica, 2004. Disponível em: <http://www.numaboa.com.br/criptologia/lab/quantica.php.>. Acesso em: 20 set. 2006.

MURK, **Beginner Guide to Cryptography**, 2004. Disponível em: <http://www.murky.org/cryptography/index.shtml>. Acesso em: 22 set. 2006.

RAPOPORT, EDUARDO, **VPN - Virtual Private Network**, 2003. Disponível em: < http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/index.html>. Acesso em: 22 set. 2006.