UniFOA Centro Universitário de Volta Redonda
NUPEE Núcleo de Pós-graduação, Especialização e Extensão

Curso de Pós-graduação
"Lato-Sensu" em Projeto, Suporte e Administração
de Redes de Computadores

Chaves de Segurança

André Luis de Sousa Almeida
Jussara Roberta Freitas Silva

Resumo

Ao citarmos segurança na rede de computadores, estamos falando puro e simplesmente em criptografia. A criptografia assume um papel cada vez mais importante devido à globalização atual, onde uma grande massa de informações viajam pela Internet. Mesmo que se tenha um servidor protegido, também é preciso transportar com segurança as informações por meio de uma rede pública. E essa segurança só se consegue por meio da criptografia. Neste trabalho apresentamos uma introdução sobre os métodos de transporte e autenticação de dados baseados em sistema criptográficos, cada uma atendendo a uma necessidade diferente.

Palavras-chave

Criptografia; Chave Pública; Chave Privada; Internet; Segurança; Mensagem; Correio Eletrônico; Programa; Assinatura Digital; Certificado Digital.

Security Keys

Summary

When we mention safety on the network, we're talking about pure and simply in cryptography. The cryptography assumes a paper more and more important due to the current growing of networks, where a great mass of information travels through the Internet. Even if there is a protected server , it's also necessary to transport with safety the information by public network. And this safety is gotten by cryptography. In this work we presented an introduction about the transport methods and autentication of data based on cryptographics systems, each one assisting to a different need.

Keywords

Criptography; Public Key; Secret Key; Internet; Security; Message; E-mail; Program; Digital Signature; Digital Certificate.

1. Introdução

Muitas pessoas não sabem, mas seus emails são enviados pela rede como uma espécie de cartão postal, ou seja, qualquer um na rede pode ler o conteúdo de qualquer email, pois estes passam por inúmeros servidores e podem no meio desse caminho ser interceptado por pessoas ou hackers.

Obviamente, em muitos casos isso gera um problema; pois as pessoas que precisam se comunicar por emails muitas vezes trocam informações ou arquivos confidenciais, por exemplo, uma empresa precisa mandar um relatório confidencial para sua matriz no exterior.

É lógico que essa transmissão deva ser feita por um método seguro, e este método existe, e o que é melhor, é inteiramente gratuito. Estamos falando de usar cirptografia para transmissão de dados na grande rede, garantindo um direito constitucional de todo cidadão brasileiro que é o sigilo nas suas comunicações de dados, ou seja, sua proteção contra hackers na utilização principalmente de seu email.

2. Criptografia e a Web

A criptografia é a tecnologia fundamental que protege a informação que viaja pela Internet. Mesmo que uma segurança forte envolvendo o host posssa evitar que pessoas invadam seu computador - ou pelo menos evite que elas causem muitos danos, uma vez que tenham conseguido entrar - não há como transportar em segurança a informação de seu computados para outro computador por meio de uma rede pública sem a utilização da criptografia.

Mas, não existe apenas uma tecnologia criptográfica: existem muitas, cada uma atendendo a uma necessidade diferente. Em alguns casos, as diferenças entre sistemas criptográficos representam diferenças técnicas - afinal, nenhuma solução pode resolver todos os problemas. Em outros, as diferenças resultam de patentes ou segredos comerciais. E, por fim, as restrições à criptografia por vezes resultam de decisões políticas.

2.1 - Criptografia e Segurança na Web

Os profissionais de segurança identificaram quatro palavras chave usadas para descrever todas as diferentes funções que a criptografia desempenha nos sistemas modernos de informação. São as seguintes:

Confidencialidade

A criptografia é usada para embaralhar as informações enviadas pela Internet e armazenada em servidores, de forma que os invasores não possam acessar o conteúdo dos dados. Alguns chamam isso de "privacidade", mas a maioria dos profissionais reserva esta palavra para referir-se à proteção de informações pessoais (confidenciais ou não) do uso ou da agregação de impróprios.

Autenticação

Assinaturas digitais são usadas para identificar o autor de uma mensagem; a pessoa que recebe a mensagem pode verificar a identidade da pessoa que a assinou. Podem ser usadas em conjunto ou como alternativa às senhas.

Integridade

Existem alguns métodos para verificar se uma mensagem não foi modificada em trânsito. Eles são feitos por meio de códigos de mensagem assinados digitalmente.

Não-repúdio

Recibos criptográficos são criados, de forma que o autor de uma mensagem não possa negar falsamente que a tenha enviado.

Estritamente falando, há certa sobreposição entre essas áreas. Por exemplo, quando se usa o algoritmo DES para garantir que haja confidencialidade, assegura-se a integridade ao mesmo tempo. Isso porque, se uma mensagem criptografada for alterada, não será decifrada apropriadamente. No entanto, na prática é melhor usar algoritmos diferentes que sejam criados para garantir a integridade para esse fim do que confiar no subproduto de outros algoritmos. Assim, se o usuário decide não incluir um aspecto (como criptografia) por razões legais ou de eficiência, o usuário ainda terá um algoritmo padrão para as outras exigências do sistema.

2.2 - O que a Criptografia Não Pode Fazer

A criptografia desempenha um papel tão importante na segurança da Web que muitos usam a expressão *servidor Web seguro* quando querem dizer *servidor Web capacitado* para criptografia. De fato, é difícil imaginar dados e transações seguras na Internet sem o uso da criptografia.

No entanto, a criptografia não é todo-poderosa. Você pode usar a melhor criptografia teoricamente possível, mas, se não tiver cuidado, pode ficar vulnerável a ver suas mensagens e documentos publicados na primeira página do jornal, se um destinatário autorizado enviar uma cópia aos repórteres. Da mesma forma, a criptografia não é uma solução apropriada para muitos problemas, como os seguintes:

A criptografia não pode proteger documentos não-criptografados.

Mesmo que você configure seu servidor Web para só enviar arquivos usando a SSL de 1024 bits, lembre-se que os originais não- criptografados ainda estão em seu servidor. A menos que os criptografe separadamente, estes arquivos estarão vulneráveis. Quem invadir o computador onde o servidor se localiza terá acesso aos dados.

A criptografia não pode proteger contra chaves criptográficas roubadas.

A questão do uso da criptografia é tornar possível, às pessoas que possuem suas chaves, decifrar suas mensagens e arquivos. Dessa forma, qualquer atacante que possa roubar ou comprar suas chaves pode decifrar seus arquivos e mensagens. É

importante lembrar disso ao usar a SSL, porque ela mantem cópias da chave secreta do servidor no disco rígido. (Normalmente criptografadas, mas não necessariamente.)

A criptografia não pode proteger contra ataques ao serviço.

Protocolos criptográficos como a SSL, são bons para proteger informações de invasores. Infelizmente, um atacante pode ter outros objetivos que não a bisbilhotice. Em bancos e áreas afins, um atacante pode causar muitos danos e prejuízo simplesmente interrompendo a comunicação ou excluindo arquivos criptografados.

A criptografia não pode proteger você contra o registro de uma mensagem, ou contra o fato de que uma mensagem não foi enviada.

Suponhamos que você envie uma mensagem criptografada a João, e ele mata o amante de sua esposa, e então envia uma mensagem criptografada a você. Uma pessoa razoavelmente inteligente irá suspeitar que você tem algum envolvimento no assassinato, mesmo que não consiga ler o conteúdo de sua mensagem. Ou suponha que haja um registro de você mandando mensagens criptografadas extensas do trabalho para a concorrência. Se houver um depósito misterioros em sua conta dois dias depois de cada transmissão, um investigador provavelmente irá tirar conclusões com base nesse comportamento.

A criptografia não pode proteger de um programa de criptografia sabotado.

Alguém pode modificar seu programa de criptografia para torná-lo pior do que inútil. Por exemplo, um atacante pode modificar sua cópia do Internet Explorer, para que use sempre a mesma chave criptográfica. (Este é um dos ataques desenvolvidos na Universidade da Califórnia em Berkeley.)

Teoricamente, a não ser que você escreva todos os programas que são executados em seu computador, não há maneira de eliminar essas possibilidades. Elas existem, quer você use a criptografia ou não. No entanto, você pode minimizar os riscos obtendo programas de criptografia por meio de canais confiáveis, e minimizando as oportunidades de mudanças em seus programas. Também é possível usar assinaturas digitais e técnicas, como assinaturas em código, para detectar alterações em seu programas criptográficos.

A criptografia não pode proteger de erros ou de traidores.

Os humanos são o elo mais fraco em seu sistema. Seu sistema criptográfico não pode proteger você se seu correspondente envia suas mensagens aos jornais depois de decifrá-las legitimamente. Seu sistema também não pode protegê-lo de um de seus administradores de sistema ser forçado a revelar uma senha em alguma contingência, mesmo que absurda.

3. Sistemas Criptográficos Atualmente em Uso

Ainda que a criptografia seja uma tecnologia que certamente irá se disseminar no futuro, já está funcionando na World Wide Web hoje em dia. Recentemente, mais de uma dúzia de sistemas criptográficos foram desenvolvidos e espalhados pela rede.

Os sistemas criptográficos em uso podem ser divididos em duas categorias. O primeiro grupo é o de programas e protocolos usados para criptografia de mensagens de correio eletrônico. Estes programas pegam uma mensagem, criptografam-na e armazenam o texto cifrado ou o transmitem pela Internet. Estes programas também podem ser usados para criptografar arquivos armazenados em computadores, dando-lhes uma proteção adicional. Alguns sistemas populares deste tipo são:

- PGP
- S/MIME

A segunda categoria de sistemas criptográficos é a de protocolos de rede usados para oferecer confidencialidade, autenticação, integridade e não-repúdio em ambientes de rede. Tais sistemas exigem interação em tempo real entre cliente e servidor para funcionar adequadamente. Alguns sistemas populares deste tipo incluem os seguintes:

- SSL
- PCT
- S-HTTP
- SET e CyberCash
- PKI
- DNSSEC
- Kerberos
- SSH

Todos esses sistemas estão resumidos na Tabela 1, e são descritos nas seções a seguir.

3.1 - PGP

Um dos primeiros programas criptográficos de chave pública a se disseminar foi *Pretty Good Privacy* (PGP - Privacidade Muito Boa), escrito por Phil Zimmermann e lançado na Internet em meados de 1991. O PGP é um sistema completo para a proteção criptográfica de correio e arquivos eletrônicos. Ele também oferece uma série de padrões que descrevem os formatos das mensagens criptografadas, chaves e assinaturas digitais.

O PGP é um sistema criptográfico híbrido, que usa criptografia de chave pública RSA para gerenciamento de chave e criptografia simétrica IDEA para a cifragem dos dados brutos.

Em relação à lista de verificação criptográfica do item 2.1, o PGP oferece confidencialidade, por meio do algoritmo criptográfico IDEA; integridade, por meio da

função MD5; autenticação, pelos certificados de chave pública; e não-repúdio, por meio do uso de mensagens assinadas criptograficamente.

O PGP está disponível de duas formas, como um aplicativo isolado e como um programa de correio eletrônico integrado, disponível por meio da PGP, Inc. O programa sozinho é executável em um número muito maior de plataformas do que o sistema integrado, mas é mais difícil de usar. A PGP, Inc. também está desenvolvendo extensões para sistemas populares de correio eletrônico, para permitir-lhes enviar e receber mensagens criptografadas pelo PGP.

Um problema do PGP é o gerenciamento e a certificação de chaves públicas. As chaves do PGP nunca perdem a validade; em vez disso, quando as mesmas ficam comprometidas, cabe ao portador distribuir uma anulação especial da chave para todos com quem se comunica. Correspondentes que não sabem sobre o comprometimento das chaves e continuam a usá-las por semanas, meses ou anos para enviar mensagens criptografadas o fazem assumindo os riscos. Como efeito colateral, se você criar uma chave pública com o PGP e distribuí-la, deve resguardá-la sempre, porque ela nunca expira.

As chaves públicas do PGP são validadas por uma *cadeia de confiança*. Cada usuário do PGP pode certificar a chave que quiser, o que quer dizer que o usuário acredita que a chave realmente pertence à pessoa mencionada no certificado. Mas o PGP também permite que os usuários manifestem *confiança* em certos indivíduos para testemunhar a autenticidade de outras chaves. Os usuários do PGP assinam as chaves uns dos outros, dando testemunho de autenticidade do portador aparente da chave.

A cadeia de confiança funciona para pequenas comunidades de usuários, não para grandes. Por exemplo, uma maneira pela qual os usuários do PGP assinam as chaves uns dos outros é promovendo ritualísticas *festas de assinatura de chaves*. Os usuários se reúnem, trocam disquetes contendo chaves públicas, mostram suas cartas de motorista, sacam suas chaves privadas e participam de uma orgia de criptogramas de chave pública conforme suas chaves privadas entram em contato. É bem divertido, especialmente com turmas mistas. As assinaturas de chaves são ótimas para encontrar pessoas, porque geralmente são seguidas de viagens a estabelecimentos relacionadas ao consumo de grandes quantidades de álcool, pizza e/ou chocolate. Infelizmente, não é uma maneira prática e criar uma infra-estrutura de chaves públicas.

Outra maneira pela qual as chaves públicas do PGP são distribuídas é por meio dos servidores de chaves públicas do PGP na Internet. Qualquer usuário da Internet pode enviar uma chave pública ao servidor, que irá guardar a chave, enviar uma cópia dela a todos os outros servidores e dá-la a quem quiser. Embora haja muitas chaves legítimas no servidor, muitas são claramente fictícias. Apesar de funcionarem como se apregoa, na prática são ignoradas pela maioria dos usuários do PGP. Em lugar de colocar suas chaves nos servidores, os usuários as distribuem em suas páginas pessoais na Web. A capacidade do PGP de certificar a identidade de forma confiável é severamente prejudicada pela falta de uma infra-estrutura de chave pública.

Nossas Chaves do PGP

Outra maneira de obter uma chave do PGP é encontrar uma em um local confiável, impressa em um livro, por exemplo. Abaixo estão as IDs e as impressões digitais das chaves dos autores. As próprias chaves podem ser obtidas nos servidores de chave pública.

Pub 1024/FC0C02D5 1994/05/16 Eugene H. Spafford <spaf@cs.purdue.edu>
Key fingerprint = 9F 30 B7 C5 8B 52 35 8A 42 73 EE 55 C5 41

Pub 1024/903C9265 1994/07/15 Simson L. Garfinkel <simsong@acm.org>
Key fingerprint = 68 06 7B 9A 8C E6 58 3D 6E D8 0E 90 01 C5 DE 01

3.2 - S/MIME

O MIME (Multipurpose Internet Mail Extensions - Extensões de Correio Internet Multifunção) é um padrão para envio de arquivos com anexos binários na Internet. O Secure/MIME estende o padrão MIME para aceitar correio criptografado. Ao contrário do PGP, S/MIME não foi implementado inicialmente como um programa único, mas como um kit de ferramentas projetado para pacotes de correio eletrônico já existentes. Devido ao fato deste kit ser da RSA Data Security, e incluir licenças para todos os algoritmos e patentes necessários, e devido ao fato de as maiores empresas que vendem sistemas de correio eletrônico já terem relações comerciais com a RSA Data Security, é possível que o S/MIME seja adotado por muitos fornecedores de correio eletrônico.

O S/MIME oferece confidencialidade por meio do uso de algoritmos criptográficos especificados pelo usuário; integridade, pelo uso de funções criptográficas; autenticação, por meio dos certificados de chave pública X.509; e não repúdio, pelas mensagens assinadas criptograficamente. O sistema pode ser usado com criptografia forte ou fraca.

Para enviar correio eletrônico criptografado com o S/MIME, é preciso primeiro ter uma cópia de sua chave pública. Espera-se que a maioria dos programas S/MIME use a infra-estrutura de chave pública X.509, como as criadas pela VeriSign e outras autoridades de certificação.

3.3 - SSL

A SSL (Secure Socket Layer - Camada de Socket de Segurança) é um protocolo criptográfico de uso geral para garantir a segurança em canais de comunicação bidirecionais. Geralmente é usado com o protocolo TCP/IP da Internet. Desenvolvido pela Netscape, a SSL se tornou popular inicialmente por causa do navegador e pelo servidor de Web da Netscape. A idéia era estimular as vendas dos servidores capacitados para criptografia, distibuindo um cliente gratuito que implementava os mesmos protocolos criptográficos.

Desde então, a SSL foi incorporada a muitos outros servidores e navegadores, de forma que sua utilização já não é mais uma vantagem competitiva, mas uma

necessidade. A SSL também está sendo usada em aplicações fora da Web, como em a telnet segura e com qualquer serviço TCP/IP.

As conexões da SSL geralmente são iniciadas por um navegador de Web, pelo uso de um prefixo de URL especial. Por exemplo, o prefixo "https:" é usado para indicar uma conexão HTTP criptografada pela SSL, enquanto "snews:" é usado para indicar uma conexão NNTP criptografada pela SSL.

A SSL oferece confidencialidade pela utilização de algoritmos criptográficos definidos pelo usuário; integridade, com funções criptográficas de embaralhamento definidas pelo usuário; autenticação, por meio do uso de certificados de chave pública X.509 v3; e não-repúdio, por meio de mensagens assinadas criptograficamente.

3.4 - PCT

O PCT é um protocolo de segurança de transporte semelhante à SSL que foi desenvolvida pela Microsoft. Parece que o acrônimo já recebeu várias expansões; no momento, a preferida é a Private Communications Technology (Tecnologia de Comunicações Privadas). O PCT foi desenvolvido para resolver problemas da SSL 2.0; estes problemas também foram resolvidos na SSL 3.0.

Embora a Microsoft aceite a SSL 3.0 e o TLS, a empresa pretende continuar a dar suporte ao PCT, que está sendo usado por clientes grandes da Microsoft nas redes de suas empresas.

3.5 - S-HTTP

O primeiro grande esforço para conferir mais segurança ao HTTP foi empreendido pelo CommerceNet Consortium, em junho de 1994.Esse padrão, chamado Secure HTTP, ou, abreviadamente, S-HTTP, funciona como extensão do HTTP para fornecer serviços de segurança através de algorítmos criptográficos. O S-HTTP se empenha em fornecer bastane flexibilidade ao aceitar algortimos, gerenciamento de chaves, certificados e normas de segurança. Para proporcionar essa flexibilidade, o S-HTTP oferece compatibilidade com vários sistemas de gerenciamento de chaves, incluindo sistemas baseados em chaves públicas, o Kerberos, e modelos "de segredo compartilhado", como o usado em algoritmos de chave simétrica padrão. O S-HTTP também leva em conta o uso de chaves preestabelecidas. As mensagens do S-HTTP são comparáveis em estrutura e formato às mensagens usadas no PEM. Além disso, elas podem ser estruturadas para usar o formato de mensagem PKCS. Na verdade, esse formato de mensagem também pode ser usado para distribuir certificados, como no caso do PEM. Como alternativa, as pessoas podem ser solicitadas a recuperar certificados através de algum outro mecanismo. A principal diferença do S-HTTP é que clientes e servidores podem negociar suas normas, ou seja, podem exigir que determinado serviço de segurança seja ou não usado, ou considerar qualquer um dos dois casos. Essa flexibilidade torna-se extremamente benéfica ao montar a estrutura para que o uso do S-HTTP se difunda. Como resultado de flexibilidade, é possível possível implementar certificados de chave pública em servidores, embora sem obrigar que os usuários individuais obtenham chaves públicas e certificados. Originalmente, o S-HTTP só era

suportado pelo navegador Secure Mosaic do CommerceNet. No início de 1995, a Spyglass anunciou uma compatibilidade com o S-HTTP em seu produto Enhanced Mosaic. Mas apesar de todos estes recursos interssantes como a capacidade de ter documentos pré-assinados residentes em um servidor web, trata-se na verdade de um protocolo morto, porque a Netscape e a Microsoft não conseguiram implementá-lo em seus navegadores.

3.6 - SET

O SET é um protocolo criptográfico criado para enviar números de cartão de crédito criptografados pela Internet.

O sistema SET possui três partes: uma "carteira eletrônica" no computador do usuário; um servidor no site da Web do comerciante; e o servidor de pagamento do SET no banco do comerciante.

Para usar o sistema você precisa inserir seu número de cartão de crédito no software da carteira eletrônica. A maioria das implementações irá armazenar o número do cartão de crédito em um arquivo criptografado no disco rígido, ou em um cartão inteligente. O software também cria uma chave pública e uma secreta para criptografar suas informações financeiras antes de enviá-las pela Internet.

Quando você quiser comprar alguma coisa, seu número de cartão de crédito será criptografado e enviado ao comerciante. O software do comerciante assina digitalmente a mensagem de pagamento e a envia ao banco de processamento, onde o servidor de pagamento decifra todas as informações e executa o débito no cartão de crédito. Por fim, um recibo é enviado ao comerciante e a você, o cliente.

Os bancos que operam com cartão de crédito estão animados com o SET, pois mantém os números dos cartões longe das mãos dos comerciantes. Isso evitaria muitas fraudes, pois são os comerciantes (e seus funcionários) os responsáveis por grande parte das fraudes com cartões de crédito hoje em dia, e não os hackers adolescentes.

O SET oferece confidencialidade para os números dos cartões de crédito, pois são criptografados com o algoritmo RSA. Mas não oferece confidencialidade (portanto, nem privacidade) aos outros elementos da transação: esse compromisso teve que ser assumido para que o SET fosse aprovado para a realização de exportações sem que fossem impostas restrições. O SET oferece integridade, autenticação e não-repúdio por meio do uso de funções de codificação de mensagem e assinaturas digitais.

3.7 - PKI

PKI ou Infra-estrutura de Chaves Públicas, consiste de serviços, protocolos e aplicações utilizados para o gerenciamento de chaves públicas e certificados. O que fazem? Provêem serviços de criptografia de chave pública e assinatura digital, permitindo a interação segura entre usuários e aplicações.

Os serviços oferecidos por uma solução PKI variam: registro de chaves com a emissão de um novo certificado para uma chave pública; revogação ou cancelamento de certificados; obtenção de chaves públicas de uma autoridade certificadora; e validação

de confiança, determinando se o certificado é válido e a quais operações ele está autorizado.

Formada basicamente por software, essas soluções podem ser instaladas na maioria dos servidores existentes no mercado: Windows NT, Novell Netware, Solaris, HP-UX, AIX, Macintosh OS, etc. Contudo, ainda existem iniciativas com soluções que suportam hardware próprios de criptografia para a geração das chaves e emissão dos certificados.

O PKI oferece confidencialidade e privacidade, pois tem certeza de que a comunicação é privada mesmo via Internet; autenticação, identifica os usuários e máquinas; controle de acesso, controla quem acessa as informações e realiza as transações; integridade, garante que a informação não será alterada; não-repúdio, prover um método digital de assinatura das informações e transações.

O conceito é inovador e vem para expandir a esfera de segurança até às aplicações. Contudo é preciso definir as necessidades com clareza, para só então especificar uma solução PKI.

3.8 - CyberCash

O CyberCash é um protocolo de pagamento eletrônico semelhante ao SET em sua finalidade. De fato, partes do SET foram aproveitadas quase que integralmente para a produção do CyberCash.

3.9 - DNSSEC

O padrão DNSSEC (Domain Name System Security - Segurança de Sistema de Nome de Domínio) é um sistema criado para dar segurança ao sistema DNS (Domain Name System - Sistema de Nome de Domínio) da Internet. O DNSSEC cria uma infra-estrutura de chave pública paralela sobre o sistema DNS. Para cada domínio DNS é atribuída uma chave pública. Pode-se obter uma chave pública de domínio de forma confiável no domínio principal, ou pré-carregado em um servidor DNS usando o arquivo de "boot (partida)" do servidor.

O DNSSEC permite a autalização segura de informações armazenadas em servidores DNS, tornando-o ideal para administração remota.

3.10 - Kerberos

O Kerberos é um sistema de segurança de redes desenvolvido no MIT e usado nos Estados Unidos. Ao contrário dos outros sistemas mencionados, o Kerberos não usa tecnologia de chave pública por duas razões. A primeira é que, quando foi desenvolvido, em 1985, os computadores eram bem mais lentos. Os desenvolvedores imaginavam que a criptografia e decifragem de chave pública seriam muito lentas para autenticar conexões e requisições de correio eletrônico. A segunda foi por causa das patentes de Stanford e do MIT. Os criadores do Kerberos queriam distribuir o código gratuitamente pela Internet mas tinham preocupação com possíveis problemas de licenciamento de patentes.

O Kerberos é baseado em cifras simétricas compartilhadas entre seu servidor e os usuários. Cada usuário possui sua própria senha, e o servidor do Kerberos a utiliza para criptografar mensagens enviadas ao usuário, de forma que não possam ser lidas por mais ninguém.

É preciso adicionar suporte ao Kerberos em cada programa a ser protegido. Atualmente, há versões "Kerberizadas" de Telnet, FTP, POP e RPC Sun em uso. Um sistema que usava o Kerberos para oferecer confidencialidade em HTTP foi desenvolvido, mas nunca saiu do laboratório.

O Kerberos é um sistema difícil de configurar e administrar. Para operar um sistema Kerberos, cada site deve ter um servidor Kerberos fisicamente seguro. O servidor Kerberos mantém uma cópia da senha de cada usuário. No caso do servidor do Kerberos fica comprometido, as senhas dos usuários devem ser alteradas.

3.11 - SSH

O SSH, que quer dizer Secure Shell (Shell Seguro), possibilita operações de transferência de arquivos (rcp) e terminal virtual (Telnet) protegidas por criptografia. Há versões não-comerciais do SSH disponíveis para diversas versões do UNIX.

Em uma conexão de emulação de terminal remoto seguro através de Secure Shell (SSH), por exemplo, o servidor armazena sua chave pública e a envia ao cliente. Este, por sua vez, utiliza a chave privada correspondente para decriptografar o "desafio" criptografado pelo servidor. O problema nesta forma de autenticação é que as chaves públicas de criptografia residem dentro de um banco de dados local aos servidores e são mantidas por administradores do sistema ou usuários individuais, sem a utilização de tecnologias centralizadas e seguras para a distribuição e manipulação destas chaves. Clientes SSH podem estar configurados para aceitar e gravar automaticamente novas chaves públicas dos servidores que eles necessitam acessar, aumentando o risco de um ataque MITM quando a primeira conexão a qualquer servidor para emulação SSH é estabelecida.

Sistema	O que é?	Algoritmo	Oferece
PGP	Aplicativo para criptografia de correio eletrônico	IDEA, RSA, MD5	Confidencialidade, autenticação, integridade e não-repúdio
S/MIME	Formato para criptografia de correio eletrônico	Especificado pelo usuário	Confidencialidade, autenticação, integridade e não-repúdio
SSL	Protocolo para criptografar transmissões TCP/IP	RSA, RCZ, RC4 e outros	Confidencialidade, autenticação, integridade e não-repúdio
PCT	Protocolo para criptografar transmissões TCP/IP	RSA, RCZ, RC4 e outros	Confidencialidade, autenticação, integridade e não-repúdio
S-HTTP	Protocolo para criptografia de requisições e respostas HTTP	RSA, DES e outros	Confidencialidade, autenticação, integridade e não-repúdio; no entanto, é obsoleto
SET e CyberCash	Protocolos para enviar instruções de pagamentos com segurança pela Internet	RSA, MD5, RC2	Confidencialidade de números de cartão de crédito apenas, autenticação de comprador e vendedor, integridade de mensagem e não-repúdio de transações
PKI	Gerenciamento de chaves públicas e certificados		Confidencialidade, autenticação, integridade e não-repúdio
DNSSEC	Sistema seguro de nome de domínio	RSA, MD5	Autenticação, integridade
Kerberos	Segurança de rede para aplicações de alto nível	DES	Confidencialidade, autenticação
SSH	Terminal remoto criptografado	RSA, Diffie-Hellman, DES, Triple-DES, Blowfish e outros	Confidencialidade, autenticação

Tabela 1. Comparação dos Sistemas Criptográficas Disponíveis na Internet

5. Conclusão

O ataque só poderá ser realizado se a primeira conexão entre os dois elementos for interceptada por um suposto atacante. A partir de então, este atacante poderá personificar as duas pontas da comunicação e visualizar todo o conteúdo que trafega nesta conexão. Sendo assim concluimos que:

- Informação é essencial
- A base está na administração
- Não existe segurança total
- A maioria dos ataques é simples
- É preciso cooperação

Assim, embora a criptografia seja uma elemento importante da segurança na Web, não é o único. A criptografia não pode garantir a segurança de seu computador se as pessoas podem invadi-lo de outras formas. Mas a criptografia protege seus dados, o que ajuda a minimizar o impacto de uma invasão. Recomendamos que:

- Teste a segurança da rede
- Use criptografia
- "Assine" arquivos e programas

E como disse F.T. Grampp e R.H. Morris:

" É fácil ter-se um sistema de computação seguro.
Você meramente tem que desconectar o seu sistema de qualquer rede externa, e permitir somente terminais ligados diretamente a ele. Pôr a máquina e seus terminais em uma sala fechada, e um guarda na porta."

ANEXO

Algumas definições úteis

Assinatura Digital

A assinatura digital, assim como uma assinatura real, identifica única e exclusivamente uma pessoa. A assinatura real é definida por uma simbologia própria do autor, e não pode ser reproduzida, uma vez que o processo de escrever o símbolo é aleatório, e depende de parâmetros como estado emocional, e outras variáveis aplicáveis no contexto da situação.

Com a assinatura digital ocorre o mesmo fenômeno. Através de regras e procedimentos definidos por organizações internacionais, é possível gerar uma simbologia, representada em BITS (linguagem computacional) para cada pessoa. O processo também é ditado por variáveis como números aleatórios, e consistem de dois passos:

1) Geração de um par de chaves a partir de números aleatórios e por um algoritmo próprio e que define um número único.

2) A assinatura das informações por um algoritmo que emprega a chave privada do autor sobre estas informações, gerando um cálculo matemático único e irreversível. Nota: Quanto maior a grandeza do tamanho da chave, maior será a complexidade da assinatura.

Como utilizo isto nas minhas transações na Internet?

O processo de geração de chaves além de ser um processo trabalhoso, é dependente da guarda da chave na sua máquina, ou em seu poder.

A maioria das aplicações existentes não posuem estes benefícios por suas próprias razões, mas é totalmente adaptável a sua necessidade.

Se você não utiliza nenhum mecanismo de geração de chaves, você não possui assinatura digital.

Solicite junto ao seu prestador de serviço ou revendedor, a assinatura digital.

Certificado Digital

Certificados digitais são documentos eletrônicos que buscam associar determinadas chaves de criptografia a pessoas físicas, servidores e dispositivos de rede. Para que esta associação seja considerada válida em um determinado sistema, esta deve ser verificada e ratificada por um elemento de distribuição e delegação de confiança, a chamada autoridade certificadora.

A autoridade certificadora (AC) é uma espécie de cartório digital que assegura ao cliente que uma determinada chave pública assimétrica é realmente de um servidor idôneo. Os certificados publicam, além da chave assimétrica, o período de validade, informações sobre o detentor, propósitos de uso e especialmente a chancela - a assinatura digital das informações feita com a chave privada - da autoridade

certificadora emissora. A este processo, denominamos emissão de um certificado digital.

A assinatura digital permite que o cliente tenha a garantia de que um certificado não foi modificado. É a garantia de que uma chave pública é a correspondente da chave privada que está no servidor correto. Pelo fato do certificado estar associado ao nome de um servidor, o usuário e os aplicativos clientes podem verificar a quem ou a que endereço do web site deve pertencer aquela chave. Esta proteção poderá ser quebrada caso haja comprometimento do sistema de resolução de nomes na Internet ou da chave privada correspondente a esse certificado, que está armazenada no servidor.

Os certificados digitais são base para a autenticação e o estabelecimento de sessões de comunicação criptografadas entre diversos protocolos de aplicação no Secure Sockets Layer (SSL). Por exemplo, o estabelecimento de um acesso seguro a um servidor web - em outras palavras, uma sessão HTTP segura - pode ser dividido de forma resumida nas seguintes etapas:

1. Navegador contacta o servidor web e este lhe apresenta o certificado digital próprio e da autoridade certificadora, além de parâmetros de tamanho de chaves e algoritmos suportados. É neste momento que pode ser feito um ataque chamado "Man-in-the-Middle", que será explicado nos próximos tópicos deste documento;

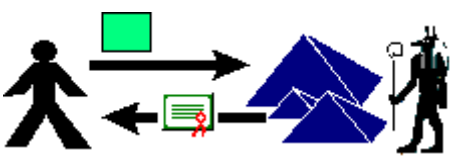
2. Navegador negocia os parâmetros de criptografia, verifica a integridade dos certificados digitais apresentados e decide confiar ou não nos certificados digitais apresentados;

3. Caso decida confiar, o navegador gera uma chave de sessão que será criptografada com a chave pública constante do certificado apresentado como sendo do servidor web. Desta forma, o servidor web poderá decriptografar com sua chave privada a chave de sessão e utilizá-la como parâmetro para o algoritmo simétrico selecionado para estabelecimento das comunicações. Caso não decida confiar no certificado apresentado, a sessão criptografada não é estabelecida.

Como funciona:

Em um momento prévio do uso dos recursos, o proponente requere um certificado ao emissor para ter a proficiência ao uso dos recursos.

Ex. Você deseja disponibilizar um meio seguro de informações no seu site www (https). Você deverá requerer o Certificado Servidor para ser instalado no seu Servidor WEB hospedeiro do seu site.



No momento de utilizar os recursos, o proponente mostrará que possue proficiência dos recursos ao emissor através de seu Certificado, e este validará através do timbre.

Ex. Você deseja acessar um site seguro; já disponibilizado pelo passo anterior com o emissor. Então, quando você solicita um endereço https, o seu browser que contém o Certificado CA instalado, solicita a verificação do Certificado Servidor do site. Caso o Certificado Servidor contenha o timbre emitido pelo Certificado CA, então é disponibilizado um canal de comunicação com o site, e todas as informações postadas a ele serão cifradas para que o site garanta a autenticidade do servidor a você e a integridade das informações a ambos.

Para email, funciona da mesma forma.

Em um momento prévio você deverá solicitar o seu Certificado de EMail, e instalá-lo no seu browser. Conforme mencionado, você deverá ter o Certificado CA para que ele verifique a autenticade do seu certificado. Para postar uma mensagem, configure no seu browser o uso de assinatura digital e/ou criptografia da mensagem, e envie a mensagem normalmente. Para receber uma mensagem assinada digitalmente, você deverá possuir o Certificado do emissor da mensagem em seu browser para a decriptografia e verificação da mensagem do emissor. Geralmente o emissor da mensagem emite juntamente com a mensagem o certificado. Solicite, sempre que necessário, ao emissor da mensagem o certificado. Para receber uma mensagem criptografada, você deverá enviar o seu certificado para quem você deseja receber emails protegidos. E ele irá enviar o email a você com a criptografia realizada pelo seu certificado. A recepção de mensagens criptografadas com o seu certificado é tratada normalmente pelo seu browser.

Alguns algoritmos descritos:

Algoritmos para ciframentos de dados:

DES
IDEA

Algoritmo para Gerenciamento de Chaves:

RSA

Funções de Espalhamento Unidirecional:

MD5

Algoritmo para Assinatura Digital:

RSA
DAS

Referências

Referências de Sites

http://www.artnet.com.br/tecnolog/secure-www.htm#seguro

Cersar home page
http://cras.simpleweb.com.br/

Homepage do PGP Internacional
http://www.dca.fee.unicamp.br/pgp/

Portal Módulo
www.modulo.com.br

Rede Nacional de Pesquisa
www.rnp.br

Referências Bibliográficas

[PARFINKEL & SPARFFORD] PARFINKEL,S. e SPAFFORD,G. *"Comércio e Segurança na Web*, p.208-249

[DERNSTEIN, BHIMANI, SCHULTZ & SIEGEL, 1997]. DERNSTEIN, T.; ANISH, B. B.; SCHULTZ, E. e SIEGEL, C. A. - *" Segurança na Internet". Editora Campos* , 1997, p. 219- 259