**Tema 6 - Segurança em redes de computadores**

A segurança em redes de computadores é uma preocupação fundamental para garantir a comunicação segura entre as partes envolvidas. A principal finalidade é assegurar que apenas os participantes autorizados possam compreender o conteúdo das mensagens trocadas, mesmo em meio a ambientes inseguros onde interceptações são possíveis. Esse objetivo abrange várias propriedades essenciais:

* **Confidencialidade:** Garante que apenas o emissor e o receptor possam entender o conteúdo das mensagens, necessitando, portanto, de métodos de criptografia para proteger os dados contra interceptadores.
* **Integridade de Mensagem:** Assegura que o conteúdo das comunicações não seja alterado, intencionalmente ou por acidente, durante a transmissão. Isso é alcançado através de técnicas que verificam a integridade dos dados.
* **Autenticação do Ponto Final:** Essencial para confirmar a identidade das partes na comunicação, garantindo que cada parte seja de fato quem diz ser. Isso é especialmente importante em ambientes onde a comunicação visual direta não é possível.
* **Segurança Operacional:** Com a vasta conectividade à Internet, as redes estão expostas a diversas ameaças. Mecanismos como firewalls e sistemas de detecção de invasões são fundamentais para proteger as redes de organizações contra ataques externos.

Os intrusos, sejam passivos ou ativos, podem monitorar, modificar, inserir ou eliminar mensagens, representando uma séria ameaça à segurança da rede. Tais ações podem levar a violações de confidencialidade, autenticação falsas, interrupções de serviços, entre outros ataques. Portanto, é vital implementar contramedidas eficazes para mitigar esses riscos.

Nesse contexto, técnicas criptográficas são fundamentais para a segurança na troca de informações em redes, permitindo que dados sejam transmitidos de forma que somente os destinatários autorizados possam entender seu conteúdo original. A criptografia transforma dados originais, conhecidos como texto aberto, em uma forma codificada, chamada texto cifrado, que é ininteligível para qualquer intruso. Apesar dos métodos de codificação serem amplamente conhecidos e padronizados, a segurança da criptografia reside no uso de chaves secretas que apenas os participantes autorizados conhecem, permitindo que apenas eles possam decifrar a mensagem codificada e acessar o conteúdo original.

Existem dois tipos principais de sistemas criptográficos: chaves simétricas e chaves públicas. Nos sistemas de chave simétrica, tanto o remetente quanto o destinatário utilizam a mesma chave secreta para criptografar e descriptografar mensagens, garantindo que apenas eles possam acessar o conteúdo da comunicação. Dentre as chaves semétricas, destaca-se a cifra de César, que cifra o texto substituindo cada letra por outra, deslocando-se um determinado número de posições no alfabeto. Apesar de sua simplicidade e da limitação de apenas 25 possíveis chaves de cifra, exemplifica o conceito básico de criptografia simétrica, onde a mesma chave é usada para cifrar e decifrar a mensagem. Já a cifra monoalfabética, representou um avanço em relação à cifra de César, tendo em vista que melhora a segurança ao permitir que qualquer letra seja substituída por qualquer outra, gerando um número maior de possibilidades de substituição. No entanto, mesmo com a complexidade aumentada para 26! (aproximadamente 10^26) combinações, a vulnerabilidade a ataques através da análise estatística da linguagem revela limitações desse método. Para enfrentar essas e outras limitações, desenvolveram-se as cifras polialfabéticas, que utilizam múltiplas cifras monoalfabéticas para codificar letras em diferentes posições do texto de maneira variada, aumentando significativamente a dificuldade de decifração sem o conhecimento da chave exata. Este método complica ainda mais a criptografia ao alterar a cifra aplicada de acordo com um padrão predefinido, dificultando ataques que dependem da análise da frequência das letras.

.Na criptografia de chave simétrica moderna, destacam-se duas categorias principais de técnicas: cifras de fluxo e cifras de bloco. Enquanto as cifras de fluxo são brevemente discutidas no contexto de segurança para LANs sem fio, as cifras de bloco recebem uma atenção especial por seu uso extensivo em protocolos de segurança na internet, como PGP, SSL e IPsec. Estas últimas processam mensagens em blocos de um determinado tamanho de bits (k), onde cada bloco é criptografado de forma independente utilizando um mapeamento um-para-um, transformando o texto aberto em texto cifrado.

Um exemplo simplificado, com k = 3 bits, ilustra o conceito de mapeamento um-para-um, onde 8 possíveis entradas são mapeadas em 8 possíveis saídas de forma única, exemplificando a cifra de bloco em ação. Tal sistema, embora conceitualmente simples, revela a complexidade potencial da criptografia de bloco, pois para valores de k maiores, o número de mapeamentos possíveis cresce exponencialmente, tornando-se astronômico mesmo para valores moderados de k, como 64 bits.

Na prática, cifras de bloco com valores de k maiores são utilizadas para prevenir ataques de força bruta, mas a implementação direta de mapeamentos um-para-um para grandes valores de k é impraticável devido à enorme quantidade de entradas possíveis. Como alternativa, funções que simulam tabelas permutadas aleatórias são empregadas para processar blocos de dados, incrementando a segurança sem necessitar de uma tabela de mapeamento gigantesca.

Padrões conhecidos de cifras de bloco, como DES, 3DES e AES, utilizam tal abordagem, operando com blocos e chaves de tamanhos específicos. O DES, por exemplo, usa blocos de 64 bits com chaves de 56 bits, enquanto o AES pode utilizar blocos de 128 bits com chaves que variam entre 128, 192 e 256 bits. A chave de criptografia define os mapeamentos específicos e as permutações usadas no processo de cifragem, fazendo com que o ataque de força bruta - tentar todas as chaves possíveis - seja extremamente custoso em termos de tempo e recursos computacionais, evidenciado pela estimativa do NIST que sugere ser necessário um tempo proibitivo para decifrar uma chave AES de 128 bits mesmo com uma máquina capaz de testar todas as chaves possíveis em um ritmo acelerado.

Na criptografia de mensagens longas ou fluxos de dados extensos em redes de computadores, o uso direto de cifras de bloco pode levar a vulnerabilidades. Especificamente, quando partes idênticas do texto aberto são cifradas independentemente, elas resultam em blocos de texto cifrado idênticos. Essa regularidade pode ser explorada por atacantes para inferir o conteúdo do texto aberto, especialmente se o atacante possui conhecimento sobre a estrutura do protocolo subjacente.

Para mitigar esse problema, introduz-se um elemento de aleatoriedade no processo de cifragem, assegurando que blocos de texto aberto idênticos produzam blocos de texto cifrado distintos. Uma abordagem consiste em criar um número aleatório único para cada bloco a ser cifrado, realizando uma operação de ou-exclusivo (XOR) entre esse número e o bloco de texto aberto antes da cifragem. Esse método aumenta a segurança, mas também duplica a quantidade de dados a serem transmitidos, pois tanto o texto cifrado quanto o número aleatório devem ser enviados para o receptor.

Para conciliar a necessidade de segurança e eficiência, as cifras de bloco frequentemente empregam a técnica de Encadeamento do Bloco de Cifra (CBC), que minimiza o overhead adicional. O CBC começa com um Vetor de Inicialização (IV) enviado em texto aberto. Esse IV, junto com os blocos de texto cifrado subsequentes, é utilizado em uma operação XOR com o próximo bloco de texto aberto antes de sua cifragem. Dessa forma, cada bloco cifrado depende não apenas do bloco de texto aberto correspondente, mas também de todos os blocos de texto aberto anteriores. Isso garante que blocos de texto aberto idênticos resultem em blocos de texto cifrado diferentes e reduz a quantidade de dados adicionais transmitidos, pois apenas um IV é necessário para uma mensagem longa.

O processo de decifragem no CBC permite que o receptor recupere o texto aberto original utilizando a chave compartilhada e o IV. A natureza do CBC assegura que, mesmo com a transmissão do IV em texto aberto, o texto cifrado permanece seguro contra decifragem por atacantes que não possuam a chave secreta.

Diferentemente dos sistemas de chaves simétricas, os sistemas de chave pública utilizam um par de chaves, onde uma é pública e conhecida por todos, e a outra é privada e conhecida apenas pelo destinatário da mensagem. Esse método permite que qualquer pessoa criptografe uma mensagem usando a chave pública do destinatário, mas apenas o destinatário com a chave privada correspondente pode descriptografá-la. A criptografia de chave pública representou uma revolução na forma como a comunicação segura é realizada, tendo em vista que elimina a necessidade de as partes compartilharem uma chave secreta pré-determinada para cifrar e decifrar mensagens. Até a invenção da criptografia de chave pública por Diffie e Hellman em 1976, a única forma conhecida de comunicação segura envolvia o uso de uma chave simétrica compartilhada, cujo estabelecimento seguro entre as partes representava um desafio significativo, especialmente em um contexto onde o encontro físico era impraticável.

A inovação da criptografia de chave pública reside na utilização de um par de chaves: uma pública, acessível a todos, e uma privada, conhecida apenas pelo destinatário. Isso permite que qualquer pessoa cifre uma mensagem usando a chave pública do destinatário, mas somente o detentor da chave privada correspondente pode decifrá-la. Essa abordagem não apenas simplifica a troca de mensagens cifradas em ambientes onde as partes não podem se encontrar fisicamente, mas também estabelece a base para outros usos importantes como autenticação e assinaturas digitais.

A criptografia de chave pública traz preocupações quanto à segurança e autenticidade. A ampla disponibilidade da chave pública gera o temor de que intrusos possam, em teoria, usar essa chave para cifrar mensagens fraudulentas ou tentar deduzir a chave privada correspondente. No entanto, algoritmos de criptografia de chave pública baseiam-se em problemas matemáticos complexos, como a fatoração de grandes números primos (um exemplo é o RSA) ou o problema do logaritmo discreto, tornando a dedução da chave privada ou a decifração de mensagens sem a chave privada computacionalmente inviável. Assim, mesmo conhecendo a chave pública e o algoritmo utilizado, a cifragem por terceiros não compromete a segurança da mensagem destinada ao portador da chave privada.

Quanto à autenticidade, o dilema reside na possibilidade de qualquer um enviar mensagens cifradas utilizando a chave pública do destinatário, questionando-se assim a identidade do remetente. Este desafio é superado através do uso de assinaturas digitais, que permitem ao remetente assinar a mensagem com sua chave privada, garantindo a integridade da mensagem e confirmando sua origem. Tal assinatura, verificável pela chave pública do remetente, assegura que a mensagem não foi alterada e autentica o remetente de forma inequívoca. Portanto, a criptografia de chave pública, complementada pelo uso de assinaturas digitais, oferece uma metodologia robusta para comunicações seguras e autenticadas, abordando eficientemente as preocupações inerentes à sua aplicação.

O algoritmo RSA, criado por Ron Rivest, Adi Shamir e Leonard Adleman, se destaca no campo da criptografia de chave pública, utilizando a aritmética modular como base para suas operações. Essa abordagem permite a realização segura e eficiente de comunicações cifradas sem a necessidade prévia de compartilhar uma chave secreta entre as partes envolvidas. A aritmética modular, onde operações são realizadas com números e seus resultados são tomados como o resto de sua divisão por um número n, é crucial para o funcionamento do RSA. Propriedades como (**a mod n) + (b mod n) mod n = (a + b) mod n**), e outras semelhantes para subtração e multiplicação, facilitam a realização de operações criptográficas de forma segura e previsível.

Para implementar o RSA, inicialmente selecionam-se dois números primos grandes, “p” e “q”, e calculam-se dois parâmetros chave: **n = pq** e **z = (p - 1)(q - 1)**. A chave pública (n, e) e a chave privada (n, d) são derivadas de modo que “e” seja um número menor que “n”, coprimo (dois números que não têm nenhum divisor comum além de 1) de “z”, e “d” seja escolhido tal que **ed mod z = 1**. A chave pública pode ser livremente distribuída, enquanto a chave privada deve ser mantida em segredo.

Na prática, a cifragem de uma mensagem “m” (onde m < n) com a chave pública utiliza a operação **c = me** mod n, resultando no texto cifrado “c”. Para decifrar “c”, utiliza-se a chave privada na operação inversa **m = cd mod n**, recuperando assim a mensagem original m. Este processo assegura que apenas o detentor da chave privada correspondente à chave pública usada para cifrar a mensagem possa decifrá-la.

Em aplicações de segurança, a criptografia de chave pública e a criptografia de chave simétrica são frequentemente utilizadas em conjunto para otimizar a eficiência e a segurança na transmissão de dados. Devido ao consumo de tempo significativo na exponenciação requerida pela criptografia de chave pública, como o RSA, comparada à maior velocidade da criptografia de chave simétrica, como AES, uma abordagem híbrida é adotada para a troca de dados cifrados em grande volume e alta velocidade.

Nesse processo, uma chave de sessão simétrica, temporária e única, é selecionada para cifrar os dados. Essa chave é então cifrada utilizando a chave pública RSA do destinatário, garantindo que apenas o destinatário, com a correspondente chave privada RSA, possa decifrá-la. Após a decifração da chave de sessão, ambas as partes dispõem de uma chave comum simétrica, que será utilizada para cifrar e decifrar os dados transmitidos.

Na criptografia, além de proporcionar confidencialidade na comunicação, a integridade da mensagem e a autenticação são essenciais. A integridade da mensagem visa assegurar que o conteúdo recebido não foi alterado durante o trânsito, e a autenticação confirma a identidade do remetente. Esse desafio é particularmente relevante em protocolos de rede seguros e situações onde mensagens cruciais, como atualizações de estado em algoritmos de roteamento, são transmitidas. A distribuição de mensagens de estado de enlace falsas, por exemplo, pode comprometer a eficiência e a segurança de uma rede de computadores.

Uma técnica chave para garantir a integridade e a autenticação da mensagem é o uso de funções de hash criptográficas. Estas funções processam uma entrada para produzir um hash de tamanho fixo, dificultando a criação de duas mensagens distintas com o mesmo valor de hash. Diferente de somas de verificação simples, uma função de hash criptográfica robusta torna impraticável para um atacante substituir uma mensagem protegida por outra com o mesmo valor de hash.

Entre os algoritmos de hash amplamente usados estão o MD5 e o SHA-1. O MD5 gera um resumo de mensagem de 128 bits através de um processo que inclui enchimento, anexação do comprimento da mensagem, inicialização de um acumulador e um processamento iterativo em quatro rodadas. O SHA-1, seguindo princípios semelhantes ao MD4, produz um resumo de mensagem de 160 bits, oferecendo uma camada adicional de segurança devido ao seu resultado mais longo.

Para assegurar a integridade da mensagem em comunicações digitais, o uso de funções de hash criptográficas é fundamental, mas insuficiente quando utilizado isoladamente, pois um atacante pode criar uma nova mensagem e calcular um hash válido para ela. Assim, para efetivamente garantir a integridade, é necessário o uso de um código de autenticação de mensagem (MAC), que incorpora um segredo compartilhado entre as partes comunicantes.

O processo de garantia de integridade envolve as seguintes etapas:

1. A criação da mensagem “m” seguida pela concatenação dessa mensagem com uma chave de autenticação secreta compartilhada “s”, formando **m + s**.
2. O cálculo do hash **H(m + s)**, gerando o MAC, que é anexado à mensagem original, resultando em uma mensagem estendida **(m, H (m + s))**.
3. O destinatário, ao receber **(m, h)** e conhecendo “s”, recalcula **H(m + s)** e compara o resultado com “h”. Se os valores coincidirem, a integridade da mensagem é confirmada.

O MAC serve como uma assinatura digital que valida tanto a origem quanto a integridade da mensagem, sem a necessidade de cifrar todo o conteúdo da comunicação. Isso é particularmente útil em aplicações que requerem autenticação de mensagens, mas não necessariamente a confidencialidade delas.

A popularização do HMAC, que aplica a função de hash duas vezes sobre os dados e a chave de autenticação, reforça a segurança do MAC, tornando-o compatível tanto com MD5 quanto com SHA-1. No entanto, surge a questão de como distribuir de forma segura a chave de autenticação compartilhada. Em cenários como uma rede de roteadores utilizando algoritmos de roteamento de estado de enlace, a chave pode ser distribuída manualmente por um administrador de rede ou de forma digital, cifrando-a com a chave pública de cada roteador e enviando-a pela rede, o que facilita a distribuição sem comprometer a segurança da chave compartilhada.

Outra técnica para garantir a autenticidade e integridade de documentos ou mensagens no ambiente digital, é a assinatura digital, a qual é uma técnica que funciona de forma similar às assinaturas manuscritas no mundo físico. Para ser eficaz, uma assinatura digital deve ser tanto verificável, permitindo a confirmação de que o documento foi assinado pelo declarante, quanto não falsificável, assegurando que somente o declarante poderia ter realizado a assinatura.

Para implementar uma assinatura digital, a criptografia de chave pública se apresenta como uma solução adequada, onde o remetente utiliza sua chave privada única para assinar o documento. Esse processo não visa cifrar o conteúdo para ocultação, mas sim criar uma assinatura que possa ser verificada por qualquer pessoa usando a chave pública do remetente. Essa abordagem atende aos requisitos de verificabilidade e exclusividade da assinatura digital.

No entanto, criptografar e decifrar documentos inteiros pode ser computacionalmente custoso. Para otimizar esse processo, as funções de hash criptográficas são introduzidas no processo de assinatura digital. O remetente gera um hash de tamanho fixo da mensagem original e, em seguida, assina esse resumo hash com sua chave privada. Esse procedimento reduz o volume de dados a serem criptografados na assinatura, diminuindo o esforço computacional necessário e mantendo a integridade da mensagem. Ao receber a mensagem e a assinatura, o destinatário aplica a mesma função de hash à mensagem recebida e verifica a assinatura com a chave pública do remetente. Se o hash verificado coincidir com o hash recebido, confirma-se a integridade da mensagem e a autenticidade da assinatura.

Diferentemente dos códigos de autenticação de mensagem (MACs), que também são usados para garantir a integridade da mensagem, mas dependem de uma chave compartilhada entre remetente e destinatário, as assinaturas digitais oferecem a vantagem de não exigir a pré-compartilhação de uma chave secreta, facilitando a autenticação em comunicações abertas. Enquanto os MACs são adequados para situações onde a confidencialidade da chave compartilhada pode ser assegurada, as assinaturas digitais são preferíveis em contextos onde a publicação da chave para verificação de assinaturas é necessária.

A certificação de chaves públicas é uma aplicação crucial das assinaturas digitais, essencial para assegurar a autenticidade e a propriedade de uma chave pública em protocolos de rede seguros, como IPsec e SSL. Esse processo é relevante em situações como transações de comércio eletrônico, onde a autenticação da identidade do remetente é fundamental para evitar fraudes e mal-entendidos.

Para ilustrar a importância da certificação de chaves públicas, considere o cenário do “trote da pizza” digital, onde a autenticidade da chave pública é questionável. Nesse cenário, sem uma forma confiável de verificar a autenticidade da chave pública de um remetente, um atacante poderia facilmente se passar por outra pessoa, resultando em consequências indesejadas, como pedidos falsos entregues a vítimas desavisadas.

A solução para esse problema é a emissão de certificados por Autoridades Certificadoras (CAs), que vinculam uma chave pública a uma entidade específica após um processo rigoroso de verificação de identidade. Esses certificados, assinados digitalmente pela CA, fornecem a prova necessária da autenticidade da chave pública. Quando um certificado é apresentado em uma comunicação, o receptor pode usar a chave pública da CA para verificar a assinatura do certificado e confirmar a validade da chave pública do remetente.

As CAs desempenham um papel central na infraestrutura de chave pública, estabelecendo um modelo de confiança onde a confiabilidade da identidade associada a uma chave pública depende diretamente da integridade e da confiabilidade da própria CA. As normas para autoridades certificadoras, como a recomendação ITU X.509 e o RFC 1422, especificam a sintaxe e os procedimentos para a emissão de certificados e o gerenciamento de chaves, contribuindo para uma rede de confiança que facilita transações seguras e autenticadas na internet.

Outro tipo de autenticação, é a de ponto final, que é um processo essencial em redes de computadores, onde uma entidade precisa comprovar sua identidade para outra através de uma conexão de rede. Diferentemente das interações humanas que podem usar reconhecimento visual ou de voz, a autenticação digital depende exclusivamente de dados e mensagens trocados em um protocolo de autenticação específico.

Um exemplo prático é a autenticação de um usuário em um servidor de correio eletrônico. O desafio aqui é autenticar a entidade em tempo real, diferentemente da autenticação da origem de uma mensagem recebida anteriormente. Simplesmente enviar uma mensagem afirmando a identidade não é seguro, pois qualquer intruso poderia falsificar essa mensagem. Mesmo tentativas de autenticação baseadas em endereços de rede conhecidos são vulneráveis a técnicas como a falsificação de IP, onde um atacante manipula o endereço de origem do datagrama IP para se passar por outra entidade.

Uma abordagem clássica para a autenticação é o uso de senhas secretas compartilhadas. Contudo, essa técnica expõe a senha a interceptações, especialmente em conexões não seguras onde a senha é enviada em texto aberto. Criptografar a senha com uma chave secreta compartilhada pode parecer uma solução, mas ainda deixa o sistema vulnerável a ataques de reprodução, onde um atacante reenvia uma mensagem autenticada capturada anteriormente.

Para superar esses desafios, protocolos de autenticação mais avançados incorporam o uso de um valor único conhecido como nonce, que é um número usado apenas uma vez para garantir que a entidade está "viva" no momento da autenticação. No protocolo aprimorado, a entidade que solicita a autenticação primeiro anuncia sua identidade, e a entidade que autentica responde com um nonce. A solicitante então criptografa esse nonce com uma chave secreta compartilhada e o envia de volta, permitindo que a autenticadora verifique tanto a identidade quanto a presença em tempo real da solicitante. Essa abordagem não só assegura que a entidade autenticadora conheça a chave secreta, como também confirma que a entidade está ativa no momento da autenticação, abordando efetivamente o problema dos ataques de reprodução. Além disso, a possibilidade de integrar criptografia de chave pública ao uso de nonces para a autenticação oferece uma via adicional para a segurança da autenticação em redes, permitindo um processo de verificação robusto sem a necessidade de compartilhar segredos previamente conhecidos.

O Pretty Good Privacy (PGP), criado por Phil Zimmermann em 1991, é um esquema de criptografia de e-mail amplamente utilizado que se estabeleceu como um padrão de fato. Este sistema de segurança, que atrai usuários de mais de 166 países, é acessível por meio de software disponível em domínio público, facilitando a criptografia de e-mails para assegurar tanto a confidencialidade quanto a integridade das mensagens.

O PGP adota uma abordagem semelhante ao modelo de segurança descrito anteriormente, utilizando funções de hash como MD5 ou SHA para criar resumos de mensagens, e algoritmos de criptografia como CAST, DES triplo ou IDEA para a cifração de chaves simétricas, complementado pelo uso do RSA para a criptografia de chaves públicas. Ao ser instalado, o PGP automaticamente gera um par de chaves, pública e privada, para o usuário. Enquanto a chave pública pode ser compartilhada livremente, por exemplo, em sites ou servidores de chaves públicas, a chave privada é protegida por uma senha, garantindo sua segurança.

O PGP permite ao usuário não apenas assinar digitalmente suas mensagens para provar a autenticidade e garantir a integridade, mas também criptografar suas comunicações para manter a confidencialidade do conteúdo. Essas funcionalidades podem ser usadas de forma isolada ou combinada, dependendo das necessidades de segurança do usuário.

Além disso, o PGP oferece um mecanismo único para a certificação de chaves públicas através de uma rede de confiança. Diferentemente das autoridades certificadoras convencionais, no PGP os próprios usuários podem certificar pares de chaves de outros usuários que consideram confiáveis. Isso permite a criação de um sistema de confiança descentralizado, onde os usuários também podem indicar sua confiança em outros para validar a autenticidade de mais chaves. Grupos de usuários do PGP frequentemente realizam encontros presenciais para trocar e certificar reciprocamente suas chaves públicas, fortalecendo a rede de confiança do sistema.

Nesse mesmo contexto de proporcionar segurança na rede, a criptografia é aplicada ao TCP para reforçar os serviços de segurança através do Secure Sockets Layer (SSL) e do Transport Layer Security (TLS), uma evolução padronizada do SSL pelo IETF. Desenvolvido inicialmente pela Netscape, o SSL é fundamental para transações seguras na web, sendo amplamente suportado por navegadores e sites de e-commerce, como Amazon e eBay. Indicado pela mudança de "http" para "https" na URL do navegador, o SSL é quase universalmente empregado em compras online para proteger a comunicação entre o navegador do usuário e os servidores.

O uso do SSL é crucial para prevenir várias formas de ataques cibernéticos durante transações eletrônicas. Sem criptografia, dados sensíveis do usuário, incluindo informações de pagamento, podem ser capturados por invasores. A falta de integridade dos dados permite que os pedidos sejam alterados, resultando em cobranças indevidas. Além disso, sem a autenticação do servidor, usuários correm o risco de serem enganados por sites fraudulentos, levando a possíveis roubos de identidade ou fraudes financeiras. Embora seja tecnicamente posicionado na camada de aplicação, do ponto de vista do desenvolvedor, o SSL funciona como uma extensão do protocolo de transporte. Oferece uma interface de programação de aplicações (API) que enriquece as funcionalidades do TCP com recursos de segurança adicionais. Esta abordagem não se limita ao HTTP, permitindo que qualquer aplicação operando sobre

O TCP tire proveito dos serviços de segurança do SSL, promovendo uma camada de segurança versátil para uma ampla gama de aplicações na Internet.

Após a introdução ao "quase-SSL", vamos detalhar o SSL real, preenchendo as lacunas e aprimorando o entendimento dos mecanismos subjacentes a este protocolo essencial para segurança na Internet. O SSL tem três fases principais: apresentação, derivação de chave e transferência de dados.

1. **Fase de Apresentação:** Durante esta fase inicial, o cliente estabelece uma conexão TCP com o servidor, confirma a identidade do servidor através de um certificado que vincula sua chave pública à sua identidade, e transmite uma chave secreta mestre. Esta chave mestre, depois de cifrada com a chave pública do servidor e enviada, é usada pelo servidor para decifrar usando sua chave privada.
2. **Derivação de Chave:** O Segredo Mestre (MS), agora compartilhado, inicialmente poderia funcionar como a chave de sessão simétrica para todas as operações de criptografia e verificação de integridade. No entanto, para maior segurança, o cliente e o servidor geram quatro chaves a partir do MS: duas chaves de criptografia de sessão e duas chaves MAC de sessão, cada uma para direções de comunicação distintas. Essa separação de chaves por direção e por função (criptografia versus integridade) é uma prática recomendada para manter a segurança dos dados.
3. **Transferência de Dados:** Na fase de transferência de dados, os dados são protegidos usando as chaves derivadas. O SSL trata o fluxo de dados como registros, adicionando um MAC a cada registro para integridade e, em seguida, cifrando o pacote antes de enviá-lo através do TCP. A implementação de números de sequência nos cálculos do MAC previne ataques de manipulação de sequência, como reordenação ou repetição de segmentos por atacantes.

Para finalizar uma sessão SSL, o protocolo utiliza um campo de tipo específico nos registros para indicar o término da sessão. Isso é crucial para prevenir ataques de truncamento, nos quais um atacante poderia terminar prematuramente uma sessão para causar perda de dados. O campo de tipo é autenticado juntamente com o MAC do registro, fornecendo uma confirmação segura do fim da comunicação.

O protocolo IP de segurança, conhecido como IPsec, é crucial para proteger datagramas IP entre diversas entidades, como hospedeiros e roteadores, e é amplamente utilizado para criar redes virtuais privadas (VPNs) que operam sobre a Internet pública. Este protocolo proporciona uma solução econômica e eficaz para instituições geograficamente dispersas ao garantir "cobertura total". Isto significa que todas as cargas úteis dos datagramas enviados entre as entidades são cifradas, oferecendo sigilo completo e impedindo que partes não autorizadas acessem dados sensíveis, incluindo e-mails, páginas web e outras formas de dados digitais.

Além do sigilo, o IPsec autentica a origem dos datagramas, permitindo que a entidade destinatária confirme a identidade do remetente, e garante a integridade dos dados, assegurando que o conteúdo não seja alterado durante o trânsito. O protocolo também protege contra ataques de repetição, evitando a aceitação de datagramas duplicados.

No uso prático, muitas instituições empregam o IPsec para criptografar o tráfego interdepartamental que transita pela Internet pública, enquanto a comunicação interna dentro de uma localidade, como entre hospedeiros em uma matriz ou filial, usa o IPv4 padrão. Por exemplo, quando um hospedeiro em uma matriz envia um datagrama para um vendedor em um hotel, o roteador na matriz converte esse datagrama de IPv4 para IPsec e o encaminha pela Internet. O cabeçalho IPv4 do datagrama IPsec permite que os roteadores da Internet pública o processem como um datagrama IPv4 comum, mas sua carga útil, que inclui um cabeçalho IPsec, é criptografada. Quando o datagrama chega ao dispositivo do vendedor, o sistema operacional decodifica essa carga útil e realiza outras verificações de segurança, como a integridade dos dados, antes de passar a carga útil decodificada para o protocolo da camada superior, como TCP ou UDP.

As entidades que enviam datagramas IPsec, como hospedeiros ou roteadores, estabelecem uma associação de segurança (SA) antes da transmissão dos dados. Uma SA é uma conexão lógica unidirecional que define os parâmetros para a troca de datagramas seguros. Se a comunicação bidirecional for necessária, duas SAs devem ser configuradas. Por exemplo, em uma VPN corporativa que conecta uma sede a uma filial e a vendedores viajantes, várias SAs são necessárias para cobrir todas as conexões bidirecionais. Quando um datagrama IPsec é enviado, ele pode assumir duas formas: modo túnel ou modo transporte. O modo túnel é predominantemente usado em VPNs, encapsulando o datagrama IP inteiro para cifragem e autenticação, adequado para passar por qualquer parte da Internet pública sem revelar a carga útil ou as informações de roteamento original.

O IKE (Internet Key Exchange) é uma peça fundamental no funcionamento do IPsec, sendo responsável pela configuração segura das Associações de Segurança (SAs) que são cruciais para a operação do protocolo. Ele facilita a negociação de parâmetros de segurança e a troca de chaves entre entidades de rede, permitindo comunicações protegidas. O IKE realiza essa tarefa em duas fases distintas: a primeira fase cria um canal seguro chamado IKE SA, usando o método Diffie-Hellman para estabelecer uma chave segura sem revelar as identidades dos participantes externamente. Na segunda fase, este canal seguro é usado para negociar as SAs do IPsec que protegerão efetivamente os dados, estabelecendo os algoritmos e as chaves a serem usados.

No que diz respeito à segurança de redes Wi-Fi, o WEP (Wired Equivalent Privacy) foi uma das primeiras tentativas de implementar segurança sob o padrão IEEE 802.11. Seu objetivo era oferecer uma segurança comparável à de redes cabeadas, mas o WEP foi rapidamente descoberto por ter falhas críticas. Seu uso de IVs (Vetores de Inicialização) curtos e a repetição de chaves tornam a rede vulnerável a ataques, e o algoritmo RC4 usado no WEP é suscetível a análises de tráfego que podem quebrar a criptografia. Além disso, a integridade dos dados é comprometida pelo uso do CRC, que pode ser manipulado por atacantes.

Diante dessas falhas, o IEEE 802.11i foi desenvolvido para superar as deficiências do WEP, introduzindo um nível de segurança muito mais alto para redes Wi-Fi. Este padrão melhorado usa o Protocolo de Autenticação Extensível (EAP) sobre LAN (EAPOL) e pode integrar servidores de autenticação baseados em RADIUS ou DIAMETER para oferecer uma autenticação robusta. Ele também implementa uma gestão de chaves mais eficiente e usa o AES (Advanced Encryption Standard) para a criptografia, substituindo o fraco RC4. Com esses aprimoramentos, o IEEE 802.11i proporciona uma segurança robusta para redes sem fio, mantendo os dados seguros mesmo em ambientes de alta utilização.

A implementação de firewalls robustos é igualmente essencial na proteção das fronteiras de uma rede interna contra ameaças externas. Um firewall é uma combinação de hardware e software que isola a rede interna de uma organização da Internet em geral, permitindo que alguns pacotes passem e bloqueando outros. Ele permite ao administrador de rede controlar o acesso entre o mundo externo e os recursos da rede que administra, gerenciando o fluxo de tráfego de entrada e saída. Um firewall tem três objetivos principais: garantir que todo o tráfego de fora para dentro e vice-versa passe por ele, permitir apenas o tráfego autorizado pela política de segurança local e ser imune a penetrações, o que significa que se não for adequadamente projetado ou instalado, pode oferecer uma falsa sensação de segurança. Companhias como Cisco e Check Point são líderes no fornecimento de firewalls. É possível criar um firewall com o uso de iptables em sistemas Linux, uma ferramenta de domínio público comumente incluída nesses sistemas. Firewalls podem ser classificados em três tipos: filtros de pacotes tradicionais, filtros de estado e gateways de aplicação, cada um abordado detalhadamente nas subseções seguintes.

Como descrito, a filtragem de pacotes em uma organização é uma prática de segurança essencial para controlar o acesso entre a rede interna e a internet. Essa filtragem é realizada no roteador de borda, que conecta a rede interna ao provedor de serviços de internet (ISP) e ao ambiente da internet mais amplo. Este roteador é estrategicamente colocado para inspecionar cada datagrama individualmente, utilizando regras específicas para determinar se o tráfego deve ser permitido ou bloqueado.

As regras de filtragem podem incluir critérios como endereços IP de origem e destino, tipos de protocolo, portas TCP ou UDP, e outros atributos dos datagramas, permitindo uma administração minuciosa do que entra e sai da rede. Isso inclui o bloqueio de conexões TCP não autorizadas, o gerenciamento do uso de largura de banda para aplicações como rádio via internet, e a prevenção de mapeamentos não autorizados da rede interna por meio de mensagens ICMP.

Além disso, a filtragem de pacotes pode ser finamente ajustada para permitir que clientes internos iniciem conexões com servidores externos, enquanto bloqueiam tentativas de conexão externas para servidores internos, usando o estado do bit TCP ACK como critério. Por exemplo, se uma organização decidir que nenhuma conexão TCP de entrada deve ser permitida, exceto para o seu servidor web público, pode configurar o roteador para bloquear todos os segmentos TCP SYN de entrada, exceto aqueles destinados à porta 80 com o endereço IP do servidor web. Essa configuração detalhada é realizada nas listas de controle de acesso (ACLs) de cada interface do roteador, que especificam as regras para lidar com os datagramas que passam por essas interfaces.

Os filtros de pacotes tradicionais baseiam-se na inspeção isolada de cada pacote, aplicando regras estáticas que não levam em conta o contexto de uma sessão de comunicação. Esse método pode ser eficaz para políticas simples de controle de acesso, mas apresenta limitações significativas quando se trata de tráfego dinâmico, como o das conexões TCP, que necessita de uma análise mais contextual para assegurar tanto a segurança quanto a funcionalidade da rede.

Para superar essas limitações, os filtros de estado são implementados. Esses filtros mantêm um rastreamento das conexões TCP em toda a sua duração, desde a inicialização com o handshake de três vias (SYN, SYN-ACK, ACK) até o término, identificado por um pacote FIN ou por um timeout de inatividade. Essa capacidade de manter um estado de conexão permite que o firewall aplique regras de segurança que consideram o contexto completo da sessão, não apenas informações isoladas de pacotes individuais.

Por exemplo, na prática, uma lista de controle de acesso pode inicialmente permitir que todos os pacotes TCP com porta de origem 80 e o bit ACK marcado passem, uma vez que isso é típico para respostas de servidores web a solicitações iniciadas internamente. No entanto, essa abertura pode ser explorada por atacantes para enviar pacotes maliciosos. Para mitigar esse risco, os filtros de estado verificam se cada pacote que chega é parte de uma conexão estabelecida e autorizada. Se um pacote não corresponde a uma sessão ativa na tabela de conexões do firewall, como no caso de um pacote com origem e porta inesperadas, ele é prontamente rejeitado.

Esse método oferece uma camada adicional de segurança, assegurando que apenas tráfego legítimo e esperado possa fluir para dentro e para fora da rede. O filtro de estado não apenas bloqueia tentativas de conexão não solicitadas, mas também permite uma navegação segura e eficiente para os usuários internos, pois reconhece e facilita o retorno do tráfego legítimo. A integração de filtros de estado com as políticas tradicionais de filtro de pacotes resulta em uma abordagem de segurança mais robusta, adaptativa e contextual para a proteção de redes corporativas contra ameaças externas e internas.

Para garantir a segurança em redes corporativas, onde requisitos específicos como acesso restrito e autenticação são necessários para aplicações sensíveis como Telnet, os gateways de aplicação são uma solução eficaz. Esses gateways vão além dos tradicionais firewalls e filtros de pacotes ao adicionar uma camada de controle baseada nos próprios dados da aplicação, não apenas nos cabeçalhos de pacotes.

Um gateway de aplicação atua como um intermediário para todas as comunicações de uma aplicação específica, garantindo que apenas usuários autorizados possam acessar serviços externos. Por exemplo, no caso do Telnet, um gateway de aplicação pode ser configurado para permitir conexões somente de usuários verificados internamente. Esse processo começa quando o usuário tenta iniciar uma sessão Telnet: ele deve primeiro autenticar-se no gateway de aplicação, que verifica suas credenciais antes de permitir qualquer comunicação externa.

Se as credenciais forem validadas, o gateway de aplicação então atua duplamente como cliente e servidor Telnet, estabelecendo uma conexão segura com o destino externo e repassando os dados entre o usuário e o hospedeiro externo. Esta abordagem não só garante que apenas usuários autorizados possam iniciar sessões Telnet para fora da rede, mas também mantém a gestão centralizada do tráfego de saída.

Embora eficazes, os gateways de aplicação vêm com suas próprias limitações. Eles podem introduzir latência devido ao processamento adicional necessário para inspecionar e redirecionar o tráfego de aplicativos. Além disso, cada aplicação que requer esse nível de controle de segurança precisa de seu próprio gateway dedicado, o que pode complicar a infraestrutura de rede e aumentar os custos operacionais. O gerenciamento de múltiplos gateways pode se tornar uma tarefa complexa, especialmente em ambientes com muitos serviços críticos. Além disso, é essencial que os softwares clientes sejam configurados para interagir corretamente com os gateways, especificando corretamente para onde as solicitações devem ser enviadas, o que adiciona uma camada de complexidade na configuração dos sistemas dos usuários finais.

Os sistemas de detecção de invasão (IDS) e sistemas de prevenção de invasão (IPS) desempenham um papel crucial na segurança de rede, monitorando e analisando o tráfego para detectar atividades suspeitas ou maliciosas. Diferente dos firewalls e filtros de pacotes, que se concentram apenas nos cabeçalhos dos pacotes para filtragem baseada em regras predefinidas, os sistemas IDS/IPS realizam uma inspeção profunda de pacotes. Esta abordagem não se limita apenas aos cabeçalhos, mas também analisa os dados contidos nos pacotes, proporcionando uma avaliação mais detalhada e abrangente do tráfego de rede.

A necessidade de uma inspeção mais profunda surge da limitação dos métodos de filtragem tradicionais em detectar ataques sofisticados, que podem se disfarçar dentro de fluxos de dados aparentemente normais. Os IDS/IPS são especialmente equipados para identificar esses tipos de ameaças ao comparar os pacotes contra um banco de dados de assinaturas de ataques conhecidos ou ao identificar padrões de tráfego que desviam de um perfil de normalidade estabelecido. Por exemplo, um IDS pode detectar uma varredura de porta, um ataque de negação de serviço (DoS), ou tentativas de exploração de vulnerabilidades conhecidas por meio da correspondência com assinaturas previamente definidas.

Os sistemas IDS/IPS operam em duas modalidades principais: detecção baseada em assinaturas e detecção baseada em anomalias. Os sistemas baseados em assinaturas comparam o tráfego de rede com um conjunto de assinaturas digitais que representam atividades maliciosas conhecidas. Essa abordagem é eficaz para detectar ataques previamente identificados, mas pode falhar na identificação de novas ameaças que ainda não foram catalogadas. Por outro lado, os sistemas baseados em anomalias trabalham estabelecendo uma linha de base do que é considerado tráfego normal e, em seguida, detectam desvios significativos desse padrão, o que pode indicar uma potencial ameaça.

Além de monitorar, os sistemas IDS/IPS podem tomar medidas proativas para prevenir uma intrusão, bloqueando tráfego suspeito ou executando ações para mitigar uma ameaça em andamento. Essa capacidade de resposta imediata transforma um IDS passivo em um IPS ativo, capaz de intervir diretamente para proteger a rede. No contexto organizacional, os IDS/IPS são tipicamente distribuídos em pontos estratégicos da rede para monitorar eficazmente o tráfego de entrada e saída. Eles podem ser posicionados na zona desmilitarizada (DMZ), onde servidores que necessitam de interação com a internet estão localizados, ou em segmentos de rede que contêm dados críticos. Essa disposição permite que os sistemas de segurança tenham uma visão abrangente do tráfego, garantindo que qualquer atividade suspeita seja rapidamente identificada e tratada. A implementação de IDS/IPS, juntamente com firewalls e outras medidas de segurança, forma uma defesa em camadas que é crucial para proteger recursos valiosos de informações contra uma variedade de ameaças, desde ataques automatizados até tentativas de intrusão por agentes mal-intencionados.

Em resumo, a segurança em redes de computadores abrange uma ampla gama de técnicas e estratégias, desde a criptografia básica até complexos sistemas de monitoramento de tráfego como IDS e IPS. A evolução contínua das ameaças cibernéticas exige que as medidas de segurança sejam igualmente dinâmicas e adaptáveis, capazes de proteger contra tanto ataques conhecidos quanto novas vulnerabilidades emergentes. O emprego de tecnologias como a criptografia de chave pública e sistemas simétricos, além do uso rigoroso de firewalls, gateways de aplicação e sistemas de detecção e prevenção de invasões, constitui uma estratégia integrada e robusta para salvaguardar as redes e os dados que elas suportam. À medida que os métodos de ataque se tornam mais sofisticados, também deve evoluir a abordagem para a segurança da rede, garantindo não apenas a proteção dos dados, mas também a integridade e disponibilidade dos sistemas de rede que sustentam as operações críticas das organizações modernas.

**Referências**

Redes de Computadores e a internet: Uma abordagem Top-down (capítulo 8)