INTRODUÇÃO

Neste trabalho abordaremos o tema segurança de redes. Nele explicaremos de forma detalhada e clara a política de segurança, alguns dos mecanismos de segurança, os critérios de segurança de um sistema de computação, e também a segurança na Internet TCP/IP.

O primeiro capítulo tem por objetivo dar uma abordagem introdutória e básica à segurança de redes de computadores, mostrando alguns conceitos básicos, política de segurança e os principais métodos de segurança.

Já o segundo apontará os critérios de segurança de um sistema de computação, o livro laranja do DoD.

E finalmente no terceiro capítulo abordaremos a segurança na rede Internet TCP/IP, falando de segurança em correio eletrônico, segurança Web, roteamento, dentre outros.

1. CONCEITOS BÁSICOS.

O termo segurança é usado com o significado de minimizar a vulnerabilidade de bens (qualquer coisa de valor) e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém [ISO 89f].

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação, intencional ou não, de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou de seus dispositivos periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizados nos termos de uma política de segurança.

Mesmo o conceito de uma rede segura sendo atraente para a maioria dos usuários, as redes não podem ser classificadas simplesmente como seguras ou não-seguras porque o termo não é absoluto, cada organização define o nível de acesso que é permitido ou negado. Pois pode haver a necessidade de armazenar dados que valiosos, assim define-se uma rede segura como um sistema que impede que estranhos acessem os computadores e consequentemente aos dados. Ou então, pode haver a necessidade de disponibilizar informações, assim defini-se uma rede segura como uma rede que permite acesso arbitrário a dados, mas inclui mecanismos que impedem mudanças sem autorizações. Ainda outros grupos se concentram em manter a comunicação privada: definem uma rede segura como uma rede em que ninguém além do receptor pretendido possa interceptar e ler uma mensagem. Finalmente, muitas organizações grandes necessitam de uma definição complexa de segurança, que permite acesso a dados ou serviços selecionados que a organização decide tornar público, ao impedir acesso ou modificação de dados e serviços sensíveis que são mantidos privados.

Como não existe nenhuma definição absoluta de rede segura, o primeiro passo que uma organização deve tomar para obter proteção é afirmar claramente e de forma não-ambígua os itens que devem ser protegidos.

1.1 AMEAÇAS E ATAQUES

Uma ameaça consiste em uma possível violação da segurança de um sistema. Alguns exemplos de ameaças são: destruição de informação ou de outros recursos, modificação ou deturpação da informação, roubo, remoção ou perda da informação ou de outros recursos, revelação de informação, interrupção de serviços, entre outros.

As ameaças podem ser acidentais ou intencionais. As ameaças acidentais são as que não estão associadas à intenção premeditada. Já as ameaças intencionais variam desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema. A realização de uma ameaça intencional configura um ataque.

Alguns dos principais ataques que podem ocorrer em um ambiente de rede são:

- Personificação (masquerade): uma entidade faz-se passar por outra.
- Replay: uma mensagem, ou parte dela, é interceptada, e posteriormente transmitida para produzir um efeito não autorizado.
- Modificação: o conteúdo de uma mensagem é alterado implicando em efeitos não autorizados sem que o sistema consiga detectar a alteração.
- Recusa ou impedimento de serviço: ocorre quando uma entidade não executa sua função apropriadamente ou atua de forma a impedir que outras entidades executem sua funções.

- Ataques internos: ocorrem quando usuários legítimos comportam-se de modo não autorizado ou não esperado.
- Armadilhas (trapdoor): ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando,ou evento, predeterminado.
- Cavalos de Tróia: nesse ataque, uma entidade executa funções não autorizadas, em adição às que está autorizada a executar.

1.2 POLÍTICA DE SEGURANÇA

Uma política de segurança é um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos.

Um dado sistema só é considerado seguro em relação a uma política de segurança, caso garanta o cumprimento das leis, regras e práticas definidas nesta política.

Uma política de segurança deve:

- Apoiar sempre os objetivos da organização e nunca apoiar-se em ferramentas e plataformas.
- Descrever o programa geral de segurança da rede.
- Demonstrar os resultados de sua determinação de risco, com as ameaças que está combatendo e as proteções propostas.
- Definir responsabilidades para implementação e manutenção de cada proteção.
- Definir normas e padrões comportamentais para usuários, para que o documento seja utilizado como prova se ocorrer alguma violação.

- Relacionar os recursos que se quer proteger e que softwares são permitidos em quais locais.
- Relatar o que acontece quando programas e dados não homologados são detectados no ambiente operacional.
- Relacionar quem desenvolveu as orientações, quem as aprovou, quem detém privilégios e determina autorizações e quem é afetado pelas orientações.
- Descrever procedimentos para fornecimento e revogação de privilégios, informação de violação de segurança.
- Determinar gerência específica e responsabilidades dos envolvidos no controle e manuseio do ambiente operacional.
- Trazer explicações da importância da adoção dos procedimentos de segurança justificando-os junto aos usuários para que o entendimento dos mesmos leve ao comprometimento com todas as ações de segurança.

Antes de uma política ser implementada os usuários devem ser treinados nas habilidades necessárias para segui-la. As boas políticas de segurança dependem do conhecimento e cooperação dos usuários. Isto é particularmente relevante para segurança contra vírus e políticas sobre gerencia de senhas. Segurança requer mais que conhecimento. Todos os usuários devem saber como agir quando se virem diante de uma violação ou possível violação. Todos usuários devem saber quem chamar se tiverem perguntas ou suspeitas, e devem saber o que fazer e o que não fazer, para minimizar riscos de segurança. Estes usuários devem ser incentivados a sentir que as medidas de segurança são criadas para seu próprio benefício.

1.3 MECANISMOS DE SEGURANÇA

Uma política de segurança pode ser implementada com a utilização de vários mecanismos. A seguir alguns dos principais mecanismos de segurança adequados a ambientes de comunicação de dados.

1.3.1 **Criptografia**

O envio e o recebimento de informações sigilosas é uma necessidade que existe há centenas de anos. Com o surgimento da Internet e sua praticidade na entrega de informações de maneira precisa e extremamente rápida, a criptografia tornou-se uma ferramenta essencial para permitir que somente o emissor e o receptor tenham acesso livre a tal informação.

1.3.1.1 Introdução à criptografia e sua história

Criptografia (do grego: *kriptós* = escondido, oculto; *gráphein* = grafia) é a arte ou ciência de escrever em cifra ou em códigos a fim de permitir que apenas o destinatário decifre e compreenda, evitando que um intruso consiga interpretá-la, ou seja, é o ato de codificar dados em informações aparentemente sem sentido para que pessoas não consigam ter acesso às informações que foram cifradas.

Figura 1 – Criptografia

A criptografia não é uma técnica recente, pelo contrário, é bem antiga, pois foram encontradas numerosas mensagens codificadas às quais eram atribuídos poderes mágicos e religiosos no sistema de escrita hieroglífica dos egípcios, nas pedras sepulcrais do Antigo Egito e os romanos utilizavam um código secreto para comunicar planos de batalha.

Com o advento da Revolução Industrial, mais precisamente depois da Segunda Guerra Mundial, com a invenção do computador, a área evoluiu no sentido da mecanização, automatização e informatização, incorporando complexos algoritmos matemáticos. Durante a Segunda Guerra, os ingleses ficaram conhecidos por seus esforços para a decifração de códigos. Todo esse trabalho criptográfico formou a base para a ciência da computação moderna. Na mesma época, o uso de códigos secretos era praticamente exclusivo de militares e diplomatas. Com o passar dos anos, a criptografia foi gradualmente difundida, estendendo-se, hoje, a fichas médicas em hospitais; a empresas, cuja intenção é preservar informações técnicas da sua laboração e dos seus equipamentos; às atividades bancárias; ao tratamento e circulação de dados científicos, bem como a

salvaguarda de informação em redes informáticas. Tudo isto faz com que a criptografia seja hoje uma disciplina científica, ativamente estudada por matemáticos, especialistas em estatística e cientistas ligados a sistemas informáticos.

No nosso cotidiano, a criptografia pode ser usada para várias coisas, como proteger documentos secretos, transmitir informações confidenciais pela Internet ou por uma rede local.

1.3.1.2 Objetivo da Criptografia

O objetivo da criptografia é fornecer técnicas que permitam a codificação e decodificação de dados, onde os mesmos podem ser transmitidos e armazenados sem que haja alterações ou a sua exposição à entidade não autorizada provendo assim uma comunicação segura, ou seja, garantir aos serviços confidencialidade, autenticidade, integridade:

a) Confidencialidade ou sigilo: apenas os usuários autorizados podem ter acesso à informação;

b) Integridade: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencionalmente, nem acidentalmente;

c) Autenticação do usuário: é o processo pelo qual o sistema verifica se a pessoa com quem se está comunicando é de fato a pessoa que alega ser;

d) Autenticação de remetente: é o processo pelo qual um usuário certifica-se que a mensagem recebida foi de fato enviada pelo remetente,

podendo, inclusive, provar perante um juiz, que o remetente enviou aquela mensagem;

e) Autenticação do destinatário: consiste em provar que a mensagem enviada foi corretamente recebida pelo destinatário;

f) Autenticação de atualidade: consiste em provar que a mensagem recebida é atual, e não mensagens antigas reenviadas.

O único método disponível para oferecer essas proteções, tanto durante o armazenamento quanto em trânsito, é a criptografia.

Cifrar, sendo o ato de transformar dados em alguma forma ilegível, tem o propósito de garantir a privacidade, mantendo a informação escondida de qualquer pessoa não autorizada, mesmo que esta consiga visualizar os dados criptografados.

Decifrar é o processo inverso, ou seja, transformar os dados criptografados na sua forma original, inteligível.

Para cifrarmos ou decifrarmos uma mensagem, necessitamos de informações confidenciais geralmente denominadas chaves ou senhas. Dependendo do método de criptografia empregado, a mesma chave pode ser utilizada tanto para criptografar como para decriptografar mensagens, enquanto outros mecanismos utilizam senhas diferentes.

1.3.1.3 Cifras de substituição

No método de cifra de substituição, cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, com a finalidade escondê-la. Exemplo: determina-se que, para cifrar um texto, as letras que formam cada

palavra desse texto devem ser deslocadas em n letras. Nesse caso, n vira uma chave para a técnica.

Um exemplo clássico de substituição é a cifra de César, que substitui as letras avançando três casas dentro do alfabeto.

ACESSO NEGADO ==>	**ENCRIPTAÇÃO ==>** Troca de cada letra pela próxima letra do alfabeto	**BDFTTP OFHBEP**

Figura 2 – Cifra de Substituição por Letras

ACESSO NEGADO ==>	**ENCRIPTAÇÃO ==>** Troca de cada letra pelo número de representação da letra dentro do alfabeto	**010305181815 140507010415**

Figura 3 – Cifra de Substituição por Números

1.3.1.4 Cifras de transposição ou cifra de permutação

No método de cifra de transposição, as letras não são ocultas, são apenas reordenadas. A cifra é chaveada por uma palavra ou chave que contém nenhuma letra repetida.

Um exemplo muito simples de transposição é embaralhar as letras do texto original. Com esse tipo de cifra, as letras originais do texto plano são preservadas, existe somente uma troca de posições.

ACESSO NEGADO ==>	**ENCRIPTAÇÃO ==>**	**SEOSCA DGOAEN**

Figura 4 – Cifra de Transposição

1.3.1.5 Cifras de uso único

Só existe um método de cifra de uso único que é a Cifra de Vernam ou One-time pad. Nesta cifra dois elementos que desejam se comunicar possuem cópias idênticas de uma seqüência de valores, os quais são usados como chave. Porém, o método exige que cada chave seja usada uma única vez e que o comprimento da chave seja maior, ou no mínimo igual ao comprimento da mensagem a ser cifrada.

1.3.1.6 Dois Princípios fundamentais da criptografia

Os atuais algoritmos de encriptação podem ser classificados em dois tipos, dependendo do esquema de chaveamento que utilizam: algoritmos de chave única (simétrica) e algoritmos de chave pública e privada (assimétrica).

1.3.1.6.1 Algoritmo de chave simétrica

Os algoritmos de chave simétrica utilizam a mesma chave tanto para codificar quanto para decodificar os dados. Para que esse método funcione, todas as pessoas envolvidas devem conhecer a chave, pois quando uma mensagem criptografada chega à caixa de entrada, ela só pode ser aberta por quem possui a chave.

Os algoritmos de chave simétrica ou única também são chamados de criptografia tradicional ou convencional.

Infelizmente, de modo genérico, esse método não funciona muito bem, exceto em aplicações limitadas, como as dos militares, onde o emissor e o receptor podem se preparar antecipadamente para trocar a chave. Isso acontece porque trocar chaves secretas com todos os destinatários é praticamente impossível.

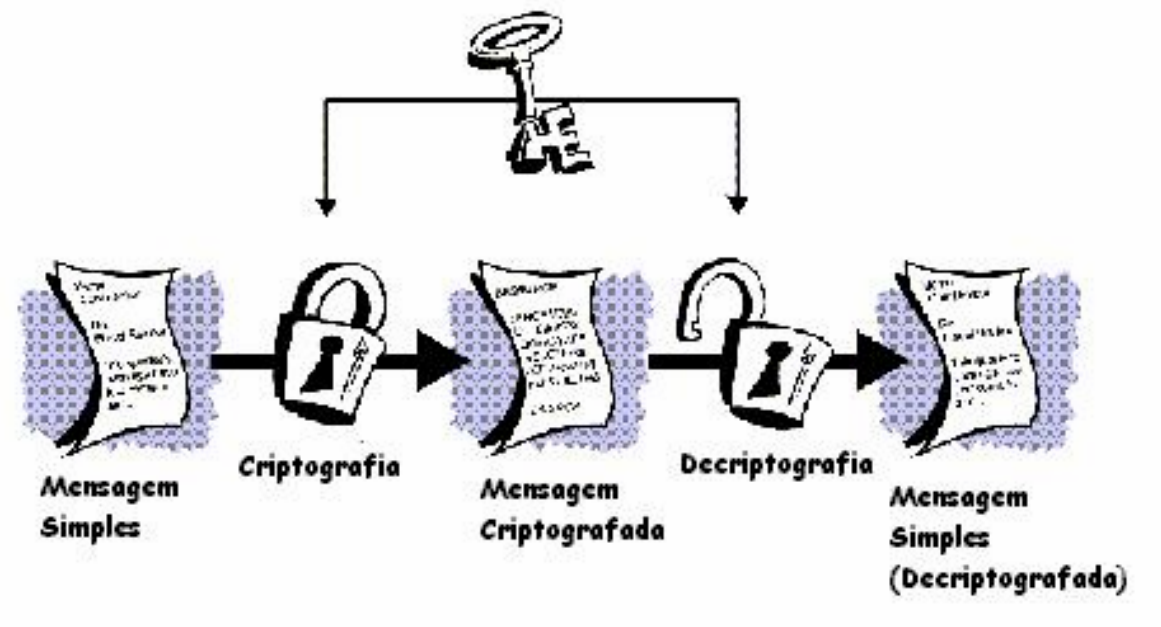

Figura 5 – Chave Simétrica

1.3.1.6.1.1 DES – Data Encryption Standart

O DES é um algoritmo de chave simétrica, ele é uma cifra de bloco, o que significa que atua sobre blocos de texto claro de determinado tamanho (64 bits) e retorna blocos de texto cifrado do mesmo tamanho. Portanto, o DES resulta numa permutação entre os 2^{64} (leia como "2 elevado a 64") arranjos possíveis de 64 bits, cada um deles podendo ser 0 ou 1. Cada bloco de 64 bits é dividido em dois

blocos de 32 bits, um sub-bloco esquerdo L e um sub-bloco direito R (esta divisão é usada apenas em certas operações).

O DES atua sobre blocos de 64 bits usando tamanhos de chave de 56 bits. Na realidade, as chaves são armazenadas com 64 bits, mas passando por um processo que "retira" 8 bits, são reduzidas para 56 bits. Estes 8 bits estão presentes nas chaves para garantir a integridade das mesmas, ou seja, o último bit de cada um dos 8 bytes da chave é um bit verificador, chamado de bit de paridade. Bits de paridade indicam quantos bits estão setados (têm valor 1) nos sete primeiros bits do byte. Quando este número for par (daí paridade), o último bit recebe o valor 1, caso contrário, recebe o valor 0. Por exemplo, o byte 00010010 possui 2 bits setados nos primeiros sete bits, por isso o byte é completado com 0; o byte 00110101 possui três bits setados nos primeiros sete bits, por isso o byte é completado com 1.

Foi descrita em um documento uma "máquina de um milhão de dólares" que seria capaz de violar chaves DES rapidamente. Como o projeto dessa máquina somente era possível para o orçamento de governos federais e de grandes corporações, várias pessoas e pequenas empresas começaram a endossar a utilização do DES triplo, no qual um bloco de dados é criptografado três vezes com diferentes chaves, sendo uma alternativa ao DES.

1.3.1.6.1.2 AES – Advanced Encryption Standart

O algoritmo Rijndael surgiu em 1998, criado por Vincent Rijmen e Joan Daemen, consistindo de uma cifra de blocos baseado em uma rede de permutação em blocos de 128, 160, 192, 224, e 256 bits e chaves de 128, 160, 192, 224, e 256 bits, sendo submetido ao National Institute of Standards and Technology com o objetivo de ser aceito como padrão do governo americano em sucessão ao DES. Em 2001 ao final do processo de seleção foi escolhido entre 12

algoritmos como padrão sob o nome de AES e somente com blocos de 128 bits e chaves de 128, 192 e 256 bits. O algoritmo é baseado em um trabalho anterior de Rijmen e Daemen chamado Square, que por sua vez é derivado do algoritmo Shark, também de ambos.

Os blocos consistem de matrizes de 4x4 bytes (blocos de Rijndael com mais de 128bits usam matrizes maiores). As chaves de cada iteração são calculadas em operações de campo finito (a maioria das operações dentro desse algoritmo é feita dessa forma).

Cada iteração (com excessão da última) consiste em quatro etapas, primeiro cada byte da matriz é substituído em uma S-Box, então cada linha da matriz é deslocada N posições, em seguida as colunas são substituidas numa operação de campo finito (com excessão da ultima iteração) e então é aplicada a chave da iteração a matriz resultante. Este processo é repitido 10, 12 e 14 vezes dependendo do tamanho da chave utilizada (128, 192, 256).

Não existem ataques efetivos conhecidos contra o AES, em 2002 um ataque teórico conhecido como “XLT attack” foi proposto por Nicolas Courtois porém estudos conseqüentes não reproduziram os termos de Courtois, ataques “XLT” são considerados especulativos e nunca foram reproduzidos, em Abril de 2005 Daniel J. Bernstein propôs um ataque chamado “cached timing”, que devido a impraticidade de reprodução (foram usandos 200 milhões de “chosen plaintexts”) foi considerado impraticavel. O governo americano considera AES como utilizável em proteção de dados considerados secretos.

1.3.1.6.2 Algoritmo de chave assimétrica

Os algoritmos de chave pública e privada ou assimétrica trabalham com duas chaves: uma pública que pode ser divulgada e outra secreta (privada) que apenas pessoas autorizadas têm ciência. As mensagens que são encriptadas com

uma das chaves do par podem ser decriptadas somente com a outra chave correspondente; logo, qualquer mensagem que for cifrada com a chave privada só pode ser decifrada com a chave pública e vice-versa. Conforme o nome insinua, geralmente a chave pública fica à disposição de todos. Já a chave privada, permanece secreta.

O algoritmo que permanece até os dias de hoje é o RSA, que é franqueado pela RSADSI (RSA Data Security Incorporated) nos Estados Unidos.

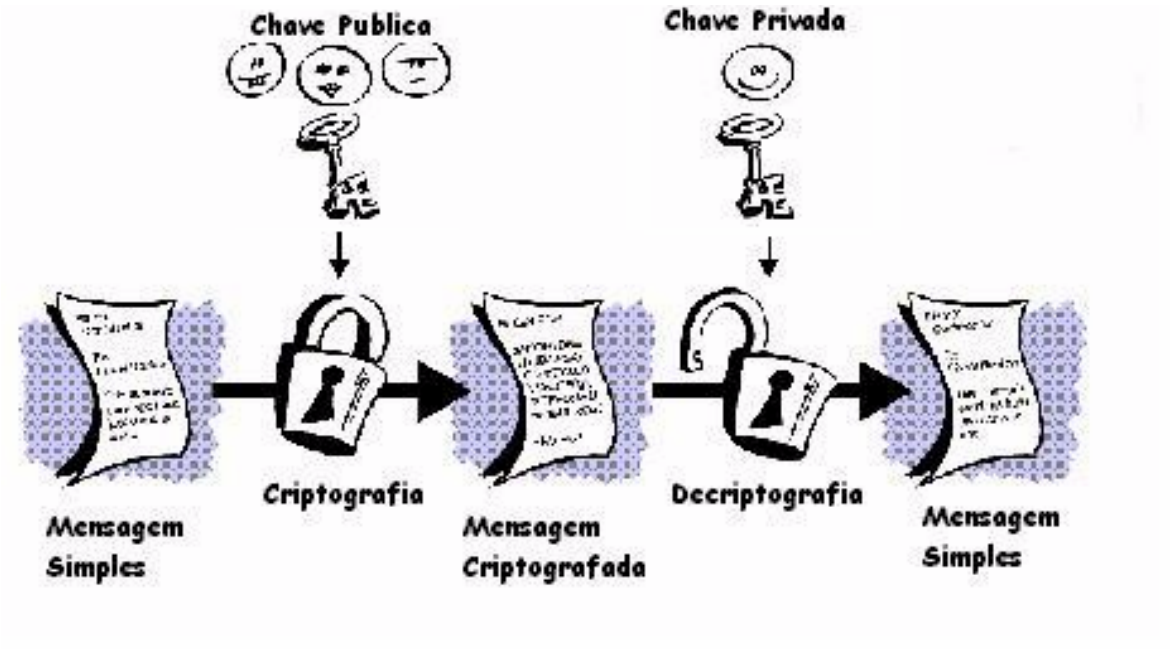

Figura 6 – Chave Assimétrica

1.3.1.6.2.1 RSA

Desenvolvido em 1978, o nome “RSA” deriva do nome de seus criadores: professores do MIT Ronald Rivest, Adi Shamir e o professor do USC Leonard Adleman.

Esse algoritmo faz o uso de expressões com exponenciais. O texto é cifrado em blocos de um valor binário menor que um número n, ou seja, 2 elevado ao tamanho do bloco tem que ser menor ou igual a n. Na prática tem-se que o tamanho do bloco é 2^k , sendo que $2^k < n <= 2^k + 1$.

1.3.1.6.2.2 Outros algoritmos de chave assimétrica

Existem ainda outros algoritmos, como o DSA (Digital Signature Algorithm), ElGamal e Diffie-Hellman.

O DAS (Digital Signature Algorithm) foi desenvolvido pelo NSA (National Security Agency) e adaptado pelo Federal Information Processing Standard (FIPS). Mesmo que a chave do DSA possa ser de qualquer tamanho, são permitidas dentro do FIPS apenas chaves entre 512 e 1024 bits. O DSA pode ser usado somente para assinatura digital, mesmo sendo possível utilizá-lo para outros tipos de criptografia. O DSA é também referenciado como DSS, como DEA é usualmente referenciado como DES.

Já o ElGamal é um algoritmo com base em exponenciação e aritmética modular. Ele é usado para criptografia e assinatura digital de forma similar ao algoritmo RSA. Chaves longas são geralmente consideradas mais seguras.

O Diffie-Hellman é um sistema para troca de chaves entre duas partes ativas. Não é um método atual de codificação e decoficação, e sim um método que cria e troca chaves privadas por um canal de comunicação público: as duas partes concordam com um valor numérico comum, e então estas partes criam as chaves. As transformações matemáticas das chaves também são trocadas. Assim, as partes podem realizar os cálculos da terceira parte da chave e não é fácil para um violador derivar as chaves através dos valores trocados.

Há várias versões deste protocolo relacionadas a diferentes números de partes e transformações diferentes. Deve ser dada muita atenção a escolha do

número e nos cálculos utilizados, pois, caso contrário, a troca de valores pode ser facilmente comprometida.

1.3.1.7 Criptoanálise

Criptoanálise é a ciência de quebrar uma mensagem cifrada. É diferente de decifrar, pois decifrar é obter a mensagem original quando se conhece o sistema e usando a chave também conhecida e quebrar é hackear o sistema e descobrir a chave. Sendo que essa quebra é feita através de um conjunto de métodos matemáticos.

Como não há um meio matemático de se provar que esse algoritmo é ou não é seguro, então ele é seguro até que se consiga decodificacá-lo. Essa segurança dura até que alguém consiga descobrir um método de decodificação. A grande dificuldade que um criptoanalista encontra ao tentar quebrar um algoritmo, está no número de chaves que esse utiliza.Quanto maior o número de chaves, maior a dificuldade de se conseguir obter sucesso na criptoanálise de um determinado sistema.

Um sistema que não se consegue quebrar é conhecido como sistema de segurança perfeita. Para se chegar perto de um sistema de segurança perfeito, é necessário que o número de chaves seja maior do que o tamanho do comprimento do texto legível, e que a probabilidade de ocorrência de cada chave seja o mesmo. Um algorítmo que satisfaz essas condições é o One-Time-Pad. Mas ele é inviável de ser implementado, pois ainda não se sabe construir um gerador de chaves realmente aleatória, que é necessário para que todas as chaves tenham a mesma probabilidade de ocorrer.

1.3.1.7.1 Criptoanálise de chave simétrica

A criptoanálise se tratando de algoritmos simétricos consiste em se tentar todo o espectro possivel de chaves que certo algoritmo suporta, por exemplo o algortimo DES usa chaves de 56 bits sendo 2^56 (72.057.594.037.927.936 chaves possiveis).

1.3.1.7.2 Criptoanálise de chave assimétrica

A criptoanálise com algoritmos assimétricos varia entre problemas como fatorização de números inteiros ou no cálculo de um logarítmo discreto, por exemplo, o algoritmo RSA que usa o produto de 2 números primos, sendo o brute force se fatorar esse produto em seus 2 termos originais, o número de chaves possíveis aumenta exponencialmente quanto maior (mais digitos) os números primos tiverem.

1.3.1.8 O que a criptografia não protege

A criptografia não impede um violador de:

- Deletar todos os seus dados;
- Danificar seu programa de criptografia, modificando-o para usar uma chave diferente da que você criou;
- Gravar todas chaves de criptografia em um arquivo para análise posterior;
- Encontrar uma forma relativamente fácil de decifrar as mensagens de acordo com o algoritmo que você esteja usando;

- Acessar seus arquivos antes de você criptografá-los ou após a decodificação.

Em virtude dos fatos mencionados, a criptografia deve fazer parte da sua estratégia de segurança, mas não deve ser a substituta de outras técnicas.

1.3.2 Assinatura Digital

A Assinatura Digital é um caso particular de um código de integridade de mensagens no qual o código pode ter sido gerado por apenas um participante esse mecanismo envolve dois procedimentos: assinatura de uma unidade de dados e verificação em uma unidade de dados. O primeiro procedimento baseia-se em informação privada (única e secreta), o segundo utiliza informação pública para reconhecer a assinatura.

O procedimento de assinatura envolve a codificação da unidade de dados completa ou a codificação de uma parte, por exemplo, de um campo de verificação, da unidade de dados utilizando informação privada do signatário.

A assinatura digital consiste no uso da chave privada para a escrita. Assim, o sentido das chaves acaba sendo outro, uma vez que todos que possuem a chave pública poderão visualizar essa mensagem, porém, apenas quem possui a chave privada conseguirá escrever. Portanto, a mensagem deixa de ser secreta para se tornar uma mensagem autêntica.

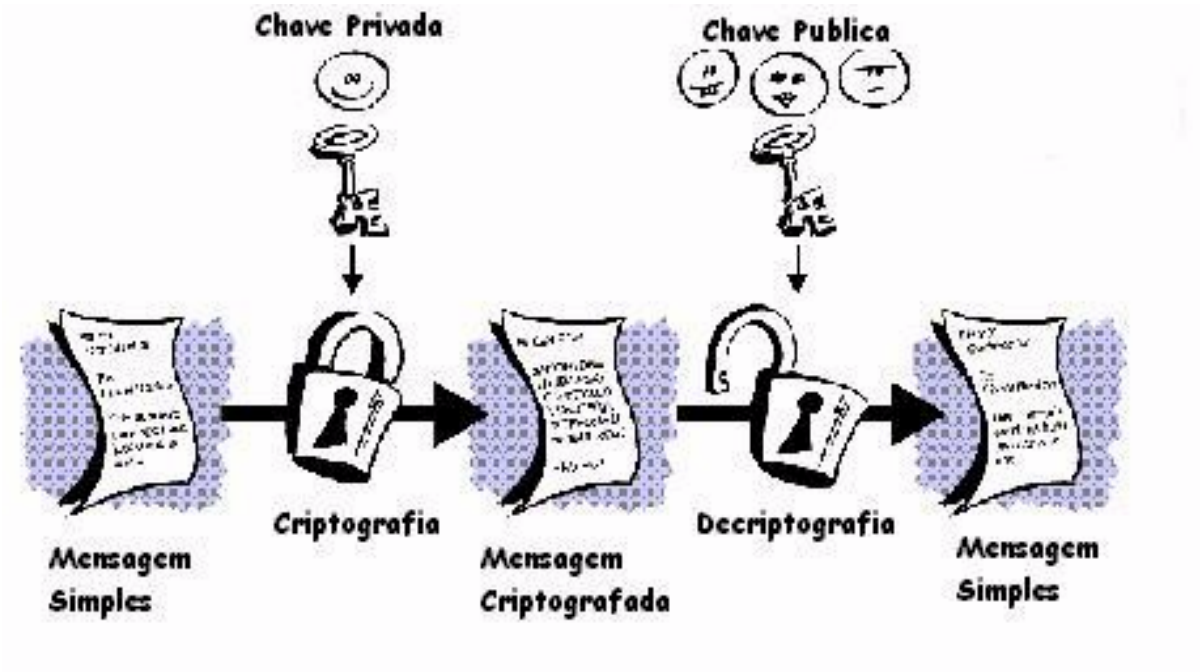

Figura 7 – Assinatura Digital

1.3.2.1 Sumários de mensagens (Message Digests)

Message digest é uma função que obtém uma mensagem como entrada e produz um código de tamanho fixo como saída. Por exemplo, uma função de message digest de 10 bytes: qualquer texto que fosse executado através dessa função produziria 10 bytes de saída, como “suy74hsdhh”. Qualquer mensagem deverá produzir de modo fácil um message digest eventual, específico.

Existem diversos algoritmos de hash (algoritmo usado para produzir um código hash para uma entrada e assegurar que esse código é único para cada entrada; código hash = sistema de codificação derivado dos códigos ASCII, onde os números de código para as primeiras três letras são somados, produzindo um

novo número usado como código hash), mas para que eles sejam úteis a esse propósito (considerados criptograficamente seguros), o algoritmo deverá exibir certas características, como as descritas abaixo:

Sem retorno - Precisa ser difícil ou impossível estabelecer qual mensagem produziu certa saída. Isso impedirá que a mensagem seja substituída por outra que tenha o mesmo message digest;

Aleatoriedade - A mensagem deve parecer aleatória para o impedimento da determinação da mensagem original;

Exclusividade - O message digest deve ser exclusivo, para que não existam duas mensagens com o mesmo message digest.

1.3.2.2 Ataque de aniversário

A idéia para esse ataque vem de uma técnica que freqüentemente os professores de matemática utilizam em probabilidade. A pergunta é: quantos alunos você deverá ter em uma sala de aula para que a probabilidade de haver duas pessoas fazendo aniversário no mesmo dia exceda1/2?

A teoria da probabilidade afirma que esse numero é 23.Se houver algum mapeamento entre as entradas e as saídas, com N entradas e K saídas possíveis, haverá n(n-1)/2 pares de entrada. Se n(n-1)/2>K a chance de haver pelo menos uma correspondência será boa. Portanto, fazendo a aproximação, é provável que haja uma correspondência para n>raiz de K. Isso significa que provavelmente um sumário de 64 bits possa ser rompido gerando-se 2 elevado a 32 mensagens e procurando-se duas mensagens com o mesmo sumário.

1.3.3 Gerenciamento de chaves públicas

O gerenciamento de chaves públicas é feito por meio de entidades conhecidas como autoridades certificadoras (CA's). São essas autoridades certificadoras que vão garantir, por exemplo, que uma chave pública pertence realmente a uma determinada empresa ou pessoa. São elas que formam a cadeia de confiança que dá segurança ao sistema. Fazem o papel desempenhado pelos notários no sistema de certificação tradicional. Da mesma forma que os cartórios tradicionais, são organizadas segundo critérios legais e obedecem, na prestação dos seus serviços de certificação, a toda uma política de procedimentos, padrões e formatos técnicos estabelecidos em regimes normativos. Obedecem, portanto, a um modelo técnico de certificação e estrutura normativa, que define quem pode emitir certificado para quem e em quais condições.

O conjunto dessas CA'S formam o PKI (Public Key Infrastructure), uma hierarquia confiável que regula as regras e procedimentos necessários para a autenticação da encriptação para usuários ou dispositivos.

1.3.3.1 Certificados

Um certificado consiste num documento digital com informações de identificação e uma chave pública. Geralmente, os certificados possuem um formato comum. Mas ainda não podemos estar certos de que o certificado é original e não é falso. É possível descobrir isso através de autoridades de certificação (CAs).

Uma autoridade de certificação assina certificados de chave pública digitalmente. Quando assina um certificado, a CA o valida. Entretanto, um problema continua: a distribuição da chave pública da CA. Também há diversos métodos para esse problema. Em um deles, se a CA for muito divulgada, como

ocorre com o serviço postal americano, ele poderá anunciar amplamente sua chave pública. Outra estratégia seria que a CA possuísse seu próprio certificado assinado por outra CA também conhecida pelo destinatário. Esse conceito de encadeamento de certificação pode ir mais além, com diversas CA's dispostas em uma hierarquia onde cada CA subordinada valida sua assinatura com a assinatura de uma CA mais elevada em tal hierarquia. Obviamente, as CA's de níveis mais elevados precisarão recorrer à estratégia de divulgação direta.

Com efeito, o certificado "Eu certifico que a chave publica neste documento pertence à entidade identifica neste documento, assinado X." Neste caso, X poderia ser qualquer um com uma chave publica.

1.3.3.2 X.509

A recomendação ITU-T X.509 define uma estrutura para certificados de chave pública, formando uma base para estabelecer ICP, e outra estrutura, para certificados de atributos, destinados à fundamentação de infra-estruturas de Gerenciamento de Privilégios (IGP, ou Privilege Management Infrastructures - PMI). As IGP complementam as ICP oferecendo a possibilidade de utilização de autenticação multi-nível, baseada em regras de acesso e nas funções de seus usuários, utilizando-se dos certificados de atributos. Elimina-se assim a necessidade de alteração e aumento da quantidade de informações nos certificados de chave pública (X.509, 2000). Essa recomendação fornece um meio para parceiros de comunicações recuperarem em informações mútuas de autenticação, de acordo com suas necessidades.

1.3.3.3 Infra-estruturas de chave pública

A tecnologia chamada de Infra-estrutura de Chaves Públicas (ICP - Public Key Infrastructure ou PKI) objetiva melhorar a segurança digital. Ela traz os meios para preservar a confidencialidade, autenticidade, integridade, não-repúdio e auditabilidade de documentos eletrônicos, transações, acesso a recursos, etc. Hoje o uso principal de uma ICP é autenticar o endereço de um serviço de página Web, conhecido como servidor Web Seguro, principalmente em transações comerciais e bancárias (home banking).

1.3.4 Segurança da Comunicação

Com o grande aumento de comunicações em redes de computadores e na Internet, é necessário que as trocas de informações ocorram em um ambiente seguro, onde há garantia da privacidade, autenticidade e integridade das informações transmitidas.

1.3.4.1 Ipsec

O IPSec é um protocolo padrão de camada 3, camada de rede, projetado pelo IETF que oferece transferência segura de informações fim a fim através de rede IP pública ou privada. Essencialmente, ele pega pacotes IP privados, realiza funções de segurança de dados como criptografia, autenticação e integridade, e então encapsula esses pacotes protegidos em outros pacotes IP para serem transmitidos. As funções de gerenciamento de chaves também fazem parte das funções do IPSec.

Tal como os protocolos de nível 2, o IPSec trabalha como uma solução para interligação de redes e conexões via linha discada. Ele foi projetado para suportar

múltiplos protocolos de criptografia possibilitando que cada usuário escolha o nível de segurança desejado.

Os requisitos de segurança podem ser divididos em 2 grupos, os quais são independentes entre si, podendo ser utilizado de forma conjunta ou separada, de acordo com a necessidade de cada usuário: Autenticação e Integridade, Confidencialidade.

Para implementar estas características, o IPSec é composto de 3 mecanismos adicionais:

AH - *Autentication Header*;

ESP - *Encapsulation Security Payload*;

ISAKMP - *Internet Security Association and Key Management Protocol*.

1.3.4.2 Firewalls

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre o computador e a Internet (ou entre a rede onde o computador está instalado e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.

O firewall é um mecanismo que atua como "defesa" de um computador ou de uma rede, controlando o acesso ao sistema por meio de regras e a filtragem de dados. A vantagem do uso de firewalls em redes, é que somente um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

Há mais de uma forma de funcionamento de um firewall, que varia de acordo com o sistema, aplicação ou do desenvolvedor do programa. No entanto, existem dois tipos básicos de conceitos de firewalls: o firewall que é baseado em

filtragem de pacotes e o firewall que é baseado em controle de aplicações. Ambos não devem ser comparados para se saber qual o melhor, uma vez que cada um trabalha para um determinado fim, fazendo que a comparação não seja aplicável.

1.3.4.2.1 Uma abrangência sobre Firewalls: Baseados em filtros, Baseados em controle de aplicações

O firewall baseado em filtros é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de firewall determina que endereços IP's e dados podem estabelecer comunicação e/ou transmitir/receber dados. Alguns sistemas ou serviços podem ser liberados completamente (por exemplo, o serviço de e-mail da rede), enquanto outros são bloqueados por padrão, por terem riscos elevados (como softwares de mensangens instantâneas, tal como o ICQ). O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficaz o suficiente.

Este tipo de firewall se restringe a trabalhar nas camadas TCP/IP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações endereço IP remoto, endereço IP do destinatário, além da porta TCP usada.

Quando devidamente configurado esse tipo de firewall permite que somente "computadores conhecidos" troquem determinadas informações entre si e tenham acesso a determinados recursos. Esse firewall também é capaz de analisar informações sobre a conexão e notar alterações suspeitas, além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior do que pode ou não ser acessado.

Já os firewalls de controle de aplicação (exemplos de aplicação: SMTP, FTP, HTTP, etc) são instalados geralmente em computadores servidores e são

conhecidos como proxy. Este tipo de firewall não permite comunicação direta entre a rede e a Internet. Tudo deve passar pelo firewall, que atua como um intermediador. O proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim uma solução é criar um "proxy genérico" através de uma configuração que informa que determinadas aplicações usarão certas portas. Essa tarefa só é bem realizada por adminstradores de rede ou profissionais de comunicação qualificados.

O firewall de aplicação permite um acompanhamento mais preciso do tráfego entre a rede e a Internet (ou entre a rede e outra rede). É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado a redes de porte médio ou grande e que sua configuração exige certa experiência no assunto.

1.3.4.3 Redes Privadas virtuais

Virtual Private Network (VPN) ou Rede Privada Virtual é a utilização de uma rede pública como a Internet em vez de linhas privativas para implementar redes corporativas. As VPNs são túneis de criptografia entre pontos autorizados, criados através da Internet ou outras redes públicas e/ou privadas para transferência de informações, de modo seguro, entre redes corporativas ou usuários remotos.

A segurança é a primeira e mais importante função da VPN. Uma vez que dados privados serão transmitidos pela Internet, que é um meio de transmissão inseguro, eles devem ser protegidos de forma a não permitir que sejam modificados ou interceptados.

Outro serviço oferecido pelas VPNs é a conexão entre corporações (Extranets) através da Internet, além de possibilitar conexões *dial-up* criptografadas que podem ser muito úteis para usuários móveis ou remotos, bem como filiais distantes de uma empresa.

1.3.4.4 Segurança sem fio

Em sistemas de rede sem fio a segurança é deixada de lado. Muitas vezes a rede corporativa cabeada, contando com diversos perímetros de segurança regidos por uma política de segurança eficaz, fica vulnerável a acessos indevidos e ataques quando a implementação inadequada de uma rede sem fio é realizada.

As soluções disponíveis no mercado de redes wireless utilizam em sua maioria o padrão WEP para garantia de sigilo das informações. O WEP ou Wired Equivalent Privacy, que utiliza a implementação do protocolo RC4 para realizar criptografia, possui falhas graves. É possível ter acesso à chave utilizada na criptografia provocando o surgimento de diversas ferramentas para quebra do WEP na Internet.

O WEP, que está disponível na maior parte dos equipamentos wireless, não é uma garantia para a segurança dos dados transmitidos.

Além do WEP, as demais características de segurança disponíveis em Access Points e interfaces de rede, controle de acesso por endereços MAC e comunidades SNMP são alguns exemplos de funcionalidades que são burladas com facilidade podem ser burladas.

Para se obter um nível de segurança satisfatório é preciso implementar controles externos aos equipamentos. Configuração adequada, criptografia, autenticação forte e monitoração dos acessos da rede sem fio são imprescindíveis. Caso contrário, a rede wireless estará com baixa segurança.

1.3.5 Autenticação

O processo de autenticação é caracterizado pela confirmação da identificação de um parceiro em uma comunicação. Em outras palavras, o processo de autenticação visa combater um elemento impostor. É complexa a tarefa de autenticação, pois em um determinado ambiente de rede um intruso ativo pode se passar por um parceiro.

As abordagens mais utilizadas de autenticação são aquelas baseadas em chaves secretas compartilhadas, por centros de distribuição de chaves, pelo uso do protocolo Kerberos e por intermédio da criptografia com chave pública.

Um conceito, que às vezes é confundido com a autenticação, é o princípio da autorização. A autorização, diferente da autenticação, é um processo no qual é solicitado ao usuário uma ou mais senhas que comprovem que o mesmo está autorizado a solicitar determinados serviços (ou acesso).

1.3.6 Controle de Acesso

Os mecanismos de controle de acesso são usados para garantir que o acesso a um recurso é limitado aos usuários devidamente autorizados. As técnicas utilizadas incluem a autorização de listas ou matrizes de controles de acesso, que associam recursos a usuários autorizados, ou passwords, apabilities, que associam recursos, cuja posse determina os direitos de acesso do usuário que as possui.

1.3.7 Integridade de Dados

Integridade de dados é uma garantia oferecida ao usuário de que os dados originais não foram alterados, nem intencionalmente, nem acidentalmente.

Os mecanismos de controle de integridade atuam em dois níveis: controle da integridade de unidade de dados isolado e controle da integridade de uma conexão, isto é, das unidades de dados e da seqüência de unidades de dados transmitidas no contexto da conexão.

Para garantir a integridade dos dados, podem ser usadas as técnicas de detecção de modificações, normalmente associadas com a detecção de erros em bits, em blocos, ou erros de seqüência introduzidos por enlaces e redes de comunicação. Entretanto, se os cabeçalhos e fechos carregando as informações de controle não forem protegidas contra modificações, um intruso, que conheça as técnicas, pode contornar a verificação. Portanto, para garantir a integridade é necessário manter confidenciais e íntegras as informações de controle usadas na detecção de modificações. Para controlar modificações na seqüência de unidades de dados transmitidas em uma conexão, devem-se usar técnicas que garantam a integridade das unidades de dados (garantindo que as informações de controle não sejam corrompidas) em conjunto com informações de controle de seqüência. Esses cuidados, embora não evitem a modificação da cadeia de unidades de dados, garantem a detecção e notificação dos ataques.

1.3.8 Segurança Física e de Pessoal e Hardware/ Software de Confiança

A segurança de qualquer sistema depende, em última instância da segurança física dos seus recursos e do grau de confiança do pessoal que opera o sistema. Ou seja, não adianta utilizar mecanismos sofisticados de segurança se os intrusos puderem acessar fisicamente os recursos do sistema. Por exemplo, não adianta usar um esquema sofisticado de autenticação para impedir acessos remotos aos arquivos em um disco, se o intruso puder ter acesso físico a maquina e roubar seu disco rígido.

Algumas das entidades que fazem parte de um sistema devem fornecer garantias que funcionam corretamente, para que se possa confiar nos mecanismos de segurança que implementam a política de segurança do sistema.

Para garantir o funcionamento correto deve-se exigir: a aplicação de métodos formais de prova, verificação e validação; a detecção e o registro das tentativas de ataque identificadas; e, adicionalmente, que a entidade tenha sido construída por pessoal de confiança em um ambiente seguro. Precauções também são necessárias para garantir que a entidade não seja acidentalmente ou deliberadamente adulterada com o intuito de comprometer seus mecanismos de segurança durante seu ciclo operacional. Nesse aspecto, merecem especial atenção às manutenções ou atualizações das entidades.

2. CRITÉRIOS PARA AVALIAÇÃO DA SEGURANÇA DE SISTEMAS DE COMPUTAÇÃO – O LIVRO LARANJA DO DoD

O livro “Trusted Computer System Evaluation Criteria” [DoD 85], ou simplesmente “O Livro Laranja”, é um documento formalizado que contém a proposta do Departamento de Defesa Americana para avaliar a segurança de sistemas de computação.

O Livro Laranja tem por objetivos fornecer aos fabricantes um padrão definindo os aspectos de segurança que deveriam ser incorporados aos seus produtos, prover aos órgãos membros do DoD uma métrica de segurança para sistemas computacionais, fornecer uma base para a definição de requisitos de segurança nas especificações de aquisição de equipamentos.

Os critérios para avaliação de segurança de sistemas de computação definidos nesse documento enquadram os sistemas em quatro divisões de proteção: D, C, B e A.

O Livro Laranja deixou de ser uma referência com o crescimento da Internet. Atualmente, não existe um mecanismo ou órgão capaz de rotular níveis de segurança para um sistema ou empresa. Ferramentas, consultorias, testes e melhorias constantes são formas de “garantir” a segurança do sistema/empresa.

2.1 Divisão D – Proteção Mínima

A divisão de proteção D engloba os sistemas que oferecem proteção mínima. Essa divisão só contém uma classe, a classe D. São classificados na classe de proteção D os sistemas que foram avaliados, mas não cumpriram os requisitos exigidos nas classes de proteção mais altas.

2.2 Divisão C – Proteção Arbitrária

Os sistemas enquadrados nas classes de divisão C são os que fornecem proteção arbitrária, isto é, fornecem mecanismos que permitem definir que indivíduos, ou grupos de indivíduos, devem ter acesso a quais recursos, e com que permissões de acesso. Os sistemas nessa divisão devem possuir mecanismos para registrar eventos relevantes à segurança do sistema, os quais serão usados no suporte de auditorias que permitam contabilizar as ações realizadas por um indivíduo. Na divisão C, os sistemas são enquadrados em duas classes: classe C1 e C2.

2.2.1 Classe C1 – Proteção com segurança arbitrária

Os sistemas devem incorporar alguma forma de controle.

2.2.2 Classe C2 - Proteção com Controle de Acesso

Igual ao C1 só que os usuários devem ser individualmente contabilizáveis pelas suas ações.

2.3 Divisão B – Proteção Obrigatória

O principal requisito dessa divisão é a preservação da integridade dos rótulos de sensibilidade e sua utilização para colocar em vigor o conjunto de regras de controle de acesso que define uma política de segurança obrigatória.

Essa divisão é dividida em classes B1, B2 e B3.

2.3.1 Casse B1 – Proteção com segurança baseada em rótulos

Igual ao C2 só que inclui declaração informal da política de segurança, dos rótulos de dados e do controle de acesso obrigatório aos serviços nomeados e objetos. Todo recurso do sistema recebe um rótulo. Todo usuário recebe um nível de credenciamento que define os rótulos sobre os quais tem direito de acesso.

2.3.2 Classe B2 – Proteção estruturada

Sistema de segurança baseado em um modelo de política de segurança formal claramente definido e documentado.

2.3.3 Classe B3 – Domínios de segurança

Implementa um monitor de referência que controla todo acesso dos usuários aos recursos do sistema. Mecanismos de auditoria são expandidos. Devem existir procedimentos de recuperação do sistema.

2.4 Divisão A – Proteção Comprovada

A divisão A é caracterizada pelo uso de métodos de verificação de segurança formais que garantam que os controles obrigatórios e arbitrários, empregados no sistema, efetivamente protejam as informações classificadas nele armazenadas e processadas.

Essa divisão é dividida em classes A1, A2 e outras.

2.4.1 Classe A1 – Projeto comprovado

Equivalente à classe B3, o que a diferencia são as técnicas de especificação e verificação formal usadas na fase de projeto e o alto grau de garantia de implementação correta do sistema de segurança.

2.4.2 Classe A2 e outras

Ainda não estão formalmente definidos.

3. SEGURANÇA NA INTERNET TCP/IP

O termo arquitetura de segurança de uma rede pode ser empregado com conotações diferentes. No caso da Internet, espera-se que a arquitetura de segurança forneça um conjunto de orientações voltado para projetistas de redes e desenvolvedores de produtos, e não apenas para projetistas de protocolos. Isso sugere que a arquitetura de segurança da Internet englobe não apenas definições de conceitos, mas inclua adicionalmente orientações mais especificas sobre como e onde implementar os serviços de segurança na pilha de protocolos da Internet.

3.1 Definição dos Serviços, Mecanismos e Ameaças

A arquitetura de segurança da Internet adota a definição de serviços, mecanismos e ameaças do padrão ISO 7498-2.

Os serviços de segurança são uma classe de proteções aplicadas a sistemas de comunicação. Alguns destes serviços são: Correio Eletrônico, Segurança na WEB, Serviço de Diretório, Gerenciamento de Redes, Terminais Virtuais e Transferência de Arquivos, Servidores de Arquivos e Roteamento.

Os mecanismos são os meios para promover e suportar os serviços de segurança. Alguns dos pricipios utilizados para escolha de mecanismos são:

- Os mecanismos de segurança devem ser escaláveis, tendo capacidade e potencial para acompanhar o crescimento da Internet.
- Os mecanismos devem ter sua segurança apoiada na tecnologia que os suporta.
- Os mecanismos de segurança não devem restringir a topologia da rede.
- Mecanismos de segurança que não sejam sujeitos às restrições de controle de exportação ou patentes devem ter preferência.

- É sabido que muitos mecanismos de segurança necessitam de uma infraestrutura de apoio, o gerenciamento dessa estrutura pode ser tão ou mais complexo que a implementação do mecanismo. Assim, deve-se dar preferência a tecnologias de segurança que possam compartilhar uma infraestrutura de segurança comum.
- algoritmos de criptografia selecionados para padronização na Internet devem ser amplamente conhecidos, devendo ser dada preferência aos que tiverem sido exaustivamente testados.

3.2 Correio Eletrônico

Os serviços de segurança necessários para o correio eletrônico na Internet incluem confidencialidade, e integridade em transmissões sem conexão, autenticação da origem das mensagens, e impedimento de rejeição pelo destinatário ou remetente.

3.2.1 PGP – Pretty Good Privacy

O PGP é um programa de criptografia de chave pública altamente seguro, originalmente escrito por Philip Zimmermann. Nos últimos anos o PGP conquistou milhares de entusiastas em todo o mundo e tornou-se de fato um padrão para a criptografia de correio eletrônico (e-mail) na Internet.

3.2.2 PEM – Privacy Enhanced Mail

É um dos padrões da Internet para o envio de mensagens de correio eletrônico criptografadas. Foi criada uma implementação utilizando a lógica do DES chamada de Riodan's Internet Privacy-Enhanced Mail (RIPEM) criada pelo

americano Mike Riordan. Possui o requisito de segurança de autenticação dos remetentes.

3.2.3 S/MIME

O empreendimento da IETF relacionado à segurança de correio eletrônico, foi denominado S/MIME (SECURE/MIME), e é descrito nas RFCs 2632 a 2643. Ele oferece autenticação, integridade de dados, sigilo e não repudio. Ele também é bastante flexível, admitindo uma variedade de algoritmos criptografados. Considerando-se o nome, não surpreende que o S/MIME se integre bem ao MIME, permitindo que todos os tipos de mensagens sejam protegidos. Foi definida uma grande variedade de novos cabeçalhos MIME, por exemplo, para conter assinaturas digitais.

O S/MIME não tem uma estrutura rígida de certificados começando em uma única raiz. Em vez disso, os usuários podem ter várias âncoras de confiança. Desde que a origem de um certificado possa ser acompanhada até alguma âncora de confiança em que o usuário acredite, ele é considerado válido.

3.3 Segurança na WEB

WEB é o lugar em que se encontra a maioria dos intrusos, espionando e fazendo seu trabalho sujo. Por isso é que a WEB precisa de um bom esquema de segurança.

3.3.1 Ameaças e ataques

As ameaças à WEB são constantes, existe um grande número de hacker's espalhados pelo mundo que invadem os sites da WEB, ou até mesmo os sites são

derrubados por ataques de negação de serviço,nos quais o hacker inunda o site sem trafego, tornando-o incapaz de responder a consultas legitimas.

Um exemplo de um ataque na WEB é quando um usuário A quer visitar o Web site do usuário B. A digita o URL de B em seu navegador e, em alguns segundos surge uma pagina Web. Um usuário C poderia interceptar todos os pacotes enviados por A e examina-los. Quando capturar uma solicitação GET de http endereçada ao site de B, C pode ir ate o site de B para obter a pagina, modifica-la como desejar e retornar para o usuário A a pagina falsa. A nem ficaria sabendo. Uma desvantagem desse clássico ataque é que C tem que estar em uma posição conveniente para interceptar o tráfego enviado por A e forjar seu trafego de entrada. Na pratica, C tem que grampear o backbone de fibra óptica. Embora a espionagem ativa seja possível ela exige um pouco de trabalho.

3.3.2 SSL – Secure Sockets Layer

Quando a Web chegou ao publico, ela foi usada no inicio apenas para distribuir paginas estáticas. Porem em pouco tempo, algumas empresas tiveram a idéia de usa-las para transações financeiras, compras,etc. Essas aplicações criaram uma demanda por conexões seguras. Em 1995 foi introduzido um protocolo de comunicação que implementa um duto seguro para comunicação de aplicações na Internet, de forma transparente e independente da plataforma o Secure Socket Layer (SSL), que atualmente está na versão 3.

SSL constrói uma conexão segura entre dois soquetes, incluindo: negociação de parâmetros entre cliente e servidor, autenticação mutua de cliente e servidor, comunicação secreta e proteção da integridade dos dados.

3.3.3 Segurança de código móvel

No início, quando as páginas eram apenas arquivos estáticos de HTML, elas não continham código executável. Agora, as paginas freqüentemente contem pequenos programas. Baixar e executar esse código móvel é sem duvida um grande risco de segurança, por essa razão foram criados vários métodos para minimiza-los. Exemplos de código móvel:

- Miniaplicativos Java:

Quando um miniaplicativo tenta usar um recurso do sistema, sua chamada é repassada a um monitor de segurança para aprovação. O monitor examina a chamada levando em conta a política de segurança local e depois toma decisão de permiti-la ou rejeita-la.

- ActiveX:

Os controladores ActiveX são programas binários do Pentium que podem ser incorporados às páginas Web. Quando um deles é encontrado, é realizada uma verificação para saber se ele deve ser executado e, se passar no teste o programa é executado.

- Vírus:

É outra forma de código móvel, diferentes dos outros, os vírus sempre chegam sem ser convidados. Os vírus são desenvolvidos para reproduzir, quando chegam pela Web em um anexo de e-mail, em geral começa infectando programas executáveis no disco. Quando um desses programas é executado, o controle é transferido para o vírus infectando toda a maquina. Os anti-vírus são usados para impedir que os vírus infectam a máquina.

3.4 Serviço de Diretório

Existem dois modelos de serviços de diretórios que podem ser usados na Internet, o Domain Name Server (DNS) e o X.500. No caso do X.500, os requisitos de segurança são bem definidos, ele incorpora em seu protocolo mecanismos de segurança para implementar esses serviços. Por outro lado o DNS não possui mecanismos de segurança.

Os requisitos de segurança do X.500 são: autenticação da origem dos dados, controle de integridade em transmissões sem conexão para proteger as consultas e respostas ao diretório, controle de acesso para permitir o armazenamento dos dados no diretório com a confiança de que esses dados só serão modificados por usuários autorizados, ou administradores, e que dados sensíveis não serão revelados para usuários não autorizados.

Na ausência de mecanismos de segurança específicos no DNS, mecanismos de níveis inferiores devem ser empregados para fornecer: autenticação, integridade e controle de acesso.

3.5 Gerenciamento de Redes

O protocolo de gerenciamento de redes na Internet é o SNMP, o qual sofreu alguns melhoramentos provendo suporte a um conjunto de requisitos de segurança. Os serviços de segurança que passaram a ser fornecidos foram: confidencialidade e integridade (com proteção contra reenvio postergado – replay) na transmissão de datagramas, autenticação da origem de dados e controle de acesso baseado na identidade. Sendo que esses serviços são empregados na proteção contra violações do intercâmbio de informações de gerenciamento, e para proteger os objetos gerenciados contra tentativas de manipulação não autorizada.

Todos esses serviços foram implementados no SNMP no nível de aplicação, incluindo um esquema de distribuição de chaves simétricas.

3.6 Terminais Virtuais e Transferência de Arquivos

A aplicação terminal virtual é fornecida pelo protocolo Telnet e as transferências de arquivos pelo protocolo FTP. Para os dois tipos de protocolos, os requisitos de segurança devem incluir integridade e confidencialidade em conexões, autenticação de parceiros e controle de acesso baseado em identidade. Esses serviços podem ser implementados por mecanismos nos próprios protocolos de aplicação, ou através do uso de mecanismos de camadas inferiores.

Um aspecto deve ser considerado na escolha do local onde serão implementados os mecanismos, no nível de aplicação ou níveis inferiores. Implementar nos níveis inferiores implica em modificações nos códigos dos sistemas operacionais, osnde são implementados os protocolos do nível de rede e de transporte. Caso os mecanismos sejam implementados nas aplicações, essas modificações não serão necessárias.

3.7 Servidores de Arquivos

Servidores de arquivos são implementados por sistemas com o NFS da Sun e o Andrew File System, e distinguem-se dos protocolos de transferência de arquivos por fornecer um conjunto de serviços mais rico, que inclui o acesso randômico a partes de um arquivo. Os requisitos de segurança nesses sistemas incluem: a integridade e a confidencialidade no intercambio de datagramas, a autenticação de parceiros, e o controle de acesso baseado em identidade. Os serviços de integridade e confidencialidade podem ser fornecidos por protocolos do nível de rede e de transporte. Porém, a granularidade necessária para o

controle de acesso a nível de arquivo ou diretório é mais fina do que a que pode ser fornecida nos níveis de rede e de transporte.

3.8 Roteamento

O roteamento na Internet é realizado por protocolos como o BGP, EGP e OSPF. Todos esses tipos de protocolos possuem requisitos de segurança semelhantes: autenticação de parceiros e integridade no intercâmbio de datagramas carregando informações de roteamento.

A maior parte dos serviços pode ser fornecida com a utilização de mecanismos genéricos da camada de rede, ou podem ser construídos especificamente para os protocolos de roteamento. Nesse caso, a granularidade da autenticação e do controle de acesso é claramente atingida pelas informações de identificação fornecidas nessa camada.

A variedade de protocolos de roteamento mostra os benefícios de se utilizar mecanismos de segurança comuns fornecidos na camada de rede.

O serviço de cofidencialidade do fluxo de tráfego ponto a ponto pode ser fornecido pelo roteador, utilizando mecanismos do nível físico.

4. CONCLUSÃO

Em virtude dos fatos mencionados observa-se que existem vários métodos de segurança para serem implementados em redes de computadores, ou para serem utilizados na Internet. Esses métodos estão evoluindo cada dia mais, tornando-se cada dia mais difícil de serem “quebrados”. Mas hoje em dia ainda não existi um método infalível, assim nenhuma rede é totalmente segura. Para se chegar o mais perto possível de uma rede segura é aconselhado usar mais de uma tecnologia de segurança ao mesmo tempo, assim se uma delas for burlada terão outras para proteger a rede.

5. BIBLIOGRAFIA

1 SITES

Criptografia, Síntese da História. Janeiro 2004. Revista da Armada Nº 371, Marinha. Disponível em: <http://www.marinha.pt/extra/revista/ra_jan2004/pag_10.html>.

Faculdade de Tecnologia Americana - Prof José Adriano. Criptografia, Disponível em: <http://web.1asphost.com/fandangos/>.

Instituto Tecnológico da Aeronáutica - RSA, Disponível em: <http://www.ime.usp.br/~capaixao/dissertacao.html>.

Instituto Tecnológico da Aeronáutica – Valdemar W. Setzer e Fábio H. Carvalheiro – Algoritmos e sua análise: uma introdução didática, Disponível em: <http://www.ime.usp.br/~vwsetzer/alg/algoritmos.html>.

Universidade de Campinas, Disponível em: <http://www.dca.fee.unicamp.br/courses/IA368F/1s1998/Monografias/rossano/rosimage1.gif&imgrefurl>.

Universidade do Algarve, Ricardo Ferraz de Oliveira - Algoritmos, Disponível em: <http://w3.ualg.pt/~hshah/algoritmos/>.

Universidade Federal de Santa Catarina - Chave Assimétrica, Disponível em: <http://www.inf.ufsc.br/~rflrueda/SegurançaEmComputacao/TrabalhoFinal/chaveAssimetrica.html>.

2 OUTROS SITES

http:// www.penta.ufrgs.br

http:// www.rnp.br

http://www.cpt.com.br/2005/nave.php?op=ajuda&int=glossario

http://www.dca.fee.unicamp.br/pgp/pgp.shtml

http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/acronimos.html

http://www.gta.ufrj.br/quaresma/atividades/2.htm

http://www.ibdi.org.br/index.php?secao=&id_noticia=537&acao=lendo

http://www.infowester.com/criptografia.php

http://www.rnp.br/_arquivo/gt/2003/icp_edu.pdf

http://www.rsasecurity.com/rsalabs/node.asp?id=2225

http://www.security.unicamp.br/docs/conceitos/o3.html

3 OUTRAS FONTES DE PESQUISA

Luiz Fernando Gomes Soares, Guido Lemos, Sérgio Colcher – Redes de Computadores – 2ª edição, Rio de Janeiro, 1998 – Editora Campus.