Segurança de sistemas
Ênfase em rede de computadores

Disciplina: Redes de Computadores I
Professor:
Aluno:
Período:

Índice:

Prefácio

Neste trabalho irei falar sobre segurança de sistemas, em específico, sistemas de computadores ligados em rede ou a Internet. Com o advento das redes de computadores e as conexões “caseiras” de banda larga, ADSL, ISDN, Rádio, Cabo, HomePNA, etc, temos cada vez mais computadores ligados em redes e à Internet executando transações importantes, desde uma simples consulta de saldo bancário de um usuário até transações entre bancos envolvendo bilhões de dólares.

É neste cenário que este trabalho se desenvolverá, cobrindo desde sistemas domésticos e suas diversas falhas de segurança até sistemas de grande porte, passando algumas noções de hardware e software a fim de evitar ser pego de surpresa por uma invasão em seu sistema. Irei comentar também sobre segurança físicas dos aparelhos bem com políticas de segurança e de senha.

Falarei de alguns dos muitos softwares utilizados para tentativas de invasões e um pouco sobre vírus e suas “aplicações”. Comentarei sobre as leis atuais que enquadram as invasões à sistemas de informação, bem como o que se pode ser feito para um futuro e o que pode ser feito no caso de uma detecção de invasão.

Por fim falarei de algumas técnicas que minimizam as falhas de segurança em computadores tais como criptografia, PKI e VPN. Darei noções também de sistemas de detecção de intrusões e como utiliza-los.

Sendo assim ao final do trabalho terei tentado passar algumas noções básicas de segurança de sistemas e algumas soluções, contudo isto é um assunto extremamente complexo e extenso onde a cada dia ou até mesmo a cada hora surgem novas variantes.

1 - Introdução

1.1 - História da Segurança

Para falar de segurança de dados e informações temos que começar com uma frase muito estranha para um profissional de TI. “Não existem sistemas 100% seguros!!! Isto é um fato.” Pode parecer absurdo uma frase dessa em um trabalho sobre Segurança de dados, mas isso é um verdade, mesmo com a tecnologia atual os profissionais de TI não podem garantir que um sistema ou uma rede de sistemas é 100% segura. O que podemos sim avaliar é o grau de segurança de um sistema.

Em sistemas bancários temos um nível de segurança, já para sistemas domésticos temos outro, com certeza de muito menor eficiência, sem falar dos sistemas militares de onde são controlados os mísseis nucleares, informações de espionagem, até mesmo a rota de aeronaves militares e espaçonaves.

É sabido que o mundo caminha para uma “informatização” total, onde todo tipo de informação estará armazenado em sistemas digital. Quando essa “onda” de evolução tecnológica inicio-se, a uns 50 anos atrás, a necessidade de uma atuação na área da segurança dos dados contidos nos sistemas não era levada muito a sério. Inicialmente os sistemas eram puramente de processamento, onde entravam dados e saíam dados processados não havia nenhum tipo de retenção permanente dos dados.

Com a evolução da tecnologia de informação foram sendo criados novos modelos de processamento, de armazenamento, de transmissão, de integração, enfim tudo o que hoje em dia nos é mais natural, o computador. Com isso informações e dados começaram a trafegar entre sistemas sendo processados e armazenados, bem agora temos “algo dentro” dos computadores, sendo assim, temos que nos certificar que estas informações fiquem disponíveis somente para que é de direito.

Hoje em dia vemos bilhões de dólares trafegando entre paises e bancos, mas não da forma antiga, em moeda corrente, mas sim em bits (!), dinheiro “virtual”, hoje temos milhões em um banco em ilha na Ásia e daqui a quinze minutos estes milhões estão em um banco qualquer da Europa. Isso pode parecer meio normal hoje em dia, além disso, temos nossos dados cadastrais, identidade, CPF, endereços, telefones até mesmo nossos hábitos armazenados em sistemas computadorizados.

Sendo assim foi-se necessário à criação de uma área da tecnologia de informação que pressuponho ser a única que nunca se extinguirá, a Tecnologia de Segurança da Informação. Hoje vemos profissionais especializados em tal área sendo contratados por bancos, administradoras de cartões, companhias telefônicas, multinacionais até mesmo no setor público. Com esse avanço brutal da Tecnologia de Informação, mais e mais dados foram sendo colocados em sistemas, e tais dados têm de ser protegidos.

Assim chegamos nos dias atuais onde todo tipo de informação trafega entre sistemas auxiliados pelo crescimento da Internet, que teve a incumbência de interligar os diversos sistemas espalhados pelo Mundo. Chegamos a criar um novo tipo de “bandido”, o hacker e suas derivações, tais “profissionais” tem somente o intuito de invadir

sistemas, quebrar senhas, destruir informações somente pelo prazer pessoal ou o sadismo de ver a desordem e o caos.

É neste contexto que se desenvolve este trabalho onde falarei sobre os diversos tipos de Tecnologia de Segurança da Informação, desde sistemas domésticos protegidos por softwares até grandes sistemas bancários e militares protegidos por hardware altamente sofisticados, passando por um ponto muito negligenciado por profissionais desta área, a segurança física dos sistemas, não somente a segurança lógica dos dados e informações.

1.2 - O ambiente doméstico

Como já foi descrito anteriormente, com o avanço das tecnologias de banda larga cada vez mais, computador doméstico, têm ficado conectados a Internet por longos períodos de tempo. Com isso já se faz a necessidade de um mínimo de segurança a estes sistemas seja para não serem invadidos através da grande rede ou até mesmo um ataque físico. A este ataque físico denoto por uma pessoa “não autorizada” ligar seu micro a acessar seus arquivos. Para resolver este problema os novos sistemas operacionais têm implementado uma política de senhas, onde não se acessa um sistema se ser um usuário cadastrado.

Já no setor de redes temos o problema que com as conecções de banda larga os micros domésticos passaram a ter IP válidos na Internet e isto é um prato cheio para os ataques vindos pela rede. Além disso, temos o crescente número de vírus de computador e uma enorme velocidade de produção destas pragas virtuais. Neste contexto faz-se uma campanha de alertar o usuário doméstico da necessidade de utilizar algum sistema de bloqueio ao micro. Este pode ser implementado via software ou hardware, os quais falarmos mais adiante.

1.3 - O ambiente corporativo

Se no ambiente doméstico a necessidade de preocupação com segurança digital no mundo corporativo ele é imprescindível. Adotaremos de agora em diante que o ambiente corporativo é descrito por uma rede local de uma empresa, conectado à Internet, através de um link.

Todas as descrições de problemas feitas anteriormente, para o caso doméstico valem em dobro para o ambiente corporativo, visto que neste envolvemos empresas com negócios e valores. Tomemos por base um banco, um caso extremo, mas ótimo para ser dar uma visão geral do problema. Em uma entidade financeira deste porte existem milhares até dezenas de milhares de equipamentos ligados em rede, e conectados a Internet pr meio de algum link. Não falo somente de microcomputadores (PC) instalados em agências, mas também de grandes servidores, terminais de clientes, caixas automáticos, enfim uma enormidade de equipamentos.

Em um ambiente deste temos um potencial problema com relação à segurança de dados e informações. Em um banco circulam por dia milhões de reais, dinheiro este em sua maior parte “virtual”, distribuído em transações financeiras, transferências, de-

pósitos, cheques e cartões, todos se utilizando sistemas de informação distribuídos. Imagine agora se um sistema deste fosse frágil com relação à segurança, teríamos problemas gravíssimos, onde sistemas poderiam ser invadidos e terem seus dados e informações alteradas.

Ainda no caso de um banco temos também os terminais de clientes e caixas automáticos (saque), que além de necessitarem de segurança digital precisam também de segurança física a fim de não serem violados. Quando falo em segurança física me refiro a colocar certos equipamentos isolados, com acessos restritos e controlados. Imagine a situação um servidor de um banco X está completamente configurado contra ataques externos, com firewalls, máquinas pote de mel, e outros sistemas de defesa, mas no acesso direto ao console é liberado e o equipamento está em um canto qualquer de sala.

Temos um outro problema que está relacionado com o pessoal. Nas empresas, diferentemente da situação de sua residência, um equipamento pode e deve ser acessado por mais de um usuário. Hoje você pode estar trabalhando em um terminal amanha estará em outro, depois em outro, enfim, uma grande rotatividade de pessoal/terminal. Neste contexto temos que garantir que o usuário somente irá ter acesso ao que lhe é de direito, independente do terminal que está “logado”. Você não poderia ter o mesmo acesso de um gerente geral de agência só porque está utilizando a máquina que está na mesa dele.

Em um ambiente corporativo existe ainda uma grande rotação de pessoal, demissões, contratações, mudanças de setor, etc. Neste “troca-troca” de pessoal você tem de continuar dando acesso ao funcionário independentemente de sua localização ou setor. E é claro, poder bloquear os ex-funcionários bem como criar novos acessos para novos funcionários.

É claro que este não é um cenário da maioria das empresas, mas serve como base quão complexo deve ser a questão de segurança de sistema em um ambiente corporativo. Por que é obvio que para um banco o mais importante é a confiança em suas transações financeiras, já para uma empresa automobilística a sua informação e dados a serem protegidos têm outra fisionomia.

1.4 - A necessidade de segurança

Vimos com tudo isso que em todo e qualquer sistema que esteja integrado e interligado a outros sistemas deve possuir um nível de segurança, nível este que será obtido de acordo com o tipo da informação e dados que serão armazenados nestes sistemas.

Com um enorme crescimento do “crime digital” todos, desde o usuário doméstico até os grandes bancos estão necessitando segurança digital. Além disso, temos a questão das “pragas virtuais” que são os vírus, que invadem sistemas e destroem ou alteram o seu conteúdo. Estas pragas se proliferam de uma forma muito simples através de Internet ou até mesmo de uma rede local, baseadas na falta de informação ou descaso por parte do usuário ou do administrador da rede, em questões de segurança.

2 - Os riscos da falta de segurança em sistemas

2.1 - Vírus e “Cavalos de Tróia”

Antes de começar a falar sobre vírus de computador, deixarei uma estatística para pensamento. De acordo com uma recente pesquisa da PC Magazine mais de 50% dos problemas existentes em informática decorrem de mau uso ou inexperiência por parte do usuário, ou até mesmo de um administrador de sistemas. De 20 a 30% dos problemas ocorrem por erros no programa, conhecidos ou desconhecidos. O restante, ou seja, 30%, mais ou menos, são problemas causados por vírus de computador e invasões de sistemas.

Um vírus de computador é um programa que pode infectar outro programa de computador através da modificação dele, de forma a incluir uma cópia de si mesmo. A denominação de programa-vírus vem de uma analogia co mo vírus biológico, que transforma a célula numa fábrica de cópias dele. Para o publico em geral, qualquer programa que apague dados, ou atrapalhe o funcionamento de um computador, pode levar a denominação de vírus. Do ponto de vista do programador, o vírus de computador é algo bastante interessante. Pode ser descrito como m programa altamente sofisticado, capaz de tomar decisões automaticamente, funcionar em diferentes tipos de computador, e apresentar um índice mínimo de problemas ou mal-funcionamento.

Stephen Hawking se referiu ao vírus de computador como a primeira forma de vida construída pelo homem. De fato, o vírus é capar de se reproduzir sem a interferência do homem e também de garantir sozinho sua sobrevivência. A auto-reprodução e a manutenção da vida são, para alguns cientistas, o básico para um organismo ser descrito como vivo. O vírus Stoned é um exemplo que resiste até hoje, anos depois da sua criação. Sendo o vírus um programa de computador sofisticado, ainda que use técnicas de inteligência artificial, ele obedece a um conjunto de instruções contidas em seu código. Portanto é possível prevenir contra seu funcionamento, conhecendo seus hábitos.

Já o cavalo de tróia se assemelha mais a um artefato militar como uma armadilha explosiva ou “boody-trap”. O princípio é o mesmo daquele cigarro-explosivo ou de um daqueles livros que dão choque. O cavalo de tróia não se “reproduz”. A expressão cavalo de tróia é usada para com programas que capturam senhas sem o conhecimento do usuário e as enviam para o seu “criado”. Muitos destes programas são utilizados para se descobrir senhas de acesso à internet banking.

Basicamente um vírus de computador tem três modos de operação. Vírus de disco infectam o boot sector, setor do disco responsável pela manutenção dos arquivos. Vírus de arquivo infectam os arquivos executáveis, somente são acionados quando o arquivo onde estão alocados é executado. E o terceiro modo, que é a união dos outros dois, infectam, tanto o boot sector quanto arquivos executáveis, normalmente são as pragas virtuais mais sofisticadas.

2.2 - Hackers

Além dos perigosos e destrutivos vírus de computadores existem os Hackers. Tal determinação está hoje em dia generalizada, abrangendo muitas categorias, entre elas os crackers, os carders, os phreacking, todos eles tem como intuito invadir, destruir, obter informações, etc. Independente da terminologia tais indivíduos tem como intuito invadir sistemas para destruí-los ou obter informações sigilosas.

Os Hackers, em sua grande maioria, utilizam-se da falta de experiência dos administradores de sistemas ou usuário para conseguirem concluir suas intenções "criminosas". Como dito anteriormente muitos "administradores de sistemas" acham que conhecem muito e acham que seu sistema está seguro, contudo por sua falta de experiência não configuram o sistema corretamente e deixam furo na segurança.

Estes furos podem ser através de softwares instalados ou portas de serviço abertas, pode haver também programas instalados por terceiros, os Hackers, que tem como base "abrir" o sistema para uma entrada não autorizada. Sem querer entrar muito em detalhamento de arquitetura TCP/IP, cada serviço da pilha de protocolos TCP/IP, por exemplo, FTP, SMTP, utiliza-se de portas para comunicar-se com o sistema operacional. Estas portas podem ser abertas por softwares instalados por padrão em um sistema, as quais o administrador do sistema não sabe como fechar ou inutilizar, caracterizando assim um furo de segurança para o Hacker invadir o seu sistema.

Existem os Hackers mais sofisticados que disponibilizam software na Internet para que os usuários utilizem-se deste sem saber que seu real conteúdo é o de abrir o seu sistema para uma invasão. Tais programas também podem vir em e-mails sob a forma de componentes ativos de uma certa linguagem de programação.

3 - Políticas de segurança

3.1 - Senhas

Todo sistema tem um certo número de usuários habilitados a utilizarem seus recursos. Tais usuários possuem uma senha de acesso que combinada com seu username (nome do usuário no sistema) dão acesso ao sistema. Tal acesso pode e deve ser configurado pelo seu administrador a fim de delegar certos níveis de autonomia aos usuários. Por exemplo, os usuários do tele marketing de uma empresa não tem, ou não deveriam ter acesso às configurações das máquinas, poderes estes delegados ao(s) administrador(s).

Normalmente uma senha de acesso a um sistema deve ser conhecida somente pelo seu usuário e ser encriptada no sistema de forma irreversível. Desta forma somente o usuário poderá ter acesso ao sistema como sendo ele, nem o administrador pode saber a senha de acesso de outro usuário, caso seja necessário uma mudança de senha este procedimento deverá ser feito pelo administrador, inutilizando a senha anterior e solicitando ao usuário que cadastre nova senha.

Desta forma mantemos um certo nível de segurança no nosso sistema, contudo temos um problema muito grave neste aspecto, que será discutido mais à frente, que é o do usuário fornecer sua senha a outro usuário, por confiança, ou até mesmo por necessidade. Temos outro caso gravíssimo, o de colocar a senha escrita em um papel colado no monitor, bem este ponto não e nem passível de discussões, isto não é segurança, é ignorância.

3.2 - Administração de pessoal

Este com certeza é o pior ponto a ser comentado ou implementado em um sistema, pois nos deparamos com a pior das variáveis, o ser humano. Comentarei sobre um caso acontecido aqui na faculdade, DEL - UFRJ, omitirei nomes por questões éticas. Aula inaugural da disciplina de Computação I, primeiro período, todos os alunos recebem uma folha para preencher com alguns dados entre eles um username, para serem cadastrados nos servidores do departamento para terem acesso ao sistema. Durante uma aula de laboratório o professor começa a cadastrar os alunos no sistema, chama um a um para poderem cadastra uma senha. O professor explica claramente que a senha não pode ser o mesmo que o username, além de outras restrições, e pede ao aluno para inserir sua senha. O sistema aceita a senha e duto certo. Não!!! Após o termino do cadastro o professor usa um programa para determinar a complexidade das senhas e descobre que o aluno colocou seu username e senhas iguais.

Isso demonstra a complexidade de trabalhar com o fator humano, você o alerta de um fato, explica-o e a pessoa ainda comete o erro. É certo que isso faz parte da concepção do ser humano, sendo assim um administrador de sistema, mesmo depois de ter explicado um milhão de vezes, tem de se certificar que o usuário não tenha feito algo errado, tal como cadastra uma senha igual ao username.

A grande maioria das empresas tem em seu departamento de informática um profissional que está incumbido de propagar as regras de utilização e políticas de segurança no sistema da empresa. Tal profissional pode ser o próprio administrador, o que ocorre na maioria dos casos, ou alguém que o auxilie. Estas regras e políticas devem sempre estar em local de fácil acesso, em panfletos, cartazes, na intranet da empresa, enfim em diversos lugares, para que posteriormente um usuário não possa negar o seu conhecimento.

Outro pesadelo para as empresas tem sido a utilização dos sistemas da empresa para acesso a site de conteúdo pornográfico e envio de e-mails com tais conteúdos. Isso tem gerado ondas de demissões e punições para os funcionários que tem somente em sua defesa o fato de não terem conhecimento da política de segurança e acesso da empresa. Isto é a mais pura falta de critério, tem cabimento um funcionário utilizar-se dos recursos da empresa para acesso a tais sites, ou enviar e-mails para vários outros funcionários, o que já é errado (SPAM), com fotos pornográficas.

Este fato tem gerado uma discussão que foi para nos tribunais de justiça. Existem leis que asseguram a privacidade de correspondência seja ela eletrônica ou não, contudo também existe uma lei que determina como justa causa de demissão a utilização indevida e fora dos regulamentos pré-estabelecidos, dos equipamentos de uma em-

presa. Sendo assim chega-se a um dilema, quem está errado, a empresa por analisar o conteúdo da correspondência eletrônica dos funcionários ou estes por estarem utilizando os equipamentos da empresa para fins irregulares.

Fora dos tribunais de justiça ocorre um outro problema, que seria o de muitos destes sites de conteúdo pornográfico possuírem pequenos programas, denominados Trojans, que são desenvolvidos para se instalarem em sistemas e permitirem o acesso do seu criador a este sistema. Isso constitui de uma grave falha na segurança que poderia ser remediada com o esclarecimento aos funcionários das políticas de acesso e segurança de sua empresa.

3.3 - Segurança física de sistemas

Um administrador de rede tem sempre em mente a questão da segurança dos seus dados, “como dados”, dentro de um HD em uma máquina. Para este fim ele configura e instala diversos programas para controle e segurança dos seus dados, contudo quase sempre negligência a segurança física dos dados.

Tomemos como exemplo o seguinte cenário. Uma empresa qualquer tem um excelente administrador de redes, este instalou e configurou diversos softwares para barrar o acesso indevido aos dados, contudo deixou o servidor, em um canto de sala qualquer. Chegando um dia na empresa ele descobre que o micro foi aberto e o HD levado, ou melhor, roubado. De que adiantou o seu perfeito sistema de segurança se ele esqueceu de proteger fisicamente as máquinas.

Outro caso se refere ao fato de desastres naturais ou casuais. Todo sistema deve ter um projeto de backup, em que seriam feitas diversas cópias do sistema, como um todo ou parcialmente, e tais cópias armazenadas em locais diferentes. Isto parece uma certa paranóia, mas imagine o departamento de vendas de uma companhia de petróleo perdendo seus dados, ou porque esqueceram ou não fazem backup, ou porque o prédio em que funcionavam seus escritórios foi acometido por um atentado terrorista ou desastre natural.

Sendo assim o esquema de segurança de um sistema deve prever a sua integridade física, alocando os equipamento em locais apropriados, de acesso restrito e controlados, além de prover um projeto de backup eficiente e eficaz. Este contexto pode também ser adotado por um usuário doméstico, em suas devidas proporções. Um esquema de backup em mídias confiáveis e duráveis (por exemplo, o CD) pode fazer parte do dia-a-dia de um simples usuário de informática.

3.4 - Tipo de sistemas de segurança

Existem duas vertentes básicas em sistemas de segurança, uma via software e outra via hardware. No aspecto de hardware pode ser confuso diferencia-lo do software, pois e este quem realmente atua na segurança. Designamos como hardware de segurança o equipamento que fica dedicado a este função, com veremos mais adiante.

O software de segurança, de que pode ser desde um programa adquirido para este fim ou um sistema operacional configurado para ser o agente de segurança. Basicamente o software é responsável por deixar um usuário entra no sistema e outro não, deixar um dado trafegar na rede e outro não, deixar um serviço acionado e outro não, etc. Todos estes processos devem ser configurados pelo administrador da rede, que deve saber diferenciar o nível de necessidade de segurança de uma determinada informação, para poder aplicar a ela o devido critério de segurança.

4 - Software de segurança

4.1 - Firewall

O termo Firewall é uma analogia a uma parede corta-fogo (tradução) que impedirá o acesso a indevido a um sistema. Muitas pessoas imaginam que um Firewall seja um hardware próprio e que impeça o acesso de fora ao seu sistema, isso é uma das suas atribuições. Podemos ter Firewalls implementados através de software ou hardware, para controle de acesso externo ou interno.

Neste ponto já podemos começar a falar sobre os métodos de controle de acesso e segurança do sistema. Existem diversas formas de se controlar o que entra e sai de um sistema, desde os softwares até mesmo os usuários. No setor de software recentemente começaram a surgir diversos programas de caça de vírus (antivírus) e firewalls. O advento desta classe começou com a introdução e popularização dos acessos de banda larga e permanente.

Temos produtos como o Zone Alarm e o Norton Internet Security, entre outros, que atendem perfeitamente aos usuários domésticos e as pequenas corporações, tais softwares se encarregam de barra o acesso tanto para fora do sistema quanto para dentro do sistema. Estes programas através de configurações feitas pelos usuários podem impedir que o seu sistema seja acessado de uma máquina externa ou até mesmo barrando o acesso a Internet a determinados sites ou serviços.

Esta categoria não se aplica com certa eficiência em sistemas de maior complexidade, para este fim utiliza-se hardwares especializados em segurança, que serão descritor mais à frente.

4.2 - Sistemas Open Source (Linux / Free BSD)

Já é sabido por todos a eficiência e ampla capacidade operacional destes sistemas, sobre alguns sistemas proprietários. Em sistemas open source temos um maior controle sobre o que pode e está acontecendo dentro dele, sendo assim, através de configurações podemos bloquear serviços, portas, endereços, enfim um gama muito maior de opções de segurança.

Tanto o Linux como o Free BSD normalmente são utilizados como servidores em uma rede com estações Windows. Nesta configuração temos um cenário razoável de segurança onde atendemos as suas necessidades básicas e não “complicamos” a vida do nosso usuário com a necessidade de aprendizado de um novo sistema operacional, no

caso o Linux ou Free BSD. Digo isso com base nos seguintes dados, 90% dos sistemas operacionais domésticos são baseados no Windows, 95% dos processadores de texto instalados são softwares Microsoft, no caso alguma versão do Word. Sendo assim um usuário comum tem maiores chances de saber operar a dupla Windows/Office do que um sistema como o Linux ou o Free BSD.

Existe ainda um contexto de criar um Firewall para uma rede através da instalação de uma máquina dedicada baseada em software Open Source. Neste cenário temos uma das melhores configurações de segurança, mantendo os servidores também em sistemas Open Source, devido a estes terem uma maior confiabilidade no quesito segurança. Um firewall Linux pode ser implementado de diversas maneiras, por exemplo, através de proxy ou filtragem de pacotes. No primeiro caso um usuário requer uma conexão ao proxy e este consulta uma tabela a fim de checar as autonomias do usuário, se ele pode requere esta conexão, se está em uma máquina que pode aceitar a conexão, enfim uma enorme gama de opções de configuração.

No segundo caso, o de filtragem de pacotes, temos um forte esquema de segurança, onde todos os pacotes entrando ou saindo da sua rede serão analisados pelo Firewall. Nesta análise são checadas as permissões de tráfego do pacote, se ele pode ou não trafegar nesta rede. Este método de configuração é um pouco mais complexo que o proxy, exigindo do administrador uma maior compreensão dos protocolos e serviços de rede. Em um firewall por filtragem de pacotes podemos configurar cada tipo de protocolo com uma política de segurança diferente, podemos configurar em separado cada equipamento de rede para ter o não acesso, podemos bloquear ou liberar as portas de serviço, enfim uma enorme gama de opções de configuração.

5 - Hardware de segurança

5.1 - Firewall

Como já foi mencionado anteriormente existem hardwares dedicados à segurança. Estes podem ser firewalls, roteadores e switch. No caso dos firewalls existem equipamentos próprios desenvolvidos por empresas de segurança que desempenham este papel de acordo com a complexidade exigida.

Há também, muito mais comum, máquinas configuradas para serem os “guardas” de uma rede. A estas máquinas firewalls e suas redes é dado o nome de DMZ (DeMilitarized Zone), que consistem em um segmento de rede intermediária, entre uma rede protegida e uma rede aberta. Como exemplo poderíamos citar um firewall entre uma rede interna protegida de uma empresa e a Internet, que seria a rede desprotegida.

Normalmente estas máquinas possuem mais de uma interface de rede a fim de poder comunicar-se com mais de uma rede fazendo o roteamento entre as redes, baseado em configurações de segurança e políticas de acesso. Este equipamento tem com finalidade filtrar, não somente o tráfego de fora da sua rede, mas também o tráfego interno bem como o que sai dela.

No firewall podemos configurar que somente uma determinada máquina acesse um serviço ou um site, podemos também definir horários de acesso, atribuir diferentes políticas de acesso a diferentes usuários ou máquinas, enfim um bom administrador de redes podem afinar o firewall de sua empresa de acordo com as necessidades.

5.2 - Roteadores

Os roteadores são equipamentos utilizados para efetuar o roteamento dos pacotes que circulam de uma rede para outra. Estes equipamentos podem ter em suas especificações um sistema operacional que contenha rotinas para que ele funcione também como um hardware de segurança. No caso dos equipamentos Cisco, o IOS, sistema operacional do roteador, possui uma rotina para serem criadas as listas de acesso (Access List). Estas listas de acesso servem para configurar o acesso as redes conectadas ao roteadores e o acesso dos hosts ao próprio roteador.

Estes equipamentos através de suas configurações um forte esquema de segurança, que pode ser baseado na filtragem de pacotes IP, através das Access Lists, ou o bloqueio de um serviço através do bloqueio da porta do serviço. Sendo assim muitos administradores gostam e utilizam as funcionalidades de firewall de um roteador.

É claro que os roteadores não foram desenvolvidos para atuarem também como firewall em uma rede, contudo em certas redes de tamanho pequeno e onde o tráfego externo não seja tão grande, ele da conta do recado. Contudo em redes de grande porte ou com grande volume de tráfego externo, para não sobrecarregar o roteador, que além de sua função básica de rotear pacotes teria de analisar o pacote em relação as suas access list, é aconselhável que seja instaladas máquinas próprias para efetuarem a função de roteador.

5.3 - Switch

Os switch são equipamentos responsáveis pela distribuição das conecções para uma rede. É neste equipamento que ligamos os segmentos de rede vindos dos hosts, montando assim uma malha entre os hosts e os servidores, que podem ser ligados também aos switch. O switch é um equipamento extremamente versátil, podendo simplesmente atuar com um repetidor multiportas, fazer a conversão de meio entre duas redes e atuar como um equipamento de segurança.

Os switch gerenciáveis têm um software instalado em seus circuitos que se encarrega de agregar certas funcionalidades a ele. Uma destas funcionalidades pode ser vista com um controle de acesso, onde podemos controlar o acesso através da habilitação/desabilitação de uma de suas portas ou mesmo através de filtragem de pacotes. Isso mesmo um switch pode atuar na camada do protocolo IP (camada 3), a este processo dá-se o nome de VLAN, que seriam redes virtuais criadas através de um switch.

Nestas VLANs podemos configurar para que um grupo de máquinas somente possas se comunicar com outro grupo, e não com toda a empresa. Isso pode ser feito somente em switch que empreguem tal tecnologia e que sejam gerenciáveis. Por exemplo, temos 24 hosts ligados a um switch, podemos através de suas configurações atribuir

políticas de acesso baseadas nas portas onde estes hosts estão conectados. Sendo assim podemos impedir ou liberar o acesso de um grupo ou de uma só máquina a uma rede, ou até mesmo bloquear o acesso a certas máquinas.

Visto isso podemos atribuir ao switch a capacidade de funcionar com um dispositivo de segurança para uma rede interna. Sempre lembrando que sua finalidade não é esta, mas que em uma pequena rede este aspecto de firewall pode ser implementado, sem o auxiliou de uma máquina dedicada.

6 - Sistemas de detecção de intrusões (IDS)

Um IDS é uma solução complementar à instalação de uma firewall. A sua função é analisar permanentemente o tráfego da rede (interno e externo) e compará-lo com padrões conhecidos de comportamento de intrusos. Por estarem situados na rede interna analisam não só o tráfego externo, vindo da Internet, como também o tráfego interno. Podem, assim, ser detectados ataques vindos de pessoas internas à empresa ou que acedem a esta por outros meios. Um IDS pode analisar o tráfego na rede de diferentes perspectivas, cada uma com objetivos e resultados diferentes:

a) Signature detection.

Consistem na procura de padrões específicos de tráfego, correspondentes a determinado ataque. A desvantagem é que o padrão de ataque tem de ser conhecido de antemão e tem de ser programado no IDS. Para além disto, em situações de alto débito, o IDS poderá não escalar, eliminando pacotes do sistema de análise.

b) Behaviour detection.

Consiste na análise e na procura de padrões de comportamento, através da identificação de anomalias estatísticas. A idéia é que uma rede segue determinados padrões de comportamento que resultam em determinadas estatísticas. Alterações dessas estatísticas (maior tráfego a horas pouco usuais, aumento do número de pacotes de determinado tipo de protocolo, etc.) resultam na identificação de um possível ataque.

c) Protocol anomaly detection.

Consiste na análise de conformidade com o standard de pacotes de determinado protocolo. A título de exemplo, os recentes ataques do Code Red são facilmente detectados por este tipo de IDS, dado que os pedidos HTTP feitos ao servidor não estão conformes com o standard, usando caracteres inválidos para conseguirem subverter o funcionamento do Web server.

7 - Criptografia e Public Key Infrastructure (PKI)

7.1 - Introdução

A criptografia já estava presente no sistema de escrita hieroglífica dos egípcios. Desde então vem sendo muito utilizada, principalmente para fins militares e diplomáticos. No âmbito da computação é importante para que se possa garantir a segurança em todo o ambiente computacional que necessite de sigilo em relação às informações que manipula. Pode ser usada para codificar dados e mensagens antes que esses sejam envi-

ados por vias de comunicação, para que mesmo que sejam interceptados, dificilmente poderão ser decodificados, garantindo a privacidade.

A criptografia computacional é usada para garantir:

- Sigilo: somente os usuários autorizados têm acesso à informação;
- Integridade da informação: garantia oferecida ao usuário de que a informação correta, original, não foi alterada, nem intencional, nem acidentalmente;
- Autenticação dos participantes: identifica a pessoa ou entidade que solicita o acesso e também o servidor acessado;

Terminologias da criptografia

Cifrar: é o ato de transformar dados em alguma forma ilegível. Seu propósito é 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.

7.2 - Método simétrico e assimétrico

Uma informação pode ser codificada através de algum algoritmo de criptografia, de modo que, tendo conhecimento do algoritmo utilizado e da chave utilizada, é possível recuperar a informação original fazendo o percurso contrário da encriptação, a decriptação.

Algoritmos criptográficos são funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação. Devem ser conhecidos e testados. A segurança reside na chave secreta que deve ter tamanho suficiente para evitar sua descoberta por teste exaustivo.

Com o aumento da capacidade computacional, podemos hoje utilizar complexos esquemas criptográficos, que antes eram impraticáveis pela demora com os quais eram codificadas pequenas informações. E, além da capacidade técnica, possuímos algumas características na criptografia moderna que a faz se subdividir em dois grandes grupos: criptografia de chave simétrica e criptografia de chave assimétrica.

A criptografia de chave simétrica é a tradicional. Nela a mesma chave utilizada na codificação deve ser utilizada na decodificação. Exemplos de algoritmos que implementam esse tipo de criptografia: IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard) da IBM e o RC2/4 da RSA Data Security.

O problema óbvio dessa simetria é: como vou informar ao destinatário a chave para a decriptação de forma segura? Se encontrar um modo seguro de lhe contar a chave, eu não poderia utilizá-lo para passar a informação de uma vez? Realmente, este não é o melhor método para trocarmos nossos segredos.

No entanto, a criptografia simétrica é bastante eficiente em conexões seguras na Internet onde processos computacionais trocam senhas temporárias para algumas transmissões críticas e, ao contrário do que você pode estar imaginando, já utilizou algumas delas: quando você navega pela Internet e visita sites ditos "seguros", onde geralmente são preenchidos dados sigilosos, você está utilizando o SSL (Secure Sockets Layer) que funciona à base de criptografia simétrica, muito provavelmente DES ou algo da RSA.

Na criptografia de chave assimétrica são usadas duas chaves ligadas matematicamente; se uma é utilizada para criptografar uma mensagem, a outra chave deve ser utilizada para decriptografar. Uma das duas é mantida em segredo e é referenciada como chave privada. Essa chave privada pode ser representada como sendo a identidade do seu proprietário; logo, sua privacidade é crucial. É necessário que o emissor e o receptor da mensagem utilizem a mesma mensagem privada sem que ninguém descubra. A outra chave, denominada chave pública é disponível a todos. Qualquer pessoa pode enviar uma mensagem confidencial apenas utilizando chave pública, mas esta mensagem só poderá ser decriptografada com a chave-privada do destinatário.

Os sistemas assimétricos geralmente não são tão eficientes computacionalmente quanto os simétricos; eles normalmente são utilizados em conjunção com sistemas simétricos para fornecer facilidades de distribuição da chave e capacidades de assinatura digital.

7.3 - Técnicas conhecidas

ROT13: é utilizada em codificação de mensagens. Nessa técnica, a letra do alfabeto move 13 casas. Por exemplo: a letra A torna-se a letra O e assim sucessivamente.

Crypt: é um utilitário baseado numa máquina de criptografia da 2a. Guerra Mundial. O software para quebrar esse tipo de criptografia é de fácil obtenção na Internet.

DES (Data Encryption Standard): foi desenvolvida na década de 70 pela IBM sendo que o governo americano adotou como método de criptografia não oficial, porém confidencial. Utiliza a mesma chave tanto para criptografia como para descriptografia. Funciona da seguinte forma: pega-se dados em grupos de 64 bits e embaralha-os 16 vezes de uma forma especial. Possui duas variações: ECB (Eletronic Code Book) e CBC (Cipher Block Chaining). Foi o primeiro código moderno a tornar-se público.

Os novos métodos de criptografia baseiam-se no DES, porém na Internet começaram a surgir boatos de que o NSA podia invadir qualquer tipo de dados que utilizava o método DES. Quando pesquisadores criaram a técnica de criptoanálise diferencial para atacar os métodos de criptografia, foi descoberto que a técnica em questão não prejudicava o DES. Ele já era protegido contra a criptoanálise diferencial, o que aumentaram

as suspeitas em relação que a NSA seria a única capaz de invadir qualquer tipo de dados.

Sua falha é no número de chaves pequeno (cerca de 56 letras). Uma ótima recomendação para a utilização de uma chave é utilizando-se uma chave composta por uma chave hexadecimal com 14 dígitos (a base hexadecimal varia do número 0-9 e de A-F).

DES Triplo: aumenta o número de chaves e codifica três vezes o dado, utilizando chaves diferentes em cada estágio da codificação tendo um efeito de 168 chaves. Alguns criptógrafos erroneamente usam a mesma chave em dois dos estágios diminuindo o efeito para 112 bits. Isso é chamado de Encode-Decode-Encode (DES-EDE). O DES triplo é vulnerável a criptoanálise diferencial meet in the middle.

O DES é um dos únicos algoritmos que tem uma reunião de pesquisadores independentes tentando detectar um método de atacá-lo. Por enquanto nenhum método de ataque foi detectado.

IDEA: desenvolvido na década de 80 por Xuejia Lai e James Massey da ASCOM Tech AG da Suiça, em Zurique, o IDEA embaralha os dados em grupos de 64 bits e utiliza uma chave de 128 bits que é suficiente para resistir à maior parte dos ataques.

RSA: foi criado por Ron L. Rivest, Adi Shamir e Leonard Adelman fundadores da RSA Data Security. Utiliza a criptografia de chave pública. A criação da chave no método RSA é através de fatoração de dois números primos. Um será sua chave de criptografia e outro de descriptografia. O computador, através de uma série de cálculos pode através do número primo de criptografia chegar a descriptografia dos dados.

Em 1977 os criadores do RSA divulgaram numa matéria da revista Scientific American o método de criptografia juntamente com uma mensagem codificada e uma chave pública com 129 dígitos e afirmaram que a utilização de uma chave poderia ficar secreta por décadas e ficou conhecido como a tarefa RSA129 onde no decorrente ano de 1993 milhares de jovens curiosos com auxílio de poderosas máquinas e troca de dados e testes através da Internet batalharam para desvendar a chave.

No ano de 1994, a famosa chave pública foi quebrada. Um segredo de muitas décadas quebrado em menos de 1 ano de tentativa. A fatoração de um código de 129 dígitos obviamente é facilmente quebrada para quem tem acesso a supercomputadores e paixão pela matemática.

Privacy-Enhanced Mail (PEM): 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.

Pretty Good Privacy (PGP): criado por Phillip Zimmermann, semelhante em conceito em relação ao RIPEM, porém utilizando o método do RSA para chave pública e a lógica do IDEA. É capaz de ocultar o nome da pessoa que enviou a mensagem.

RC2 e RC4: desenvolvido por Ron River, na RSA Data Security, mantém em chaves de criptografia inferior a chave de 40 dígitos, permitindo assim a sua exportação.

7.4 - Tipos de cifragem de blocos

ECB - Eletronic Code Book (Modo do livro de códigos): cada bloco da mensagem original é individual e independentemente cifrado para produzir os blocos da mensagem cifrada. O bloco típico tem 64 bits, o que produz um livro de códigos de 2 exp(64) entradas. E note-se que para cada chave possível existe um livro de códigos diferentes. A vantagem do método é sua simplicidade e a independência entre os blocos. A desvantagem é que um criptoanalista pode começar a compilar um livro de códigos, mesmo sem conhecer a chave.

Um problema mais grave é a chamada repetição de bloco, onde um atacante ativo pode alterar parte de uma mensagem criptografada sem saber a chave e nem mesmo o conteúdo que foi modificado. Pode-se, por exemplo, interceptar uma transação bancária de transferência de saldo de qualquer pessoa, a seguir pode-se realizar uma transferência de saldo de uma conta para a conta do atacante e interceptar a mensagem, assim pode-se identificar os blocos correspondentes ao destinatário e dessa forma substituir em todas as mensagens o destinatário pelo atacante.

CBC - Cipher Block Chaining (Modo de encadeamento de blocos): CBC realimenta a cifragem do bloco atual com o resultado das cifragens dos blocos anteriores. A operação mais utilizada é o ou-exclusivo com o bloco anterior, dessa forma os blocos iguais serão normalmente cifrados de forma diferente, desde que no mínimo um dos blocos anteriores seja diferente da mensagem. Entretanto, duas mensagens iguais serão mapeadas para os mesmos blocos. E duas mensagens com início igual serão cifradas da mesma forma até que ocorra a diferença. A maneira empregada para evitar esse problema é a utilização de um vetor de inicialização distinto para cada mensagem.

CFB - Cipher Feedback (Modo de realimentação de cifra): quando há necessidade de enviar mensagens que possuem tamanho menor que um bloco usa-se o método CFB, que trabalha com grupos (8 bits por exemplo - 1 caracter). Neste caso, a realimentação é feita sobre o grupo, utilizando-se também o ou-exclusivo.

Cifras de Substituição: troca cada caractere ou grupo de caracteres por outro, de acordo com uma tabela de substituição. Pode-se quebrar este método analisando-se a freqüência de cada caractere no texto cifrado e comparando-se estas freqüências com aquelas que normalmente aparecem em um determinado idioma. As vogais têm maior freqüência que as consoantes e alguns caracteres possuem freqüência baixíssima em relação aos demais. Para amenizar a freqüência de caracteres, podemos utilizar várias tabelas para cifragem de um texto. Para uma substituição mono alfabética podemos ter 261 tabelas de substituição. Tem-se uma chave que diz qual das tabelas será usada para cada letra do texto original. Portanto, quanto maior a chave mais seguro é o método. Entretanto, é suficiente descobrir o tamanho da chave k e analisar blocos de k caracteres no texto, verificando a freqüência de repetição dos caracteres.

Substituição Mono alfabética: cada letra do texto original é trocada por outra de acordo com uma tabela e com sua posição no texto. A Substituição de César é um exemplo de substituição mono alfabética que consiste em trocar cada letra por outra que está 3 letras adiante na ordem alfabética. Por exemplo, A=D. Pode-se usar outros valores ao invés de 3, o que constitui a chave de cifragem. Existem apenas 26 chaves, por isso é um método que visa proteger textos com pequeno grau de sigilo.

Substituição por Deslocamentos: a chave indica quantas posições deve-se avançar no alfabeto para substituir cada letra. Diferente da Substituição de César, as letras não são trocadas sempre por uma letra n posições a frente no alfabeto. Por exemplo, chave: 020813. A primeira letra é trocada pela letra que está 2 posições a frente no alfabeto, a segunda pela que está 8 posições a frente, e assim por diante, repetindo a chave se necessário. (PAI = RIV)

Substituição Monofônica: como a anterior, mas agora cada caractere pode ser mapeado para um ou vários caracteres na mensagem cifrada. Isso evita a linearidade da substituição.

Substituição polialfabética: a combinação no uso de várias substituições mono alfabéticas, usadas em rotação de acordo com um critério ou chave. Por exemplo, poderiam ser utilizadas 4 tabelas, usadas em alternância a cada 4 caracteres.

Substituição por Polígramos: utiliza grupo de caracteres ao invés de um caractere individual. Se fossem considerados trigramas, por exemplo, ABA poderia ser substituído por RTQ ou KXS.

Cifras de Transposição: troca-se a posição dos caracteres na mensagem. Por exemplo, pode-se reescrever o texto percorrendo-o por colunas. Ou então definir o tamanho para um vetor de trocas e também uma ordem em que as trocas serão feitas. Pode-se usar chave para isso. Por exemplo, em um vetor de tamanho 6 pode-se trocar o primeiro caractere pelo terceiro, o segundo pelo quinto e o quarto pelo sexto. Se a freqüência dos caracteres for à mesma do idioma, temos substituição por transposição. Se for diferente, temos por substituição. Também é possível combinar substituição e transposição, ou vice-versa.

Máquinas de Cifragem: um código trabalha com grupos de caracteres de tamanho variável, ao contrário da cifra. Cada palavra é substituída por outra. Quebrar um código equivale a quebrar uma gigantesca substituição mono alfabética onde as unidades são as palavras e não os caracteres. Para isso deve-se usar a gramática da língua e analisar a estrutura das frases. Máquinas de cifragem baseiam-se em engrenagens que têm tamanhos diferentes e que giram a velocidades diferentes, obtendo uma substituição poli alfabética com chave de 26n, onde n é o número de engrenagens.

7.5 - Tipos de ataques

Um criptosistema deve ser seguro mesmo quando os algoritmos de criptografia e descriptografia sejam conhecidos. Por esta razão são utilizadas chaves. Uma pessoa não autorizada que tem acesso a alguns dos elementos de um criptosistema é denominada de

atacante. Um atacante passivo somente obtém cópias dos elementos, enquanto um atacante ativo pode alterar alguns desses elementos. Existem cinco tipos de ataque (ou criptoanálise) mais comuns. Todos eles supõem que o criptoanalista possui conhecimento total sobre os métodos de criptografia e descriptografia utilizados, mas não sobre as chaves.

- ataque de texto cifrado (cyphertext-only): o criptoanalista tem a sua disposição uma grande quantidade de mensagens cifradas, mas desconhece as originais e as chaves utilizadas. Sua tarefa é recuperar as mensagens normais (deduzir as chaves utilizadas).

- ataque de texto conhecido (known-plaintext): o criptoanalista tem a sua disposição uma grande quantidade de mensagens criptografadas e também as mensagens originais equivalentes. Sua tarefa é deduzir as chaves utilizadas (ou um método para recuperar mensagens cifradas com a mesma chave).

- ataque adaptativo do texto escolhido (adaptative-choosen-plaintext): no método anterior, o criptoanalista poderia ser capaz de fornecer somente uma grande quantidade de mensagens de uma só vez; agora ele pode fornecer um pequeno conjunto, analisar os resultados, fornecer outro conjunto e assim por diante. Sua tarefa é deduzir as chaves utilizadas. Alguns métodos de criptografia como os RSA são muito vulneráveis a este ataque.

- ataque do texto cifrado escolhido (choosen-cyphertext): o criptoanalista não só tem uma grande quantidade de mensagens e seus equivalentes criptografados, mas pode produzir uma mensagem criptografada específica para ser decifrada e obter o resultado produzido. É utilizado quando se tem uma "caixa-preta" que faz descriptografia automática. Sua tarefa é deduzir chaves utilizadas.

- ataque de chave escolhida (choosen-key): o criptoanalista pode testar o sistema com chaves diferentes ou pode convencer diversos usuários legítimos do sistema a utilizarem determinadas chaves. Neste último caso, a finalidade imediata seria de decifrar as mensagens criptografadas com essas chaves.

Um sistema é dito seguro se ele é teoricamente inquebrável, ou seja, não interessa qual a quantidade de texto normal ou decifrado a disposição, nunca se tem informação suficiente para deduzir as chaves utilizadas ou decifrar um texto qualquer cifrado. Só se conhece um método nesta categoria: a Cifra de Vernam ou One-time pad (cifra de uso único). Em essência dois elementos que desejem comunicar-se possuam cópias idênticas de uma seqüência randômica de valores, que são utilizados como chave. O método, entretanto, exige que cada chave seja usada uma única vez e que o comprimento da seqüência (chave) seja maior, ou no mínimo igual ao comprimento da mensagem a ser criptografada.

7.6 - PKI

O PKI, ou, Public Key Infrastruture é um exemplo de novas tecnologias recém-nascidas. PKI ou Infra-estrutura de Chaves Públicas consiste de serviços, protocolos e aplicações utilizados para o gerenciamento de chaves públicas e certificados. O que fa-

zem? Provêem serviços de criptografia de chave pública e assinatura digital, permitindo a interação segura entre usuários e aplicações.

Os serviços oferecidos por uma solução PKI variam: registro de chaves com a emissão de um novo certificado para uma chave pública; revogação ou cancelamento de certificados; obtenção de chaves públicas de uma autoridade certificadora; e validação de confiança, determinando se o certificado é válido e a quais operações ele está autorizado.

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

Componentes de uma solução PKI:

- Autoridade Certificadora (CA);
- Autoridade Registradora (RA), opcional;
- Diretório;

Certification Authority (CA) ou Autoridade Certificadora é uma entidade representada por pessoas, processos e ferramentas usadas na emissão de certificados digitais que, de uma forma segura, associa o nome da entidade (usuário, máquina etc) ao seu par de chaves. Ela funciona como um agente da segurança. Desta forma, se os usuários confiam em uma CA e em sua política de emissão e gerenciamento de certificados, confiam nos certificados emitidos pela CA. Isso é o que chamamos de third-party trust ou confiança em uma terceira parte ou entidade.

O Diretório, por sua vez, pode ser entendido como um local de armazenamento (repositório) dos certificados e das listas de revogação emitida por uma CA.

Benefícios de uma solução PKI:

- Autenticação: identificar os usuários e máquinas
- Controle de Acesso: controlar quem acessa as informações e realiza as transações;
- Confidencialidade e Privacidade: ter certeza de que a comunicação é privada mesmo via Internet;
- Integridade: garantir que a informação não será alterada;
- Não-repúdio: prover um método digital de assinatura das informações e transações;

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

7.7 - Assinatura digital

Assinatura Digital é a versão digital da assinatura de punho em documentos físicos. A assinatura de punho é um componente que assegura que a pessoa em questão escreveu ou concordou com o documento no qual consta sua assinatura.

A Assinatura Digital apresenta grau de segurança muito superior ao de uma assinatura de punho. O destinatário de uma mensagem assinada digitalmente pode verificar se a mensagem foi realmente emitida pela pessoa cuja assinatura nela consta, ou se a mensagem não foi em algum ponto adulterada intencional ou acidentalmente depois de assinada. Mais ainda, uma Assinatura Digital que tenha sido verificada não pode ser negada; aquele que assinou digitalmente a mensagem não pode dizer mais tarde que sua assinatura digital foi falsificada.

Em outras palavras, Assinaturas Digitais habilitam "autenticação" de documentos digitais, garantindo ao destinatário de uma mensagem digital tanto a identidade do remetente quanto a integridade da mensagem. Por exemplo, para personalizar uma mensagem, um determinado usuário A codifica uma mensagem utilizando sua chave secreta e a envia para o destinatário. Somente a chave pública de A permitirá a decodificação dessa mensagem. Portanto é a prova de que A enviou a mensagem. A mensagem assim pode ser decodificada por qualquer um que tenha a chave pública de A.

Propriedades:

- a assinatura é autêntica: quando um usuário usa a chave pública de A para decifrar uma mensagem, ele confirma que foi A e somente A quem enviou a mensagem;
- a assinatura não pode ser forjada: somente A conhece sua chave secreta;
- o documento assinado não pode ser alterado: se houver qualquer alteração no texto criptografado este não poderá ser restaurado com o uso da chave pública de A;
- a assinatura não é reutilizável: a assinatura é uma função do documento e não pode ser transferida para outro documento;
- a assinatura não pode ser repudiada: o usuário B não precisa de nenhuma ajuda de A para reconhecer sua assinatura e A não pode negar ter assinado o documento.

8 - Rede privada virtual (VPN)

8.1 - Introdução

A tecnologia de VPN permite que as empresas com linhas dedicadas formem um circuito fechado e seguro pela Internet, entre elas próprias. Dessa maneira, essas empresas asseguram que os dados passados entre eles e suas contrapartes estejam seguros (e normalmente criptografados).

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.

Uma das grandes vantagens decorrentes do uso de VPNs é a redução de custos com comunicações corporativas, pois elimina a necessidade de links dedicados de longa distância que podem ser substituídos pela Internet.

As LANs podem através de links dedicados ou discados, conectar-se a algum provedor de acesso local e interligar-se a outras LANs, possibilitando o fluxo de dados através da Internet. Esta solução pode ser muito interessante sob o ponto de vista econômico, sobretudo nos casos em que enlaces internacionais ou nacionais de longa distanciam estão envolvidos. Outro fator que simplifica a operacionalidade da WAN é que a conexão LAN-Internet-LAN fica parcialmente a cargo dos provedores de acesso.

8.2 - Aplicação para redes privadas virtuais

A seguir, são apresentadas as três aplicações consideradas como as mais importantes para as VPNs:

Acesso remoto via Internet

O acesso remoto a redes corporativas utilizando a Internet pode ser viabilizado com a tecnologia VPN através da ligação local a um provedor de acesso (Internet Service Provider - ISP). A estação remota disca para o provedor de acesso, conectando-se à Internet e o software de VPN cria uma rede virtual privada entre o usuário remoto e o servidor de VPN corporativo através da Internet.

Conexão de LANs via Internet

Uma solução que substitui as conexões entre LANs através de circuitos dedicados de longa distância é a utilização de circuitos dedicados locais interligando-as à Internet. O Software de VPN assegura esta interconexão formando a WAN corporativa.

A depender das aplicações, também se pode optar pela utilização de circuitos discados em uma das pontas, devendo a LAN corporativa estar preferencialmente conectada à Internet via circuito dedicado local, ficando disponível 24 horas por dia para eventuais tráfegos provenientes da VPN.

Conexão de computadores numa intranet

Em algumas organizações, existem dados confidenciais cujo acesso é restrito a um pequeno grupo de usuários. Nestas situações, redes locais departamentais são implementadas fisicamente separadas da LAN corporativa. Esta solução apesar de garantir a "confidencialidade" das informações, cria dificuldades de acesso a dados da rede corporativa por parte dos departamentos isolados.

As VPNs possibilitam a conexão física entre redes locais, restringindo acessos indesejados através da inserção de um servidor VPN entre elas. Observe que o servidor VPN não irá atuar como um roteador entre a rede departamental e o resto da rede corporativa uma vez que o roteador permitiria a conexão entre as duas redes permitindo o acesso de qualquer usuário à rede departamental sensitiva.

Com o uso da VPN o administrador da rede pode definir quais usuários estarão credenciados a atravessar o servidor VPN e acessar os recursos da rede departamental restrita. Adicionalmente, toda comunicação ao longo da VPN pode ser criptografada assegurando a "confidencialidade" das informações. Os demais usuários não credenciados sequer enxergarão a rede departamental.

Em resumo, as VPNs podem-se constituir numa alternativa segura para a transmissão de dados através de redes públicas ou privadas, uma vez que já oferecem recursos de autenticação e criptografia com níveis variados de segurança, possibilitando eliminar os links dedicados de longa distância, de altos custos, na conexão de WANs.

Entretanto, em aplicações onde o tempo de transmissão é crítico, o uso de VPNs através de redes externas ainda deve ser analisado com muito cuidado, pois podem ocorrer problemas de desempenho e atrasos na transmissão sobre os quais a organização não tem nenhum tipo de gerência ou controle, comprometendo a qualidade desejada nos serviços corporativos.

A decisão de implementar ou não redes privadas virtuais requer uma análise criteriosa dos requisitos, principalmente aqueles relacionados a segurança, custos, qualidade de serviço e facilidade de uso que variam de acordo com o negócio de cada organização.

9 - Conclusão

Ao fim deste trabalho percebemos que a segurança vem sendo uma das áreas de maior crescimento dentro da Informática, devido ao aumento de casos de invasão de sistemas, alteração e roubo de dados, "derrubar" um servidor, enfim todo tipo de "crime digital".

Vimos também que tanto em um ambiente doméstico como em um corporativo temo a necessidade de um nível de segurança, nível este que será dado através de uma criteriosa análise dos dados e informações a serem resguardados.

Contudo como sendo o projeto de um sistema seguro um projeto de engenharia, este deve ser executado e posteriormente administrado com competência sem negligenciar os ponto levantados, pois vemos que muitos projetos foram bem elaborados, contudo executados com enorme incompetência. E por último, mas não menos importante, a figura de um administrador, que deve estar sempre ativo ao sistema, "ligado" nas mais novas formas de invasão e destruição de dados e suas prevenções, e um administrador que saiba instruir seu pessoal, seja ele até mesmo um simples usuário.

10 - Bibliografia:

- Sites:

Comitê gestor da Internet no Brasil
http://www.cg.org.br

Linux Security Brasil
http://www.linuxsecurity.com.br

Tópicos Selecionados em Segurança Computacional - UNB
http://www.cic.unb.br/docentes/pedro/sdtopicos.htm

Criptografia e Segurança de Redes de Computadores
http://www.redes.unb.br/security/

Look Abit
http://www.lockabit.coppe.ufrj.br/

Computer Emergency Response Team - Rio Grande do Sul
http://www.cert-rs.tche.br/outros.html

SANS Institute: Information Security Reading Room
http://rr.sans.org

Cisco
http://www.cisco.com

CERT Coordination Center
http://www.cert.org

Inform IT
http://www.informit.com

- Livros:

Título: Computer Networks
Autor: Andrew S. Tanenbaum
Editora: Prentice Hall PTR
Publicação: 1996

Título: Network Security in the 90's: Issues and Solutions for Managers
Autor: Thomas W. Madron
Editora: John Wiley & Sons
Publicação: 1992

Título: Segurança de Redes - Projeto e Gerenciamento de Redes Seguras
Autor: Thomas A. Wadlow

Editora: Campus
Publicação: 2000

Título: Segurança de Redes em ambientes cooperativos
Autores: Emilio Tissato Nakamura e Paulo Lício Geus
Editora: Berkeley
Publicação: 2002

Título: Segurança em Informática de Informações
Autores: Carlos Caruso e Flavio Deny Steffen
Editora: Senac
Publicação: 1999

Título: Building Internet Firewalls
Autor: Chapman
Editora: O'Reilly
Publicação: 1995

Título: Hackers Expostos (Segredos e soluções para a segurança de redes)
Autores: George Kurtz , Stuart McClure e Joel Scambray
Editora: Makron Books
Publicação: 2000

Título: Segurança Total (protegendo-se contra os Hackers)
Autor: Olavo José Ancheeschi Gomes
Editora: Makron Books
Publicação: 2000