

Cybersecurity

LAAD
DEFENCE & SECURITY

2017

04 - 07 | ABRIL
RIOCENTRO
RJ | BRASIL

LAAD
SECURITY

2018

10 - 12 | ABRIL
NUEVA UBICACIÓN
TRANSAMERICA EXPO CENTER
SP | BRASIL

LAAD
DEFENCE & SECURITY

2019

02 - 05 | APRIL
RIOCENTRO
RJ | BRAZIL



07/11/2008

prof.brunotsouza

2023 || 2024

RC

[15/09/2022]

Texto original do artigo técnico que ainda está sob revisão e que precisa ser atualizado)

Redes de Computadores.

Introdução

No período compreendido entre o final dos anos sessenta e início dos anos setenta, a microinformática ainda estava longe de se tornar uma realidade, as pessoas que acreditavam no seu desenvolvimento baseavam-se em especulações sem muito fundamento mercadológico para os padrões da época. Para a maioria dos profissionais que já estavam na área há muito tempo, e que testemunharam o crescimento dos "mainframes" (computadores de grande porte), a microinformática nada mais era do que um sonho com o qual os analistas alimentavam suas projeções para as próximas gerações. Basicamente esta descrença ocorria por dois motivos: primeiro a tecnologia a ser implementada no que poderia ser chamado de microcomputador era extremamente aquém das necessidades impostas pelas grandes organizações, sendo portanto incomparável em termos de recursos com a que era empregada nos computadores de grande porte; segundo, já existia toda uma base de profissionais habilitados a operar com a realidade do "mainframe", tais como administradores de CPD (Central de Processamento de Dados) e operadores, que obviamente não gostaram muito deste novo paradigma.

Mas afinal de contas como era baseada a estrutura operacional das empresas que utilizavam os mainframes? Na década de mil novecentos e sessenta a empresa norte-americana IBM (Industrial Business Machines) dava as cartas, impondo, por assim dizer, soluções a nível de hardware e software que exigiam um investimento extremamente elevado (a manutenção apresentava um custo consequentemente alto para as organizações). No início a Informática ainda era considerada uma área estratégica pelo governo, e realmente o foi, por isso toda uma série de artifícios e facilidades políticas fizeram da IBM uma das maiores multinacionais dos Estados Unidos. Em meados dos anos sessenta uma empresa até então com uma participação relativamente pequena no mercado chamada Digital Equipments (DEC), hoje parte integrante da Compac, lançou no mercado uma série de máquinas de "baixo" custo que, embora não apresentassem um vasto poder de processamento, eram adequadas àquelas empresas de médio porte que não poderiam gastar muitos dólares com um servidor IBM, mas podiam pagar por um

professor Bruno Tavares de Souza

RC

Digital Série DVD. E foi a partir do DVD-5 que as vendas da Digital começaram a crescer, assustando o pessoal da IBM com aquelas suas máquinas "baratas" que podiam ser transportadas no banco traseiro de um Fusca. Mas afinal de contas, o que esta história tem a ver com a estrutura operacional das empresas que utilizavam os mainframes? É simples, a popularização dos mainframes foi o primeiro passo para o avanço desta tecnologia no mundo corporativo, e a definição de novos padrões (ou conceitos) depende muito de fatores econômicos.

A topologia dos CPDs interagindo com os diversos departamentos de uma empresa era, em sua essência, algo bem simples. Uma máquina central comportava e processava todas as informações, e o seu escopo de atuação estava limitado fisicamente. No início não havia interação, a comunicação com o mundo exterior era feita através dos funcionários. Nesta época os profissionais responsáveis pela manutenção dos computadores e sistemas eram poucos, e muito bem qualificados. Depois surgiram terminais "burros", constituídos de um teclado e monitor, em cada departamento ou setor do edifício, que se comunicavam passivamente com o mainframe. O usuário solicitava que uma informação fosse exibida ou processada, esta solicitação era encaminhada para o servidor e o mesmo se encarregava de enviar a resposta. O maior problema apresentado neste tipo de relacionamento passivo era que, embora muitas das informações utilizadas por um departamento fossem necessárias para o pessoal de outro departamento, as aplicações utilizadas pela equipe de R.H poderiam não ser as mesmas utilizadas pelo setor financeiro. Logo, como o desenvolvimento dessas aplicações dependia totalmente da disponibilidade dos analistas e projetistas que gerenciavam a Central de Processamento de Dados, os funcionários de um setor muitas vezes se viam obrigados a esperar pela resposta durante meses. Este ambiente centralizado, por conseguinte, elevava os custos.

No final dos anos setenta os primeiros modelos de microcomputador nada mais eram do que "brinquedos" caros, verdadeiras coqueluches para aficionados por informática que podiam pagar caro por uma máquina simples, com baixo poder de processamento, pura e simplesmente destinada às tarefas ditas domésticas. Algumas pessoas arriscaram dizer que estava chegando o dia em que todos os lares iriam ter um microcomputador, e essas pessoas apostaram nisso. Foi quando surgiu a Microsoft Corp., hoje dirigida por Bill Gates, uma softhouse que como várias outras estava se especializando no desenvolvimento de sistemas simples, que rodassem em plataformas "modestas", sem que houvesse a necessidade de recorrer aos serviços prestados por um servidor. Não era

RC

loucura, a Microsoft nasceu de acordos com a IBM, que estava no desenvolvimento de máquinas "desktop" (computadores de mesa) destinadas em primeira mão ao mercado corporativo e, quando viável financeiramente, ao mercado doméstico. Esta história é recheada de detalhes que não convém mencionar agora, mas faço questão de frisar o quanto importante foi a participação da IBM, e consequentemente da Microsoft, no processo de descentralização dos CPDs com seus mainframes caros e robustos.

Em 1981 foi lançado o primeiro computador de uso pessoal da IBM, o IBM PC, uma máquina considerada rápida para os padrões da época. Possuía um clock de 4.77 Mhz e 64 Kbytes de memória RAM. Pouco? Não, era mais do que suficiente para quem já fazia uso de terminais burros. Afinal de contas, era uma máquina IBM rodando sistemas que satisfaziam às necessidades reais, sem a interferência de um analista indiferente aos anseios do usuários, "pobres mortais". Este processo de transição não foi excessivamente tão traumático quanto pode estar parecendo, pois foi gradativo. Nós estamos falando de investimentos altíssimos, e os mainframes continuaram existindo por um bom tempo (e ainda existem), embora com uma maior distribuição da carga de processamento. Um exemplo prático: o funcionário do setor financeiro não dependia mais dos aplicativos residentes no servidor, como antes, para executar suas tarefas. As longas esperas também não tinham mais razão de ser, pois com um PC sistemas mais adequados, e eficientes, cumpriam o papel das aplicações residentes no computador central. Os terminais agora cumpriam basicamente a tarefa de transmitir e receber dados.

Nos anos oitenta a indústria de hardware e software cresceu muito rápido, com a popularização dos microcomputadores entre os usuários domésticos. O preço do PC ainda era um tanto quanto alto no início, mas a IBM - ao perceber a importância do crescimento no setor - licenciou a tecnologia do IBM PC para outros fabricantes. Logo, rapidamente o PC se tornou um padrão de fato, estabelecendo os pilares para as redes distribuídas de hoje. O PCDOS e o MSDOS, sistemas operacionais monusuário desenvolvidos respectivamente pela IBM e pela Microsoft, foram de grande importância no processo de popularização do PC. Com comandos simples já era possível trabalhar com um microcomputador em casa. Por isso, gradativamente muitos profissionais passaram a executar cópias dos sistemas que utilizavam no escritório nos PCs que estavam em suas casas, e as tarefas que antes só podiam ser realizadas no trabalho passaram a ser implementadas no lar. Como pode ser notado, na década de 1980 a informática deixou de ser uma ferramenta para poucos e passou a entrar na vida das pessoas que não tinham nenhum relacionamento

professor Bruno Tavares de Souza

RC

direto com ela. No momento em que este ramo de tecnologia passou a ter um apelo mais comercial, as renovações que antes já estavam num ritmo crescente passaram a ser constantes, gerando a concorrência necessária ao crescimento do setor.

Na década de 1990 o termo rede de computadores se relaciona com a vida do profissional e das pessoas comuns dentro de um contexto mais amplo, e as tecnologias da informática passam a ser interpretadas como tecnologias da informação (TIs), pela sua junção com as telecomunicações. Os anos setenta e oitenta viram passar uma série de pesquisas de âmbito acadêmico e militar que objetivavam a interconexão entre diferentes redes de informação, localizadas remotamente. A Arpanet (rede de informações desenvolvida pelos militares norte-americanos no final dos anos sessenta) foi um dos primeiros passos nesta jornada, já que foi a partir dela que a Internet evoluiu. As redes locais, hoje, comunicam-se entre si: seja interligando andares diferentes de um mesmo prédio ou filiais localizadas em diferentes continentes. Quando se fala em comunidade global estamos nos referindo à possibilidade tecnológica de trocar informação com alguém, ou até mesmo com uma máquina, localizado no outro lado do mundo em questão de poucos minutos ou até segundos, e isso hoje é uma realidade. As redes globais de informação estão mudando o comportamento e atitude das pessoas, justamente naqueles lugares nos quais normalmente nos sentimos mais seguros: nosso trabalho e nossa casa.

Definição

Basicamente, uma rede de informação é um sistema que permite a comunicação entre pontos distintos, ou seja, um sistema que permite a troca de informações. Os componentes básicos de uma rede de informação (ou rede de informações) são um emissor (origem da informação), o meio através da qual a informação trafega (o canal), um receptor (o destino da informação) e finalmente a mensagem, que nada mais é do que a informação em si. Um exemplo comum seria uma pessoa falando no telefone com outra pessoa: O emissor seria quem está falando, o canal seria a linha telefônica, o receptor a pessoa que está ouvindo e a mensagem seria a própria mensagem que está sendo comunicada. Ao longo dos anos as ferramentas para a comunicação de dados foram evoluindo

RC

gradativamente, de modo a tornar a troca de informações rápida, fácil e mais eficiente.

Uma rede de computadores baseia-se nos princípios de uma rede de informações, implementando técnicas de hardware e software de modo a torná-la efetivamente mais dinâmica, para atender às necessidades que o mundo moderno impõe. Redes de computadores incluem todos os equipamentos eletrônicos necessários à interconexão de dispositivos, tais como microcomputadores e impressoras. Esses dispositivos que se comunicam entre si são chamados de nós, estações de trabalho, pontos ou simplesmente dispositivos de rede. Dois computadores, ou nós, seria o número mínimo de dispositivos necessários para formarmos uma rede. O número máximo não é predeterminado, teoricamente todos os computadores do mundo poderiam estar interligados.

Quanto à natureza podemos ter dois tipos de redes de computadores: cliente-servidor (client-server) e ponto-a-ponto (peer-to-peer). Na rede cliente-servidor uma máquina, ou um pequeno grupo de máquinas, centraliza os serviços da rede oferecidos à demais estações, tais como aplicativos e filas de impressão. As máquinas que requerem esses serviços são chamadas de clientes, e as máquinas que os fornecem são chamadas de servidores. Na rede ponto-a-ponto não existem servidores, todas as estações compartilham seus recursos mutuamente. A grande desvantagem que as redes ponto-a-ponto oferecem com relação às redes cliente-servidor é a dificuldade de gerenciar os seus serviços, já que não existe um sistema operacional que centralize a administração da rede. Também não é possível estendê-las excessivamente, já que um número elevado de nós sobrecarregaria o fluxo de dados, tornando-a lenta e por conseguinte ineficaz. Aos poucos as empresas estão substituindo suas redes ponto-a-ponto por redes cliente-servidor, e o número de redes ponto-a-ponto está diminuindo.

O principal motivo para a implementação de redes de computadores nas organizações, sejam elas simples escritórios ou empresas de âmbito internacional, resume-se em uma única palavra: dinheiro! Os custos reduzidos com a automatização dos processos mediante a utilização de redes é realmente muito significativo. Por exemplo, se uma empresa pudesse optar entre adquirir cem impressoras independentes ou apenas dez compartilhadas, sem dúvida alguma a segunda opção seria mais interessante. Também é preferível adquirir o direito de compartilhar um aplicativo (chamados de

RC

pacotes para vários usuários) entre um número predeterminado de usuários, do que adquirir várias cópias unitárias.

Tipos

Quanto à área de atuação geográfica podemos classificar as redes de computadores em três tipos: Redes Locais (LAN - Local Area Network), Redes Metropolitanas (MAN - Metropolitan Area Network) e Redes Remotas (WAN - Wide Area Network). Redes que ocupam um pequeno espaço geográfico são chamadas de redes locais; redes que ocupam uma vasta área são chamadas de redes metropolitanas (este termo é pouco utilizado) ou redes remotas.

Redes Locais

Este é o tipo mais comum de rede de computadores. Redes que interligam salas em um edifício comercial ou prédios de um campus universitário são exemplos de redes locais. Até mesmo quem tem dois computadores ligados em sua própria casa possui uma rede local. No princípio a maioria das redes locais era ponto-a-ponto, e duas redes locais normalmente não eram interligadas. Com a expansão das redes cliente-servidor, foi viabilizado a interconexão de diferentes redes locais, dando origem às redes metropolitanas e redes remotas. As redes locais caracterizam-se por altas taxas de transferência, baixo índice de erros e custo relativamente pequeno.

Redes Metropolitanas

O conceito de rede metropolitana pode parecer um tanto quanto confuso, e algumas vezes há uma certa confusão no que diz respeito às diferenças existentes entre uma MAN e uma rede remota. Na verdade, a definição para este tipo de rede de computadores surgiu depois das LAN e WANS. Ficou estabelecido que redes metropolitanas, como o próprio nome já diz, são aquelas que estão compreendidas numa área metropolitana, como as diferentes regiões de toda uma cidade. Normalmente redes metropolitanas são constituídas de equipamentos sofisticados, com um custo alto para a sua implementação e manutenção, que compõem a infra-estrutura

RC

necessária para o tráfego de som, vídeo e gráficos de alta resolução. Por serem comuns nos grandes centros urbanos e econômicos, as rede metropolitanas são o primeiro passo para o desenvolvimento de redes remotas.

Redes Remotas

Redes remotas são aquelas que cobrem regiões extensas. Na verdade redes remotas são um agrupamento de várias redes locais e/ou metropolitanas, interligando estados, países ou continentes. Tecnologias que envolvem custos elevados são necessárias, tais como cabeamento submarino, transmissão por satélite ou sistemas terrestres de microondas. As linhas telefônicas, uma tecnologia que não é tão sofisticada e nem possui um custo muito elevado, também são amplamente empregadas no tráfego de informações em redes remotas. Este tipo de rede caracteriza-se por apresentar uma maior incidência de erros, e também são extremamente lentas. Novas técnicas estão surgindo de modo a subverter esses problemas, mas a sua implementação depende de toda uma série de fatores, logo o processo é gradativo. Um exemplo de rede remota muito popular é a Internet, que possibilita a comunicação entre pessoas de lugares totalmente diferentes.

Aplicações Utilizadas em Redes de Computadores

Basicamente existem dois tipos de aplicações em redes de computadores: Aplicações de Rede Residentes (Stand Alone Applications) e Aplicações de Rede, ou Aplicações Puramente para Redes (Pure Network Applications). Aplicações residentes são aquelas ferramentas que, por cobrirem tarefas comuns ao cotidiano, normalmente estão presentes nas redes de informação de uma determinada empresa. No entanto, tais aplicações não foram desenvolvidas com o propósito exclusivo de servirem à um ambiente multiusuário, podendo facilmente ser encontradas nos computadores independentes. Exemplos de aplicações residentes são os processadores de texto e planilhas eletrônicas. Quando aplicações residentes são adaptadas para rodarem numa rede cliente-servidor (em redes ponto-a-ponto todas as aplicações são executadas da mesma forma que o seriam se estivessem numa máquina particular) elas costumam ser quebradas e duas partes: a primeira, que envolve a interface com o usuário e consequentemente requer menos poder de

professor Bruno Tavares de Souza

RC

processamento, fica na estação (ou cliente). A segunda parte, composta de rotinas pesadas como a varredura de dados, fica localizada no servidor. Desta forma, o rendimento obtido é muitas vezes superior ao de programas instalados em uma máquina comum. Vários são os motivos que levam ao processo constante de adaptação de aplicativos monousuário para ambientes multiusuário, entre os quais podemos citar a facilidade de adaptação, compartilhamento de arquivos, e melhor relação custo x benefício.

Aplicações de rede são sistemas desenvolvidos com a finalidade de executar tarefas típicas de um ambiente multiusuário, logo não faz sentido instalar um desses programas numa máquina que não está conectada à uma rede. Essas tarefas necessitam de um prévio conhecimento, por parte do usuário, das estruturas operacionais básicas de uma rede de computadores, logo não é tão simples utilizar uma aplicação de rede quanto o seria com uma aplicação residente, mesmo porque aplicações de rede residentes são similares às suas versões monousuário: de uso simples e intuitivo, cujos processos relacionados com a troca de informações entre uma estação e outra quase sempre são transparentes para quem o está utilizando. São exemplos de aplicações puramente para redes de computadores:

Correio Eletrônico

Aplicações de correio eletrônico são a forma mais simples e comum de comunicação interdepartamental, que possibilitam a troca de mensagens entre usuários da rede. As mensagens enviadas ficam residentes numa área selecionada de um dos volumes (discos rígidos) do servidor chamada de caixa postal, e lá permanecem até que o destinatário as recolha para a sua própria estação.

Transferência de Arquivos

Este é um tipo de aplicação importantíssimo. Ele permite a troca de arquivos entre os diferentes nós de uma rede, como por exemplo de um PC para outro. As vantagens oferecidas por este recurso são muitas, e vão depender da situação que o trabalho das pessoas conectadas à rede vai demonstrar. Entretanto, a principal vantagem oferecida é óbvia: um grupo que esteja trabalhando em cima de um mesmo projeto, seja ele uma planilha de custos ou o desenvolvimento de um sistema, poderão compartilhar os resultados e atualizações dinamicamente, sem a necessidade de reuniões

professor Bruno Tavares de Souza

R C

constantes ou encontros diretos. É importante frisar que a abrangência de uma rede pode englobar várias plataformas, e que, nestes casos, a comunicação entre estações diferentes requer a tradução do formato daquele arquivo do computador de origem para o de destino.

Emulação de Terminal

Os emuladores de terminal constituem uma das aplicações de rede mais antigas utilizadas hoje em dia, e remontam ao tempo em que os terminais burros foram sendo substituídos por microcomputadores. Nessa época, muitos usuários já estavam habituados a utilizar os aplicativos que ficavam residentes no servidor, e com a popularização dos PCs tornou-se necessário prepará-los para reconhecer essas aplicações como se os mesmos fossem terminais atados ao mainframe. Desta forma, os emuladores possibilitam aos usuários da rede tirar proveito de ambos os recursos: aplicações multiusuário e aplicações residentes na sua própria estação.

Aplicações para Grupo de Trabalho (Groupware)

Aplicações que possibilitam a automatização dos processos relacionados com a administração dos serviços da empresa são importantes, pois otimizam tarefas repetitivas, que consomem muito tempo dos gerentes e executivos. O aspecto financeiro, como sempre, pesa muito na hora de optar por esses aplicativos, já que ao se economizar tempo também economizamos dinheiro. Podemos citar como exemplos dessas tarefas chamadas telefônicas, coordenação de calendários, encontros a serem marcados e outros. Muitas vezes aplicações residentes e outras aplicações de rede acabam por fazer parte desses pacotes de aplicativos. Aplicações de Groupware podem incorporar programas de correio eletrônico e gerenciadores de informação (agendas eletrônicas) de modo a facilitar a organização dos compromissos típicos daquele pessoal que trabalha em ambientes que envolvam muitos escritórios e departamentos.

Arquitetura de Redes de Computadores Baseada em Camadas

RC

As redes de computadores são sistemas muito complexos, e esta complexidade é causada em parte pelas diferenças encontradas nas diversas plataformas que podem compor uma mesma rede. Tomemos como exemplo a própria Internet: são milhões de usuários espalhados pelo mundo, usuários estes que podem estar utilizando uma máquina da Apple, uma estação baseada em Windows ou um servidor Unix. Máquinas que podem ser rápidas, ou lentas, que empregam tecnologias diferentes. São várias as possibilidades, e é por isso que fica tão difícil estabelecer regras que determinem como máquinas tão distintas em funcionamento podem trocar informações entre si. Desta forma, a arquitetura de uma rede é subdividida em camadas menores, facilitando a compreensão individual de cada uma. Camadas compreendem conjuntos de funções que se relacionam diretamente, ou seja, processos semelhantes.

Analogamente, vamos imaginar como é realizada a produção industrial de veículos automotores. No princípio, as técnicas utilizadas para a produção de um carro eram bem simples, e quase todos os seus componentes eram desenvolvidos na mesma fábrica. Com o aumento das marcas e modelos, a tecnologia foi gradativamente evoluindo, e aqueles componentes individuais foram sendo aperfeiçoados de tal modo que uma única equipe de projetistas não tinha mais condições de cuidar do veículo todo. Funções foram sendo atribuídas a grupos diferentes: um grupo cuidaria da parte elétrica, outro ficaria com determinado componente do motor, e assim por diante. As pessoas que lidavam com a parte elétrica se especializavam nessa área, facilitando a resolução de problemas. Todos os componentes elétricos do veículo a ser produzido trabalhavam de forma semelhante, funcionavam baseados em princípios elétricos. E claro, o objetivo maior é integrar todos esses subsistemas (motor, parte elétrica, carburação, etc) de modo a tornar possível a utilização do veículo. A arquitetura de uma rede funciona da mesma forma, camadas (ou módulos) interagem uns com os outros para possibilitar o tráfego de informações entre diferentes nós. Os problemas que surgem quando o funcionamento de uma estação difere do funcionamento de outra ficam mais fáceis de serem resolvidos quando especialistas de cada plataforma, baseados num modelo de camadas comum para todos, implementam técnicas de hardware e software adequadas ao seu escopo. As camadas mais altas estão próximas do usuário, e as camadas de nível mais baixo estão próximas do meio físico pelo qual as informações trafegam.

Outra vantagem que os modelos baseados em camadas oferecem é com relação à maior compatibilidade oferecida. Se as soluções para cada plataforma fossem baseadas num modelo integral, sem subdivisões, provavelmente elas iriam se distanciar com mais

professor Bruno Tavares de Souza

RC

facilidade. Agora, como essas soluções são baseadas em componentes menores, os problemas que surgem são detectados com mais facilidade pela maioria dos projetistas. Logo, as diferentes soluções encontradas para esses problemas passam a ser muito semelhantes, permitindo uma maior compatibilidade.

O Modelo de Referência OSI (Open Systems Interconnection – Sistemas Abertos de Interconexão)

Um modelo de referência nada mais é do que uma arquitetura estabelecida de modo a possibilitar uma maior compatibilidade entre diferentes plataformas. No caso do OSI (criado pela ISO – International Organization for Standardization), que divide a comunicação das redes em camadas, a preocupação surgiu com a necessidade de integração entre diferentes redes de computadores. Deve ser deixado bem claro que um modelo de referência estabelece um padrão de direito, abrangendo funções gerais, não se prendendo à especificações de implementação. Não são todos os sistemas de rede que o utilizam exatamente da forma como ele é oferecido, na verdade a maioria dos protocolos de implementação adotam um menor número de camadas, agrupando camadas redundantes.

O modelo OSI é dividido em sete camadas diferentes. Toda informação a ser enviada parte da camada mais alta ("Aplicação", camada número sete), e segue pelas demais camadas que incluem, uma a uma, novas informações de controle. Essas informações de controle é que são responsáveis pela maior compatibilização entre máquinas de tecnologias diferentes, e são encaminhadas juntamente com a informação real para as demais estações da rede. A camada mais baixa determina o meio físico através do qual a mensagem irá trafegar, logo percebemos que o modelo OSI, assim como outros, especifica padrões de software e hardware a serem implementados pelos fabricantes. Quando a mensagem atinge o seu destino, novamente ela passa através das mesmas camadas, só que inversamente até chegar ao nível mais alto.

Cada camada possui tarefas específicas a serem realizadas, incluindo informações de controle à mensagem de tal forma que o nó responsável pelo seu envio, e consequentemente o nó que irá recebê-la, saiba como manipulá-la. Essas informações de controle são armazenadas numa área da mensagem chamada de cabeçalho

professor Bruno Tavares de Souza

RC

(header), e podem incluir informações de endereçamento, controles que bloqueiam a sobrecarga que estações mais lentas eventualmente sofreriam ao tentar receber mensagens provenientes de estações mais rápidas, informações para controle e depuração de erros e outras mais. É importante deixar duas coisas bem claras: uma camada somente irá se comunicar com as suas camadas adjacentes, e toda informação de controle armazenada em uma camada do nó que está enviando a mensagem será utilizada na decodificação da mensagem na camada equivalente do nó que está recebendo (logo, toda informação de controle armazenada durante a passagem da mensagem na camada cinco somente será reconhecida pelo nó destinatário quando aquela estiver atravessando a camada cinco do mesmo) .

Muitos protocolos implementados pelos fabricantes não utilizam todas as sete camadas do modelo OSI, o que não impede o funcionamento correto da rede. Um determinado fabricante pode considerar desnecessário aplicar, à nível de software, toda uma série de testes na verificação e depuração de possíveis erros por considerar o meio físico de comunicação suficientemente confiável. Isto eliminaria alguma funcionalidade, mas iria tornar o tráfego da mensagem mais rápido. Normalmente, as camadas do modelo OSI são agrupadas em três grupos: camada de Aplicação (responsável pela interface com o usuário), que corresponde à camada sete; camadas para Decodificação (responsáveis pela "tradução" da linguagem humana em uma linguagem comprehensível pela máquina, onde as informações de controle são acrescentadas à informação real), que englobam as camadas seis, cinco, quatro e três; e finalmente as camadas que providenciam a Conexão Física, que são as de número dois e um. Note que o sentido parte do emissor (camadas mais altas) para o receptor (camadas mais baixas).

Meios Físicos ou Canais de Comunicação

Como já foi dito anteriormente, o canal nada mais é do que o meio físico através do qual a informação trafega de um ponto até outro. A partir do modelo OSI desenvolvido pela ISO os fabricantes implementam tecnologias de comunicação com base nas camadas mais baixas (camada dois e um). Essas tecnologias classificam os meios físicos, quanto à sua natureza, em dois tipos: Encapsulados e Não Encapsulados. Este último é o meio mais comum, e o melhor exemplo é o próprio ar propagando a informação na forma de ondas

professor Bruno Tavares de Souza

RC

eletromagnéticas (como no caso da fala, que utiliza o ar para emitir som na forma de ondas sonoras). Outros exemplos de meios não encapsulados são a água, o solo e o espaço sideral, mas estes meios ainda são pouco explorados pelo ser humano. Os meios de transmissão encapsulados são aqueles no qual a informação trafega sem contato com o ar, estando atada às propriedades físicas do mesmo.

Sistemas Baseados em Meios Físicos Encapsulados

Cabo Coaxial

O cabo coaxial é constituído de dois condutores dispostos axialmente (na forma de eixo), separados entre si e envoltos por material isolante. O condutor interno, mais rígido, é feito de cobre e pode ser torcido ou sólido (o condutor sólido é mais indicado em redes locais, já que os dados fluem com mais facilidade num meio homogêneo). O condutor externo é uma malha metálica que, além de atuar como a segunda metade do circuito elétrico, também protege o condutor interno contra interferências externas (campos eletromagnéticos estranhos). Quando esta malha externa é feita de alumínio o cabo coaxial é dito cabo coaxial grosso (especificação RG-213 A/U), ou de banda larga, pois possui uma resistência de 75 ohms, transmitindo dados numa velocidade de até 10 mbps (megabits por segundo) à freqüência de 10 ghz (gigahertz). Os cabos coaxiais de banda larga obedecem ao padrão 10Base5, e são muito utilizados em circuitos internos de TV. Este tipo de cabo é indicado para instalações externas, como aquelas que fazem a conexão de redes de computadores situadas em diferentes prédios num mesmo campus universitário. Se a malha externa for de cobre a resistência obtida é de 50 ohms, o que permite a transmissão de dados à velocidade de 10 mbps a uma freqüência de 2 ghz. Este cabo é chamado de cabo coaxial fino (especificação RG-58 A/U), ou cabo coaxial de banda base. Este tipo de cabo obedece ao padrão 10Base2, sendo utilizado em redes padrão Ethernet com baixo escopo de atuação (veremos os diferentes padrões de mercado mais tarde).

Existem cinco tipos de conectores para serem utilizados com cabos coaxiais em redes de computadores: conector BNC, padrão macho para as pontas do cabo coaxial e fêmea para as placas de rede (que, ao serem instaladas, atrelam as estações de trabalho à rede); conector BNC tipo "T", liga dois conectores BNC macho (dois segmentos de cabo coaxial, cada um com destino a uma outra

professor Bruno Tavares de Souza

RC

estaçao) ao conector BNC fêmea da placa de rede, logo é formado de duas entradas (BNC fêmea) e uma saída (BNC macho); conector BNC tipo "I", que serve para ligar as extremidades de dois segmentos de cabo coaxial, muito utilizado para aumentar a distância entre um nó e outro; conector Transceiver (ou conector "Vampiro") que serve para ligar um cabo coaxial grosso à estação; e finalmente conector BNC de terminação, ou simplesmente terminador, que deve ser colocado na extremidade final localizada no último segmento de rede. Uma atenção especial deve ser dada à este último conector. Numa rede padrão Ethernet os dados trafegam serialmente através de uma linha única de dados, linha esta hora formada pelos segmentos de cabo coaxial, hora pelos conectores que fazem a ligação destes com as placas de rede ou entre si. De modo a evitar que um sinal seja refletido de volta ao se chocar na extremidade da rede, utilizamos os terminadores, que "absorvem" os sinais para um perfeito casamento de impedância. Esses terminadores podem ser de 50 ou 75 ohms, variando de acordo com o cabeamento. Os cabos coaxiais possibilitam uma taxa de transferência de até 10 mbps, e se forem instalados adequadamente oferecem uma boa resistência contra interferências externas, ou ruídos (EMI - Eletromagnetic Interference, Interferência Eletromagnética; RFI - Radiofrequency Interference, Interferência de Radiofreqüência). Não obstante, o seu processo de instalação é mais complicado e também tem custo elevado.

Cabo de Par Trançado

O cabo de par trançado é formado de pares de fios entrelaçados, separados por material isolante, que normalmente são recobertos por uma proteção de PVC (Poly Vinyl Chloride). Cada par constitui um condutor positivo (normalmente um fio de cor laranja, verde, azul ou marrom) e negativo (normalmente de cor branca), que ao serem dispostos como estão geram um campo eletromagnético que faz o papel de barreira contra interferências externas ("Cross Talk"), reduzindo a diafonia (ruídos provocados pelos sinais elétricos que trafegam em sentidos opostos). Muitos tipos de cabo de par trançado, como os cabos telefônicos, não são protegidos por uma blindagem externa. Esses cabos são chamados de Cabos de Par Trançado Sem Blindagem (UTP - Unshielded Twisted Pair), mas não devem ser utilizados em redes de computadores. Como já foi dito, a maioria dos Cabos de Par Trançado Blindado (STP - Shielded Twisted Pair) utilizam um encapsulamento de PVC , o que, no entanto, não é indicado em instalações próximas à dutos de ar, já que este material emite gases tóxicos quando é inflamado (nesses casos outro material deve ser utilizado, normalmente teflon). Em redes de computadores encontramos três tipos de cabos de par trançado,

RC

que são classificados quanto à sua amperagem: nível 3 (para redes de até 10 mbps, padrão 10BaseT para redes Ethernet), nível 4 (16 mbps, padrão 16BaseT, pouco utilizado) e nível 5 (100 mbps, padrão 100BaseT). O primeiro é mais comum, sendo o mais indicado para a maioria das instalações, como LANs que interligam salas de aula e escritórios.

O conector utilizado em redes de computadores baseadas no cabo de par trançado é o RJ-45 (similar ao conector RJ-11, de aparelhos telefônicos), macho para os segmentos de par trançado e fêmea para as placas de rede. Este conector possui oito pinos internos: T2, R2, T3, R1, T1, R3, T4, R4, sendo que em redes que operam com uma taxa de até 10 mbps são utilizados os conectores T2, R2, T3 e R3, logo será necessário um cabo com dois pares de fios (nível 3). Em redes de 100 mbps utilizamos os oito conectores, e quatro pares de fios (nível 5). O cabo de par trançado é economicamente mais viável do que o cabo coaxial, e sua instalação também é mais fácil. Essas vantagens associadas a sua predisposição contra ruídos internos e/ou externos torna cada vez menos popular a implementação de cabos coaxiais nas redes locais, principalmente em redes padrão Ethernet (a qualidade de transmissão depende muito do material condutor, sendo o cobre o mais indicado). Redes cliente-servidor já não utilizam cabos coaxiais, mesmo porque HUBs com conectores BNC fêmea estão gradativamente saindo do mercado. O HUB é um equipamento necessário em redes cliente-servidor, e mesmo em redes ponto-a-ponto baseadas em cabos de par trançado, que concentra todos os segmentos da rede. É por isso que não existem conectores de terminação para este tipo de cabo, cabos coaxiais necessariamente não precisam de um concentrador, os de par trançado sim.

Cabo de Fibra Óptica

O cabo de fibra óptica possui um filamento condutor interno feito de substância derivada de material vítreo ou plástico, revestida por um material com baixo índice refratário, normalmente silicone ou acrilato. Podemos ter um agrupamento de fibras envoltas por gel, encapsuladas num revestimento secundário de náilon e, finalmente, uma capa externa de PVC. Como pode ser notado, a tecnologia empregada em cabos de fibra óptica é muito complicada se comparada com a que é empregada em cabos coaxiais. Seu custo de produção ainda é elevado, e sua instalação também requer a utilização de equipamentos sofisticados. Por isso, a fibra óptica não é tão empregada em redes locais como o cabo coaxial ou o cabo de par trançado. Dois problemas oferecidos: a conexão com a fibra

RC

óptica é ponto-a-ponto, não podemos "espetar" um novo segmento de rede à um que já existe, como se faz com cabos coaxiais; o cabo de fibra óptica também não pode apresentar uma curvatura intensa, primeiro porque ele quebra com facilidade, e segundo porque o sinal emitido poderia chocar-se com a superfície do revestimento e ser refletido, interferindo na transmissão.

Os dados trafegam pela fibra óptica, como o próprio nome indica, na forma de sinais luminosos que são gerados ou por tecnologia laser (Light Amplification by Stimulated Emission of Radiation) ou por um diodo emissor de luz (LED - Light Emissor Diode). Tirando o alto custo e a dificuldade de instalação (os repetidores de sinal devem ser colocados numa faixa que pode ir de dois a cem quilômetros, de acordo com as especificações) a fibra óptica apresenta, na prática, uma série de vantagens com relação ao cabo coaxial e cabo de par trançado. Primeiro a velocidade de transmissão, conseguimos taxas de até 16 tbps (terabits por segundo, ou 16 trilhões de bits por segundo), operando à freqüências de até 800 terahertz. Outra vantagem é a economia de espaço (nesse aspecto a fibra óptica facilita o processo de instalação). Um cabo de um centímetro de diâmetro pode comportar 144 fibras, possibilitando até oito mil conversações simultâneas em ambos os sentidos de transmissão. Por último, a fibra óptica é totalmente imune à variações eletromagnéticas externas, o que torna a transmissão altamente confiável. Ambientes sujeitos a uma variação extrema de ruídos EMI e/ou RFI requerem a implementação de redes de computadores baseadas em fibra óptica. A tendência atual é que nos próximos anos ocorra uma queda brusca de preços nas tecnologias envolvidas com este tipo de cabeamento.

Sistemas Baseados em Meios Físicos Não Encapsulados

Microondas

A comunicação através de sistemas de microondas existe sob duas formas: sistemas terrestres, e sistemas baseados em satélites. Embora apresentem um funcionamento similar, essas duas formas possuem características próprias e devem ser aplicadas em situações distintas. Na primeira o fluxo do sinal dá-se através de antenas convencionais, sendo muito indicado na troca de informações entre dois ou mais edifícios nos casos em que a instalação de cabos seria problemática ou dispendiosa. Antenas também são muito empregadas em regiões remotas, não só com redes de computadores como também na transmissão de canais de telefone

professor Bruno Tavares de Souza

RC

e/ou televisão, através de áreas inóspitas como desertos e regiões montanhosas. Antenas comuns não são eficientes se a distância entre o emissor e o receptor for muito extensa, chuva, neblina e outros desvios do tempo tornam-se um problema já que há uma grande chance do sinal transmitido atenuar-se. A transmissão por satélite é feita a partir de antenas parabólicas, localizadas no solo e no próprio satélite, possibilitando um vasto escopo de atuação. Os sistemas de transmissão por satélite são indicados no tráfego intercontinental de dados, ou até mesmo em regiões muito distantes como um país e outro. A conexão por satélite exige modernos sistemas espaciais, ela introduz longos períodos de transmissão adequados às distâncias pela quais o sinal deverá trafegar. Por isso, este tipo de tecnologia permite comunicação com regiões remotas. Ela requer uma licença especial.

Laser

Um estreito feixe de luz (normalmente luz infravermelha) é modulado em pulsos para transmitir dados na forma de bits. A transmissão a laser é mais rápida e direcionável do que a transmissão por microondas, mas tem um escopo de atuação limitado e também é relativamente sujeita às variações do tempo (por isso, a instalação dos equipamentos deve seguir determinadas regras). O laser também apresenta o problema de ser potencialmente prejudicial à nossa saúde (uma vez que emite um baixo nível de radiação), logo os equipamentos de transmissão e recepção devem ser encapsulados de acordo com as normas de segurança, também estando o seu uso regulamentado pela lei.

Raios Infravermelho

Constituída de um sistema simples, e consequentemente de baixo custo, a transmissão de dados através de raios infravermelho apresenta um sério problema: o sinal é obstruído com facilidade por superfícies sólidas, barreiras essas que podem ser desde uma parede (dificultando a comunicação entre salas) e, quando o transceiver é mal posicionado, até mesmo o corpo de alguém. O alcance dos raios infravermelho também é muito pequeno, além do sinal ser facilmente atenuado por condições atmosféricas desfavoráveis. É por esses fatores que este tipo de tecnologia praticamente não é utilizado, embora possibilite altas taxas de transmissão.

RC

Rádio

Sistemas de radiofonia não são muito utilizados em redes de computadores, mas se apresentam como uma alternativa viável em lugares afastados dos grandes centros, já que o seu custo de implementação é inexpressivo se comparado com os modernos recursos oferecidos pelos satélites. As estações de transmissão e/ou recepção aplicam determinados tipos de freqüência de acordo com as necessidades impostas: sistemas globais usam ondas curtas, que são propagadas a longas distâncias, e sistemas locais normalmente se comunicam utilizando sinais de VHF ou UHF.

Topologias de Rede

Topologia de rede é a forma através da qual ela se apresenta fisicamente, ou seja, com os nós estão dispostos. A topologia de uma rede descreve como o é o "layout" do meio através do qual há o tráfego de informações, e também como os dispositivos estão conectados a ele. São várias as topologias existentes, podemos citar o Barramento, Estrela, Anel, Malha, e topologias Híbridas. Um conceito um pouco mais amplo abrange as diferenças entre topologias físicas e topologias lógicas, mas veremos isto depois.

Barramento

Esta topologia é caracterizada por uma linha única de dados (o fluxo é serial), finalizada por dois terminadores (casamento de impedância), na qual atrelamos cada nó de tal forma que toda mensagem enviada passa por todas as estações, sendo reconhecida somente por aquela que está cumprindo o papel de destinatário (estação endereçada). Nas redes baseadas nesta topologia não existe um elemento central, todos os pontos atuam de maneira igual, algumas vezes assumindo um papel ativo outras vezes assumindo um papel passivo.

As redes locais Ethernet ponto-a-ponto usam essa topologia, entretanto ela apresenta uma série de desvantagens com relação às demais topologias. Por exemplo, como todas as estações estão atreladas a uma linha única (normalmente um cabo coaxial), o

professor Bruno Tavares de Souza

RC

número de conexões é muito grande, proporcional ao número de nós. Logo, se a rede estiver apresentando um problema físico, são grandes as chances deste problema ser proveniente de uma dessas conexões (conectores e placas de rede) ou até mesmo de um segmento de cabo. A maior dificuldade está em localizar o defeito, já que poderão existir vários segmentos de rede. Outro problema existente é o fato de que, já que a troca de informações dá-se linear e serialmente, quando ocorrem tais defeitos toda a rede fica comprometida, e ela pára de funcionar. A única vantagem que este tipo de rede pode oferecer é o baixo custo, sendo ideal quando implementada em lugares pequenos.

Estrela

A topologia estrela é caracterizada por um elemento central que "gerencia" o fluxo de dados da rede, estando diretamente conectado (ponto-a-ponto) a cada nó, daí surgiu a designação "Estrela". Toda informação enviada de um nó para outro deverá obrigatoriamente passar pelo ponto central, ou concentrador, tornando o processo muito mais eficaz, já que os dados não irão passar por todas as estações. O concentrador encarrega-se de rotear o sinal para as estações solicitadas, economizando tempo. Existem também redes estrela com conexão passiva (similar ao barramento), na qual o elemento central nada mais é do que uma peça mecânica que atrela os "braços" entre si, não interferindo no sinal que flui por todos os nós, da mesma forma que o faria em redes com topologia barramento. Mas este tipo de conexão passiva é mais comum em redes ponto-a-ponto lineares, sendo muito pouco utilizado já que os dispositivos concentradores (HUBs, Multiportas, Pontes e outros) não apresentam um custo tão elevado se levarmos em consideração as vantagens que são oferecidas.

Uma vez que o sinal sempre será conduzido para um elemento central, e a partir deste para o seu destino, as informações trafegam bem mais rápido do que numa rede barramento. Essa é a melhor vantagem oferecida por uma rede estrela, sendo a mesma ideal para redes em que imperam o uso de informações "pesadas", como a troca de registros de uma grande base de dados compartilhada, som, gráficos de alta resolução e vídeo. O custo de instalação de uma rede estrela também é elevado, quanto maior for a distância entre um nó e o concentrador maior será o investimento, já que cada "braço" é representado por um segmento de cabo coaxial, par trançado ou fibra óptica. Mas as vantagens oferecidas na prática são muitas: a instalação de novos segmentos não requer muito trabalho, a localização de problemas fica mais

RC

fácil; a rede estrela é mais fácil de dispor fisicamente mediante as dificuldades encontradas no ambiente de trabalho (no momento de instalação, expansão, e mesmo se a rede tiver de ser deslocada); se um problema ocorrer num segmento os outros permaneceram em atividade; e, como já foi dito, a rede estrela geralmente oferece taxas de transmissão maiores. Toda rede cliente-servidor, como pode ser notado, segue a topologia estrela.

Malha

Nesta topologia todos os nós estão atados a todos os outros nós, como se estivessem entrelaçados. Já que são vários os caminhos possíveis por onde a informação pode fluir da origem até o destino, este tipo de rede está menos sujeita a erros de transmissão, o tempo de espera é reduzido, e eventuais problemas não iriam interromper o funcionamento da rede. Um problema encontrado é com relação às interfaces de rede, já que para cada segmento de rede seria necessário instalar, numa mesma estação, um número equivalente de placas de rede. E, uma vez que cada estação envia sinais para todas as outras estações freqüentemente, a largura de banda da rede (em termos teóricos, a largura de banda de uma rede seria a taxa máxima de transferência que poderíamos obter com ela, mas a prática quase sempre mostra que esses índices são mais baixos do que o estimado) não é bem aproveitada. Como este tipo de topologia traz umas série de desvantagens para a maioria das instalações, ele é raramente usado.

Anel

Como o nome indica, uma rede anel é constituída de um circuito fechado, tal como a rede elétrica. A maior vantagem: não há atenuação do sinal transmitido, já que ele é regenerado cada vez que passa por uma estação (a atenuação é diretamente proporcional à distância entre um nó e outro). A maior desvantagem: todas as estações devem estar ativas e funcionando corretamente. A implementação mais comum da topologia estrela são as redes Token-Ring, de propriedade da IBM. Esta topologia oferece uma taxa de transmissão maior da que é oferecida nas redes de topologia barramento, veremos melhor o seu funcionamento na seção seguinte.

Híbrida

RC

Redes híbridas são aquelas que utilizam mais de uma das topologias citadas acima, e normalmente surgem da fusão de duas ou mais LANs entre si ou com MANs. Os serviços comerciais "on-line" e as redes públicas são exemplos de redes híbridas, como a Internet e até mesmo redes fechadas que estão sob o controle de organizações empresariais.

Métodos de Acesso

A maioria das redes de computadores utilizam um mesmo meio físico para a troca de informações entre uma estação e outra, já que desta forma há uma maior economia de recursos (menor custo com uso mais eficiente da largura de banda que o canal oferece). Há portanto o risco de duas ou mais estações transmitirem simultaneamente, acarretando em perda de dados já que os impulsos eletromagnéticos entrariam em choque tornando a mensagem irreconhecível. Para evitar tal tipo de problema foi estabelecido um conjunto de regras que asseguram que dois sinais não serão transmitidos ao mesmo tempo, controlando a forma pela qual os dispositivos irão acessar o canal, daí surgiu o nome métodos de acesso. São três os principais métodos de acesso: Contenção, Apuração ("Polling") e Passagem de Ficha.

Contenção

Nos sistemas de contenção mais antigos, as estações transmitiam toda vez que fosse solicitado, não havendo por conseguinte qualquer procedimento que regularizasse a ordem de transmissão entre os dispositivos que constituíam a rede. Embora apresentassem um funcionamento bem simples, tais métodos apresentavam um mal uso da capacidade total que os meios físicos normalmente oferecem. Com o aumento gradativo do fluxo de dados, o número de colisões cada vez mais freqüentes foi tornando o funcionamento correto da rede inviável.

Sistemas de contenção mais recentes, chamados de CSMA/CA (Carrier Sense, Multiple Access / Collision Avoidance - Percepção de Mensagem, Acesso Múltiplo / Evitando Colisões) são do tipo probalístico, já que não se sabe ao certo quanto tempo será necessário para que um sinal seja efetivamente transmitido. Neste

RC

método de contenção, mais eficiente que o anterior, a rede verifica a existência de sinal no meio físico (fazendo chamadas a cada estação transmissora). Se o sinal estiver presente, todos os dispositivos irão aguardar. Caso contrário, os dispositivos enviam um pequeno sinal (controle) para simular eventuais colisões, evitando a perda de informações importantes. Finalmente o dispositivo, uma vez liberado, poderá efetuar a transmissão. A largura de banda oferecida pelo canal passou a ser melhor aproveitada e, desde de que o funcionamento da rede permanecesse correto, o índice para a ocorrência de colisões é bem baixo. Duas desvantagens: este método gasta muito tempo tentando localizar e se recuperar de colisões.

Hoje em dia, os sistemas de contenção utilizados são os do tipo CSMA/CD (Carrier Sense, Multiple Access / Collision Detection – Percepção de Mensagem, Acesso Múltiplo / Detectando Colisões), mais rápidos na detecção de colisões. Diferentemente dos métodos antigos e dos métodos CSMA/CA, não há mais choque de dados importantes ou sinais de controle, economizando um tempo precioso e tornando o uso do canal mais eficiente. Este é o método de acesso mais comum, já que ele é implementado em redes Ethernet (topologia barramento).

Apuração ("Polling")

Neste método, um dispositivo de rede é designado para atuar como administrador de acesso ao canal, dispositivo este chamado de dispositivo primário, controlador ou mestre. O dispositivo primário verifica, numa ordem predeterminada, se as demais estações (chamadas de dispositivos secundários) possuem alguma informação para transmitir. O tempo disponível para cada dispositivo secundário transmitir em cada apuração é determinado por regras estabelecidas neste sistema. Mesmo quando os dispositivos secundários não possuem dados para transmitir, a largura de banda da rede ainda é utilizada no troca de mensagens decorrentes do processo de apuração. As colisões são completamente abolidas com este método de acesso, nas situações em que os dispositivos permanecem enviando informações regularmente a largura de banda é bem aproveitada. Normalmente este método de acesso é usado em conjunto com a topologia estrela, já que um HUB (normalmente o elemento central em redes deste tipo) sempre irá cumprir o papel de dispositivo mestre.

Passagem de "Ficha"

professor Bruno Tavares de Souza

RC

Similar ao método de apuração, a passagem de ficha apresenta como diferença básica o fato de não ter um elemento centralizador fixo, e por isso HUBs não são utilizados nessas redes. Diferentes dispositivos primários são designados na passagem, de um para outro, de uma entidade (não física) especial denominada "ficha" (token). O token atribui todos os direitos necessários ao controle de acesso ao meio físico para aquela estação que o mantém por aquele momento, cada dispositivo sabe de quem recebeu a ficha e para quem deverá enviá-la. Devido à sua estrutura, este método usa a topologia anel.

Assim como o método de apuração a passagem de ficha oferece um uso mais eficiente da largura de banda quando o fluxo de dados na rede é constante e também evita a ocorrência de colisões, no entanto a melhor vantagem oferecida é a descentralização do gerenciamento do acesso que os demais dispositivos irão ter ao canal. Se houver algum problema no funcionamento de um dispositivo existirão outros para cumprir o papel de dispositivo primário, não comprometendo todo o funcionamento da rede. Os padrões de rede mais populares que utilizam este método de acesso são o IEEE 802.5 (Token Ring) e IEEE 802.4 (IBM Token Bus).

Protocolos

Um protocolo nada mais é do que a implementação na prática de um modelo de referência, mas é evidente que por questões de interesse comercial nem sempre o modelo é seguido à risca pelos fabricantes, mesmo porque a maioria dos protocolos são criados com base na realidade do mercado. Instituições tradicionais como a ISO cuidam de formalizar a oficialização de um protocolo, e muitas vezes quando um mesmo tipo de produto é produzido por vários fabricantes diferentes espalhados pelo mundo perde-se muito tempo tentando estabelecer um padrão em comum que satisfaça a todos, e com redes de computadores não é diferente. Uma observação deve ser feita com relação aos fabricantes, pois podemos classificá-los em dois tipos: grandes empresas que lançam novas tecnologias no mercado (e consequentemente influenciam nas características de um protocolo); e empresas pequenas, que adquirem o direito de comercializar as tecnologias lançadas pelo grandes. Quanto maior for a disseminação de uma tecnologia (padrão de fato) mais fácil será torná-la um padrão oficialmente seguido pelo fabricantes "passivos" e

professor Bruno Tavares de Souza

R C

reconhecidos pelas organizações internacionais de controle (padrão de direito) .

Uma especificação de protocolo descreve formalmente com são as características físicas de uma rede de computadores (resistência e tipo de cabeamento, topologia, método de acesso, tamanho dos pacotes de informação etc). Uma implementação de protocolo nada mais é do que a implementação de um fabricante baseado num protocolo específico. Os fabricantes produzem suas próprias implementações, e quanto maior for a semelhança entre essas implementações maior será a compatibilidade oferecida. Como pode ser notado, esse processo de compatibilização depende das especificações de protocolo oficialmente divulgadas pelos organismos responsáveis.

Protocolos desenvolvidos a partir das camadas físicas do modelo OSI

IEEE 802.3/Ethernet

A especificação de protocolo IEEE 802.3 (IEEE - Institute of Electrical and Electronic Engineers) foi determinada com base no padrão Ethernet (sistema criado no final do anos setenta), por isso eles são tão semelhantes. Juntos, representam o mais popular dos protocolos de implementação. O padrão 10BaseT combina as vantagens oferecidas pelas altas taxas de transferência (10 mbps) e pela facilidade em se resolver problemas com o uso de topologia estrela.

Observação Importante: O padrão Ethernet utiliza a topologia barramento, por vezes chamada de topologia lógica já que a especificação IEEE 802.3 normalmente utiliza a topologia estrela. Na verdade, internamente ao HUB o fluxo dos dados dá-se de forma linear, tal como a topologia barramento. É por isso que a topologia estrela oferecida no padrão 10BaseT é dita topologia física (externamente).

- Ethernet

Topologia: Barramento

professor Bruno Tavares de Souza

R C

Método de Acesso: Contenção (CSMA/CD)

Canal: 50 ohms

Taxa de Transferência: 10 mbps

- IEEE 802.3:

Topologia: Várias

Método de Acesso: Contenção (CSMA/CD)

Canal: Vários

Taxa de Transferência: 1-10 mbps

IEEE 802.5/Token Ring

Por utilizarem o método de passagem de ficha, as redes 802.5 e Token Ring são chamadas de determinísticas, já que é possível calcular o tempo necessário para que a informação flua de um nó até outro. Essas redes também possuem alguns mecanismos para a resolução de erros que as redes do tipo Ethernet não possuem, além de evitar colisões.

- IEEE 802.5

Topologia: Não especificada

Método de Acesso: Token Passing

Canal: Não especificado

Taxa de Transferência: 1 ou 4 mbps

Nº máx. de nós / Anel: Não especificado

- IBM Token Ring

Topologia: Estrela / Anel

Método de Acesso: Token Passing

Canal: UTP ou FO

Taxa de Transferência: 4 ou 16 mbps

Nº máx. de nós / Anel: 260 / UTP

IEEE 802.2

professor Bruno Tavares de Souza

R C

Também chamado de LLC (Logical Link Control - Controle Lógico para Conexão), este protocolo roda em cima das especificações IEEE 802.3 e IEEE 802.5, determinando a metade superior da camada de Conexão de Dados (Data Link). Desta forma, o IEEE 802.2 providencia uma barreira que separa os mecanismos envolvidos com o meio físico da camada de Rede (Network), controlando o fluxo de dados e a detecção e correção de possíveis erros de transmissão.

Arcnet

O Arcnet (Attached Resource Computer Network - Redes de Computadores com Recursos Atados), voltado para pequenas redes de informação, foi desenvolvido nos anos setenta pela Datapoint Corporation, sendo portanto um dos protocolos que estão a mais tempo no mercado (juntamente com o Ethernet). Embora não seja muito popular, oferece uma série de vantagens com relação os anteriores, já que é fácil de instalar e configurar e não oferece um custo muito elevado, apresentando um baixo índice de erros. Muito flexível, ele oferece um recurso de auto-reconfiguração utilizado com o processo de passagem de ficha, através do qual os nós são inseridos e excluídos por si só. Os sistemas Arcnet atuais, denominados Arcnet Plus, oferecem taxas de transferência de até 20 mbps.

Topologia: Barramento / Estrela

Método de Acesso: Token Passing

Canal: Encapsulado

Taxa de Transferência: 4 mbps

Local Talk

De propriedade da Apple, o Local Talk também é voltado para pequenas redes de informação baseadas em estações Machintosh (todos os computador da Apple possuem uma interface de rede pré-instalada própria para o uso com o Apple Talk). Este protocolo possibilita taxas de transferência de até 230.4 kbps, muito baixa se comparada com as demais. No entanto, ele apresenta um algoritmos de endereçamento dinâmico, que ao invés de utilizar endereços fixos (determinados pelo fabricante da placa de rede no momento de sua manufatura), como em redes baseadas na série IEEE

professor Bruno Tavares de Souza

R C

802, designa um novo endereço para cada nó toda a vez que a rede é inicializada, diminuindo as chances de ocorrerem conflitos de endereçamento.

Topologia: Barramento

Método de Acesso: Contenção (CSMA/CA)

Canal: UTP

Taxa de Transferência: 230.4 kbps

e-o-f

SEGURANÇA EM REDES PRIVADAS

Autores:

ZAMITH JR., Antonio Carlos

Profissional autônomo, engenheiro eletrônico formado pela UERJ
Endereço: av. Maracanã 470 apto. 207, Maracanã - Rio de Janeiro (RJ)

SOUZA, Bruno Tavares

Professor, analista de sistemas formado pela Unigranrio
Endereço: rua Dionísio 63 apto. 206, Penha - Rio de Janeiro (RJ)

Abstract

This project synthetizes the basic issues related to private networks security, embodying the more usual kinds of attack and the main technics to defeat them: firewalls and cryptography. The first topic introduces the real threat originated from Internet growth, exposing the ways data can be represented through the network, and also lists five typical attacks. The second topic describes the layer oriented reference model for communication systems, comparing the seven-layers ISO/OSI model with the five-layers TCP/IP model (each layer corresponds to a set of familiar Internet protocols, most of them handled by firewalls). The third topic defines a firewall system, which includes the concepts of security policies and network security perimeter, exploring the most important features of each firewall generation (there's a brief description of the four generations most used). The fourth, and last, topic concludes the project by explaining the cryptography principles, relating its two basic methods, from which all the encryption systems are developed: symmetric encryption and public-key encryption.

Key-words: Computer networks, systems security, firewalls, cryptography.

Resumo

Este projeto sintetiza as questões básicas relacionadas com a segurança de redes privadas, englobando os tipos de ataque mais comuns e as técnicas principais para anulá-los: os sistemas de parede corta-fogo e a criptografia. O primeiro tópico introduz o leitor a cerca da ameaça real originada a partir do crescimento da Internet, expondo as formas pelas quais os dados podem ser representados através da rede, além de listar cinco tipos de ataques típicos. O segundo tópico descreve o modelo para sistemas de comunicação orientado a camadas, comparando o modelo de sete camadas ISO/OSI com o modelo de cinco camadas do TCP/IP (cada camada corresponde a um conjunto de protocolos familiares que são usados na Internet, a maioria gerenciada pelos sistemas de parede corta-fogo). O terceiro tópico define um sistema de parede corta-fogo, o que inclui os conceitos de políticas de segurança e perímetro de

segurança, explorando as características mais importantes de cada geração (há uma breve descrição das quatro gerações mais usadas). O quarto, e último, tópico conclui o projeto ao explicar os princípios da criptografia, relatando seus dois métodos básicos, a partir dos quais todos os sistemas de encriptação são desenvolvidos: criptografia simétrica e criptografia com chave pública.

Palavras-Chave:

Redes de computadores, segurança de sistemas, sistemas de parede corta-fogo, criptografia.

1. INTRODUÇÃO

Com a popularização do acesso à Internet nas empresas, processo iniciado em meados da década de 1990, a questão da segurança passou a ser tratada com mais critério pelos administradores de sistemas (é deles a responsabilidade maior de preservar a integridade dos dados corporativos). Se antes já era relativamente difícil manter a situação sob controle, há de se convir que com as “portas abertas” para um ambiente hostil, repleto de pessoas mal intencionadas, o problema tende a se agravar. Hoje, os projetistas gastam mais tempo para definir políticas de segurança e estabelecer mecanismos de proteção para as redes privadas, e mesmo assim há um certo grau de risco.

Quando uma rede privada é ligada à Internet, que abrange cerca de um milhão de redes (estimativa em 1997) [Comer 98] com todos os seus usuários e recursos, uma série de novos serviços são agregados, o que é muito bom em termos de produtividade. Por outro lado, ao mesmo tempo que diversifica as atividades do grupo ao disponibilizar novas ferramentas, além de facilitar o compartilhamento das informações, a Internet traz consigo o risco de acessos não autorizados por parte de estranhos.

De fato, este tipo de problema é cada vez mais comum, e pode acontecer até mesmo dentro da própria rede corporativa, a partir de alguma falha na administração. Como ponto de partida, temos uma pergunta-chave que dá início a formulação das políticas de segurança: O que deve ser feito para proteger os dados, isolando-os de eventuais ataques? O termo “ataque”, neste contexto, abrange qualquer tentativa de roubo, destruição, corrupção ou alteração dos dados, visando sabotagem de qualquer natureza.

1.1. Técnicas Mais Usadas para a Invasão de Sistemas

Quando se comunicam, os computadores que estão ligados a uma rede local quebram a informação em pequenas unidades, ou pacotes, que são transmitidas em série através do canal até o receptor, para então serem reagrupadas. Esta técnica é necessária em virtude da limitação de memória (“buffer”) que é usada em cada interface física de rede, nos processos de transmissão e recepção, e de outras características relacionadas com a política de alocação de recursos adotada pelo protocolo de comunicação. A princípio, esses pacotes são enviados sem qualquer tipo de encriptação, isto é, os dados são encapsulados em um datagrama (representação lógica do pacote, expresso em uma seqüência ordenada de bits) que segue um padrão aberto, podendo ser facilmente identificado nos casos de interceptação - os dados até poderiam estar codificados, mas a nível de aplicação. Percebe-se aqui a potencial vulnerabilidade

dos sistemas de comunicação, já que boa parte das técnicas de invasão baseia-se nesta característica.

Os dados confidenciais poderão estar fisicamente representados na estrutura da rede corporativa de duas maneiras: residindo em dispositivos de armazenamento primário ou secundário, como memória e unidades de disco rígido, ou em trânsito pelo canal de comunicação, na forma de pacotes. Esses dois estados apresentam múltiplas possibilidades de ataques internos e externos, mas agora vamos nos concentrar na segunda categoria, que engloba os ataques provenientes de usuários que invadem a rede privada através da Internet. As cinco técnicas mais usadas são a *Sondagem de Pacotes de Rede* (“Network Packet Sniffers”), *Simulação de Endereço IP de Origem* (“IP Spoofing”), *Ataques sobre Senhas* (“Password Attacks”), *Distribuição de Dados Sensíveis para Fontes Externas* (“Distribution of Sensitive Internal Information to External Sources”), *Sondagem em Pontos de Interconexão Intermediários* (“Man-in-the-Middle Attacks”), *Ataques a Nível de Aplicação* (“Application Layer Attacks”) e ataques a partir de *Recusa de Sistema* (“Denial-of-Service Attacks”).

1.1.1. Sondagem de Pacotes de Rede (“Network Packet Sniffers”)

O protocolo de comunicação determina como os pacotes são identificados e rotulados, de modo que o computador de destino possa verificar sua autenticidade, isto é, se aquele grupo de pacotes realmente foi endereçado para ele; o grande problema é que a especificação do TCP/IP está amplamente publicada na literatura e na própria Internet, e qualquer pessoa com conhecimentos em redes locais e desenvolvimento de sistemas é capaz de escrever um programa para sondar o conteúdo dos pacotes. Tais programas, chamados de Farejadores de Pacotes (“Packet Sniffers”), capturam todo o conteúdo que é recebido pela interface de rede, de modo a serem posteriormente processados (muitos protocolos da camada de Enlace, como o Ethernet e suas variações, operam com difusão de quadros). Pior, hoje em dia é comum encontrar este tipo de programa em vários sítios eletrônicos para distribuição de “freeware”, facilitando a vida dos invasores que não têm o perfil de desenvolvedor.

Mas, afinal de contas, quais informações poderiam ser interceptadas pelos Farejadores? Por exemplo, em redes baseadas na plataforma NT (Microsoft) os pacotes são transmitidos na forma de texto puro (ASCII), e dados como o nome de login e a senha dos usuários - que costumam ser usados como recursos de validação em várias aplicações comerciais - viajam pelo canal sem qualquer proteção. Poderíamos ter ainda um SGBD (Sistema Gerenciador de Banco de Dados) constituindo a base de toda a empresa, com tabelas do departamento Financeiro, Diretoria ou até mesmo da Presidência, o que claramente caracteriza informação confidencial. Também é comum que administradores de sistema, por trabalharem com Farejadores para diagnosticar e corrigir problemas na rede, possam agir de má fé, sabotando dados importantes. Os “hackers” que violam as informações de um sistema conhecem as características do usuário, fazendo uso deste conhecimento (o que chamamos de Engenharia Social de Ataque), e sabem que a grande maioria das pessoas costuma empregar a mesma senha para diferentes contas de acesso (muitas vezes, a mesma senha que utilizam em cartões de banco), e quase sempre óbvias, com a própria data de nascimento ou até mesmo nomes de parentes ou de animais de estimação.

1.1.2. Simulação de Endereço IP de Origem (“IP Spoofing”)

Neste tipo de ataque o invasor se faz passar por um elemento confiável, substituindo seu endereço IP de origem por um que esteja dentro da faixa de endereços alocados para a rede

privada (ou subrede, quando o invasor é um funcionário da empresa), ou de outra fonte externa conhecida que tenha acesso aos seus recursos (ex.: usuários de uma filial consultando a base de dados disponibilizada na matriz). O computador do invasor é interpretado pelo sistema como se fosse mais um ponto da rede privada, seja local ou não. Geralmente este tipo de ataque é limitado ao acréscimo de dados ou comandos a um fluxo já existente entre a aplicação cliente e o servidor, ou para estabelecer uma conexão de rede ponto-a-ponto (uma possível abordagem seria sabotar o sistema para o envio não autorizado de correio eletrônico com informações sigilosas).

1.1.3. Ataques sobre Senhas (“Password Attacks”)

Os ataques para identificação de senhas são quase sempre executados com a ajuda de programas que utilizam a técnica de tentativa-e-erro sucessivas vezes, de forma automática, a partir de combinações definidas com base nas sequências mais usadas (este tipo de ataque também é conhecido como ataque de “força bruta”). O invasor tem acesso aos recursos quando o programa acerta a sequência definida para a senha e nome de login, com os mesmos direitos de acesso do usuário. Uma situação pior ocorre quando o usuário tem direitos exclusivos de administrador, já que neste caso pode ser criada uma “backdoor” (porta dos fundos) para novos ataques, como por exemplo a criação de uma conta não-autorizada.

1.1.4. Distribuição de Dados Sensíveis para Fontes Externas (“Distribution of Sensitive Internal Information to External Sources”)

Controlar a distribuição de dados sensíveis é a primeira etapa para se chegar a uma boa conduta de segurança. Funcionários podem, eventualmente, vender informações confidenciais para empresas concorrentes, ou gerar falhas de segurança a partir de um simples compartilhamento de disco. Uma boa política restringe de forma adequada o acesso à informação e os meios de transmiti-la dentro ou fora da rede privada, para evitar uma situação comprometedora. Um exemplo simples: determinado usuário poderia copiar para um servidor de FTP remoto (não confiável) dados importantes, mesmo sem a intenção de prejudicar a empresa para a qual trabalha, dados esses que poderiam ser interceptados por estranhos.

1.1.5. Sondagem em Pontos de Interconexão Intermediários (“Man-in-the-Middle Attacks”)

Para efetuar este tipo de ataque, o invasor deve atuar em um ponto intermediário entre o usuário que está acessando os recursos e a rede externa, como por exemplo o funcionário que trabalha no provedor de acesso à Internet (muitos provedores comerciais definem cláusulas de segurança no contrato de prestação de serviços, mas do ponto de vista técnico este tipo de situação é possível). Tais ataques costumam ser implementados com a ajuda de Farejadores de Pacotes e protocolos de transporte e roteamento. O invasor poderia se aproveitar de uma sessão em andamento para obter, por exemplo, o nome de login e a senha do usuário.

1.1.6. Ataques a Nível de Aplicação (“Application Layer Attacks”)

Ataques a nível de aplicação podem ser implementados usando vários métodos, o mais comum é explorar falhas encontradas em programas que são carregados no servidor, como o Sendmail, o PostScript e o FTP (os invasores ganham acesso aos recursos da rede com as mesmas permissões do usuário que faz a chamada e gerencia tais aplicações, ou seja, o administrador). Outro método muito comum é a técnica de se escrever um programa que simula condições regulares do sistema, chamado de Cavalo de Tróia (“Trojan Horse”), agregando funções e rotinas específicas para a invasão e ou destruição de dados.

Um Cavalo de Tróia poderia, por exemplo, substituir a sequência de validação do usuário, objetivando capturar o nome de login e a senha de modo a enviá-los, posteriormente, para o invasor (poderia fazê-lo através de correio-eletrônico). O usuário, a princípio, não percebe que está sendo monitorado pelo Cavalo de Tróia, porque o mesmo faz chamada às rotinas normais do sistema depois de cumprir sua função.

Nos sistemas modernos, as técnicas mais usadas tiram proveito das facilidades proporcionadas pela especificação do HTML (“Hyper Text Markup Language”) e do HTTP (“Hyper Text Transfer Protocol”), através de programas maliciosos desenvolvidos em Java Script ou a partir de controles do ActiveX que, ao serem carregados em navegadores como o Netscape Communicator e o Internet Explorer, executam operações de acesso não autorizado aos recursos do computador (neste caso, é o próprio usuário que faz chamada ao Cavalo de Tróia quando acessa a página HTML com o código).

1.1.7. Recusa de Sistema (“Denial-of-Service Attacks”)

Neste tipo de ataque, o invasor (ou grupo de invasores) sobrecarrega o sistema-alvo com um número muito grande de solicitações, tirando proveito de alguma restrição do sistema operacional, aplicação ou até mesmo da própria rede, com o objetivo específico de “derrubar o servidor” (isto é, impossibilitar que os usuários tenham acesso aos recursos). Quando este tipo de ataque envolve aplicações de rede, como o HTTP ou o FTP, tal objetivo pode ser atingido alocando-se todas as conexões suportadas, o que efetivamente bloqueia qualquer tentativa do usuário de acessar tais recursos. O invasor também pode se valer de fragilidades encontradas em protocolos usados na Internet, como o ICMP, sobrecarregando o canal com pacotes desnecessários, ou ainda fornecendo informações falsas sobre o estado da rede.

2. CONSIDERAÇÕES SOBRE A PILHA DE PROTOCOLOS TCP/IP

Um protocolo de rede, ou protocolo de comunicação, engloba determinado conjunto de regras estabelecidas para viabilizar a troca de dados entre computadores, ou nós, através de um enlace físico. Pela definição, percebe-se que o protocolo é responsável pelas diretrizes básicas de comunicação, exercendo papel equivalente ao da língua para as pessoas; analogamente, como não é possível estabelecer um diálogo entre duas pessoas que não falam o mesmo idioma, também não é possível intercambiar dados entre computadores que utilizam protocolos diferentes. Logo, em uma mesma rede de computadores todos os nós devem adotar o mesmo protocolo, isto é, utilizar regras de comunicação equivalentes. O TCP/IP existe para permitir que não só os computadores (identificados pelo termo “host”) de uma mesma rede possam se comunicar, como também para tornar possível a comunicação inter-redes, ou seja, fazer com que computadores de redes distintas possam se “falar”.

Os problemas inerentes ao projeto de um protocolo já são difíceis de solucionar quando tratamos de uma única rede; ao passar para um escopo mais amplo, o que inclui várias redes de computadores e, consequentemente, muitas tecnologias, o trabalho passa a ser extremamente complexo. A melhor estratégia para resolver um problema muito grande é quebrá-lo em partes menores, que possam ser analisadas individualmente até atingirmos o resultado final (“dividir para conquistar”). Desta forma, a ISO (“International Standardization Organization” - Organização para Padronização Internacional), estabeleceu um modelo de referência baseado em sete camadas - Física (1), Enlace (2), Rede (3), Transporte (4), Sessão (5), Apresentação (6) e Aplicação (7) - que tratam, uma a uma, de aspectos correlacionados: o OSI (“Open Systems Internconnection” - Modelo de Referência para a Interconexão de Sistemas Abertos) [Soares 97]. A mensagem a ser transmitida pelo usuário viaja pelas sete camadas, partindo da camada de nível superior (“Aplicação”) até atingir a camada de nível um (“Física”); quando a mensagem chega no destino ela faz o caminho inverso, até a camada de nível sete.

A pilha de protocolos TCP/IP divide os sistemas de comunicação em quatro camadas conceituais que foram construídas sobre uma primeira camada de nível físico (os trabalhos de pesquisa que levaram ao desenvolvimento do TCP/IP não se basearam no ISO/OSI) - Interface de Rede (2), Inter-Rede (3), Transporte (4) e Aplicação (5). Cada camada corresponde a um grupo de protocolos, como o IP e o ICMP (“Inter-Rede”), o UDP e o TCP (“Transporte”), e os demais protocolos da camada de Aplicação. Uma vez mais, vale lembrar que múltiplos protocolos são usados para o tratamento das diversas tarefas envolvidas com o processo de transmissão/recepção de mensagens; similarmente às etapas empregadas na tradução de sistemas em desenvolvimento, onde temos um compilador (“compiler”), montador (“assembler”), editor de vínculos (“link editor”) e carregador (“loader”), também nos sistemas de comunicação se faz necessário especificar as interfaces entre os quatro módulos (camadas), ou seja, temos uma seqüência linear bem definida. O formato dos dados que trafegam da camada de Aplicação para a camada de Transporte, durante a transmissão da mensagem, será o mesmo aplicado nos dados que irão trafegar da camada de Transporte para a camada de Aplicação, durante a recepção da mensagem.

Excetuando-se os módulos da camada de Aplicação, o restante da pilha de protocolos, ou pilha de rede, é implementada no núcleo do sistema operacional (“kernel”); consequentemente, passar dados entre as camadas inferiores do sistema de comunicação é muito mais complexo do que entre programas aplicativos e a camada de Transporte. Outra observação importante é que a camada de Interface de Rede lida diretamente com endereços físicos (ex.: “MAC addresses”), ou seja, ela é responsável pela transmissão de datagramas IP através de uma rede com tecnologia específica, baseada em padrões como o Ethernet ou o Token Ring.

3. PAREDES CORTA-FOGO

Um sistema de parede corta-fogo, ou “firewalls”¹, atua como um portal de rede cuja finalidade é garantir que a comunicação ponto-a-ponto entre hosts localizados em segmentos distintos respeite determinadas regras que estão agrupadas no que chamamos de política de

¹ Antigamente, nos EUA, paredes de tijolos eram usadas como forma de proteção contra incêndios; elas eram construídas entre os apartamentos de um condomínio e, devido ao papel exercido, eram chamadas de “firewalls” (adaptando para o português, parede corta-fogo). Analogamente, o termo “firewall” passou a ser adotado pela indústria para designar os sistemas de proteção que são usados como barreira entre duas redes, isolando a rede interna das ameaças provenientes do mundo exterior.

segurança para a rede privada (o sistema de parede corta-fogo analisa cada pacote de rede individualmente, de modo a bloquear qualquer tentativa de invasão).

Ao se definir a política de segurança que será aplicada na rede privada, é necessário estabelecer procedimentos de modo a salvaguardá-la de ataques, protegendo seus dados e usuários contra perdas e danos. A partir deste ponto de vista, a política de segurança adotada especificamente na rede privada exerce um papel fundamental quando analisamos a organização como um todo, reforçando a própria política de segurança da empresa. O tráfego de dados e a alocação de recursos passam a ser controlados, identificando não só os componentes da rede como também seus pontos vulneráveis, de forma a isolar possíveis ameaças, além de especificar as medidas a serem tomadas (planos de ação) caso a política de segurança seja violada.

Um sistema de parede corta-fogo, portanto, caracteriza-se por oferecer um ponto central de defesa entre duas redes - geralmente a Internet e uma rede privada - de modo a bloquear possíveis ataques externos. Os sistemas de parede corta-fogo podem ser implementados no próprio roteador que atua como interface física de interconexão, a partir de filtros de pacotes, ou através de uma estratégia mais complexa, agrupando vários roteadores associados à procuradores ("proxies"), sistemas que atuam na camada de aplicação.

3.1. Histórico

A tecnologia empregada nos sistemas de parede corta-fogo evolui a passos largos, a medida que a demanda por segurança aumenta novos aprimoramentos são desenvolvidos pela indústria, facilitando a vida dos administradores de sistema. A primeira geração surgiu por volta de 1985, com o advento dos roteadores que empregam filtros de pacotes, mas sua especificação formal só foi publicada em 1988 por Jeff Mogul (Digital Equipments) [Cisco].

A segunda geração, os sistemas de parede corta-fogo que atuam a nível de circuito, foi elaborada por Dave Presotto e Howard Trickey (ambos dos Laboratórios Bell - AT&T) no período de 1989-1990 [Cisco]. Eles chegaram a trabalhar, posteriormente, em uma terceira geração da tecnologia, que atua a nível de aplicação, mas não publicaram nenhum documento descrevendo suas características e nem lançaram um produto no mercado baseado em seus estudos.

Na prática, a terceira geração foi desenvolvida por várias pessoas no decorrer da década de 1990, com destaque para Gene Spafford (Universidade de Purdue), Bill Cheswick (Laboratórios Bell - AT&T) e Marcus Ranum, que descreveu os sistemas de parede corta-fogo que atuam a nível de aplicação (procuradores) no período de 1990-1991 (seu trabalho resultou no primeiro produto lançado no mercado pela Digital Equipments) [Cisco].

Por volta de 1991, Bill Cheswick e Steve Bellovin (este último também dos Laboratórios Bell - AT&T) iniciaram as pesquisas no desenvolvimento de um filtro de pacotes dinâmico, a quarta geração dos sistemas de parede corta-fogo, participando do projeto de um novo produto a ser lançado pela Bell, que não chegou a ser concluído. Em 1992, Bob Braden e Annette DeSchon (Instituto de Ciências da Informação da Universidade de Santa Clara) engendraram novas pesquisas, que resultaram no primeiro produto comercial baseado na quarta geração, lançado pela Check Point Software [Cisco].

3.2. Perímetro de Segurança

Quando implementamos uma política de segurança para a rede privada, estamos na verdade fortalecendo pontos estratégicos que fazem parte do que podemos chamar de limites fronteiriços (como pontos de interconexão); esses pontos estratégicos constituem o perímetro da rede. Na verdade, podemos ter vários perímetros de rede - segmentos da rede privada -, cada um agrupando um determinado número de hosts que demandam um certo nível de proteção, e que devem se comunicar com os demais perímetros através de um ponto central: o sistema de parede corta-fogo.

Os perímetros são classificados de acordo com o seu posicionamento relativo: o perímetro de rede mais externo identifica o ponto de separação entre os recursos que estão sob o controle do administrador de sistema e a rede externa - geralmente um roteador que interliga a rede privada a um provedor de acesso à Internet -, os perímetros internos representam pontos intermediários onde mecanismos de segurança são posicionados de acordo com a estrutura de segurança. Na prática, para os usuários externos o sistema de parede corta-fogo representa todos os recursos que pertencem à rede confiável, definindo um ponto de foco pelo qual todo tráfego deverá passar.

3.3. Redes Confiáveis, Redes Não-Confiáveis e Redes Desconhecidas

Redes confiáveis são as redes que estão localizadas dentro do perímetro de segurança, ou seja, justamente aquelas que demandam proteção, estando aos cuidados do administrador de sistemas. Quando um sistema de parede corta-fogo é configurado pela primeira vez, é necessário identificar de forma explícita os tipos de rede que irão se comunicar com o mesmo através das interfaces físicas; depois deste processo inicial, as redes confiáveis englobam o sistema de parede corta-fogo e todos os segmentos de rede protegidos².

Já as redes não-confiáveis, como o próprio nome sugere, são aquelas redes que não estão sob o controle do administrador de sistemas, localizadas fora do perímetro de segurança. Em outras palavras, compreendem as redes externas com as quais é necessário se estabelecer um canal de comunicação sem que, para isso, a segurança deva ser comprometida. Assim como no caso das redes confiáveis, também é necessário identificá-las de forma explícita quando o sistema de parede corta-fogo é configurado pela primeira vez, definindo quem poderá ter acesso aos recursos situados dentro do perímetro de segurança.

As redes não identificadas no sistema de parede corta-fogo como redes confiáveis ou redes não-confiáveis são chamadas de redes desconhecidas, abrangendo todas as redes externas ao perímetro de segurança que não se comunicam diretamente com a rede privada (por padrão, toda rede não-confiável é considerada, a princípio, uma rede desconhecida). A Tabela 1 descreve as designações aplicadas para cada segmento de rede que constitui o perímetro de segurança.

Tabela 1 - Segmentos do Perímetro de Segurança

Redes Comuns	Designação	Descrição
Perímetro mais interno	Confiável	Protege os recursos mais internos, anterior aos demais perímetros de rede
Perímetros de rede internos	Confiável	Perímetros de rede intermediários, anteriores ao

² As redes virtuais privadas (VPNs - “Virtual Private Networks”), mesmo transmitindo dados através da infraestrutura de uma rede não confiável, também podem ser classificadas como redes confiáveis. Seus pacotes se originam a partir do perímetro de segurança, e mecanismos são adotados de modo que o sistema de parede corta-fogo possa validar a autenticidade da origem.

Tabela 1 - Segmentos do Perímetro de Segurança		
Redes Comuns	Designação	Descrição
		sistema de parede corta-fogo
Perímetro de rede mais externo	Confiável, embora sujeito a ataques	O perímetro de rede que está localizado entre o roteador mais externo (que atua como ponte de comunicação com a Internet) e o sistema de parede corta-fogo.
Redes externas identificadas	Não-confiável	Acesso restrito aos recursos internos para usuários autorizados
Redes externas não-identificadas	Desconhecida	O sistema não reconhece

3.4. Soluções Existentes

Duas questões principais devem ser analisadas ao se escolher uma estratégia de implementação a partir dos sistemas de parede corta-fogo existentes: segurança e desempenho. Um nível de segurança mais acentuado compromete o desempenho geral, visto que os pacotes trafegam até as camadas superiores da pilha de rede, onde serão inspecionados com mais critério. Logo, os sistemas de parede corta-fogo que atuam a nível de aplicação são considerados mais seguros do que as demais tecnologias; porém, em contrapartida, esta arquitetura é também a de operação mais lenta, efetuando um número de verificações bem superior.

3.4.1. 1ª Geração (“Packet Filter Firewalls”)

Sistemas de Parede Corta-Fogo Baseados em Filtros de Pacotes Camadas de Inter-Rede e Transporte

Os filtros de pacotes são a primeira geração de sistemas de parede corta-fogo, atuando ao nível da camada de Transporte, a partir da análise do conteúdo de quadros que estão encapsulados no campo de dados dos pacotes IP (TCP, UDP ou ICMP). Cada pacote IP é examinado de modo a verificar se o conteúdo encontrado em seu cabeçalho e no cabeçalho do quadro TCP, UDP ou ICMP obedece às regras estabelecidas pela política de segurança, regras essas que têm por finalidade determinar que tipo de comunicação é permitida, baseando-se no sentido do fluxo (da rede externa para a rede interna e vice-versa). Os filtros de pacotes nos permitem manipular a transferência de dados baseando-se nos seguintes critérios:

- A interface física de rede pela qual os pacotes são recebidos
- O endereço de origem do pacote (no caso, endereço IP de origem)
- O endereço de destino do pacote (no caso, endereço IP de destino)
- O tipo de protocolo encapsulado no campo de dados (TCP, UDP ou ICMP)
- A porta de origem identificada na camada de transporte (TCP ou UDP)
- A porta de destino identificada na camada de transporte (TCP ou UDP)

Os filtros de pacotes não interpretam os protocolos do nível de aplicação que são usados nos pacotes, ao invés disso eles operam a partir de um conjunto de regras que está mantido no núcleo do TCP/IP, contendo uma ação associada que será aplicada em qualquer pacote que não atenda às regras definidas a partir dos critérios listados acima. A ação tomada seguirá um dos dois valores possíveis para o pacote que está em trânsito: recusado ou permitido.

Duas listas são mantidas no núcleo do TCP/IP, uma para pacotes que devem ser recusados e outra para pacotes permitidos; um pacote de rede só poderá ser roteado para o seu destino após passar pelas duas listas, isto é, ele não deve ser recusado e deve ser permitido. Alguns filtros de pacotes que estão incorporados no hardware dos roteadores implementam uma política diferente, o pacote deve ser recusado ou então ele é permitido (para se entender as regras de filtragem, é necessário conhecer o critério de segurança adotada pelo hardware).

Filtros de pacotes implementam um conjunto de comandos para a verificação das portas de origem e de destino identificadas nos cabeçalhos dos quadros TCP ou UDP, checando a existência de uma regra aplicável para a combinação encontrada (tipo de protocolo + porta específica). Entretanto, uma vez que o ICMP não utiliza números de porta durante o processo de comunicação fica mais difícil para o filtro de pacotes aplicar uma política de segurança para este tipo de tráfego; para tal, é necessário manter tabelas de estado de modo a assegurar que as respostas dos pacotes ICMP foram, de fato, requisitadas por um “host interno” (esta capacidade de monitorar o estado das comunicações é uma das diferenças primárias entre os filtros de pacotes simples e os filtros de pacotes dinâmicos).

A inspeção completa dos pacotes de rede segue o seguinte algoritmo geral:

- (1) Se nenhuma regra aplicável é encontrada, então o pacote é descartado
- (2) Se uma regra aplicável que permita a comunicação é encontrada, o pacote é liberado
- (3) Se uma regra aplicável que bloqueie a comunicação é encontrada, o pacote é descartado

Uma vez que este tipo de sistema não verifica os pacotes a nível de aplicação, e nem monitora o estado das conexões, de todas as tecnologias desenvolvidas para os sistemas de parede corta-fogo esta é a menos segura; por outro lado, justamente por requerer menos tempo de processamento, além de quase sempre ser implementada em hardware (roteadores IP), é também a mais rápida. Outra característica dos filtros de pacotes é o processo de alterar os endereços IP de origem dos pacotes que são roteados para as redes externas (NAT - “Network Address Translation”), fazendo-os parecer procedentes do próprio sistema de parede corta-fogo - a tradução de endereços IP oculta a topologia e o esquema de endereçamento adotados na rede privada.

3.4.2. 2^a Geração (“Circuit Level Firewalls”)

Sistemas de Parede Corta-Fogo que Atuam a Nível de Circuito Camadas de Inter-Rede e Transporte

Segunda geração da tecnologia, os sistemas de parede corta-fogo que atuam a nível de circuito baseiam-se no fato de que o pacote analisado ou procede de uma requisição para se estabelecer conexão ou carrega dados de uma conexão já iniciada³, o que chamamos de circuito virtual. O termo circuito virtual⁴ é usado para descrever essas conexões porque, embora os programas aplicativos considerem a conexão um circuito de hardware dedicado, a confiabilidade é uma ilusão proporcionada pelo serviço de transmissão de “streams” [Tanenbaum 96].

³ Os pares atuando ao nível da camada de transporte, através do TCP.

⁴ Existem duas definições para circuito virtual: uma relativa ao tipo de serviço, outra ao encaminhamento de pacotes. No primeiro caso, o serviço de circuito virtual é um outro nome que se dá ao serviço com conexão. A nível de encaminhamento de pacotes, uma conexão de circuito virtual é aquela em que todos os pacotes seguem a mesma rota determinada durante a abertura da conexão. Note que podemos ter um serviço de circuito virtual implementado ou não em uma conexão de circuito virtual [Soares 97].

Para validar uma sessão, o sistema de parede corta-fogo examina cada processo ativo para se estabelecer uma determinada conexão, deste modo é possível assegurar que o mesmo segue um procedimento de negociação (“handshake”) legítimo para o protocolo de transporte que está sendo empregado. Ademais, os pacotes de dados não são encaminhados até o término do procedimento de negociação.

O sistema de parede corta-fogo mantém uma tabela de conexões válidas (o que inclui informações de seqüenciamento e referentes ao estado das sessões), liberando os pacotes quando as informações coletadas coincidem com uma das entradas cadastradas na tabela de circuitos virtuais; quando a conexão é finalizada, a entrada correspondente é removida e o circuito virtual estabelecido entre os pares da camada de transporte é fechado. Quando um processo para o estabelecimento de determinada conexão está ativo, o sistema de parede corta-fogo armazena as seguintes informações a cerca da conexão:

- Um identificador de sessão único para a conexão (para monitoramento)
- O estado da conexão: em negociação, estabelecida ou encerrada (fechada)
- Informação de seqüenciamento
- O endereço IP de origem
- O endereço IP de destino
- A interface física de rede pela qual o pacote foi recebido
- A interface física de rede pela qual o pacote será encaminhado

A partir dessas informações, o sistema verifica se o computador de origem tem permissão para transmitir e se o computador destino tem permissão para receber o pacote que está sendo examinado. Os sistemas de parede corta-fogo que atuam a nível de circuito também são limitados no que diz respeito aos tipos de protocolos com os quais eles são capazes de lidar, restringindo sua operação na camada de transporte, ou seja, operam sobre o TCP (similarmente aos filtros de pacotes, esses sistemas trabalham a partir de um conjunto de regras mantido no núcleo do TCP/IP). Os pacotes também são reendereçados antes de serem encaminhados para a rede externa, usando a tradução de endereços de rede (NAT), o que os faz parecer procedentes do sistema de parede corta-fogo ao invés dos hosts internos (como o sistema mantém informações sobre cada sessão, é possível mapear as repostas para os hosts internos da forma adequada).

Quando um pacote solicitando a abertura de uma nova conexão é recebido pelo sistema de parede corta-fogo, este último determina, a partir das regras definidas na política de segurança, se o processo pode realmente ser iniciado. Todos os demais pacotes associados a esta conexão são encaminhados pelo sistema, seguindo sua tabela de roteamento, sem verificações adicionais de modo a não comprometer o desempenho (verificações adicionais até podem ser aplicadas para identificar eventuais tentativas de invasão, a partir da simulação de endereços IP, além de checar se o conteúdo dos cabeçalhos TCP segue as definições para este protocolo).

3.4.3. 3^a Geração (“Application Level Firewalls”)

Sistemas de Parede Corta-Fogo que Atuam a Nível de Aplicação

Camadas de Inter-Rede, Transporte e Aplicação

Os sistemas de parede corta-fogo que atuam a nível de aplicação examinam os dados obtidos a partir dos pacotes de rede, mantendo registro das informações de seqüenciamento e referentes ao estado das conexões; outros itens de segurança que só podem aparecer na camada de aplicação, como senhas de usuário e requisição para serviços, também podem ser vali-

dados. Este tipo de sistema inclui aplicações especializadas, os procuradores⁵ (“proxies”), programas que têm por finalidade gerenciar o tráfego de protocolos específicos, como o HTTP ou o FTP, provendo melhor controle de acesso, validação dos dados (cuidadosamente detalhada) e geração de registros para auditoria. Os procuradores também podem executar funções adicionais, como alteração dos dados interceptados, autenticação, validação de usuário, filtragem de URL e cache para objetos transferidos através do HTTP.

O procurador, para operar adequadamente, requer dois componentes que costumam ser implementados em um único módulo executável: o servidor (“proxy server”) e o cliente (“proxy client”). O servidor administra todas as requisições de conexão originadas na rede confiável, isto é, toda a comunicação entre os usuários internos e a Internet passa através do proxy (os usuários não têm permissão para se comunicar diretamente com hosts situados fora do perímetro de segurança, eles não enxergam o roteador). A requisição gerada pela estação de trabalho para conectar o usuário a um serviço externo, como FTP ou Telnet, é recebida pelo servidor; este, por sua vez, avalia a solicitação baseando-se em um conjunto de regras definidas para o serviço em questão, decidindo se a mesma deve ser atendida. Obviamente, se o servidor é capaz de interpretar o protocolo referente ao serviço que está sendo avaliado, só serão liberados os pacotes que atendem às especificações formais definidas para este protocolo.

Já o proxy client é a parte da aplicação que se comunica diretamente com o servidor externo (Internet), atuando com um representante do host interno, sempre que as requisições encaminhadas para o servidor (“proxy server”) são validadas após o processo de verificação - esta é a razão pela qual o termo “procurador” é usado para identificar a aplicação que está sendo executada no sistema de parede corta-fogo. Os pacotes enviados pelo servidor externo são recebidos pelo cliente, passam pelo componente servidor, até chegar à estação de trabalho que gerou a solicitação. A comunicação entre os hosts internos e externos nunca é realizada de forma direta, sempre sendo intermediada pelo procurador, de forma que o tráfego de entrada e saída é monitorado. A princípio, todo o processo é transparente, porque do ponto de vista do usuário a estação de trabalho está lidando diretamente com o servidor externo, e vice-versa.

Determinados serviços de rede, como o SMTP, são temporariamente colocados em espera pelos servidores antes de serem processados (“store-and-forward”, ou seja, os dados são armazenados para transmissão posterior). Este tipo de serviço pode ser intermediado pelo procurador sem que, para tal, sejam efetuadas quaisquer alterações no cliente (estação de trabalho), ficando a cargo do usuário contatá-lo através de comandos específicos (por exemplo, usando TELNET). Outros serviços de rede, como o FTP, não foram projetados com base neste tipo de procedimento, isto é, não requerem pontos intermediários de replicação, o que inclui o próprio procurador. Nesses casos o software cliente deve ser adaptado de modo a viabilizar a comunicação com o sistema de parede corta-fogo. Na primeira hipótese, a maior desvantagem é o fato de que o usuário deve lidar diretamente com o procurador, sabendo de sua existência (cada sessão aberta por ele se dá através de um terminal virtual de rede, simulando a “shell” do procurador); já na segunda hipótese o processo é totalmente transparente para o usuário, mas os custos são bem maiores, visto que todas as estações de trabalho da rede interna deverão dispor de clientes modificados, e o host bastião terá que realizar a comunicação nos dois sentidos de forma automática.

⁵ O computador onde reside o sistema de parede corta-fogo que atua a nível de aplicação é chamado de bastião (“bastion host”), termo usado para identificar as saliências existentes em muralhas de fortificações (essas saliências existem para facilitar o trabalho dos soldados que cuidam da vigilância, por oferecerem melhor campo de visão).

Os serviços do procurador são implementados no topo da pilha de rede do host onde o sistema de parede corta-fogo está sendo executado, operando na área de memória reservada pelo sistema operacional para programas aplicativos; consequentemente, cada pacote deve passar através de protocolos de baixo-nível no núcleo (“kernel”) antes de passar para a área de programas, onde será inspecionado. Após a inspeção, o pacote faz a viagem de volta ao núcleo, descendo pela pilha de rede para ser distribuído. Como todos os pacotes de uma sessão estão sujeitos a este processo, a validação é bem mais demorada que nas tecnologias citadas anteriormente; os sistemas de parede corta-fogo que atuam a nível de aplicação, tal como os que operam a nível de circuito, também podem executar verificações adicionais para constatar se os pacotes foram simulados (“IP Spoofing”), além de utilizar tradução de endereços.

3.4.4. 4^a Geração (“Dynamic Packet Filters”)

Sistemas de Parede Corta-Fogo Baseados em Filtros de Pacotes Dinâmicos Camadas de Inter-Rede e Transporte

A principal vantagem desta tecnologia em relação aos filtros de pacotes convencionais é a sua capacidade de trabalhar com o UDP (transporte), associando este tipo de quadro a uma conexão virtual (o que, em circunstâncias normais, é implementado através do TCP, já que o UDP não fornece a transmissão de “stream” confiável) sempre que os pacotes trafegam de dentro do perímetro de segurança para redes externas e vice-versa. Quando um pacote é gerado no servidor externo, atendendo à solicitação do host interno, a conexão virtual é estabelecida e a permissão para transpassar o filtro é concedida; a informação vinculada a esta conexão é mantida durante um certo período de tempo, e se nenhuma resposta for recebida neste intervalo o circuito virtual é invalidado.

Esta tecnologia apresenta as mesmas vantagens e desvantagens encontradas na primeira geração dos filtros de pacotes, com o diferencial de bloquear pacotes de rede carregando quadros UDP que não foram solicitados pelos usuários do perímetro de segurança (qualquer pacote carregando resposta para uma solicitação interna deverá conter o endereço de destino equivalente ao endereço do hospedeiro de origem, a mesma porta e o mesmo tipo de protocolo da camada de transporte). Esta característica é muito útil, por exemplo, ao permitir que protocolos da camada de aplicação, como o DNS, possam operar através do sistema de parede corta-fogo (um servidor DNS interno deve encaminhar as solicitações para resolução de nomes a servidores DNS externos, o que pode ser efetuado através de conexões TCP ou UDP).

4. CRIPTOGRAFIA

Criptografar é o processo de converter uma mensagem em outra, codificada, valendo-se de funções matemáticas e uma senha especial, chamada de chave. A criptografia já era empregada por diversas culturas da antigüidade, os egípcios, os persas, os gregos e os romanos utilizavam esta técnica, principalmente para fins militares e diplomáticos - a expressão tem origem nas palavras gregas “kryptos” (escondida) e “graphia” (escrever).

No âmbito da computação, a criptografia é um recurso importante, porque com sua ajuda é possível garantir a segurança das informações que demandam sigilo. Ela pode ser usada para codificar os dados que devem ser enviados através de uma rede pública, como a Internet,

assegurando a privacidade em casos de interceptação. Conseqüentemente, a criptografia se tornou parte indispensável dos sistemas modernos.

Quando uma mensagem criptografada é enviada de um computador para outro, os seguintes requisitos devem ser obtidos: integridade (a mensagem recebida pelo destinatário deve ser igual à mensagem gerada na origem), sigilo (a mensagem enviada só poderá ser acessada pelas pessoas autorizadas), autenticidade (o remetente é indiscutível, ninguém poderá se fazer passar por ele) e não repúdio (se o remetente estiver solicitando mil pares de sapatos a R\$ 15,00 cada, não poderá dizer que foi por R\$ 10,00).

A criptografia é constituída de duas etapas: *encriptar* é o ato de transformar os dados, dificultando sua interpretação; *decriptar* é o processo inverso, ou seja, converter os dados criptografados para a sua forma original, inteligível. Chaves - valores numéricos, expressos no sistema hexadecimal, que devem ser trocados entre os usuários envolvidos na comunicação - são empregadas durante a encriptação/decriptação de uma mensagem; dependendo do método de criptografia empregado, a mesma chave pode ser usada nas duas etapas do processo, enquanto outros mecanismos utilizam chaves diferentes.

4.1. Métodos Simétrico e Assimétrico

A mensagem pode ser codificada a partir de um determinado algoritmo de criptografia, de modo que, tendo conhecimento do algoritmo e da chave adotados, é possível recuperar a mensagem original fazendo o percurso contrário da encriptação, a decriptação. Algoritmos criptográficos são funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação; eles devem ser conhecidos e testados, a segurança reside na chave secreta que deve ter um comprimento suficiente para evitar sua descoberta por teste exaustivo.

Com o aumento da capacidade computacional, hoje podemos empregar complexos esquemas criptográficos, antes impraticáveis em função do tempo de processamento que seria alocado, mesmo na codificação de mensagens pequenas. E, além da capacidade técnica, a criptografia moderna apresenta algumas características que a faz se subdividir em dois grandes grupos: *criptografia simétrica*, ou criptografia com chave secreta, e *criptografia assimétrica*, que também é chamada de criptografia com chave pública.

A criptografia de chave simétrica é a técnica mais tradicional; nela, a mesma chave é utilizada nos processos de codificação e decodificação. O problema óbvio deste método é que o destinatário deve ser informado de forma segura sobre a chave para a decriptação, e, se encontramos um modo de lhe passar a chave, a princípio seria mais fácil utilizá-lo para transmitir a própria mensagem. São exemplos de algoritmos que implementam este tipo de criptografia o IDEA (“International Data Encryption Algorithm” - Algoritmo Internacional para a Encriptação de Dados), o DES (“Data Encryption Standard” - Padrão para a Encriptação de Dados) e o RC2/4.

Por ser mais simples, a criptografia simétrica é muito eficiente em determinados casos, quando é adotada, por exemplo, em conexões na Internet onde processos computacionais trocam senhas temporárias para a transmissão de informações críticas. Quando o usuário navega pela WEB e visita sítios eletrônicos classificados como seguros, contendo formulários para o preenchimento de dados sigilosos, ele na verdade está utilizando o SSL (“Secure Sockets Layer” - Camada de Interfaces Seguras) que opera a partir de criptografia simétrica, muito provavelmente DES ou algo da RSA (Rivest, Shamir e Adleman).

Na criptografia assimétrica são empregadas duas chaves ligadas matematicamente: a primeira, que está disponível a todos e é denominada chave pública, entra no processo de codificação da mensagem; a segunda chave, que deve ser mantida em segredo e é referenciada como chave privada, entra no processo de decodificação (a chave privada pode ser representada como sendo a identidade do seu proprietário; logo, sua privacidade é crucial). Antes de enviar a mensagem, o emissor deverá encriptá-la valendo-se da chave pública do receptor, que irá decriptá-la usando sua chave privada; é claro que ambos deverão estar utilizando o mesmo algoritmo criptográfico.

Por serem mais complexos, os sistemas baseados no método assimétrico não são tão eficientes computacionalmente quanto aqueles que foram escritos a partir do método simétrico; para contornar este problema, podemos utilizar o método assimétrico para codificar a chave de um método simétrico, usando este último para codificar a mensagem [Soares 97]. Assim, é possível obter um ganho considerável de performance sem comprometer a segurança.

5. CONCLUSÃO

Nos dias de hoje, é imprescindível a adoção de políticas de segurança adequadas para que possamos garantir a integridade dos dados corporativos, restringindo o acesso às informações de modo que somente as pessoas autorizadas possam, efetivamente, utilizá-las. A eficiência dos hackers atesta claramente a vulnerabilidade dos sistemas, que demandam um nível de proteção cada vez maior. Ao combinarmos as diversas tecnologias de firewalls com as técnicas de criptografia existentes, fortalecemos a estrutura da nossa rede corporativa, dificultando a ação dos invasores. É claro que os usuários também devem ser educados no sentido de manter um conduta compatível com as regras estabelecidas pela equipe de suporte, evitando erros comuns como a troca de mensagens com arquivos em anexo ou a cópia de programas a partir de sítios eletrônicos não-confiáveis (veículos para a propagação de vírus e cavalos de tróia). Em linhas gerais, pode-se afirmar que não existe sistema totalmente a prova de invasões; entretanto, de posse dos recursos existentes, é possível neutralizar uma gama bem variada de ataques, dificultando a ação dos hackers.

AGRADECIMENTOS

Gostaríamos de agradecer, primeiramente, aos nossos pais, pelo carinho e dedicação que sempre nos foram reservados; também queremos agradecer a atenção conferida por todos os membros que compõe o corpo docente do curso de Especialização em Telemática, destacando nosso orientador, Prof. Marcos Tadeu.

REFERÊNCIAS

[Comer 98]

COMER, DOUGLAS E. “Interligação em Rede com TCP/IP - Volume 1: Princípios, protocolos e arquitetura”. Segunda Edição. Editora Campus, 1998.

[Soares 97]

SOARES, LFG; LEMOS, G; COLCHER, S. “Redes de Computadores: das LANs, MANs e WANs às Redes ATM”. Segunda Edição. Editora Campus, 1997.

[Tanembaum 96]

TANEMBAUM, A. “Computer Networks”. Third Edition. Prentice Hall International, 1996.

[Cisco]

Documento publicado no sítio eletrônico da Cisco [<http://www.cisco.com>], intitulado “*Securing Your Network with the Cisco Centri Firewall*”.



2023

11 A 14 DE ABRIL DE 2023

11 - 14 | APRIL 2023

Riocentro - Exhibition and Convention Center
Av. Salvador Allende, 6555 - Recreio dos Bandeirantes
Rio de Janeiro - RJ



SUA ENTRADA

Para a sua comodidade e para agilizar o seu processo de entrada na LAAD Defence & Security 2023, por favor, imprima em cores a credencial abaixo.

Assegure-se de que esta página seja impressa com clareza em papel A4 comum.

Para garantir que a sua credencial se encaixe no porta-credencial, você deve imprimi-la na proporção 100%.

Por favor checar os ajustes da sua impressora, já que algumas delas imprimem em escala.

Pegue o seu porta-credencial e o seu cordão na entrada principal do evento, na área de credenciamento (Pavilhão 1).

Essa credencial não permite acesso à montagem e desmontagem do evento.

Para mais informações, acesse o site www.laadexpo.com.br

Essa credencial é pessoal e intransferível.

YOUR ENTRY

For your convenience and to speed up your LAAD Defence & Security 2023 entry process, print in full color the conference badge below.

Please ensure this page prints clearly on plain A4 paper.

To ensure that your conference badge fits in the badge holder, you must print it at 100% ratio.

Please check your printer's settings, as some printers print to scale.

Take your badge holder and lanyard at the event's main entrance in the accreditation area (Pavilion 1).

This conference badge does not allow access to the event installation and dismantling.

For more information, visit the website www.laadexpo.com.br

This conference badge is personal and non-transferable.

IMPORTANTE

Por se tratar de um evento de negócios, o acesso à LAAD Defence & Security 2023 é restrito a profissionais do setor.

Não é permitida a entrada de menores de 18 anos, mesmo que acompanhados pelo responsável, assim como de pessoas usando bermudas, regatas, bonés ou chinelos.



É proibida a circulação de pessoas sem credencial durante todo o evento.

IMPORTANT

As it is a business event, access to LAAD Defence & Security 2023 is restricted to industry professionals.

The entrance of people under the age of 18 is not allowed, even if accompanied by guardians. Shorts, tank tops, caps and flip-flops are not part of the dress code and are not permitted.



The conference badge must be used at all times; entrance without is not allowed.



11 A 13 DE ABRIL - 10H ÀS 18H | 14 DE ABRIL - 10H ÀS 17H
APRIL 11 TO 13 - 10 A.M. TO 6 P.M. | APRIL 14 - 10 A.M. TO 5 P.M.



CYBERSECURITY

FAETEC RJ

TEACHER

BRASIL



- VISITANTE

VISITANTE
VISITOR

PATROCINADOR MASTERS/MASTER SPONSOR



ORGANIZAÇÃO / ORGANISED BY

