1. Segurança de rede

A tecnologia de sistema e rede é uma tecnologia chave

para uma ampla variedade de aplicações. A segurança é crucial

2

para redes e aplicativos. Embora, rede

a segurança é um requisito crítico em países emergentes

redes, há uma falta significativa de segurança

métodos que podem ser facilmente implementados.

Existe uma “lacuna de comunicação” entre o

desenvolvedores de tecnologia de segurança e desenvolvedores

de redes. O projeto de rede é um bem desenvolvido

processo baseado nos Sistemas Abertos

Modelo de interface (OSI). O modelo OSI tem vários

vantagens ao projetar redes. Oferece

modularidade, flexibilidade, facilidade de uso e

padronização de protocolos. Os protocolos de

diferentes camadas podem ser facilmente combinadas para criar

pilhas que permitem o desenvolvimento modular. O

a implementação de camadas individuais pode ser alterada

posteriormente sem fazer outros ajustes, permitindo

flexibilidade no desenvolvimento. Ao contrário da rede

projeto, projeto de rede segura não é um bem desenvolvido

processo. Não existe uma metodologia para

gerenciar a complexidade dos requisitos de segurança.

O design de rede segura não contém o mesmo

vantagens como projeto de rede.

Ao considerar a segurança da rede, deve-se

enfatizou que toda a rede é segura.

A segurança da rede não diz respeito apenas ao

segurança nos computadores em cada extremidade do

cadeia de comunicação. Ao transmitir dados, o

canal de comunicação não deve ser vulnerável

atacar. Um possível hacker poderia ter como alvo o

canal de comunicação, obtenha os dados, descriptografe-os

e reinserir uma mensagem falsa. Protegendo a rede

é tão importante quanto proteger os computadores e

criptografando a mensagem.

Ao desenvolver uma rede segura, os seguintes

precisam ser considerados [1]:

1. Acesso - os usuários autorizados recebem o

significa comunicar de e para um

rede particular

2. Confidencialidade – Informação na rede

permanece privado

3. Autenticação – Certifique-se de que os usuários do

rede são quem dizem ser

4. Integridade – Certifique-se de que a mensagem não

foi modificado em trânsito

5. Não-repúdio - Certifique-se de que o usuário não

refutar que ele usou a rede

Um plano de segurança de rede eficaz é desenvolvido

com a compreensão das questões de segurança, potencial

invasores, nível de segurança necessário e fatores que

tornar uma rede vulnerável a ataques [1]. Os passos

envolvidos na compreensão da composição de um

rede segura, internet ou outra, é seguido

ao longo desta empreitada de pesquisa.

Para diminuir a vulnerabilidade do computador ao

rede existem muitos produtos disponíveis. Esses

ferramentas são criptografia, mecanismos de autenticação,

detecção de intrusão, gerenciamento de segurança e

firewalls. As empresas em todo o mundo estão

usando uma combinação de algumas dessas ferramentas.

“Intranets” estão conectadas à internet e

razoavelmente protegido dela. A Internet

arquitetura em si leva a vulnerabilidades no

rede. Compreender os problemas de segurança do

a internet ajuda muito no desenvolvimento de novos sistemas de segurança

tecnologias e abordagens para redes com

acesso à Internet e a própria segurança na Internet.

Os tipos de ataques pela internet precisam ser

também ser estudado para ser capaz de detectar e proteger

contra eles. Os sistemas de detecção de intrusão são

estabelecido com base nos tipos de ataques mais

comumente usado. As invasões de rede consistem em

pacotes que são introduzidos para causar problemas para

as seguintes razões:

• Consumir recursos inutilmente

• Para interferir com qualquer recurso do sistema

função pretendida

• Para obter conhecimento do sistema que pode ser

explorado em ataques posteriores

A última razão para uma invasão de rede é mais

comumente guardado e considerado pela maioria

como o único motivo de invasão. As outras razões

mencionados precisam ser frustrados também.

3

A segurança típica existe atualmente nos computadores

conectado à rede. Protocolos de segurança

às vezes geralmente aparecem como parte de uma única camada

do modelo de referência de rede OSI. Trabalho atual

está sendo executado usando uma abordagem em camadas para

projeto de rede segura. As camadas da segurança

modelo correspondem às camadas do modelo OSI. Esse

abordagem de segurança leva a uma abordagem eficaz e

design eficiente que contorna alguns dos

problemas comuns de segurança.

2. Diferenciando segurança de dados e

Segurança de rede

A segurança dos dados é o aspecto da segurança que permite

os dados do cliente sejam transformados em ininteligíveis

dados para transmissão. Mesmo que isso seja ininteligível

dados são interceptados, uma chave é necessária para decodificar o

mensagem. Este método de segurança é eficaz para um

certo grau. Criptografia forte no passado pode

ser facilmente quebrado hoje. Métodos criptográficos

tem que continuar a avançar devido ao

avanço dos hackers também.

Ao transferir texto cifrado em uma rede, é

útil ter uma rede segura. Isso permitirá

o texto cifrado a ser protegido, de modo que seja menos

provável que muitas pessoas até tentem quebrar

o código. Uma rede segura também evitará

alguém de inserir mensagens não autorizadas

na rede. Portanto, as cifras rígidas são

necessários, bem como redes de ataque rígido [2].

A relação entre segurança de rede e dados

segurança para o modelo OSI é mostrado na Figura 1.

pode ser visto que a criptografia ocorre no

camada de aplicação; portanto, os criadores de aplicativos

estão cientes de sua existência. O usuário pode eventualmente

escolher diferentes métodos de segurança de dados.

A segurança da rede está principalmente contida no

camada física. As camadas acima da camada física são

também usado para realizar a segurança da rede

necessário [2]. A autenticação é realizada em um

camada acima da camada física. segurança de rede em

a camada física requer detecção de falha, ataque

mecanismos de detecção e inteligência

estratégias de contramedidas [2].

HISTÓRICO DE SEGURANÇA DE REDE

O interesse recente em segurança foi alimentado pelo crime

cometido por Kevin Mitnick. Kevin Mitnick

cometeu o maior crime relacionado com computadores em

história dos Estados Unidos [3]. As perdas foram de oitenta milhões

dólares em propriedade intelectual e código-fonte dos EUA

de uma variedade de empresas [3]. Desde então,

a segurança da informação ganhou destaque.

As redes públicas estão sendo confiadas para entregar

informações financeiras e pessoais. devido ao

evolução da informação que é disponibilizada

pela internet, a segurança da informação também é

necessário para evoluir. Devido ao ataque de Kevin Mitnick,

empresas estão enfatizando a segurança para o

propriedade intelectual. Internet tem sido um impulsionador

vigor para a melhoria da segurança de dados.

Os protocolos da Internet no passado não foram desenvolvidos

para se proteger. Dentro do TCP/IP

pilha de comunicação, os protocolos de segurança não são

implementado. Isso deixa a internet aberta para

ataques. Desenvolvimentos modernos na internet

arquitetura tornaram a comunicação mais

seguro.

1. Breve História da Internet

O nascimento da interna acontece em 1969, quando

Rede de agências para projetos de pesquisas avançadas

(ARPANet) é encomendado pelo departamento de

defesa (DOD) para pesquisa em redes.

A ARPANET é um sucesso desde o início.

Embora originalmente projetado para permitir que os cientistas

compartilhar dados e acessar computadores remotos, e‐mail

rapidamente se torna o aplicativo mais popular. O

A ARPANET torna-se uma agência postal digital de alta velocidade

como as pessoas o usam para colaborar em projetos de pesquisa

e discutir temas de vários interesses. O

O Grupo de Trabalho InterNetworking torna-se o primeiro

de várias entidades definidoras de padrões para governar o

rede crescente [10]. Vinton Cerf é eleito o

primeiro presidente do INWG, e mais tarde torna-se

conhecido como o "Pai da Internet". [10]

Na década de 1980, Bob Kahn e Vinton Cerf são fundamentais

membros de uma equipe que criam o TCP/IP, o

linguagem comum de todos os computadores da Internet. Para

a primeira vez que a coleção solta de redes

que compunha a ARPANET é vista como um

"Internet", e a Internet como a conhecemos hoje é

nascer. A metade dos anos 80 marca um boom na vida pessoal

indústrias de computadores e superminicomputadores. O

combinação de máquinas desktop baratas e

servidores poderosos e prontos para rede permitem que muitos

empresas a aderirem à Internet pela primeira vez.

Corporações começam a usar a Internet para

comunicar uns com os outros e com os seus

clientes.

Na década de 1990, a internet começou a se tornar

disponível ao público. A World Wide Web foi

nascer. Netscape e Microsoft foram ambos

competindo no desenvolvimento de um navegador para o

Internet. A Internet continua a crescer e a navegar

a internet tornou-se equivalente a assistir TV

para muitos usuários.

2. Linha do tempo de segurança

Vários eventos importantes contribuíram para o nascimento e

evolução da segurança de computadores e redes. O

linha do tempo pode ser iniciada já em 1930.

Criptógrafos poloneses criaram uma máquina de enigmas

em 1918 que converteu mensagens simples em

texto criptografado. Em 1930, Alan Turing, um brilhante

matemático decifrou o código do Enigma.

Proteger as comunicações era essencial no mundo

Guerra II.

Na década de 1960, o termo “hacker” é cunhado por um

casal do Instituto de Tecnologia de Massachusetts

(MIT). O Departamento de Defesa começou

a ARPANet, que ganha popularidade como canal

para a troca eletrônica de dados e

informações [3]. Isso abre caminho para a criação

da rede de operadora conhecida hoje como Internet.

Durante a década de 1970, o protocolo Telnet foi

desenvolvido. Isso abriu a porta para o uso público de

redes de dados originalmente restritas a

contratados do governo e pesquisadores acadêmicos

[3].

Durante a década de 1980, os hackers e os crimes relacionados

aos computadores estavam começando a surgir. o 414

gangue são invadidas pelas autoridades depois de nove dias

cracking spree onde eles invadem o ultrassecreto

sistemas. A Lei de Fraude e Abuso de Computador de

1986 foi criado por causa do crime de Ian Murphy

roubar informações de computadores militares. A

estudante de pós-graduação, Robert Morris, foi condenado por

liberando o Morris Worm para mais de 6.000

computadores vulneráveis ​​conectados à Internet.

Com base em preocupações de que o calvário Morris Worm

poderia ser replicado, o Computer Emergency

Equipe de Resposta (CERT) foi criada para alertar

usuários de computador de problemas de segurança de rede.

Na década de 1990, a Internet tornou-se pública e o

as preocupações com a segurança aumentaram tremendamente.

Aproximadamente 950 milhões de pessoas usam a internet

hoje em todo o mundo [3]. Em qualquer dia, há

aproximadamente 225 grandes incidentes de segurança. Essas falhas de segurança também podem

resultar em perdas monetárias de alto grau.

Investimento em segurança adequada deve ser prioridade

para grandes organizações, bem como usuários comuns.

ARQUITETURA DE INTERNET E

ASPECTOS DE SEGURANÇA VULNERÁVEIS

O medo de violações de segurança na Internet está causando

organizações a usar redes privadas protegidas ou

intranets [4]. A Força-Tarefa de Engenharia da Internet

(IETF) introduziu mecanismos de segurança em

várias camadas do Internet Protocol Suite [4].

Esses mecanismos de segurança permitem a lógica

proteção de unidades de dados que são transferidas através

a rede.

A versão atual e a nova versão do

Protocolo de Internet são analisados ​​para determinar o

implicações de segurança. Embora a segurança possa existir

dentro do protocolo, certos ataques não podem ser

protegido contra. Esses ataques são analisados ​​para

determinar outros mecanismos de segurança que possam ser

necessário.

A arquitetura de segurança do protocolo de internet,

conhecido como IP Security, é uma padronização de

segurança da Internet. A segurança IP, IPsec, cobre o novo

geração de IP (IPv6), bem como a atual

versão (IPv4). Embora novas técnicas, como

IPsec, foram desenvolvidos para superar os

deficiências mais conhecidas, elas parecem ser

insuficiente [5]. A Figura 2 mostra um visual

representação de como o IPsec é implementado para

fornecer comunicações seguras.

IPSec é um protocolo ponto a ponto, um lado

criptografa, o outro descriptografa e ambos os lados compartilham

chave ou chaves. O IPSec pode ser usado em dois modos,

nomeadamente modo de transporte e modos de túnel.

1. Arquiteturas IPv4 e IPv6

O IPv4 foi projetado em 1980 para substituir o NCP

protocolo da ARPANET. O IPv4 exibiu muitos

limitações após duas décadas [6]. O protocolo IPv6

foi projetado com as deficiências do IPv4 em mente.

O IPv6 não é um superconjunto do protocolo IPv4; em vez de

é um novo projeto.

O design do protocolo de internet é tão vasto e não pode

ser totalmente coberto. As principais partes da arquitetura

relacionados à segurança são discutidos em detalhes.

1.1 Arquitetura IPv4

O protocolo contém alguns aspectos que

causou problemas com seu uso. Esses problemas fazem

nem todos estão relacionados à segurança. Eles são mencionados para

obter uma compreensão abrangente do

protocolo de internet e suas deficiências. As causas

dos problemas com o protocolo são:

1. Espaço de Endereçamento

2. Roteamento

3. Configuração

4. Segurança

5. Qualidade do Serviço

A arquitetura IPv4 tem um endereço de 32 bits

largo [6]. Isso limita o número máximo de

computadores que podem ser conectados à internet.

O endereço de 32 bits fornece no máximo dois

bilhões de computadores conectados à Internet.

O problema de ultrapassar esse número não era

previsto quando o protocolo foi criado. O pequeno

espaço de endereçamento do IPv4 facilita o código malicioso

distribuição [5].

O roteamento é um problema para este protocolo porque o

tabelas de roteamento estão constantemente aumentando de tamanho. O

tamanho teórico máximo do roteamento global

tabelas foi de 2,1 milhões de entradas [6]. Os métodos têm

foi adotada para reduzir o número de entradas em

a tabela de roteamento. Isso é útil por um curto período

de tempo, mas mudanças drásticas precisam ser feitas para

resolver este problema.

A rede baseada em TCP/IP do IPv4 requer que

o usuário fornece alguns dados para configurar um

rede. Algumas das informações necessárias são as

endereço IP, endereço do gateway de roteamento, máscara de sub-rede,

e servidor DNS. A simplicidade de configuração do

rede não é evidente no protocolo IPv4. O

o usuário pode solicitar a rede apropriada

configuração a partir de um servidor central [6]. isso facilita

problemas de configuração para o usuário, mas não para o

administradores da rede.

A falta de segurança embutida no IPv4

protocolo levou a muitos ataques vistos hoje.

Existem mecanismos para proteger o IPv4, mas existem

nenhum requisito para seu uso [6]. IPsec é um específico

mecanismo usado para proteger o protocolo. IPsec

protege as cargas úteis do pacote por meio de

criptografia. O IPsec fornece os serviços de

confidencialidade, integridade e autenticação [6].

Esta forma de proteção não leva em conta a

hacker habilidoso que pode ser capaz de quebrar o

método de criptografia e obter a chave.

Quando a internet foi criada, a qualidade do serviço

(QoS) foi padronizado de acordo com o

informações que foram transferidas através do

rede. A transferência original de informações foi

principalmente baseados em texto. À medida que a internet se expandia e

tecnologia evoluiu, outras formas de comunicação

começou a ser transmitido pela internet. O

qualidade de serviço para streaming de vídeos e música

são muito diferentes do texto padrão. O

protocolo não tem a funcionalidade de

QoS dinâmico que muda com base no tipo de

dados sendo comunicados [6].

1.2 Arquitetura IPv6

Quando o IPv6 estava sendo desenvolvido, a ênfase era

colocados sobre os aspectos do protocolo IPv4 que precisavam

ser melhorado. Os esforços de desenvolvimento foram

colocados nas seguintes áreas:

1. Roteamento e endereçamento

2. Arquitetura multiprotocolo

3. Arquitetura de segurança

4. Controle de tráfego

O espaço de endereços do protocolo IPv6 foi estendido por

suportando endereços de 128 bits. Com 128 bits

endereços, o protocolo pode suportar até

3.4 10 38 máquinas. Os bits de endereço são usados

menos eficiente neste protocolo porque simplifica

configuração de endereçamento.

O sistema de roteamento IPv6 é mais eficiente e

permite tabelas de roteamento globais menores. O host

a configuração também é simplificada. Os anfitriões podem

configuram-se automaticamente. Esta nova

design permite facilidade de configuração para o usuário como

bem como administrador de rede.

A arquitetura de segurança do protocolo IPv6 é de

grande interesse. O IPsec está embutido no IPv6

protocolo. A funcionalidade IPsec é a mesma para IPv4

e IPv6. A única diferença é que o IPv6 pode utilizar

o mecanismo de segurança ao longo de todo o percurso [6].

O problema de qualidade de serviço é tratado com IPv6.

O protocolo de internet permite o tratamento especial de

determinados pacotes com maior qualidade de serviço.

De uma visão de alto nível, os principais benefícios do IPv6

são sua escalabilidade e maior segurança. IPv6 também

oferece outros recursos interessantes que estão além

o escopo deste artigo.

Deve ser enfatizado que depois de pesquisar sobre IPv6

e seus recursos de segurança, não é necessariamente mais

seguro que o IPv4. A abordagem da segurança é apenas

ligeiramente melhor, não uma melhoria radical.

2. **Ataques pela Internet Atual**

Protocolo IPv4

Existem quatro atributos principais de segurança do computador.

Eles foram mencionados antes de uma forma ligeiramente diferente

forma, mas são reapresentados por conveniência e

ênfase. Esses atributos de segurança são

confidencialidade, integridade, privacidade e disponibilidade.

Confidencialidade e integridade ainda mantêm o mesmo

definição. Disponibilidade significa os ativos do computador

pode ser acessado por pessoas autorizadas [8]. Privacidade é

o direito de proteger os segredos pessoais [8]. Vários

métodos de ataque se relacionam a esses quatro métodos de segurança

atributos. A Tabela 1 mostra os métodos de ataque e

soluções.

|  |  |  |
| --- | --- | --- |
| **Atributos da Segurança da informacao** | **Métodos de ataque** | **Tecnologia para seguranca na internet** |
| Confidencialidade | Espionagem, Ilacking, phishing, DoS e falsificação de IP | IDS, Firewall, Sistemas criptografados, IPSec e SSL |
| Integridade | Virus, worms, trojas, DoS e falsificação de IP | IDS, Firewall, Software Anti-Malware, IPSec e SSL |
| Privacidade | Bombardeio de email, spamming, hacking DoS e Cookies | IDS, Firewall, Software Anti-Malware, IPSec e SSL |
| Disponibilidade | DoS, bombardeio de email, spamming e infecções no resgitro do sistema de boot | IDS, Software Anti-Malware, IPSec e Firewall |

2.1 Métodos comuns de ataque na Internet

Métodos comuns de ataques na Internet são quebrados

para baixo em categorias. Alguns ataques ganham sistema

conhecimento ou informações pessoais, como

espionagem e phishing. Os ataques também podem

interferir com a função pretendida do sistema, como

como vírus, worms e trojans. A outra forma de

ataque é quando os recursos do sistema são

consome inutilmente, estes podem ser causados ​​por negação

de serviço (DoS). Outras formas de rede

invasões também existem, como ataques terrestres, smurf

ataques e ataques de lágrima. Esses ataques são

não são tão conhecidos como ataques DoS, mas são

usados ​​de uma forma ou de outra, mesmo que não sejam

mencionado pelo nome.

2.1.1 Espionagem

Interceptação de comunicações por um

parte não autorizada é chamada de espionagem. Passiva

espionagem é quando a pessoa apenas secretamente

ouve as mensagens em rede. No outro

lado, espionagem ativa é quando o intruso

ouve e insere algo no

fluxo de comunicação. Isso pode levar ao

mensagens sendo distorcidas. Informação sensível

podem ser roubados desta forma [8].

2.1.2 Vírus

Os vírus são programas de auto-replicação que usam arquivos

infectar e propagar [8]. Quando um arquivo é aberto,

o vírus será ativado dentro do sistema.

2.1.3 Vermes

Um worm é semelhante a um vírus porque ambos são

auto-replicante, mas o worm não requer um

arquivo para permitir que ele se propague [8]. Existem dois principais

tipos de worms, worms de envio em massa e

vermes. Worms de correspondência em massa usam e-mail como um

significa infectar outros computadores. Com reconhecimento de rede

worms são um grande problema para a Internet. A

worm com reconhecimento de rede seleciona um alvo e uma vez que o

worm acessa o host de destino, ele pode infectá-lo por

meio de um Trojan ou de outra forma.

2.1.4 Cavalos de Tróia

Trojans parecem ser programas benignos para o usuário,

mas na verdade terá algum propósito malicioso.

Trojans geralmente carregam alguma carga útil, como um vírus

[8].

2.1.5 Phishing

Phishing é uma tentativa de obter informações confidenciais

informações de um indivíduo, grupo ou

organização [9]. Phishers enganam os usuários para que divulguem

dados pessoais, como números de cartão de crédito, online

credenciais bancárias e outras informações confidenciais

Informação.

2.1.6 Ataques de IP Spoofing

Spoofing significa ter o endereço do

computador espelha o endereço de um computador confiável

para obter acesso a outros computadores. O

identidade do intruso é escondida por diferentes

significa dificultar a detecção e a prevenção.

Com a atual tecnologia de protocolo IP, IPspoofed

os pacotes não podem ser eliminados [8].

2.1.7 Negação de Serviço

Negação de serviço é um ataque quando o sistema

receber muitos pedidos não pode retornar

comunicação com os solicitantes [9]. O

sistema então consome recursos esperando pelo

aperto de mão para completar. Eventualmente, o sistema

não pode responder a mais pedidos tornando-o

sem serviço.

2.2 Tecnologia para Segurança na Internet

As ameaças da Internet continuarão a ser um problema importante em

o mundo global, desde que a informação seja

acessíveis e transferidos através da Internet.

Diferentes mecanismos de defesa e detecção foram

desenvolvido para lidar com esses ataques.

2.2.1 Sistemas criptográficos

A criptografia é uma ferramenta útil e amplamente utilizada em

engenharia de segurança hoje. Envolvia o uso de

códigos e cifras para transformar informações em

dados ininteligíveis.

2.2.2 Firewall

Um firewall é um mecanismo típico de controle de borda ou

defesa perimetral. O objetivo de um firewall é

bloquear o tráfego do lado de fora, mas também pode ser usado para bloquear o tráfego por dentro. Um firewall é

o mecanismo de defesa da linha de frente contra

intrusos. É um sistema projetado para evitar

acesso não autorizado de ou para uma rede privada.

Os firewalls podem ser implementados tanto no hardware

e software, ou uma combinação de ambos [8].

2.2.3 Sistemas de Detecção de Intrusão

Um Sistema de Detecção de Intrusão (IDS) é um sistema adicional

medida de proteção que ajuda a afastar o computador

invasões. Os sistemas IDS podem ser software e

dispositivos de hardware usados ​​para detectar um ataque. IDS

produtos são usados ​​para monitorar a conexão em

determinar se os ataques foram lançados.

Alguns sistemas IDS apenas monitoram e alertam sobre um

ataque, enquanto outros tentam bloquear o ataque.

2.2.4 Software Anti-Malware e scanners

Vírus, worms e cavalos de Tróia são exemplos

de software malicioso, ou Malware para abreviar. Especial

as chamadas ferramentas antimalware são usadas para detectar

eles e curar um sistema infectado.

2.2.5 Secure Socket Layer (SSL)

O Secure Socket Layer (SSL) é um conjunto de protocolos

essa é uma maneira padrão de atingir um bom nível de

segurança entre um navegador da Web e um site. SSL

é projetado para criar um canal seguro, ou túnel,

entre um navegador da web e o servidor da web, então

que qualquer informação trocada é protegida dentro

o túnel seguro. O SSL fornece autenticação de

clientes para o servidor através do uso de certificados.

Os clientes apresentam um certificado ao servidor para provar

sua identidade.

3. Questões de segurança do protocolo IP IPv6

Do ponto de vista da segurança, o IPv6 é um

avanço sobre o protocolo de internet IPv4.

Apesar dos ótimos mecanismos de segurança do IPv6, ele

ainda continua vulnerável a ameaças. Algumas áreas do protocolo IPv6 ainda representam um potencial

problema de segurança.

O novo protocolo de internet não protege contra

servidores mal configurados, mal projetados

aplicativos ou sites mal protegidos.

Os possíveis problemas de segurança surgem devido à

seguinte [5]:

1. Problemas de manipulação de cabeçalho

2. Problemas com enchentes

3. Problemas de mobilidade

Problemas de manipulação de cabeçalho surgem devido ao IPsec

funcionalidade incorporada [7]. Cabeçalhos de extensão

dissuadir algumas fontes comuns de ataques por causa de

manipulação de cabeçalho. O problema é que

cabeçalhos de extensão precisam ser processados ​​por todos

pilhas, e isso pode levar a uma longa cadeia de

cabeçalhos de extensão. O grande número de extensões

cabeçalhos podem sobrecarregar um determinado nó e é um

forma de ataque se for deliberado. A falsificação continua

ser uma ameaça à segurança no protocolo IPv6.

Um tipo de ataque chamado varredura de porta ocorre quando um

seção inteira de uma rede é escaneada para encontrar

alvos potenciais com serviços abertos [5]. O

espaço de endereço do protocolo IPv6 é grande, mas o

protocolo ainda não é invulnerável a este tipo de

ataque.

A mobilidade é um novo recurso que está incorporado

o protocolo de internet IPv6. O recurso requer

medidas especiais de segurança. Administradores de rede

precisam estar cientes dessas necessidades de segurança quando

usando o recurso de mobilidade do IPv6.

SEGURANÇA EM DIFERENTES REDES

As empresas hoje usam combinações de firewalls,

criptografia e mecanismos de autenticação para

criar “intranets” que estão conectadas ao

internet, mas protegido dela ao mesmo tempo.

Intranet é uma rede privada de computadores que utiliza

protocolos de internet. Intranets diferem de

"Extranets" na medida em que as primeiras são geralmente

restrito aos funcionários da organização enquanto

extranets geralmente podem ser acessadas por clientes,

fornecedores ou outras partes aprovadas.

Não necessariamente tem que haver qualquer acesso

da rede interna da organização para o

A própria Internet. Quando esse acesso é fornecido, é

geralmente através de um gateway com firewall, juntamente

com autenticação de usuário, criptografia de mensagens,

e muitas vezes faz uso de redes privadas virtuais

(VPN).

Embora as intranets possam ser configuradas rapidamente para compartilhar

dados em um ambiente controlado, esses dados ainda estão

em risco, a menos que haja forte segurança. O

desvantagem de uma intranet fechada é que os dados vitais

pode não chegar às mãos de quem precisa.

As intranets têm um lugar dentro das agências. Mas pelo

compartilhamento de dados mais amplo, pode ser melhor manter

as redes abertas, com estas salvaguardas:

1. Firewalls que detectam e relatam invasões

tentativas

2. Verificação sofisticada de vírus no firewall

3. Regras aplicadas para abertura de e-mail por funcionários

anexos

4. Criptografia para todas as conexões e dados

transferências

5. Autenticação por temporização sincronizada

senhas ou certificados de segurança

Foi mencionado que se a intranet quisesse ter acesso

à Internet, as redes privadas virtuais são frequentemente

usado. Intranets que existem em vários locais

geralmente executado em linhas alugadas separadas ou um mais novo

abordagem de VPN pode ser utilizada. VPN é privada

rede que usa uma rede pública (geralmente o

Internet) para conectar sites ou usuários remotos.

Em vez de usar uma conexão dedicada do mundo real

como linha alugada, uma VPN usa "virtual"

conexões roteadas através da Internet a partir do

rede privada da empresa para o site remoto ou funcionário.

**DESENVOLVIMENTOS ATUAIS NA REDE**

**SEGURANÇA**

O campo de segurança de rede continua abaixo do

mesma rota. As mesmas metodologias estão sendo

usado com a adição de identificação biométrica.

A biometria fornece um método melhor de

autenticação do que senhas. Isso pode muito

reduzir o acesso não autorizado de sistemas seguros.

Novas tecnologias, como o cartão inteligente, estão surgindo

em pesquisas sobre segurança de rede. O software

aspecto da segurança de rede é muito dinâmico.

Constantemente novos firewalls e esquemas de criptografia

estão sendo implementados.

A pesquisa que está sendo realizada auxilia na

entender o desenvolvimento atual e projetar

os desenvolvimentos futuros do campo.

**1. Desenvolvimentos de hardware**

Os desenvolvimentos de hardware não estão se desenvolvendo

rapidamente. Sistemas biométricos e cartões inteligentes são os

apenas novas tecnologias de hardware que são amplamente

impactando a segurança.

O uso mais óbvio de biometria para rede

security é para logons de estações de trabalho seguras para um

estação de trabalho conectada a uma rede. Cada

estação de trabalho requer algum suporte de software para

identificação biométrica do usuário, bem como,

dependendo da biometria que está sendo usada, alguns

dispositivo de hardware. O custo dos dispositivos de hardware é

uma coisa que pode levar ao uso generalizado de

identificação de segurança biométrica por voz, especialmente

entre empresas e organizações de baixo

orçamento. Dispositivo de hardware, como mouses de computador

com leitores de impressão digital embutidos seria o próximo

Passo acima. Esses dispositivos seriam mais caros para

implementar em vários computadores, pois cada máquina

exigiria seu próprio dispositivo de hardware. A

mouse biométrico, com o software para suportá-lo, é

disponível a partir de cerca de US$ 120 nos EUA.

vantagem do software de reconhecimento de voz é que ele

pode ser centralizado, reduzindo assim o custo de

implementação por máquina. No topo da gama um

pacote biométrico de voz centralizado pode custar até

$ 50.000, mas pode ser capaz de gerenciar o login seguro

de até 5.000 máquinas.

O principal uso da segurança da rede biométrica será

para substituir o sistema de senha atual.

Manter a segurança da senha pode ser uma tarefa importante

mesmo para uma pequena organização. As senhas devem

ser alterado a cada poucos meses e as pessoas esquecem

sua senha ou bloquear-se fora do

sistema digitando incorretamente sua senha

repetidamente. Muitas vezes as pessoas escrevem suas senhas

para baixo e mantê-lo perto de seu computador. isso é de

curso mina completamente qualquer esforço de

segurança de rede. A biometria pode substituir isso

método de identificação de segurança. O uso de

a identificação biométrica acaba com esse problema e

embora possa ser caro configurar no início, esses

dispositivos economizam em administração e assistência ao usuário

custos.

Os cartões inteligentes são geralmente um cartão digital do tamanho de um cartão de crédito.

mídia eletrônica. O cartão em si é projetado para

armazenar chaves de criptografia e outras informações usadas

na autenticação e outras identificações

processos. A ideia principal por trás dos cartões inteligentes é

fornecer prova inegável da identidade de um usuário. Inteligente

os cartões podem ser usados ​​para tudo, desde o login até

a rede para fornecer Web segura

comunicações e transações seguras de e‐mail.

Pode parecer que os smart cards nada mais são

do que um repositório para armazenar senhas. Obviamente,

alguém pode facilmente roubar um cartão inteligente de

alguém. Felizmente, há segurança

recursos embutidos em cartões inteligentes para evitar que alguém

de usar um cartão roubado. Os cartões inteligentes requerem

qualquer um que os esteja usando para entrar em uma conta pessoal

número de identificação (PIN) antes de serem

concedido qualquer nível de acesso ao sistema. O

O PIN é semelhante ao PIN usado pelos caixas eletrônicos.

Quando um usuário insere o cartão inteligente no cartão

leitor, o smart card solicita ao usuário um PIN.

Este PIN foi atribuído ao usuário pelo

administrador no momento em que o administrador emitiu

o cartão ao usuário. Como o PIN é curto e

puramente numérico, o usuário não deve ter problemas

lembrando-se disso e, portanto, seria improvável que

anote o PIN.

o usuário insere o PIN. O PIN é verificado por dentro

o cartão inteligente. Como o PIN nunca é

transmitidos pela rede, há absolutamente

nenhum perigo de ser interceptado. O principal

benefício, porém, é que o PIN é inútil sem

o cartão inteligente, e o cartão inteligente é inútil

sem o PIN.

Existem outros problemas de segurança do cartão inteligente.

O cartão inteligente é econômico, mas não tão seguro

como os dispositivos de identificação biométrica.

2. Desenvolvimentos de software

O aspecto de software da segurança de rede é muito

grande. Inclui firewalls, antivírus, vpn, intrusão

detecção e muito mais. A pesquisa

o desenvolvimento de todos os softwares de segurança não é viável

para estudar neste momento. O objetivo é obter uma visão de onde o software de segurança está indo com base em

ênfase sendo colocada agora.

A melhoria do padrão de segurança

software ainda permanece o mesmo. Quando novos vírus

surgir, o antivírus é atualizado para poder

proteger contra essas ameaças. Este processo é o

o mesmo para firewalls e sistemas de detecção de intrusão.

Muitos trabalhos de pesquisa que foram lidos

basearam-se na análise de padrões de ataque para

criar um software de segurança mais inteligente.

À medida que o hardware de segurança faz a transição para a biometria,

o software também precisa ser capaz de usar o

informações adequadamente. A pesquisa atual é

sendo executado em software de segurança usando neural

redes. O objetivo da pesquisa é utilizar

redes neurais para o software de reconhecimento facial.

Muitos dispositivos pequenos e complexos podem ser conectados

para a internet. A maior parte da segurança atual

algoritmos são computacionais intensivos e requerem

poder de processamento substancial. Este poder,

no entanto, não está disponível em pequenos dispositivos como

sensores. Portanto, há a necessidade de projetar

algoritmos de segurança leves. Pesquisa neste

área está sendo executada.

TENDÊNCIAS FUTURAS EM SEGURANÇA

O que vai impulsionar a segurança da Internet é o

conjunto de aplicativos mais do que qualquer outra coisa. O

futuro possivelmente será que a segurança é semelhante a

um sistema imunológico. O sistema imunológico combate

ataca e se constrói para lutar contra inimigos mais difíceis.

Da mesma forma, a segurança da rede será capaz de

funcionam como um sistema imunológico.

A tendência para a biometria poderia ter ocorrido

lugar há um tempo atrás, mas parece que não está sendo

perseguido ativamente. Muitos desenvolvimentos de segurança que

estão ocorrendo estão dentro do mesmo conjunto de segurança

tecnologia que está sendo usada hoje com alguns

pequenos ajustes.

CONCLUSÃO

A segurança de rede é um campo importante que é

ganhando cada vez mais atenção à medida que a internet

expande. As ameaças de segurança e protocolo de internet

foram analisados ​​para determinar a segurança necessária

tecnologia. A tecnologia de segurança é principalmente

baseado em software, mas muitos hardwares comuns

dispositivos são usados. O desenvolvimento atual em

segurança de rede não é muito impressionante.

Originalmente, assumiu-se que com a importância

do campo de segurança de rede, novas abordagens para

segurança, tanto de hardware quanto de software, seria

pesquisado ativamente. Foi uma surpresa ver a maioria

o desenvolvimento que ocorre no mesmo

tecnologias que estão sendo usadas atualmente. o embutido

segurança do novo protocolo de internet IPv6 pode

oferecem muitos benefícios aos usuários da Internet. Embora

alguns problemas de segurança foram observados, o IPv6

protocolo de internet parece fugir de muitos dos

ataques populares atuais. Uso combinado de IPv6 e

ferramentas de segurança, como firewalls, detecção de intrusão,

e os mecanismos de autenticação serão eficazes

na guarda de propriedade intelectual para o próximo

futuro. O campo de segurança de rede pode ter que

evoluir mais rapidamente para lidar com as ameaças ainda mais

no futuro.