ESAB – ESCOLA SUPERIOR ABERTA DO BRASIL - ESAB

REDES DE COMPUTADORES, TCP/IP E IPv6: O Caminho da segurança

Vagner Kunz Cabral [1]

Resumo

Este estudo teve o objetivo de analisar a concepção e evolução das redes de computadores e o principal protocolo de comunicação da Internet (TCP/IP), com olhos voltados para a segurança nessa comunicação. Dentre os autores pesquisados para a constituição conceitual deste trabalho, destacaram-se Tanenbaum (1997), Murhammer (2000), Marques (2000). A metodologia utilizada foi a pesquisa bibliográfica, tendo como coleta de dados o levantamento bibliográfico dos autores citados somado a artigos relacionados ao conteúdo bem como teses e trabalhos acadêmicos. As conclusões mais relevantes deram-se na observação de que o aspecto de segurança está em constante teste e evolução, acompanhando as evoluções na tecnologia envolvida no processo de comunicação via redes de computadores.

Palavras-chave: Redes, OSI, TCP/IP, Criptografia, Segurança.

1. Introdução

A comunicação faz parte da evolução humana desde os primórdios. A evolução é constante na história, e o processo de comunicação não poderia ter ficado para trás. Assim, a necessidade obrigou o homem a trabalhar de forma a ampliar o alcance e otimizar as comunicações. Com o surgimento de máquinas computacionais, estudos e pesquisas produziram o que hoje conhecemos como redes de computadores, em que o termo Internet é praticamente conhecido (e utilizado) em todo o planeta.

A partir de estudos realizados sobre o trabalho de grandes profissionais e idealizadores das redes de computadores, é possível contribuir de forma resumida, o histórico das redes de computadores, particularidades na padronização da comunicação e a questão segurança envolvida nestes processos.

[1] Pós graduando em Redes de Computadores na Escola Superior Aberta do Brasil – ESAB.
vagnerpantufa@gmail.com / vagner.cabral@corsan.com.br

O presente estudo delimita-se a descrever de forma sucinta a evolução das redes de computadores e do protocolo TCP/IP utilizado na Internet, além de rápidas palavras sobre a transição entre as versões 4 e 6 do protocolo IP, e como se dá a segurança em redes associada a estes protocolos. O objetivo geral é demonstrar, com o apanhado da bibliografia, o histórico das redes de computadores, mais especificamente da Internet e algumas particularidades, momento em que trata-se a respeito dos protocolos.

A justificativa da escolha do tema bem como o discorrer sobre o assunto dá-se pelo alinhamento do tema ao curso que se objetiva concluir, além de representar o *core* ou *cerne* dos conceitos apresentados e estudados no decorrer do curso. A metodologia utilizada para compor este documento foi a pesquisa bibliográfica e cruzamento de informações entre os autores, bem como compilação de informações disponíveis na própria Internet a respeito do conteúdo escolhido.

2. Desenvolvimento

O termo "redes de computadores" trata a respeito da conexão de dispositivos computacionais com o objetivo de compartilhar recursos e/ou informações. Para Tanenbaum(1997), é natural que empresas possuam um número significativo de computadores em operação instalados em locais distantes entre si oportunizando o tráfego de informações, conceituando o termo "redes corporativas".

A conexão entre estes recursos computacionais em uma rede sugere características que devem ser apuradas. Desde um contexto mais estratégico para o negócio (economia, lucro, *compliance*, etc.) quanto em se tratando de um foco mais técnico (eficiência, segurança da informação, controle de acesso, garantia da comunicação, disponibilidade, etc.), e até mesmo voltado para o aspecto humano e social (ergonomia, segurança física, salubridade, periculosidade, etc.). (TANENBAUM, 1997).

A partir da implementação das primeiras redes de computadores, até então heterogêneas (MARQUES, 2000), a Agência de Projetos e Pesquisas Avançadas – ARPA (*Advanced Research Projects Agency*), órgão do governo americano, na década de 70, voltava suas pesquisas à interconexão de redes de computadores e tinha seu foco em interconexão de

redes heterogêneas. Tais pesquisas culminaram em uma rede chamada ARPANET que viria futuramente a originar a INTERNET.

Com a chegada e estabelecimento da INTERNET como a grande rede mundial de computadores, amplia-se o espectro de possibilidades de uso desta rede, deixando de possuir características específicas para fins militares e acadêmicos. Inicia-se o uso comercial desta rede, com um alcance e ritmo de crescimento acelerado (MURHAMMER, 2000). Assim, o sucesso da Internet, aliado à frustração da comunidade de pesquisa que já não desfrutava mais com exclusividade no uso da Internet, formaram o projeto Internet2 com os seguintes objetivos:

Largura de banda: prover uma alta largura de banda para a comunidade de pesquisa dos EUA;

Exploração da banda: desenvolver tecnologias de comunicação e aplicativos a fim de explorar as possibilidades da rede ao máximo;

Difundir e disponibilizar as tecnologias para toda a comunidade envolta na Internet, tanto nos EUA quanto fora dele;

As redes de computadores passam a ser classificadas segundo Marques (2000, p.7) como:

> "a) Redes Locais: *Local Area Nets* (LANs). Surgiram da necessidade de compartilhamento de recursos (impressoras, hds, multimídias, fitas, discos, etc.), bem como para agilizar comunicação entre usuários. As LANs normalmente são encontradas (restritas ou não) em empresas, repartições públicas, etc.
> b) Redes Metropolitanas: *Metropolitan Area Nets* (MANs). Surgiram da necessidade de comunicação e copmpartilhamento de recursos por usuários geograficamente distantes.
> c) Redes de Longa Distância: Wide Area Networks (WANs). Diferenciam-se das MANs simplesmente pelo atributo distância."

Conforme Marques (2000, p.12) a Interoperabilidade é a solução que visa permitir que sistemas desenvolvidos por diferentes grupos em diferentes plataformas e/ou sistemas operacionais possam se comunicar. A necessidade de padronização torna-se iminente, visto o potencial alcance da Internet, atingindo usuários corporativos e domésticos.

A padronização da comunicação nas redes inicia com um conjunto de protocolos que pudessem tratar diferentes camadas de comunicação, proporcionando a diferentes fabricantes uma comunicação única. Em um primeiro momento, deveriam ser contemplados serviços de

comunicação com o foco no hardware para a composição do modelo ideal a ser seguido. À medida em que a necessidade de hardware fosse atendida, haveria uma abstração em níveis mais acima para o atendimento via software. Assim, foi constituído um modelo de hierarquia de protocolos, em camadas, e com interface entre camadas de forma a definir operações e serviços que a camada imediatamente inferior oferece à camada imediatamente superior. Sobre a hierarquia de protocolos, segue bloco extraído de TANENBAUM (1997, p.19):

> "[...] a maioria das redes foi organizada como uma série de camadas ou níveis, que são colocados um em cima do outro. O número, o nome, o conteúdo e a função de cada camada difere de uma rede para outra. Em todas as redes, no entanto, o objetivo de cada camada é oferecer determinados serviços para as camadas superiores, ocultando detalhes da implementação desses recursos.
>
> A camada n de uma máquina se comunica com a camada n da outra máquina. Coletivamente, as regras e convenções usadas nesse diálogo são chamadas de protocolo da camada n. Basicamente, um protocolo é um conjunto de regras sobre o modo como se dará a comunicação entre as partes envolvidas. Como uma analogia, quando uma mulher é apresentada a um homem, pode estender a mão pra ele, que, por sua vez, pode apertá-la ou beijá-la, dependendo, por exemplo, se ela for uma advogada americana que esteja participando de uma reunião de negócios ou uma princesa europeia presente em um baile de gala. A violação do protocolo dificultará a comunicação e em alguns casos poderá impossibilitá-la."

Abaixo podemos observar na figura 1 um esboço da comunicação entre as camadas de um modelo padronizado de protocolos e as interfaces associadas:

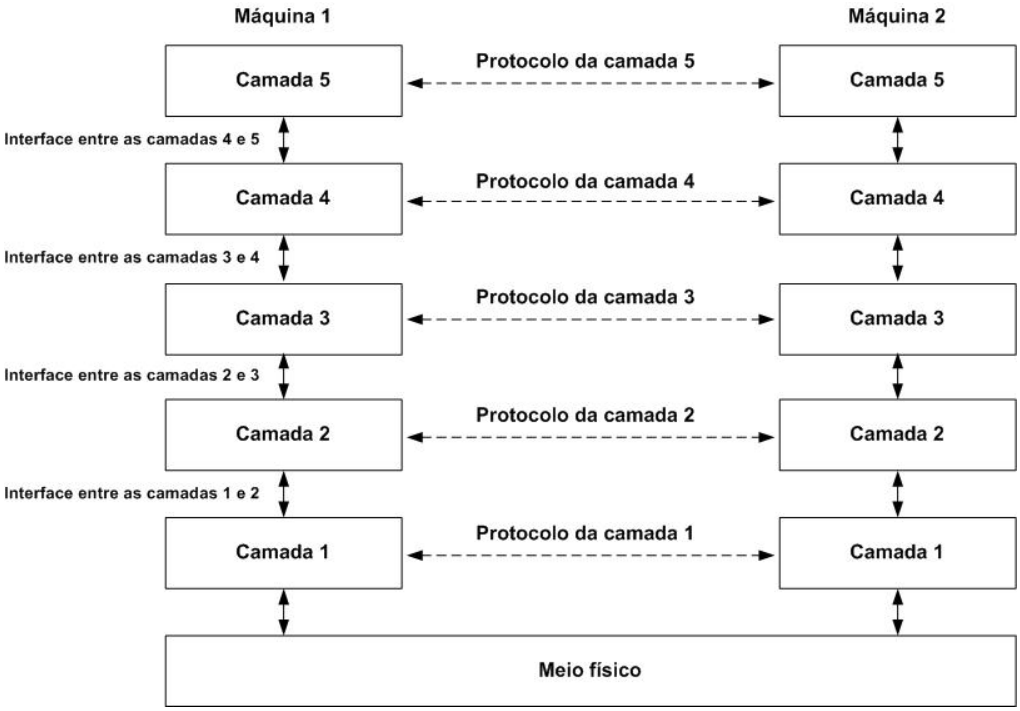

Figura 1: Camadas Protocolos e interfaces
Fonte: TANENBAUM (1997)

2.1 Modelo OSI e o protocolo TCP/IP

Esforços de diferentes organizações e comitês voltados à padronização de um modelo de camadas a ser seguido para estabelecimento de uma solução comum resultaram no Modelo de Referência (ISSO 7498) OSI (*Open Systems Interconect* – Interconexão de Sistemas Abertos). Este modelo propunha a concepção de sete camadas de comunicação com protocolos para cada camada (MURHAMMER, 2000 p. 9). Tais camadas são, sempre, percorridas tanto no envio (de cima pra baixo) quanto na recepção (de baixo pra cima) de pacotes por uma determinada estação. Cada uma das camadas deve atender as solicitações da imediatamente superior (MARQUES, 2000 p. 13).

Como podemos observar na figura 2, as camadas do modelo OSI tem seu início na forma física de comunicação, crescendo em abstração e dividindo a comunicação em sete camadas diferentes, cada uma com uma lógica e função específica.

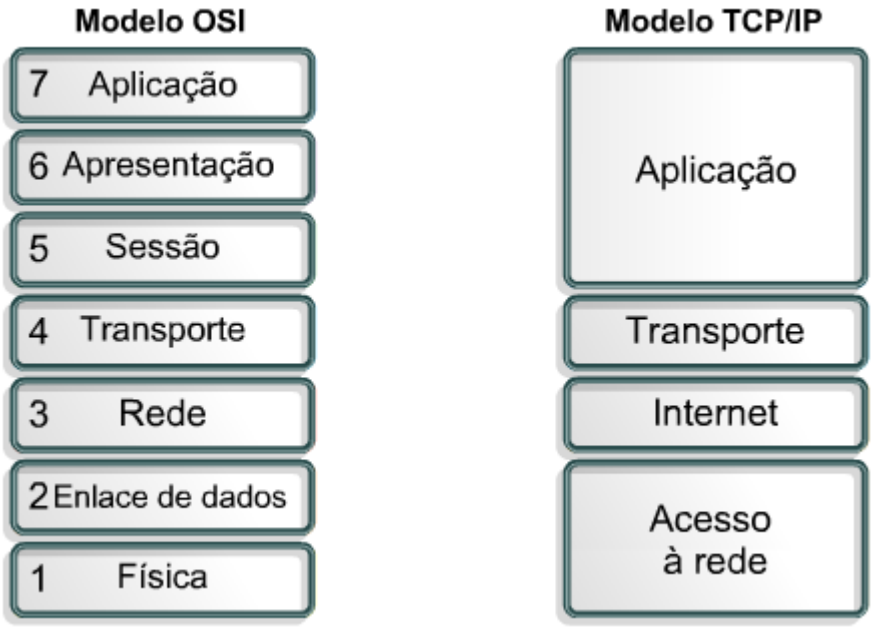

Figura 2: Ilustração de camadas no modelo OSI e no modelo TCP/IP
fonte: https://jbgsm.wordpress.com/2010/05/31/camadas-tcpip/

Conforme Tanenbaum (1997, p. 32-38), as camadas do modelo OSI possuem as seguintes funções:

> Camada Física: trata da transmissão de bits brutos através de um canal de comunicação(...). As questões acerca desta função são: quantidade de volts a ser usada para representar bits 0 e 1; quantidade de microssegundos que um bit deve durar; se a transmissão dar-se-á nas duas direções; forma de estabelecimento e encerramento da conexão; quantidade de pinos que o conector precisará e de que maneira serão utilizados;
>
> Camada de Enlace de dados: transforma um canal de transmissão bruta de dados em uma linha que pareça livre de erros de transmissão não detectados na camada de rede;
>
> Camada de Rede: controla a operação da sub-rede. Diz respeito ao modo como os pacotes são roteados da origem para o destino;
>
> Camada de Transporte: aceita dados da camada de sessão, divide-os em unidades menores em caso de necessidade e os passa para a camada de rede garantir que cheguem corretamente à outra extremidade;
>
> Camada de Sessão: permite que os usuários de diferentes máquinas estabeleçam sessões entre eles;
>
> Camada de Apresentação: executa determinadas funções solicitadas com muita frequência. Gerencia estruturas de dados abstratas (tabelas diferentes de caracteres e o complemento de um e de dois, por exemplo) e converte a representação utilizada na representação padrão de rede;
>
> Camada de Aplicação: Possui uma variada série de protocolos. A principal função é a interpretação de ações e informações como interface para e com o usuário. A transferência de arquivos entre sistemas diferentes também cabe a esta camada.

Já o modelo TCP/IP (*Transmission Control Protocol/Internet Protocol*), utilizado na configuração de equipamentos conectados à Internet, suprime algumas camadas e é demonstrado em apenas quatro níveis. Conforme Murhammer (2000, p.12), a camada de "Acesso à rede" também chamada de camada de enlace, trata da interface com o hardware de rede, isto é, padroniza e trata o sequenciamento de bits de dados em meio físico por meio da

administração dos aparelhos (hardwares) utilizados. No outro oposto da pilha de camadas TCP/IP temos a camada de aplicação, em que roda o programa que utiliza o TCP/IP para comunicação. Marques (2000, p.18) afirma que a Camada de Aplicação abriga os protocolos capazes de traduzir os objetos de cada pacote recebido. Exemplos de pacotes da camada de aplicação são: SMTP, POP3, HTTP, FTP, Telnet, etc. As camadas centrais do modelo TCP/IP podem ser explicadas por Murhammer (2000, p.12):

> "A camada de transporte fornece a transferência de dados de uma ponta a outra. Aplicações múltiplas podem ser suportadas simultaneamente. A camada de transporte é responsável pelo fornecimento de um intercâmbio de informações confiável. O principal protocolo da camada de transporte é o TCP[...].
>
> A camada de inter-redes, também chamada de *camada de internet* ou *camada de rede*, fornece a imagem da "rede virtual" de uma inter-rede (Istoé, esta camada protege os níveis mais altos da arquitetura de rede física que está abaixo). O IP (*Internet Protocol*) é o protocolo mais importante nesta camada. É um protocolo *sem conexão* que não pressupõe confiabilidade das camadas mais baixas. O IP *não* fornece confiabilidade, controle de fluxo ou recuperação de erros. Estas funções devem ser fornecidas em um nível mais alto."

2.2 IP, IPV4 e IPV6

O protocolo IP (*Internet Protocol*) encontra-se nas camadas de nível mais baixo. É um protocolo de entrega de pacote não confiável, de melhor esforço e sem conexão (MURHAMMER, 2000). Isto significa que os pacotes enviados por este protocolo podem ser perdidos, por vezes chegarem em duplicidade no destino ou até mesmo fora de ordem, situação esta em que o tratamento não depende deste protocolo, mas sim de protocolos referentes a camadas mais altas do modelo.

O endereçamento IP é formado por conjuntos de 4 Bytes ou 32 bits (conjunto de quatro sequencias de 8 bits), separados por pontos, como no exemplo: *200.114.207. 71*. Cada octeto de bits pode ser representado por um número que vai de 0 a 255. Para que esta técnica pudesse prever o maior número de registros IP possíveis, de forma organizada, surge o conceito de Classes de IP.

Sobre classes de IP, Marques (1997, p.27-29) diz:

> "O endereço IP deve ser capaz de informar não somente a máquina à qual está associado, mas, logicamente, também a rede em que está conectado (ou as informações a ele nunca chegariam). Para tanto os endereços IPs foram divididos em "Classes" as quais informam a separação entre endereços de rede e de

> computadores. Vale salientar que os três primeiros algarismos (bits), de um endereço IP, identificam a classe à qual pertence à rede."

Segundo a matéria sobre IP na revista INFOWESTER, um esquema de distribuição estabelecido pelas entidades IANA (*Internet Assigned Numbers Authority*) e ICANN (*Internet Corporation for Assigned Names and Numbers*) divide os endereços em três classes principais e mais duas complementares.

As classes são assim divididas:

Classe A: IP 0.0.0.0 a IP 127.255.255.255 - até 128 redes, até 16 milhões de dispositivos conectados em cada uma;

Classe B: IP 128.0.0.0 a IP 191.255.255.255 - até 16.384 redes, até 65 mil dispositivos em cada uma das possíveis redes;

Classe C: IP 192.0.0.0 a IP 223.255.255.255 - até 2.097.152 redes, até 254 dispositivos em cada uma destas possíveis redes;

Classe D: IP 224.0.0.0 a IP 239.255.255.255;

Classe E: IP 240.0.0.0 a IP 255.255.255.255.

Até então falamos sobre a composição e organização de números IP na versão 4, ou seja, o conceito de IPV4. Observe que esta metodologia foi criada em meados dos anos 70, sem que se pudesse prever o crescimento das redes e quantidade de dispositivos distintos candidatos a troca de informações.

Para que pudesse ser ampliado o alcance da numeração/identificação dos dispositivos conectados a redes, em virtude do previsível esgotamento de endereços IPV4, foi implementada e homologada uma nova versão de endereçamento IP, conhecida como IPV6.

A diferença notável entre as versões 4 e 6 é o formato: o IPV4 é constituído por 32 bits, enquanto que o IPV6 é formado por 128 bits. Assim, teoricamente, a quantidade de endereços disponíveis no IPV6 pode chegar a um número infinitamente maior de dispositivos. O IPv6 utiliza oito sequências de até quatro caracteres separado pelo sinal de "dois pontos", considerando o sistema hexadecimal. Exemplo: 2F5C:34D3:123C:0:0:29:A4B3:F2CF (INFOWESTER).

Duarte (2013) analisa em seu trabalho titulado “IPv4 to IPv6 *transition: security challenges*” (Transição IPv4 para IPv6: desafios da segurança), as dificuldades encontradas na substituição prática de endereços IPv4 para endereços reais IPv6. O autor trata com bastante precaução a conversão, em detrimento de toda uma base de segurança construída para o IPv4 e que necessita ser aprimorada e/ou modificada a fim de atender a versão 6 do protocolo IP. Mas também compila em sua análise as questões que levam a necessidade de evoluir e adaptar-se, à medida em que a necessidade de evolução surge.

> “Os fatores chave da gestão de redes (e também na Internet) são a disponibilidade de serviço e a segurança do mesmo. Com este novo protocolo, surgem também novos ataques de segurança, um novo paradigma de redes e inicia-se a troca do principal meio de comunicação da Internet - a mudança de IPv4 para IPv6 levanta desafios na transição dos serviços e utilizadores de forma segura e economicamente sustentável. Mesmo conseguindo uma transição suave, aguarda-nos ainda o desafio de garantir (pelo menos) o mesmo nível de segurança informática existente hoje nas nossas redes com um conjunto tão diferente de protocolos.” (DUARTE, 2013).

Após a contextualização de como são constituídas as redes de computadores e de uma breve visão da implementação dos números IP, identificadores dos equipamentos ou pontos de acesso em uma rede, vale lembrar que a tecnologia tem evoluído ao passar dos anos. Esta evolução tecnológica contribui para a transparência, o acesso a informações, a comodidade e tantos outros aspectos positivos do cotidiano. Mas também é preciso salientar que a tecnologia alimenta também o viés negativo, proporcionando apropriação indevida de informações e constrangimentos, fraudes, roubos e etc. Assim, cabe uma análise sobre aspectos comportamentais dos usuários, em associação com os recursos que as redes de computadores proporcionam.

2.3 Segurança em redes

O autor ESTRELA (1998) em sua dissertação de mestrado, analisa, sob diversos aspectos o quesito segurança em redes de computadores. Segundo este autor:

> “O problema da segurança de redes de computadores não se pode considerar de forma alguma um assunto resolvido e já com soluções cabais para os diferentes problemas de segurança que se colocam e que sejam adaptáveis de forma simples a qualquer rede particular [...]
>
> As dificuldades inerentes a uma solução deste gênero centram-se na constante evolução das tecnologias de rede e nas potenciais falhas de segurança que poderão ser exploradas e, por outro lado, a abertura à Internet das redes de computadores tornam-nas vulneráveis a enorme quantidade de utilizadores mal intencionados. [...]

> A **segurança da informação** teve sempre uma enorme relevância para as pessoas e organizações. A obtenção de determinada informação relevante permite obter vantagem competitiva, sem que o detentor dessa informação possa sequer ter conhecimento disso. O acesso e a alteração de dados de forma ilícita pode levar uma organização a tomar ações que de outro modo não tomaria, e pode acarretar enormes prejuízos para organização ou pessoas, em beneficio do próprio atacante." ESTRELA (1998, p.14-18)

O relato de Estrela (1998) traz uma análise sobre a preocupação da segurança em redes de computadores, ainda atual. A evolução da segurança é diretamente proporcional ao esforço para burlá-la.

Esta análise contempla itens importantes na caracterização de problemas de segurança em redes, tais como tipos de ataque à segurança, modelos de segurança, estratégias de segurança e políticas de segurança, entre outros.

Com relação a soluções para eventuais problemas na segurança de redes, é ponto recorrente a ser destacado, o uso da Criptografia a fim de promover o encapsulamento de dados e informações, de forma a oportunizar a compreensão do conteúdo apenas aos interessados e envolvidos (emissor e receptor de conteúdo).

Sobre Criptografia em redes, segundo ChesBe94 (1994, apud ESTRELA, 1998 p. 30):

> "A criptografia é a solução usual para a necessidade de comunicar sobre ligações inseguras sem a exposição do sistema. A utilização mais comum da criptografia é, obviamente, a manutenção da comunicação secreta. A autenticação está também relacionada com a criptografia, quer dizer, um pacote que não seja cifrado com uma chave correta não será decifrado em algo que faça sentido, o que limita consideravelmente a possibilidade de injeção de falsas mensagens."

Ainda, Stall94a (1994, apud ESTRELA, 1998 p. 30):

> "Um número crescente de aplicações e protocolos usados sobre a Internet tem facilidades significativas relacionadas com a segurança ou tem como finalidade primária a provisão de alguma facilidade de segurança. Ao nível da aplicação temos os exemplos da segurança de *e-mail* (*Privacy Enhanced Mail* – PEM, *Pretty Good Privacy* – PGP), gestão de rede (*Simple Network Management Protocol version 2* – SNMPv2), e autenticação remota (*Kerberos*). Uma facilidade comum em todas estas aplicações e protocolos é a utilização de algoritmos criptográficos para implementar serviços de segurança particulares. A maioria destes algoritmos cabem em três categorias: algoritmos de cifragem convencional, algoritmos criptográficos de chave pública, e funções de *hash* seguras."

Já sobre os aspectos legais de criptografia, observamos em DornDC98 (1998, apud ESTRELA, 1998 p.44):

> "A criptografia está sujeita às políticas dos vários governos que detém o direito de controlar a exportação, importação, e uso da cifragem no interesse da segurança nacional. Alguns países permitem-na, muitos restringem-na, e outros proíbem-na

> completamente, não deixando outra alternativa aos gestores de rede senão utilizar a cifragem mais forte disponível.”

A criptografia utilizada para cifragem de mensagens pode ser aplicada por meio de algoritmos em softwares, nas camadas mais altas do protocolo TCP/IP (sessão e apresentação), como o algoritmo RSA (chave pública).

A implementação de segurança sobre protocolo de Internet age como uma subcamada entre os protocolos (TCP/IP). Esta implementação é conhecida como SSL (*Secure Sockets Layer*) e seu sucessor TLS (*Transport Layer Security*).

Segundo E-COMMERCEBRASIL: “Uma vez que o cliente e o servidor tenham decidido usar TLS/SSL, eles negociam um estado de conexão usando um procedimento de *handshaking*, no qual o cliente e o servidor concordam em vários parâmetros utilizados para estabelecer a conexão segura.”.

Para entendermos melhor como ocorre o processo de estabelecimento de canal confiável utilizando a técnica de SSL/TLS em comunicação TCP/IP, foi extraído o passo a passo de como dá-se o *handshaking* entre os pares, isto é, o efetivo processo de autenticação entre os entes da comunicação:

> “Uma sessão SSL sempre começa com uma troca de mensagens chamada SSL *handshake*. ◦Aqui está o resumo das etapas envolvidas no *handshake* SSL.
> **1.** O cliente envia ao servidor o número de versão SSL do cliente, configurações de criptografia, dados gerados aleatoriamente e outras informações que o servidor precisa para se comunicar com o cliente usando SSL.
> **2.** O servidor envia ao cliente o número de versão SSL do servidor, definições de cifra, dados gerados aleatoriamente e outras informações que o cliente necessita para comunicar com o servidor através de SSL. O servidor também envia seu próprio certificado digital e, se o cliente está solicitando um recurso de servidor que requer autenticação de cliente, solicita o certificado digital do cliente.
> **3.** O cliente usa as informações enviadas pelo servidor para autenticar o servidor. Se o servidor não pode ser autenticado, o usuário é avisado do problema que uma conexão criptografada e autenticada não pode ser estabelecida. Se o servidor pode ser autenticado com êxito, o cliente prossegue.
> **4.** Usando todos os dados gerados no *handshake* até o momento, o cliente cria o segredo *premaster* para a sessão, criptografa-o com a chave pública do servidor (obtida a partir do certificado digital do servidor) e envia o segredo criptografado para o servidor.
> **5.** Se o servidor solicitou a autenticação do cliente (uma etapa opcional no *handshake*), o cliente também assina outro pedaço de dados, que é exclusivo para este *handshake* e conhecido tanto pelo cliente quanto pelo servidor. Nesse caso, o cliente envia tanto os dados assinados como o certificado digital do cliente para o servidor juntamente com o segredo criptografado *premaster*.
> **6.** Se o servidor solicitou a autenticação do cliente, o servidor tenta autenticar o cliente. Se o cliente não puder ser autenticado, a sessão será encerrada. Se o cliente

> pode ser autenticado com êxito, o servidor usa sua chave privada para descriptografar o segredo *premaster* e, em seguida, executa uma série de etapas que o cliente também executa, a partir do mesmo segredo *premaster* para gerar o segredo mestre.
> **7.** Tanto o cliente como o servidor usam o segredo mestre para gerar chaves de sessão que são chaves simétricas usadas para criptografar e descriptografar informações trocadas durante a sessão SSL e para verificar sua integridade.
> **8.** O cliente informa ao servidor que mensagens futuras do cliente serão criptografadas com a chave de sessão. Em seguida, envia uma mensagem criptografada separada indicando que a parte do cliente do *handshake* está concluída.
> **9.** O servidor envia uma mensagem ao cliente informando que futuras mensagens do servidor serão criptografadas com a chave de sessão. Em seguida, envia uma mensagem criptografada separada indicando que a parte do servidor do *handshake* está concluída.
> **10.** O *handshake* SSL agora está completo e a sessão SSL começou. O cliente e o servidor usam as chaves de sessão para criptografar e descriptografar os dados enviados uns aos outros e para validar sua integridade."
> Texto extraído de (PIEROBON, 2016, np) e traduzido.

Abaixo, na figura 3, podemos identificar visualmente a comparação entre comunicações entre pares, à esquerda sem a utilização de SSL e à direita com a segurança implementada sobre TCP/IP:

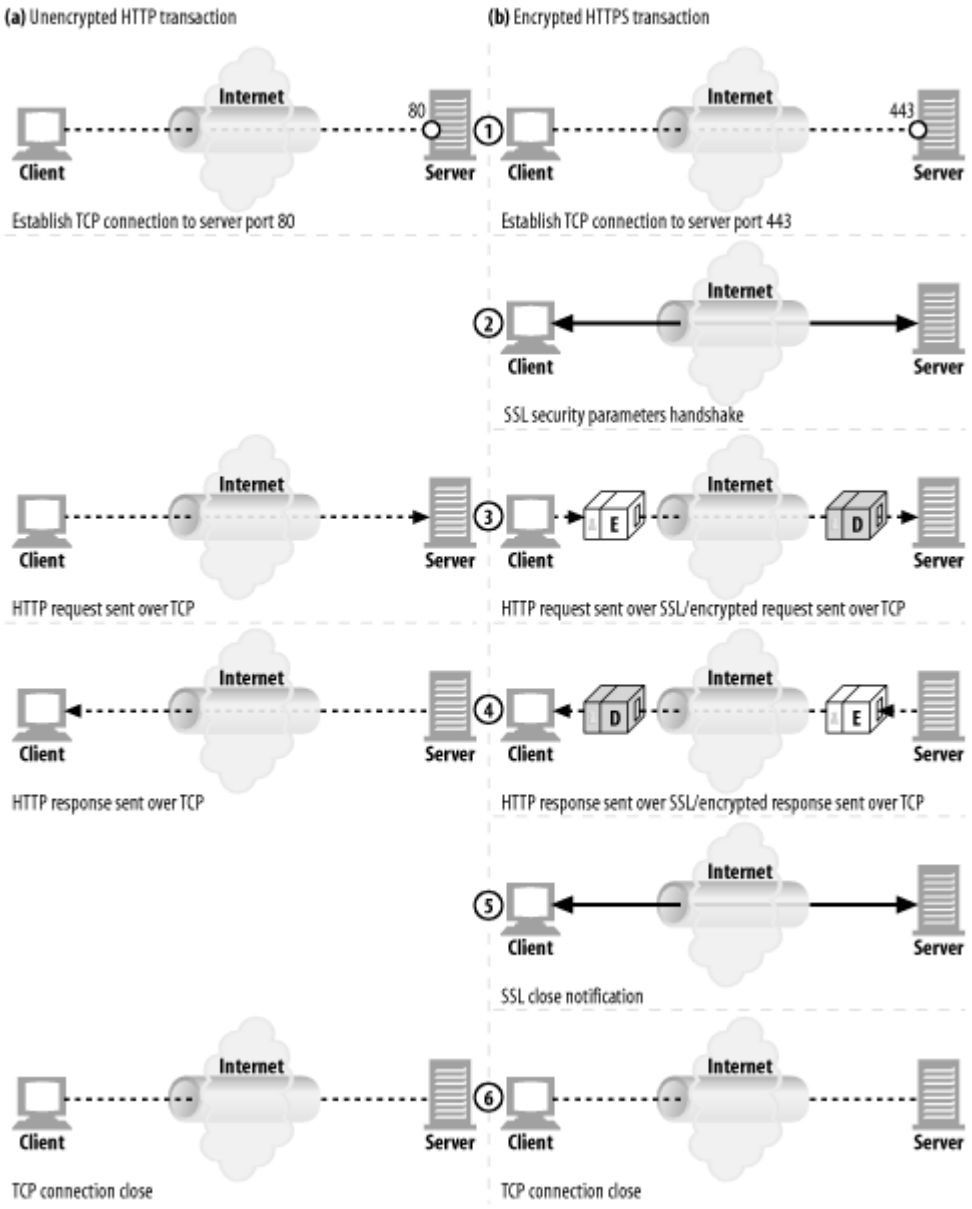

Figura 3. Comparação de comunicações com e sem SSL sobre TCP/IP
Fonte: http://flylib.com/books/en/1.2.1.138/1/

3. Conclusão

Em se tratando de redes de computadores, em geral, tanto com relação à Internet quanto a redes de menor alcance e escopo, a evolução da tecnologia envolvida é notável ao passar dos anos, como podemos observar a partir do histórico apresentado com base nos autores escolhidos.

Observa-se também que a composição das definições acerca de modelos a serem seguidos, tais como o modelo OSI, base para implementação do protocolo TCP/IP e tantos

outros, é fruto de extensas pesquisas e testes. Ainda, este trabalho dá-se visando não somente a disseminação do conhecimento, o suporte em quesitos de informações, a padronização a ser seguida por diferentes fabricantes e fornecedores, mas também a visão de crescimento em volume de equipamentos, e alcance a diferentes meios e dispositivos que podem vir a fazer parte da conexão em rede e garantias de segurança na comunicação em rede.

A evolução do protocolo IPV4 para IPV6, o uso de criptografia em sistemas e tecnologias implementadas sobre protocolos de rede (SSH sobre TCP/IP), são exemplos de nuances a serem analisadas sob o aspecto segurança em redes de computadores.

O espectro de estudos em redes de computadores é bastante vasto. Assim, é importante ressaltar como novos rumos e hipóteses de trabalhos, os estudos a respeito do comportamento humano frente a tecnologias de comunicação em rede (conceitos de *netiqueta*, comportamento, tendências, experiências, etc.), bem como novas tecnologias já em funcionamento (wireless, fibra ótica, etc.), além de pesquisas recentes na área.

4. Referências

TANENBAUM, A. S. – **Redes de Computadores** – 4ª Ed., Editora Campus Ltda., 1997.

MURHAMMER, Martin W. et al. - **Tcp/Ip: Tutorial e Técnico**. Ed. Makron Books, 2000.

MARQUES, W.S. **– TCP-IP: Projetando Redes.** Ed. Brasport, 2000.

DUARTE, T. A. **IPv4 to IPv6 transition: security challenges**. 02/02/2013. 75 folhas. Dissertação (Mestrado) – Faculdade de Engenharia da Universidade do Porto. Porto, 06/02/2013.

ESTRELA, J. M. M. **Segurança em Redes de Computadores: Estudo de um Caso**. 09/1998. 259 folhas. Dissertação (Mestrado) – Faculdade de Engenharia da Universidade do Porto. Porto, 09/1998.

FLYLIB.COM - **HTTPS: The Details**. Disponível em: <http://flylib.com/books/en/1.2.1.138/1/>. Acesso em: 24 nov. 2016

INFOWESTER 2001-2016 CONHECIMENTO TECNOLÓGICO AO SEU ALCANCE: **Endereço IP (Internet Protocol)**. Disponível em: <http://www.infowester.com/ip.php>. Acesso em: 24 nov. 2016

INFOWESTER 2001-2016 CONHECIMENTO TECNOLÓGICO AO SEU ALCANCE: **O que é IPv6?**. Disponível em: <http://www.infowester.com/ipv6.php>. Acesso em: 24 nov. 2016

E-COMMERCEBRASIL EXCELENCIA EM E-COMMERCE: **Segurança: como funciona o Protocolo SSL/TLS.** Disponível em: <https://www.ecommercebrasil.com.br/artigos/seguranca-como-funciona-o-protocolo-ssltls/>. Acesso em: 24 nov. 2016

PIEROBON, JOHN MICHAEL. **SSL Handshake Steps In Detail**. Disponível em: <http://www.pierobon.org/ssl/ch2/detail.htm>. Acesso em: 24 nov. 2016