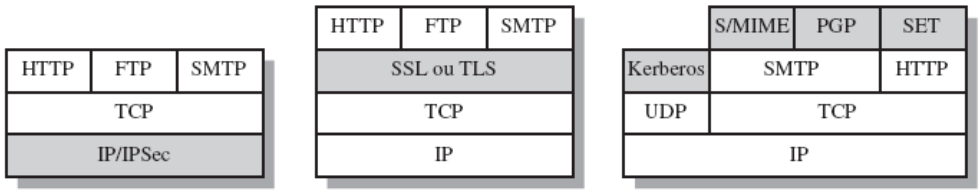
Capítulo 17

Tabela 17.1 Comparação de ameaças na Web [RUBI97].

	Ameaças	Conseqüências	Contramedidas
Integridade	• Modificação de dados do usuário • Navegador cavalo-de-tróia • Modificação de memória • Modificação de mensagens em trânsito	• Perda de informações • Comprometimento da máquina • Vulnerabilidade a todas as outras ameaças Somas de verificação (checksums) criptográficas	Somas de verificação (checksums) criptográficas
Confidencialidade	• Registro não autorizado de tráfego na rede • Roubo de informações do servidor • Roubo de dados do cliente • Informações sobre configurações de rede • Informações sobre qual cliente fala com o servidor	• Perda de informações • Perda de privacidade	Criptografia, proxies Web
Negação de serviço	• Encerramento de threads do usuário • Inundação da máquina com solicitações falsas • Preenchimento da capacidade total do disco ou da memória • Isolamento da máquina por ataques de DNS	• Interrupção • Incômodo • Impede que o usuário realize o trabalho	Difícil de impedir
Autenticação	• Simulação de usuários legítimos • Falsificação de dados	• Falsificação da identidade do usuário • Crença de que informações falsas são válidas	Técnicas criptográficas



(a) Nível de rede (b) Nível de transporte (c) Nível de aplicação

Figura 17.1 Local relativo das instalações de segurança na pilha de protocolos TCP/IP.

Figura 17.2 Pilha de protocolos SSL.

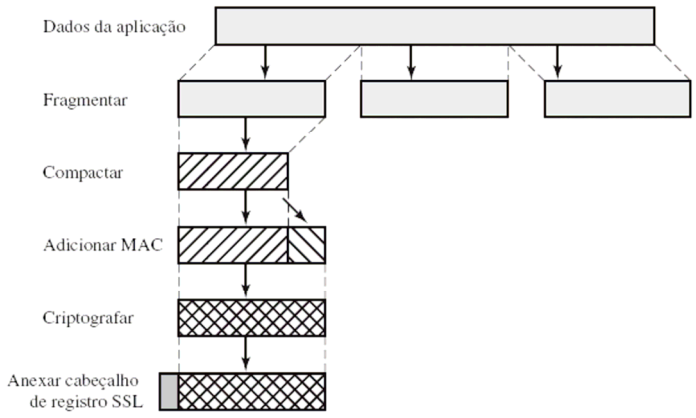


Figura 17.3 Operação do protocolo de registro SSL.

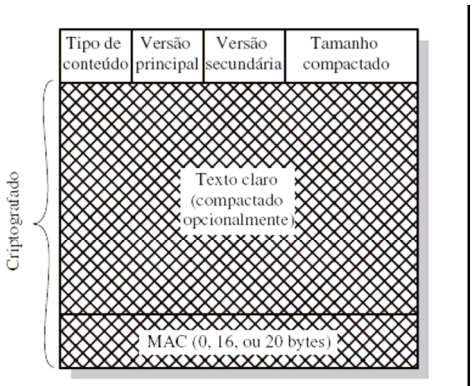


Figura 17.4 Formato do registro SSL.

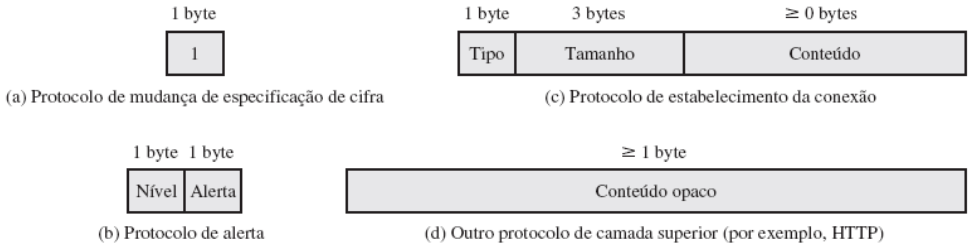


Figura 17.5 Payload do Protocolo de Registro SSL.

Tabela 17.2 Tipos de mensagem do Protocolo de Estabelecimento de Sessão SSL

Tipo de mensagem	Parâmetros
hello_request	Nulo
client_hello	versão, aleatório, ID de sessão, conjunto de cifras, método de compactação
server_hello	versão, aleatório, ID de sessão, conjunto de cifras, método de compactação
certificate	cadeia de certificados X.509v3
server_key_exchange	parâmetros, assinatura
certificate_request	tipo, autoridades
server_done	Nulo
certificate_verify	Assinatura
client_key_exchange	parâmetros, assinatura
finished	valor de hash

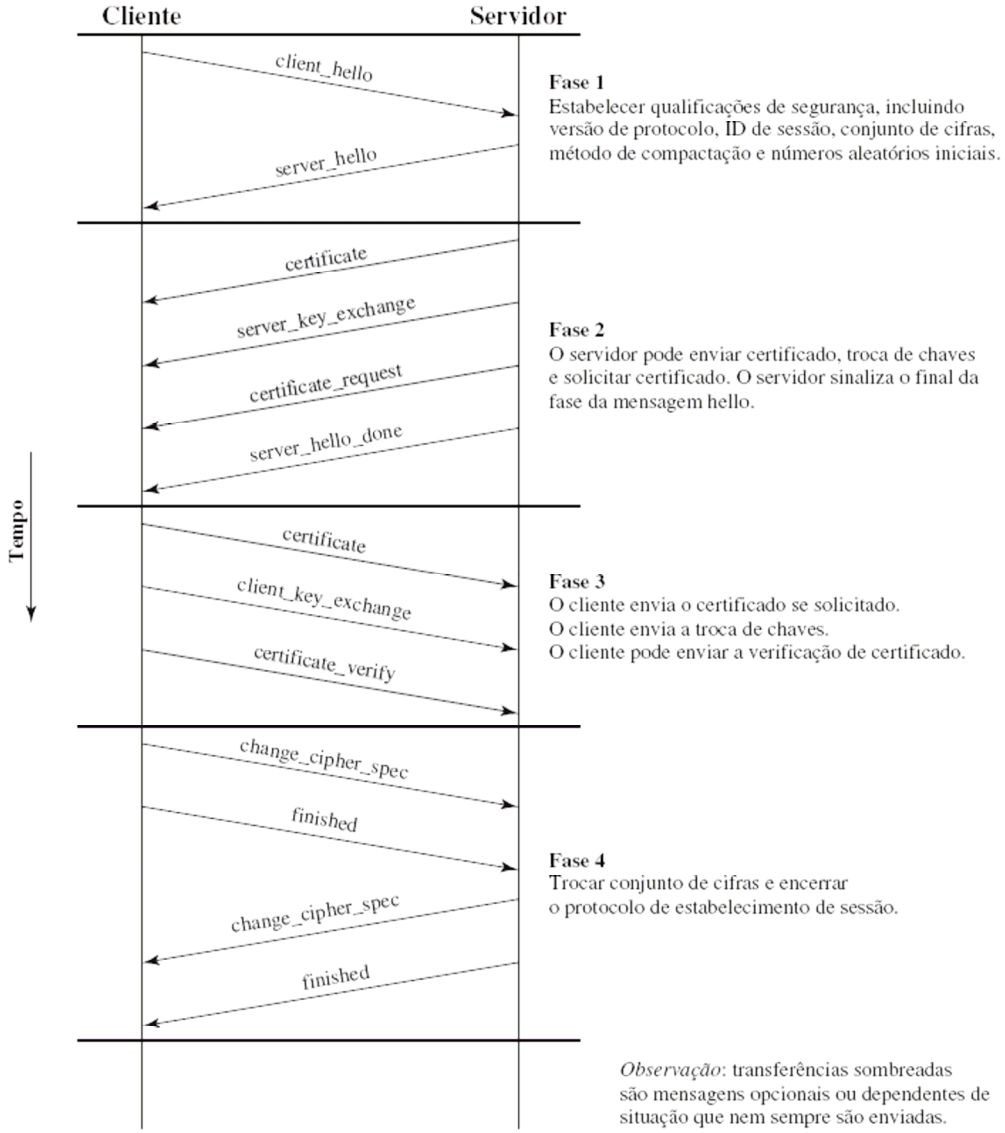


Figura 17.6 Ação do Protocolo de Estabelecimento de Sessão.

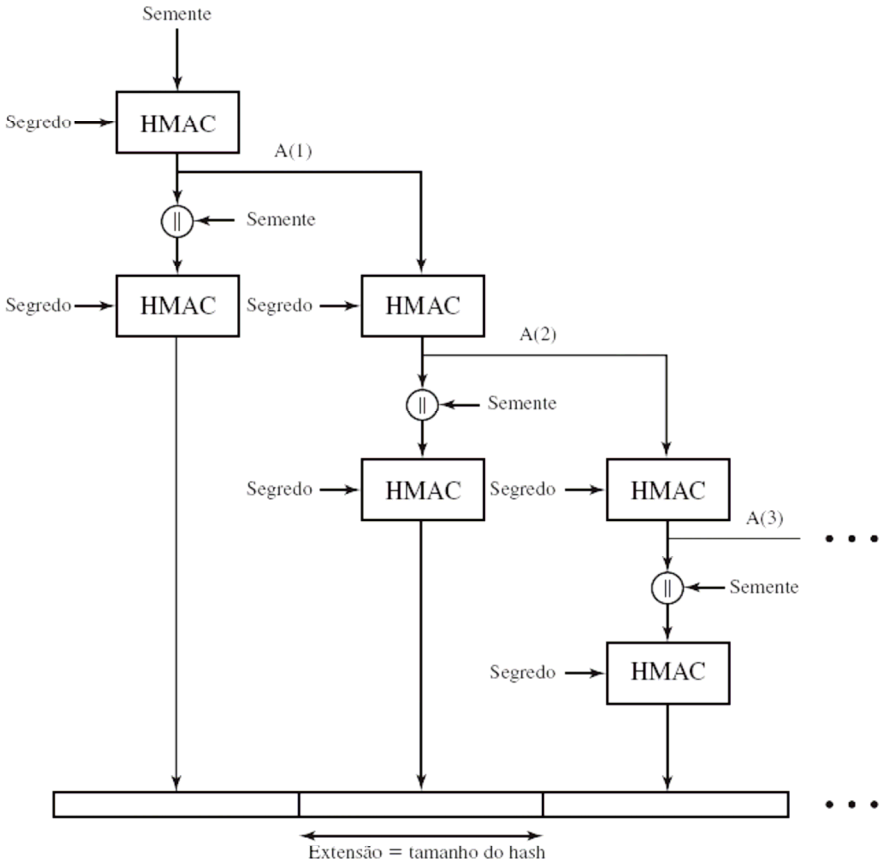


Figura 17.7 Função P_hash(segredo,semente) do TLS.

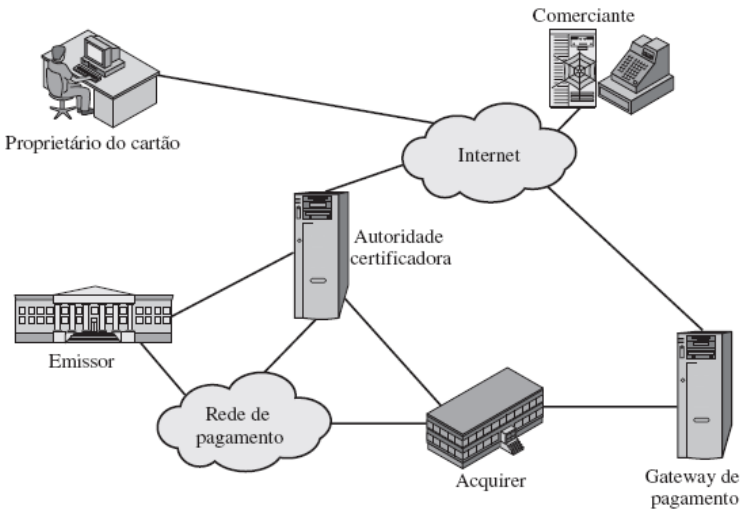
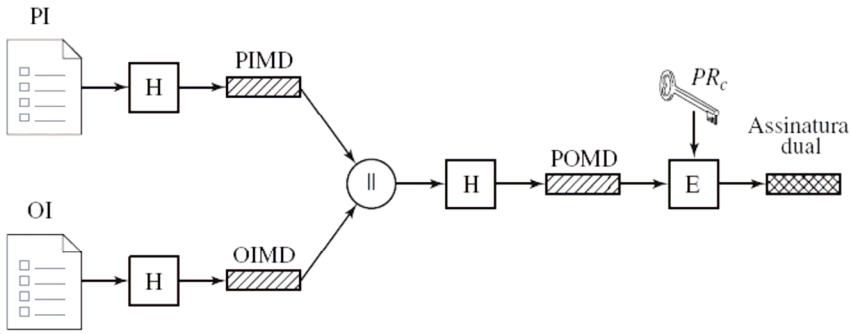


Figura 17.8 Componentes do comércio eletrônico seguro.



PI = Informações de pagamento
OI = Informações de pedido
H = Função de hash (SHA-1)
|| = Concatenação
PIMD = Resumo da mensagem de PI
OIMD = Resumo da mensagem de OI
POMD = Resumo da mensagem do pedido de pagamento
E = Criptografia (RSA)
PR_c = Chave de assinatura privada do cliente

Figura 17.9 Construção da assinatura dual.

Tabela 17.3 Tipos de transação SET

Registro do proprietário do cartão	Os proprietários de cartão precisam ser registrados em uma CA antes que possam enviar mensagens SET aos comerciantes.
Registro do comerciante	Os comerciantes precisam ser registrados em uma CA antes que possam trocar mensagens SET com clientes e gateways de pagamento.
Solicitação de compra	Mensagem do cliente a comerciante, contendo a OI para o comerciante e a PI para o banco.
Autorização de pagamento	Troca entre comerciante e gateway de pagamento para autorizar determinado valor para uma compra em determinada conta de cartão de crédito.
Captação de pagamento	Permite que o comerciante solicite o pagamento do gateway de pagamento.
Consulta e status de certificado	Se a CA for incapaz de concluir o processamento de uma solicitação de certificado rapidamente, ela enviará uma resposta ao proprietário do cartão ou comerciante, indicando que o solicitante deverá verificar novamente mais tarde. O proprietário do cartão ou comerciante envia a mensagem de consulta de certificado para determinar o status da solicitação de certificado e receber o certificado se a solicitação tiver sido aprovada.
Consulta de compra	Permite que o proprietário do cartão verifique o status do processamento de um pedido depois que a resposta da compra tiver sido recebida. Observe que essa mensagem não inclui informações como o status de bens que não estejam em estoque, mas sim o status da autorização, captação e processamento de crédito.
Cancelamento da autorização	Permite que um comerciante corrija solicitações de autorização anteriores. Se o pedido não for completado, o comerciante cancela a autorização inteira. Se parte do pedido não for completada (como quando os bens não estão em estoque), o comerciante cancela parte do valor da autorização.
Cancelamento de captação	Permite que um comerciante corrija erros nas solicitações de captação, como valores de transação que foram inseridos incorretamente por um funcionário.
Crédito	Permite que um comerciante emita um crédito para a conta de um proprietário de cartão, por exmplo quando os bens tenham sido devolvidos ou danificados durante a entrega. Observe que a mensagem de crédito do SET sempre é iniciada pelo comerciante, e não pelo proprietário do cartão. Toda a comunicação entre o proprietário do cartão e o comerciante que resulta no processamento de um crédito acontece fora do SET.
Cancelamento de crédito	Permite que um comerciante corrija um crédito solicitado anteriormente.
Solicitação de certificado de gateway de pagamento	Permite que um comerciante consulte o gateway de pagamento e receba uma cópia dos certificados atuais de troca de chaves e de assinatura do gateway.
Administração em lote	Permite que um comerciante comunique informações ao gateway de pagamento com relação a lotes do comerciante.
Mensagem de erro	Indica que um respondedor rejeitou uma mensagem porque há falha nos testes de verificação de formato ou de conteúdo.

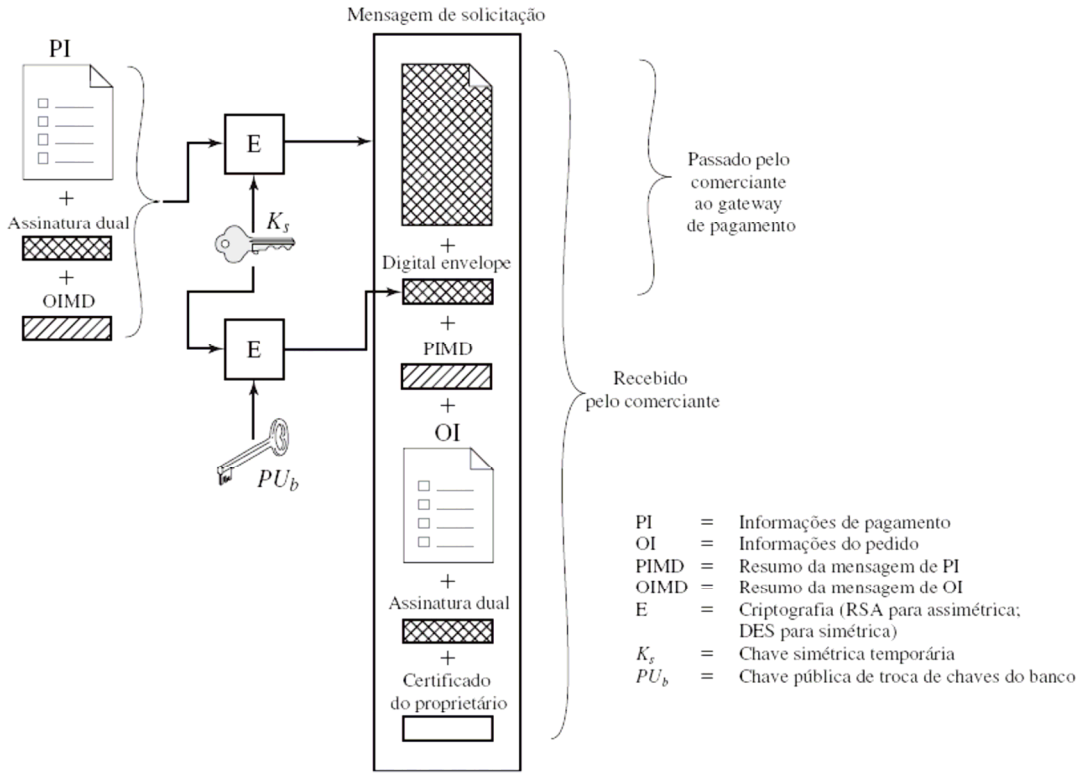


Figura 17.10 O proprietário do cartão envia a solicitação de compra.

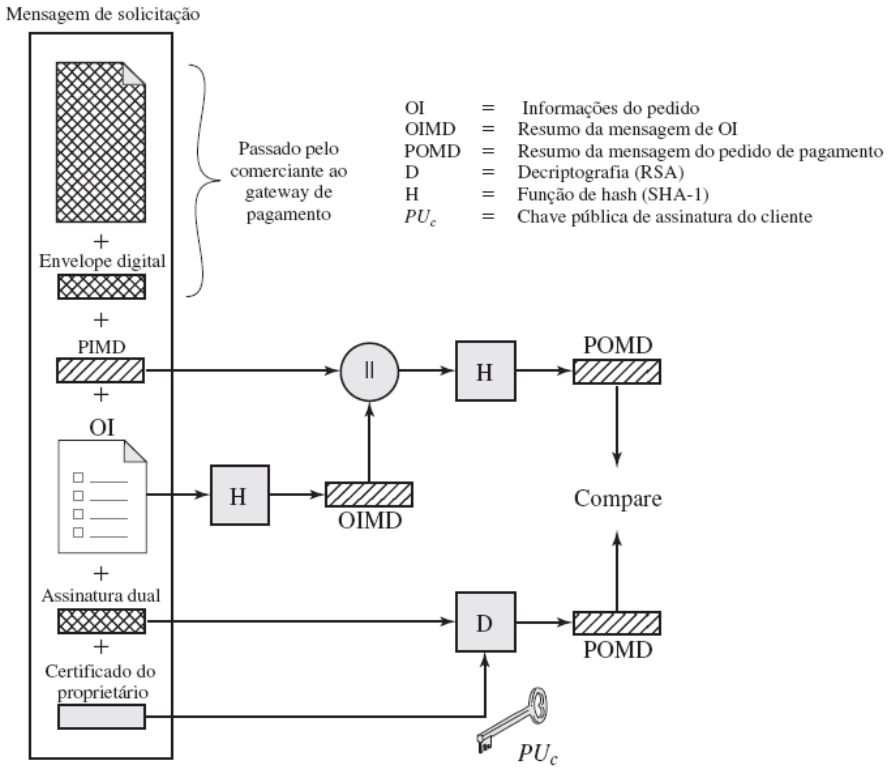


Figura 17.11 Comerciante verifica a solicitação de compra do cliente.