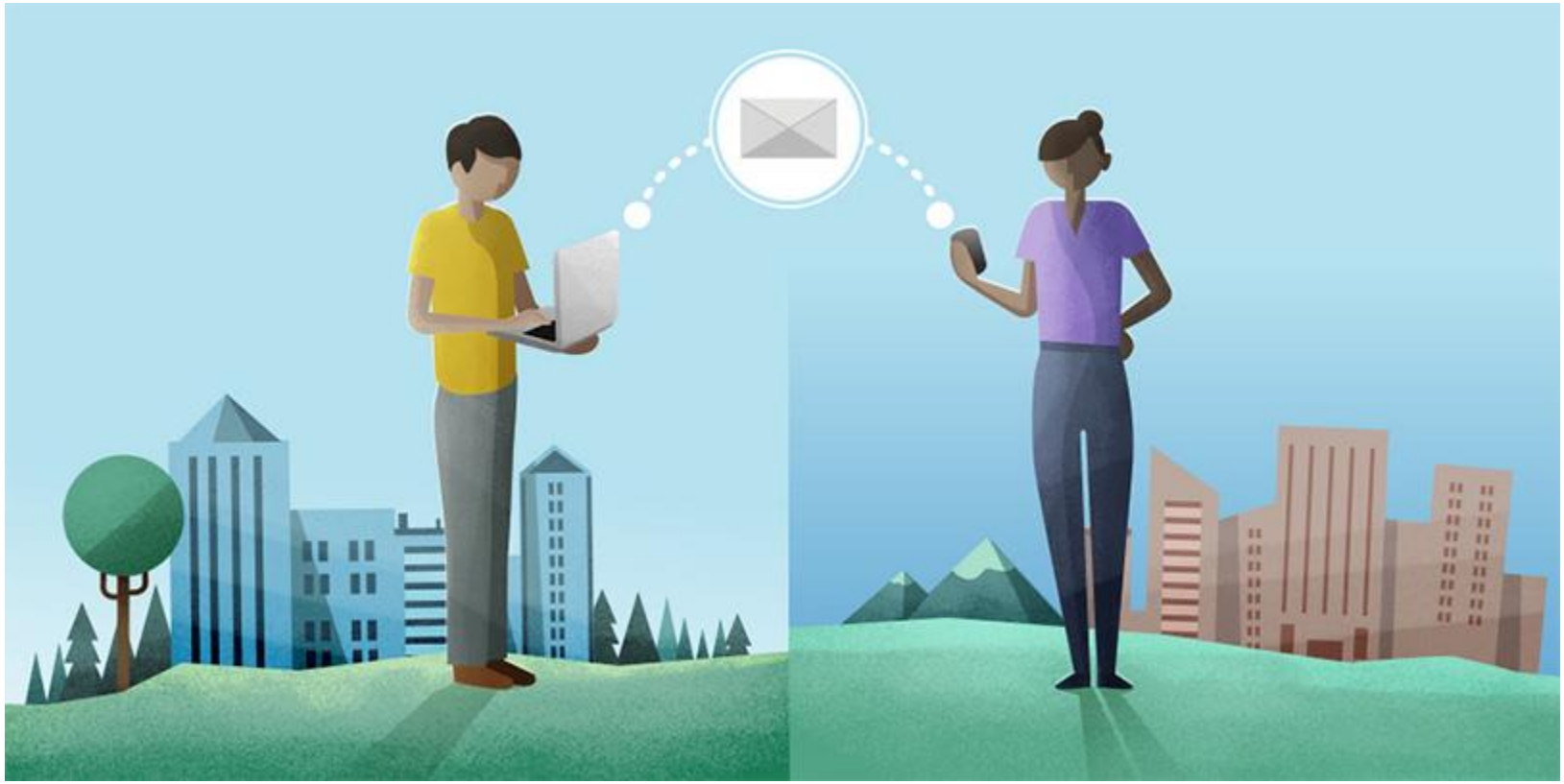
Transporte de mensagens criptografadas

Apresentação: André Luiz Marasca

Como funciona a criptografia?



A privacidade é importante para todos nós

- Ao enviar uma carta para alguém, espera-se que esta pessoa seja a única a ler.
- Mas durante o percurso, muitos curiosos podem querer ler esta carta.
- Por isso, mensagens importantes são enviadas em envelopes selados, ao invés de versos no próprios postais.

Enviar e receber email funciona de uma forma semelhante...

- Muitas coisas acontecem antes da mensagem chegar ao destinatário.
- Se a mensagem for enviadas através de um fornecedor de email que não transmite mensagem através de uma ligação segura, os seus email podem ser abertos.

A criptografia depende de todos

- A criptografia com a Transport Layer Security (TLS) mantém os olhares curiosos afastados das suas mensagens enquanto estão em trânsito.
- A TLS é um protocolo que criptografa e entrega e-mails de forma segura, tanto para o tráfego de email recebido como enviado.
- Ajuda a impedir interceptações entre os servidores de email, mantendo privadas as suas mensagens enquanto se deslocam entre os fornecedores de email.

A criptografia depende de todos

- No entanto, as suas mensagens são apenas criptografadas se o utilizador e a pessoa a quem envia o email tiverem ambos fornecedores de email que suportem a Transport Layer Security.
- Nem todos os fornecedores de email utilizam a TLS e, se enviar ou receber mensagens de um fornecedor que não a tem, a sua mensagem pode ser lida por curiosos que a interceptem.

Gmail suporta criptografia

- Gmail suporta criptografia em trânsito usando TLS, e irá criptografar automaticamente seus e-mails de entrada e saída, se puder.
- Se você ver um ícone de cadeado aberto do vermelho em uma mensagem que você recebeu, ou em que você está prestes a enviar, isso significa que a mensagem não pode ser criptografada.

Propriedades do TLS

- A conexão é privado, porque criptografia simétrica é usada para criptografar os dados transmitidos
- As chaves para essa criptografia simétrica são gerados exclusivamente para cada conexão
- o segredo negociado está indisponível para bisbilhoteiros e não pode ser obtido, mesmo por um atacante que se coloca no meio da conexão

Propriedades do TLS

- A identidade das partes que se comunicam pode ser autenticado usando criptografia de chave pública . Esta autenticação pode ser feito opcional, mas é geralmente necessário para, pelo menos, uma das partes (tipicamente o servidor)

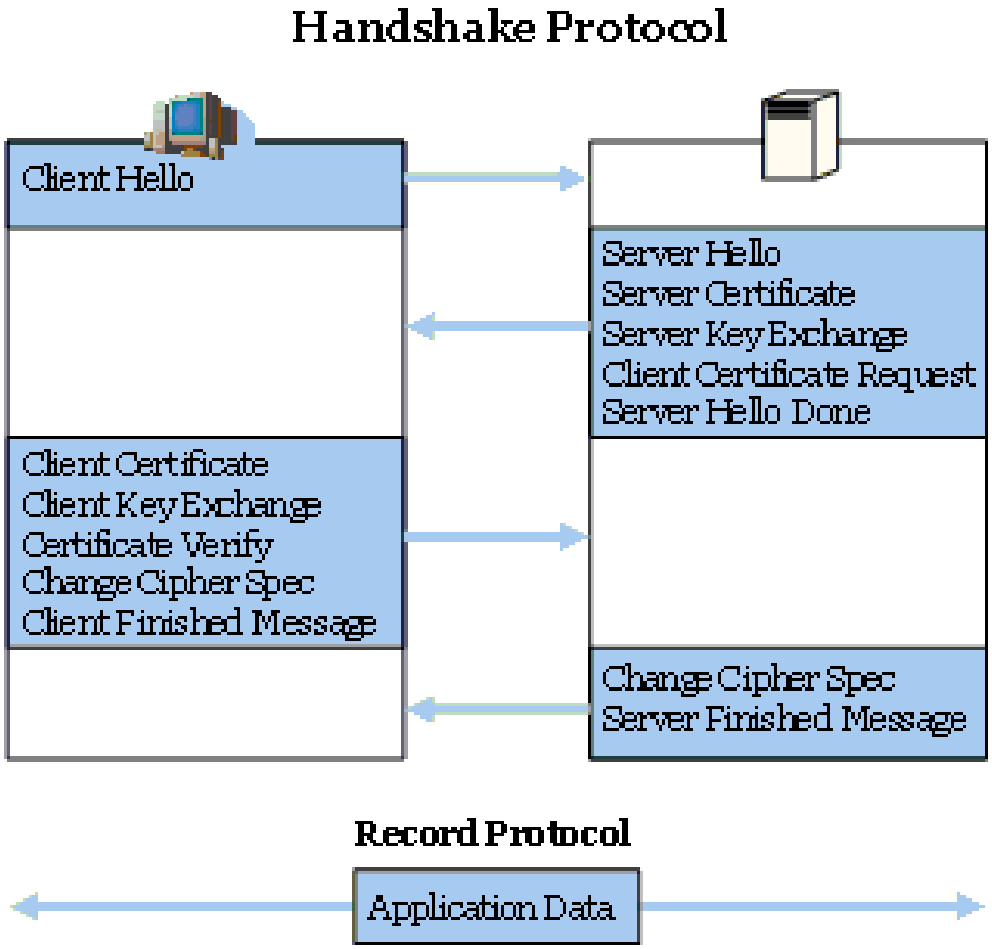
Propriedades do TLS

- A ligação é confiável, porque cada mensagem transmitida inclui uma verificação de integridade da mensagem utilizando um código de autenticação de mensagem para evitar a perda não detectada ou alteração dos dados durante a transmissão

Aperto de mão TLS

- Quando a conexão é iniciada, o registro encapsula um protocolo de “controle” ou protocolo de “mensagens de aperto de mão”.
- Este protocolo serve para trocar todas as informações para começar a usar o TLS.

Aperto de mão TLS



Aperto de mão TLS

1 – Fase de negociação

- O cliente envia um **ClientHello** especificando qual o protocolo TLS mais recente que ele suporta.
- O servidor responde com um **ServerHello** com a versão do protocolo escolhido, e o ID da sessão.
- O servidor envia seu **certificado** de mensagem.

Aperto de mão TLS

1 – Fase de negociação

- O servidor envia **ServerKeyExchange**: Este é um passo opcional no qual o servidor cria e envia uma chave temporária para o cliente. Esta chave pode ser usada pelo cliente para criptografar a mensagem C**lientKeyExchange**

- O servidor envia **ServerHelloDone**: Esta mensagem indica que o servidor está pronto e à espera de uma resposta do cliente.

Aperto de mão TLS

1 – Fase de negociação

- O cliente responde com um C**lientKeyExchange** que pode conter um *PreMasterSecret* , a chave pública, ou nada.
- O cliente e servidor, em seguida, usam os números aleatórios e o *PreMasterSecret* para calcular um segredo comum, o chamado "segredo mestre“.

Aperto de mão TLS

- Todos os outros dados importantes para esta ligação é derivado dessa segredo principal.
- Este segredo é transmitido através de uma função pseudoaleatória cuidadosamente construída.

Aperto de mão TLS

2 – O cliente envia um **ChangeCipherSpec** para informar ao servidor que tudo após esta mensagem será autenticado e criptografado.

- O cliente envia uma **mensagem de termino** autenticada e criptografada contendo hash e MAC sobre as mensagens de aperto de mão anteriores.
- O servidor tentará decifrar a **mensagem de termino** do cliente e verificar o hash e MAC. Se a descriptografia ou verificação falhar, o aperto de mão é considerado como tendo falhado e a conexão deve ser destruída

Aperto de mão TLS

3 – O Servidor envia um **ChangeCipherSpec** para informar ao cliente que tudo após esta mensagem será autenticado e criptografado.

- O servidor envia sua **mensagem de termino** autenticada e criptografada.
- O cliente executa a mesma descriptografia e verificação.

Aperto de mão TLS

4 – Fase de aplicação: neste momento, o "aperto de mão" está completo e o protocolo de aplicação é ativado.

Mensagens de aplicação trocadas entre cliente e servidor serão criptografados exatamente como descrito em suas **mensagens de finalização**.

TLS 1.0

- TLS 1.0 foi definida pela primeira vez em RFC 2246 em janeiro de 1999 como uma atualização de SSL versão 3.0

TLS 1.1

- Foi definido na RFC 4346 em abril de 2006. É uma atualização da TLS versão 1.0. diferenças significativas nesta versão incluem:
- Proteção adicional contra cifra de bloco de encadeamento ataques (CBC).
- A implícita vetor de inicialização (IV) foi substituído por um IV explícito.
- Alteração na manipulação de erros de preenchimento .
- Suporte para IANA registro de parâmetros.

TLS 1.2

- TLS 1.2 foi definido na RFC 5246 , em agosto de 2008. Ele é baseado na especificação anterior TLS 1.1. As principais diferenças incluem:
- A combinação MD5-SHA-1 na mensagem hash final foi substituída com SHA-256. No entanto, o tamanho do hash na mensagem de finalização ainda tem de ser de pelo menos 96 bits.
- A combinação MD5-SHA-1 na assinatura digital foi substituída por um único de hash negociado durante o aperto de mão , cujo padrão é SHA-1.

TLS 1.3

- TLS 1.3, janeiro 2016:
- Removendo o suporte para MD5 e SHA 224 funções hash criptográficas
- Exigindo assinaturas digitais, mesmo quando uma configuração anterior é usada.
- Integrando uso de hash de sessão.
- Proibindo SSL ou RC4 de negociação para compatibilidade com versões anteriores

Referências

- https://www.google.com/transparencyreport/saferemail/tls/?hl=pt
- https://en.wikipedia.org/wiki/Transport_Layer_Security
- https://support.google.com/mail/answer/6330403?hl=en
- https://technet.microsoft.com/en-us/library/cc785811(v=ws.10).aspx