SÃO
PAULO
TECH
SCHOOL

Computação e Sistemas Distribuídos

Security Socket Layer
Transport Layer Security

Eduardo Verri

eduardo.verri@sptech.school

Segurança da informação

Segurança da informação

A segurança da informação é a prática de **proteger dados e sistemas** contra acessos não autorizados, alterações ou destruição. O objetivo é garantir a **proteção dos ativos digitais,** mantendo a confiança, precisão e disponibilidade das informações críticas. É uma área essencial em todas as organizações que lidam com dados sensíveis, incluindo empresas, instituições governamentais e organizações sem fins lucrativos.

Os Pilares da Segurança da Informação [CIA]

Confidentiality:

- Protege informações contra acesso não autorizado.
- Garante que apenas pessoas autorizadas tenham acesso a dados sensíveis.
- Exemplos: Criptografia, controle de acesso, autenticação multifator.

Integrity:

- Garante que os dados não sejam alterados de maneira não autorizada ou acidental.
- Assegura que as informações permaneçam precisas e completas.
- Exemplos: Hashing, assinaturas digitais, controle de versionamento.

Availability:

- Assegura que as informações e sistemas estejam acessíveis a usuários autorizados sempre que necessário.
- Evita interrupções no acesso devido a falhas, ataques ou outras interrupções.
- Exemplos: Redundância, backup e recuperação de desastres, mitigação de ataques DDoS.

E o que isso tem haver com SSL e TLS?

- **SSL (Secure Sockets Layer) e TLS (Transport Layer Security)** são ferramentas essenciais que implementam esses pilares ou pelo menos parte deles. No caso do SSL e TLS, o **"A"** de **Availability** pode ser substituído pelo **"A"** de **Authentication**.

- Elas garantem que as comunicações na internet sejam seguras, protegendo dados sensíveis contra ameaças e garantindo a confiança nas interações digitais.

SSL / TLS

Security Socket Layer - SSL

Imagine que você está enviando uma carta importante e quer garantir que ninguém possa ler essa carta, exceto o destinatário. Para isso, você usa um envelope especial que só o destinatário pode abrir.

O que é SSL?

SSL (Secure Sockets Layer) é como esse envelope especial. Ele cria uma conexão segura entre seu navegador e o site que você está visitando, protegendo as informações transmitidas.

Security Socket Layer - SSL

Para que serve SSL?

- **Proteção de Dados:** SSL criptografa (codifica) as informações, como senhas e números de cartão de crédito, impedindo que sejam lidas por hackers.
- **Autenticação:** Garante que você está se conectando a um site que possui um certificado SSL válido, emitido por uma autoridade certificadora (CA).
- **Confiança:** O cadeado na barra de endereço do navegador indica que a conexão é segura, aumentando a confiança no site.

Transport Layer Security - TLS

TLS (Transport Layer Security) é a tecnologia que substituiu o SSL (Secure Sockets Layer) para garantir a segurança das comunicações na internet.

Ele cria uma conexão segura entre seu navegador e o site que você está visitando, protegendo as informações transmitidas.

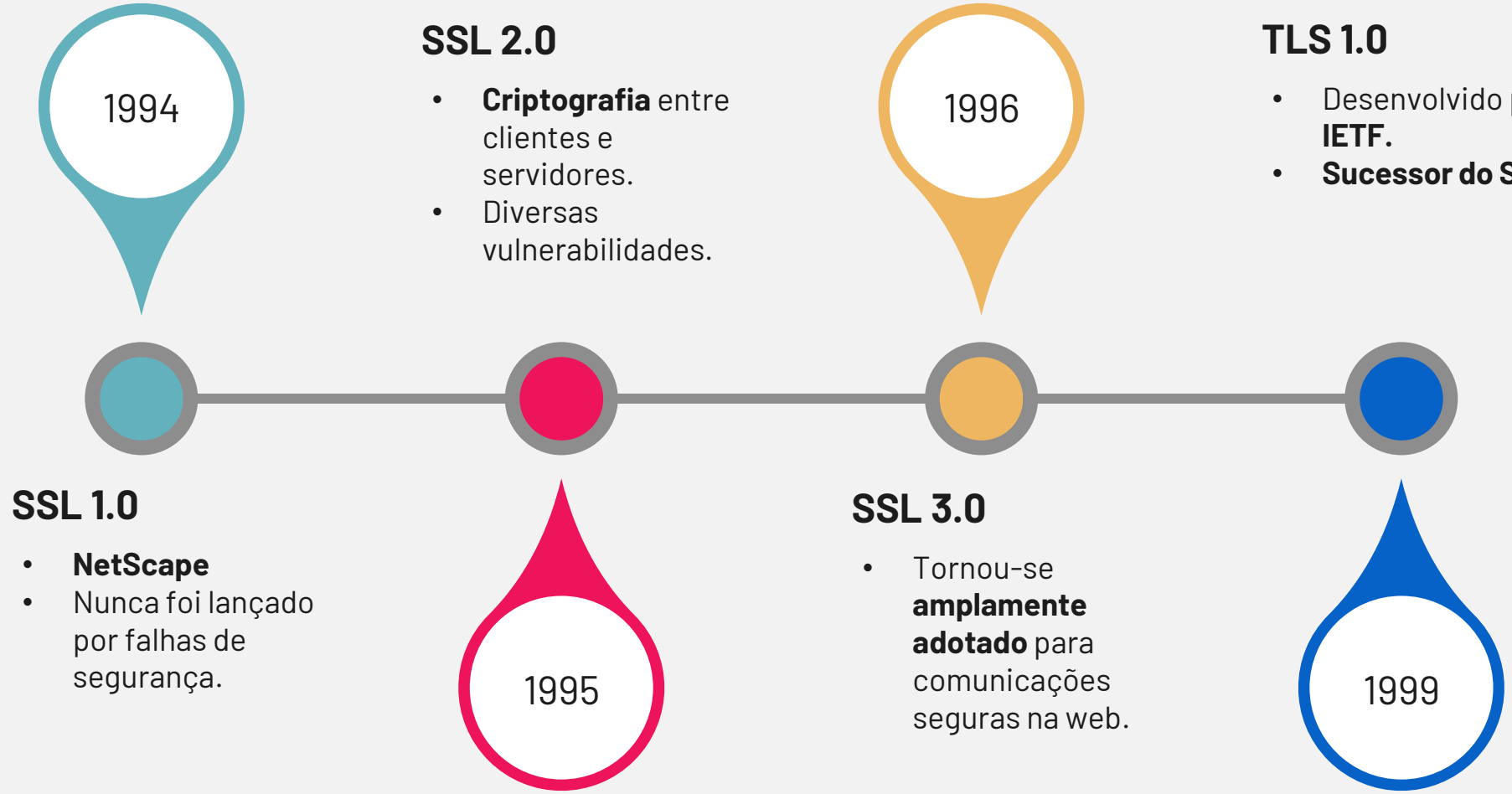
Como o TLS melhorou o SSL?

- **Segurança Aprimorada:** TLS usa algoritmos de criptografia mais fortes e seguros, corrigindo várias vulnerabilidades presentes no SSL.
- **Handshake Melhorado:** O processo de estabelecimento de conexão (handshake) no TLS é mais eficiente e seguro, reduzindo o risco de ataques de interceptação.
- **Flexibilidade:** TLS suporta uma gama maior de protocolos e algoritmos de criptografia, permitindo adaptações futuras e melhorias contínuas.

Transport Layer Security - TLS

- **Desempenho:** TLS oferece melhor desempenho, com menos impacto na velocidade da conexão, especialmente nas versões mais recentes (como TLS 1.3).
- **Autenticação Avançada:** TLS proporciona autenticação mais robusta entre cliente e servidor, garantindo maior confiança na comunicação.

TLS trouxe melhorias significativas em segurança, eficiência e flexibilidade, tornando-se o padrão para proteger comunicações na internet hoje.


1994
SSL 2.0
• Criptografia entre clientes e servidores.
• Diversas vulnerabilidades.
1996
TLS 1.0
• Desenvolvido pelo IETF.
• Sucessor do SSL.
SSL 1.0
• NetScape
• Nunca foi lançado por falhas de segurança.
1995
SSL 3.0
• Tornou-se amplamente adotado para comunicações seguras na web.
1999

Em resumo:

Não seja a pessoa chata, no fim do dia, as pessoas estão falando da mesma coisa...

SSL → TLS

TLS - Versões

TLS 1.0

- Introduzido em 1999
- Primeiro padrão do TLS, **substituiu o SSL 3.0.**
- Melhorou a segurança em relação ao SSL, mas possui vulnerabilidades conhecidas hoje.

TLS 1.1

- Lançado em 2006
- Proteções contra ataques de injeção **de CBC (Cipher Block Chaining).**
- Melhorou o gerenciamento de blocos de criptografia, mas ainda considerado insuficiente para ameaças modernas.

TLS 1.2

- Lançado em 2008
- Introduziu novos algoritmos de hash e suporte para autenticação adicional.
- Flexível e seguro, é **amplamente adotado** e considerado confiável até a introdução do TLS 1.3.

TLS 1.3

- Lançado em 2018
- Aumentou a segurança e o desempenho, **simplificando o protocolo.**
- Eliminou suportes para **algoritmos obsoletos** e proporcionou conexões mais rápidas e seguras.

E o HTTPS?

HTTPS e TLS são a mesma coisa ?

Não, HTTPS e TLS **não são a mesma coisa**, mas estão diretamente relacionados.

HTTPS (HyperText Transfer Protocol Secure):

- É uma versão segura do **HTTP** (HyperText Transfer Protocol).
- **Utiliza TLS** para criptografar os dados transmitidos entre o navegador e o servidor.

TLS (Transport Layer Security):

- É o protocolo que **fornece criptografia**, autenticação e integridade dos dados para **HTTPS** e outros protocolos como **FTP**, **SMTP**, etc.
- Garante que a comunicação via HTTPS e outros protocolos **seja segura.**
- Há um debate sobre em qual camada do modelo **OSI** o TLS se encaixa (5 ou 6).

Open
Systems
Interconnection

O S I

Um modelo conceitual criado pela ISO para padronizar as funções de uma rede de comunicação em **sete** camadas.

1. Física

Função:

Transmissão de bits (0s e 1s) através de um meio físico.

Exemplos:

Cabos Ethernet, fibra óptica, conectores, sinais elétricos.

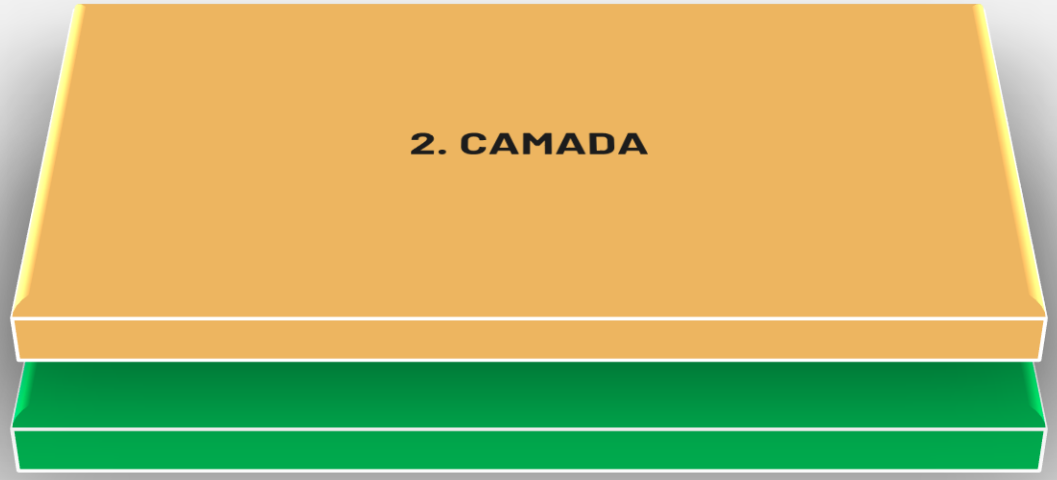
2. Enlace

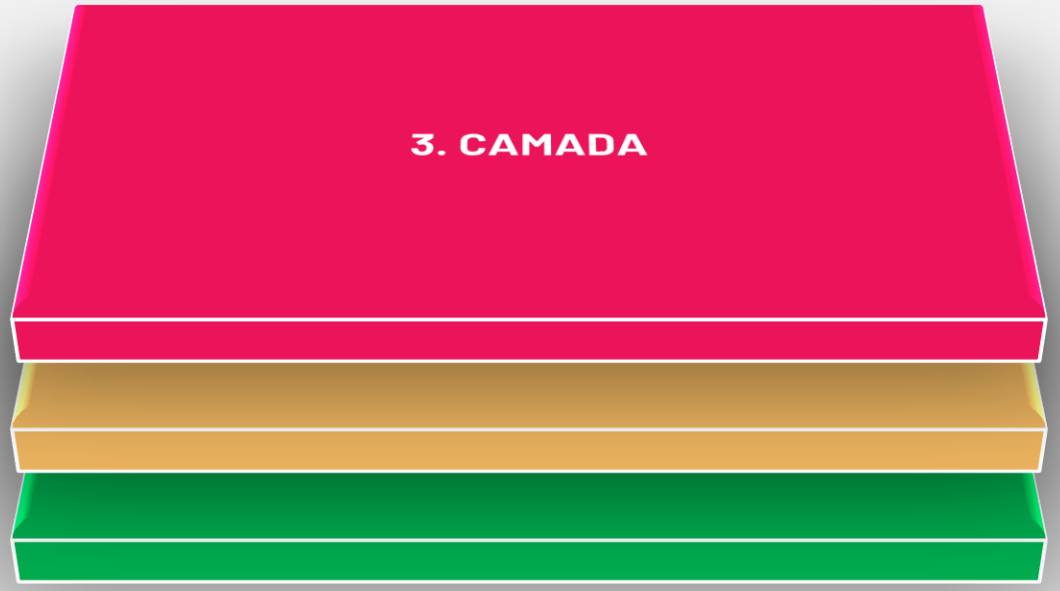
Função:

Estabelece e mantém conexões entre dispositivos na mesma rede local. Trata da detecção e correção de erros.

Exemplos:

Switches, endereçamento MAC, protocolos Ethernet, Wi-Fi.





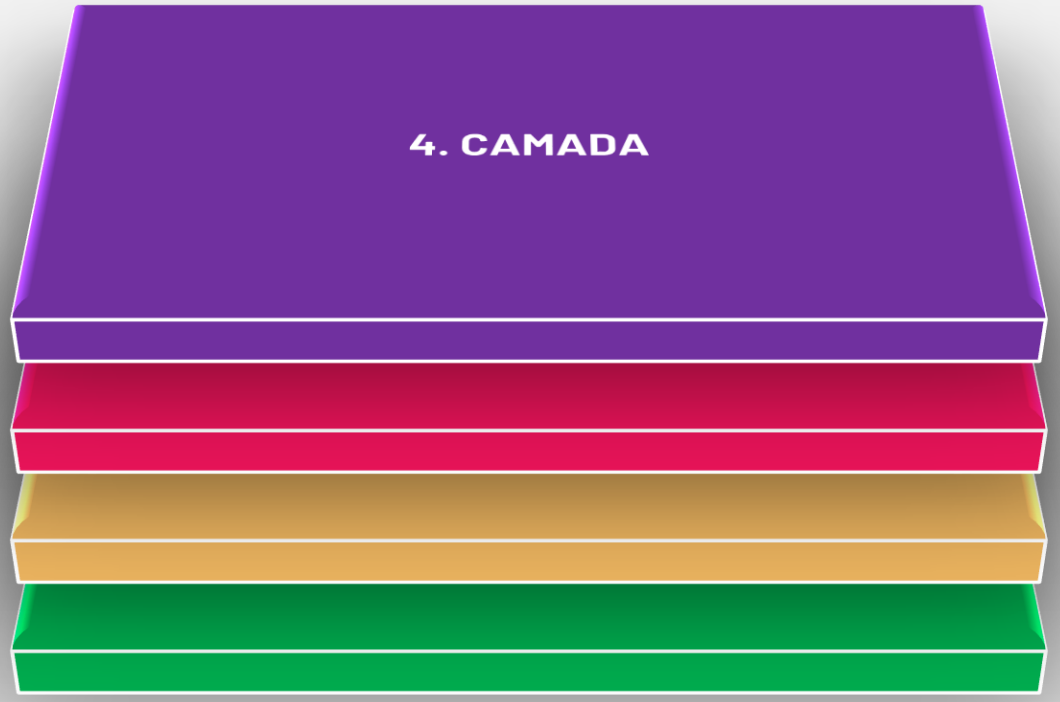
3. Rede

Função:

Roteamento de pacotes entre diferentes redes. Trata do endereçamento lógico e da determinação da melhor rota.

Exemplos:

Roteadores, endereçamento IP, protocolos como IPv4 e IPv6.



4. Transporte

Função:

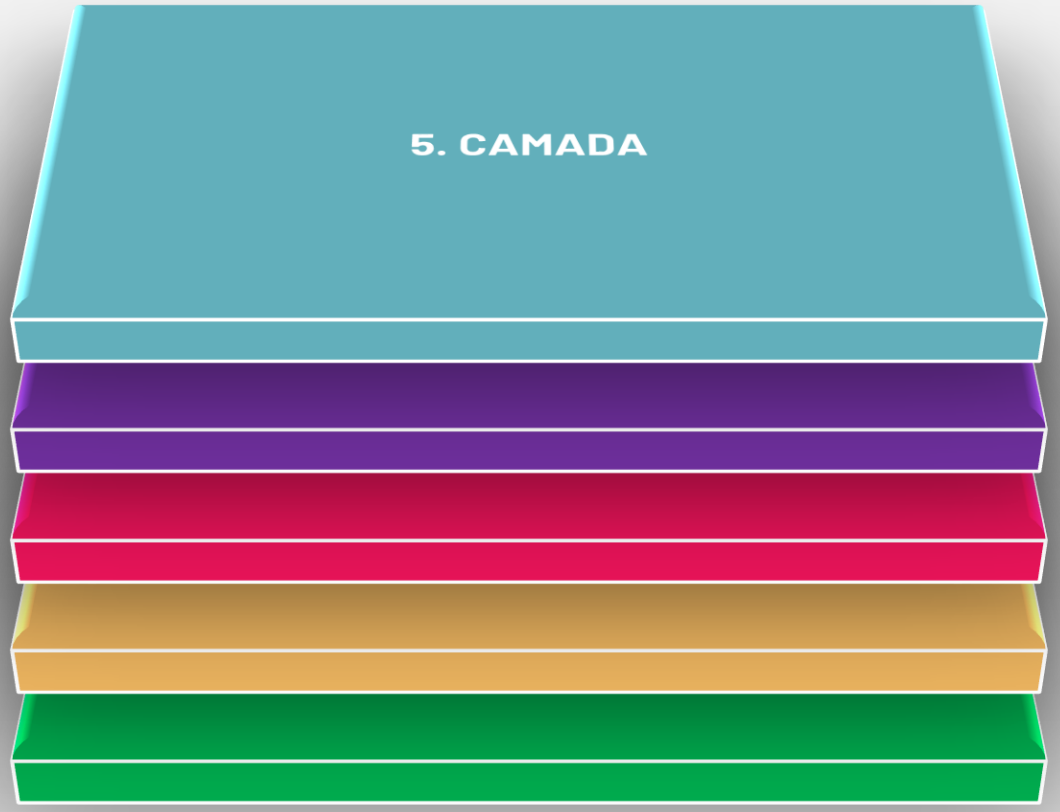
Garante a transferência confiável de dados entre sistemas finais.

Gerencia a segmentação e a reagrupamento dos dados.

Exemplos:

TCP (Transmission Control Protocol),

UDP (User Datagram Protocol).



5. Sessão

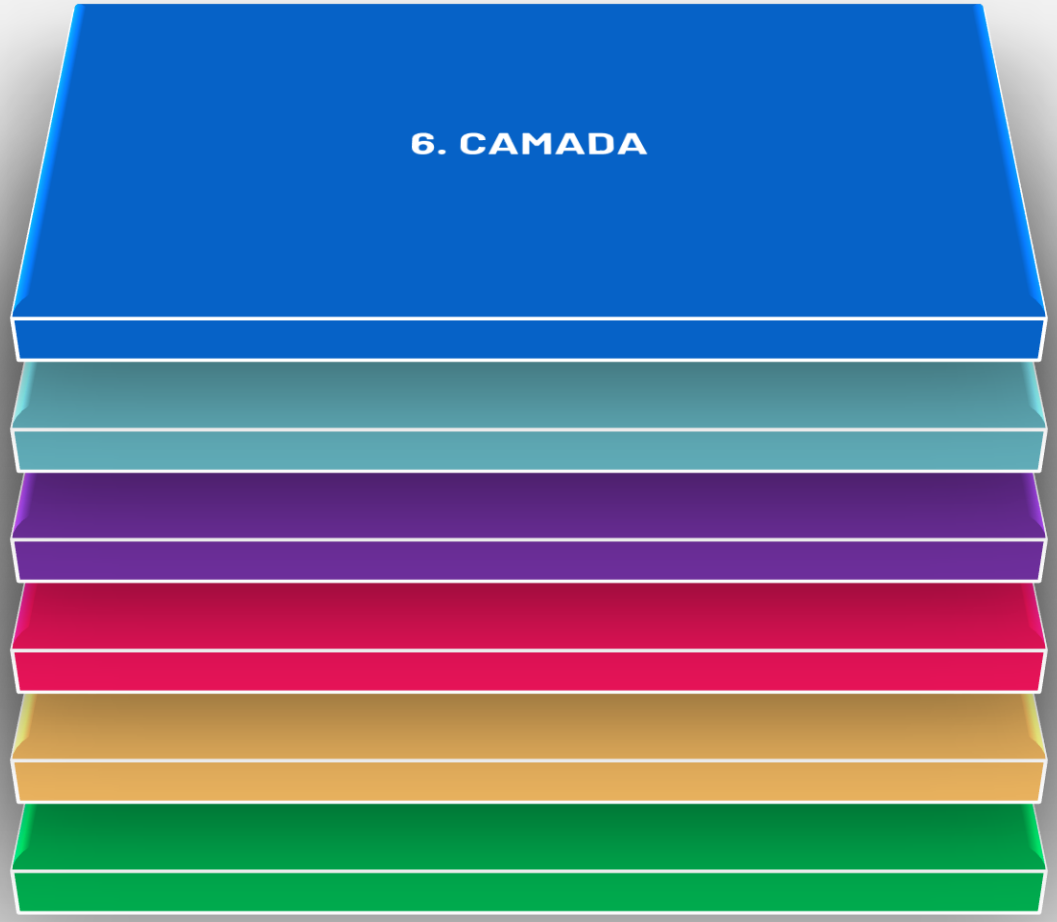
Função:

Gerencia e controla as conexões (sessões) entre computadores. Estabelece, gerencia e termina sessões.

Exemplos:

Protocolos como NetBIOS,

RPC (Remote Procedure Call).



6. Apresentação

Função:

Tradução, compressão e criptografia de dados. Transforma dados entre o formato de rede e o formato compreensível para a aplicação.

Exemplos:

Formatos de dados como JPEG, MPEG, SSL/TLS para criptografia.

7. Aplicação

Função:

Interfaces diretas para as aplicações de rede. Permite aos aplicativos acessarem os serviços de rede.

Exemplos:

HTTP/HTTPS (para navegação web),

FTP (para transferência de arquivos),

SMTP (para envio de emails),

DNS (para resolução de nomes de domínio).

Criptografia

Chave Simétrica

Chave Simétrica é um tipo de criptografia onde a **mesma chave** é usada tanto para **criptografar** quanto para **descriptografar** os dados. Esse método é conhecido por ser rápido e eficiente, mas exige que a chave seja mantida secreta e compartilhada de maneira segura entre as partes envolvidas.

Como funciona:

Criptografia:

- Os dados são criptografados usando uma chave secreta.

Descriptografia:

- A mesma chave secreta é usada para descriptografar os dados.

Exemplos:

AES (Advanced Encryption Standard): Amplamente utilizado para proteger dados em várias aplicações, como transações bancárias online e armazenamento de dados.

DES (Data Encryption Standard): Um padrão mais antigo, mas ainda usado em algumas aplicações legadas.

RC4: Um algoritmo de fluxo que foi popular em muitos protocolos, como SSL, mas agora é considerado inseguro.

Vantagens e Desvantagens

Vantagens:

- Rápido e eficiente em termos de processamento.
- Menos complexidade computacional comparada à criptografia assimétrica.

Desvantagens:

- A segurança depende da manutenção da chave secreta.
- A chave precisa ser compartilhada de maneira segura entre as partes.

Chave Assimétrica

Chave Assimétrica é um tipo de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. A chave pública é usada para criptografar os dados, enquanto a chave privada correspondente é usada para descriptografá-los. Este método permite que a chave pública seja distribuída livremente, enquanto a chave privada é mantida secreta.

Como funciona:

Criptografia:

- A chave pública é usada para criptografar os dados.
- Como a chave pública pode ser compartilhada com qualquer um, qualquer pessoa pode enviar dados criptografados ao proprietário da chave privada.

Descriptografia:

- Apenas a chave privada correspondente pode descriptografar os dados criptografados com a chave pública.
- Garante que somente o proprietário da chave privada possa ler os dados.

Exemplos:

RSA (Rivest-Shamir-Adleman): Um dos algoritmos de chave assimétrica mais utilizados, amplamente empregado em SSL/TLS, PGP e outras aplicações de segurança.

DSA (Digital Signature Algorithm): Usado principalmente para autenticação e assinatura digital.

ECC (Elliptic Curve Cryptography): Oferece a mesma segurança que RSA com chaves menores e maior eficiência.

Exemplos:

Vantagens:

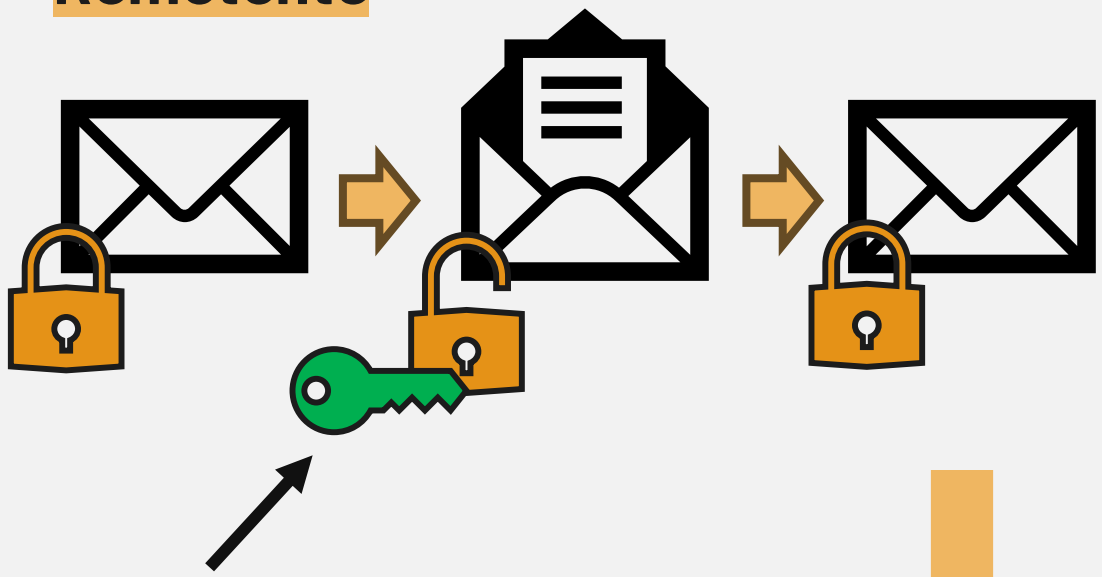
- Não é necessário compartilhar a chave privada, reduzindo o risco de comprometimento.
- Permite a verificação da identidade do remetente através de assinaturas digitais.
- Somente o destinatário pretendido pode descriptografar a mensagem.

Desvantagens:

- A criptografia assimétrica é mais lenta e requer mais poder computacional em comparação com a criptografia simétrica.
- Gerenciar pares de chaves (pública e privada) pode ser mais complexo do que gerenciar uma única chave simétrica.

Chave Simétrica

Remetente



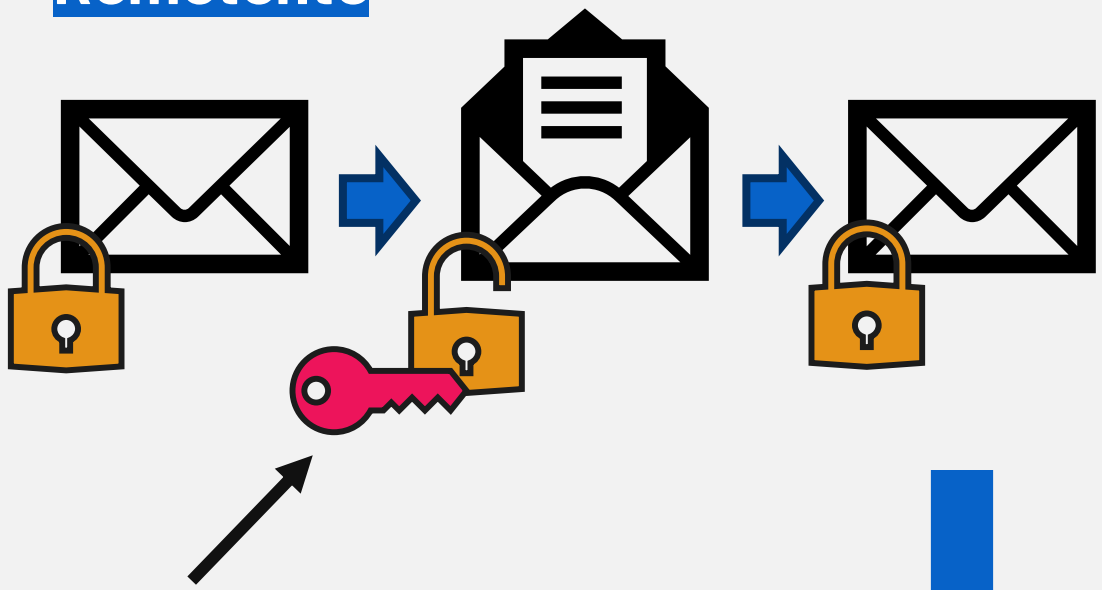
Criptografa com uma chave A

Destinatário

Descriptografa com uma chave igual

Chave Assimétrica

Remetente



Criptografa com
a chave privada

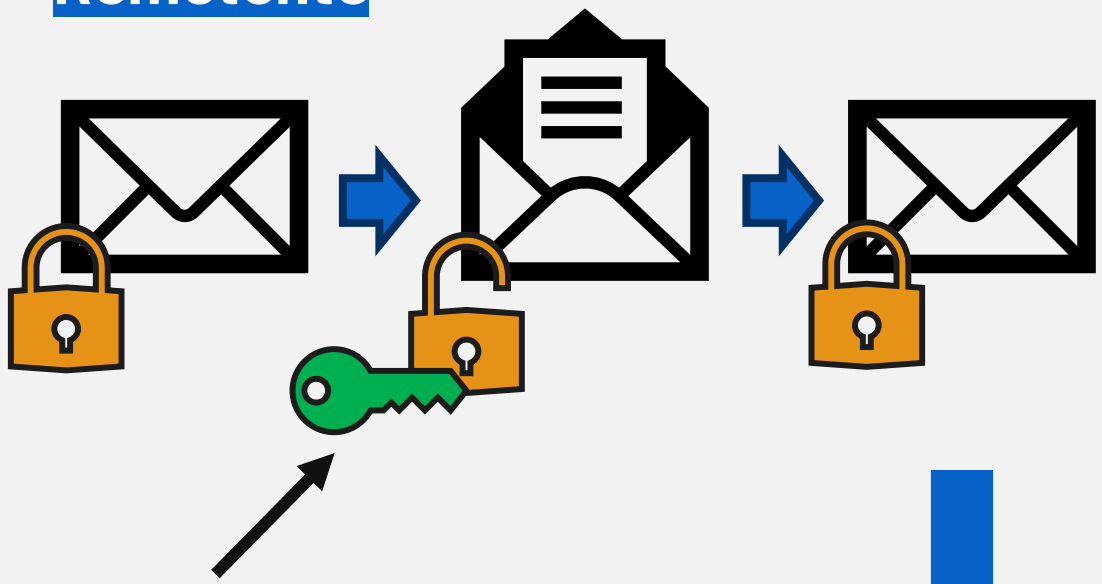
Destinatário

Descriptografa
com uma chave
pública

Isso garante a Autenticidade!

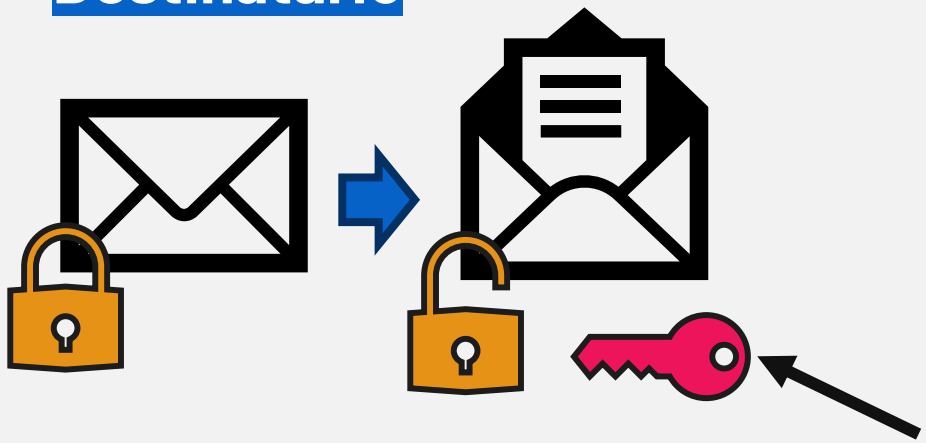
Chave Assimétrica

Remetente



Criptografa com
a chave pública

Destinatário



Descriptografa
com chave
privada

Isso garante a Confidencialidade!

TLS usa simétrica ou assimétrica?

A resposta é: ambas!

Chave Assimétrica – Durante o Handshake (Aperto de Mãos):

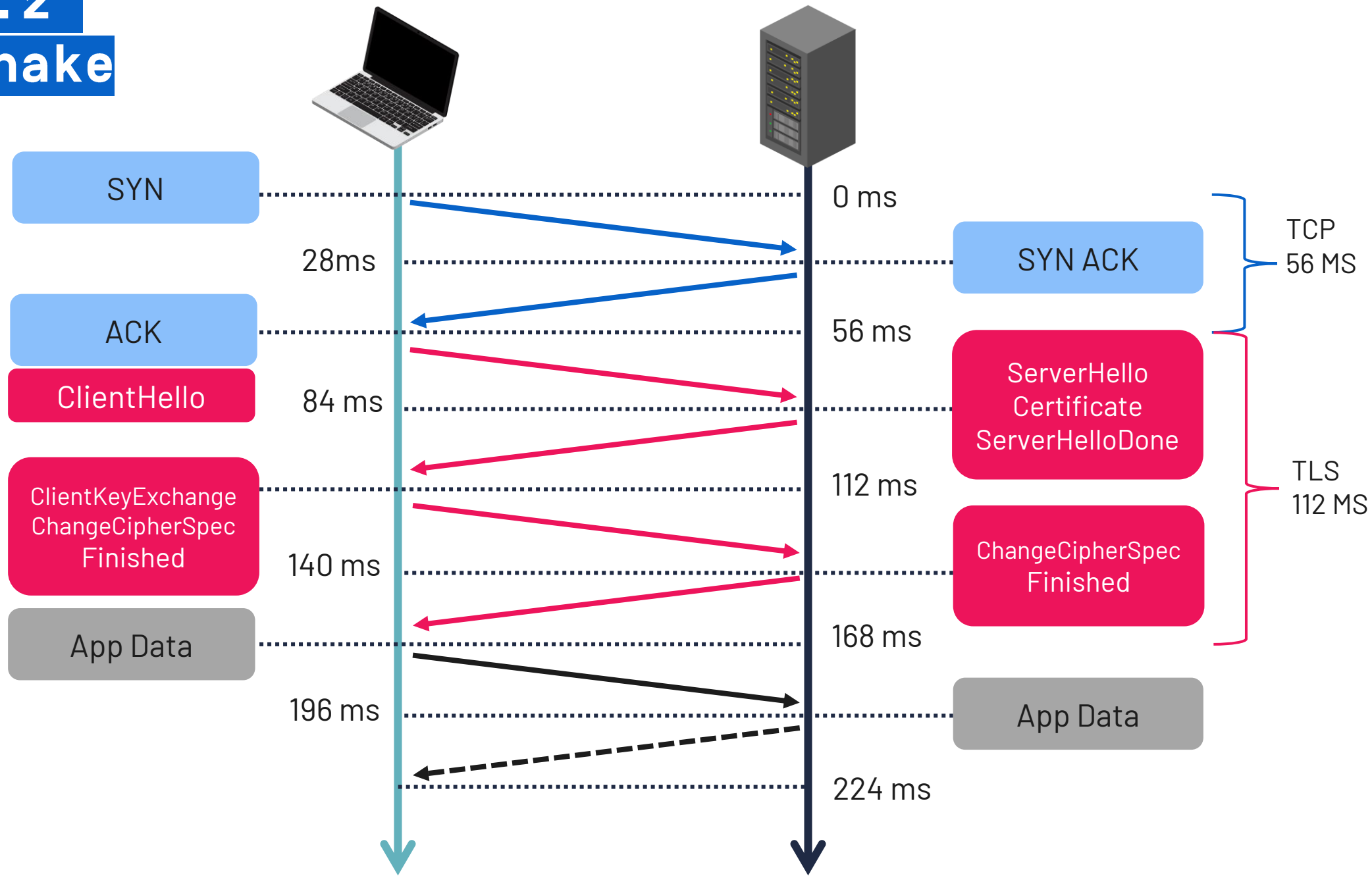
- No início de uma conexão TLS, a criptografia assimétrica é usada para estabelecer uma conexão segura.
- O cliente e o servidor utilizam pares de chaves públicas e privadas para autenticação e troca de chaves de sessão.
- Por exemplo, o cliente usa a chave pública do servidor para criptografar um segredo compartilhado (premaster secret), que só o servidor pode descriptografar com sua chave privada.

TLS usa simétrica ou assimétrica?

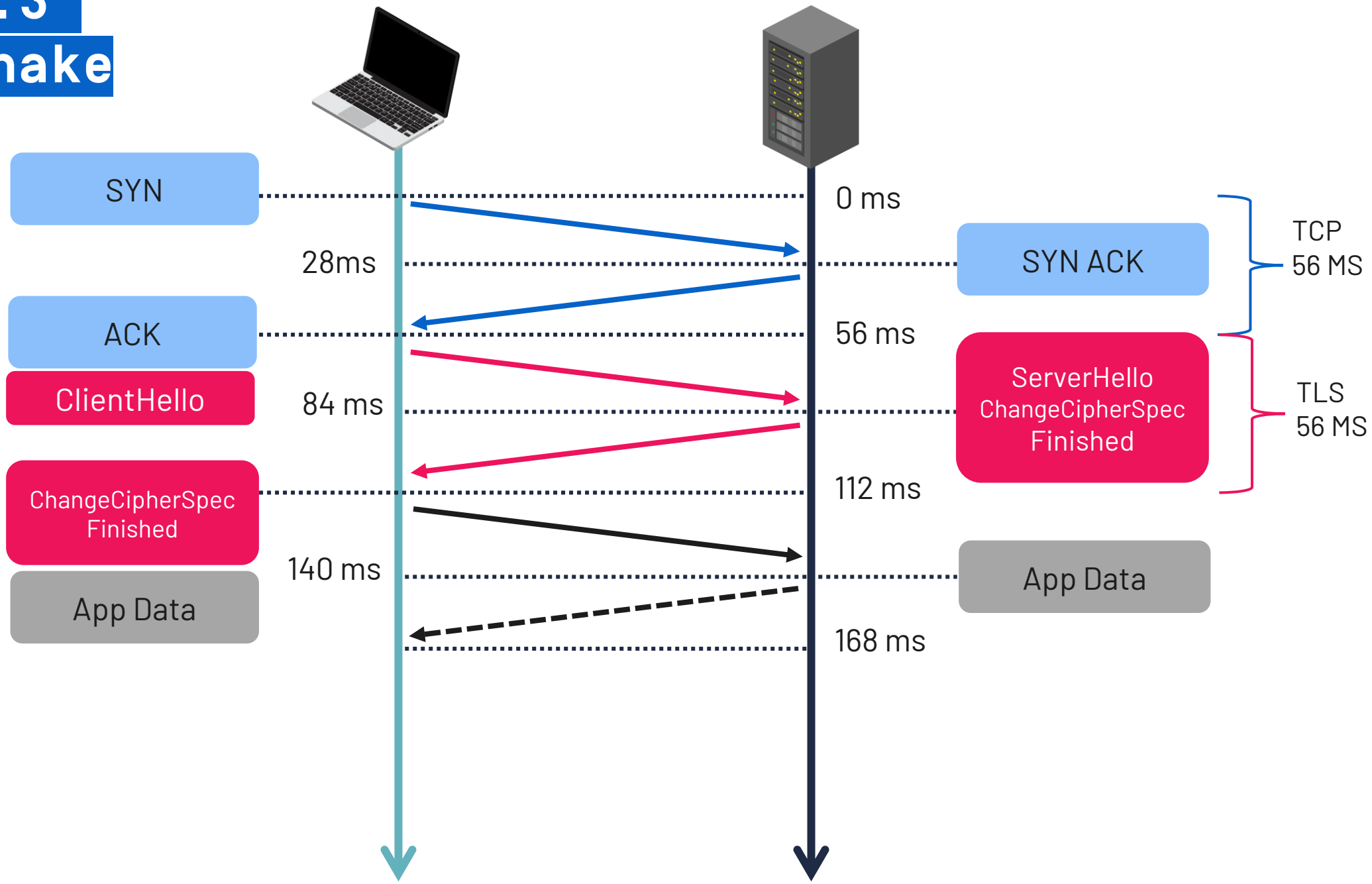
Chave Simétrica - Durante a Transmissão de Dados:

- Após o handshake, o TLS usa criptografia simétrica para a transmissão dos dados.
- As chaves simétricas (chamadas de chaves de sessão) são derivadas do segredo compartilhado estabelecido durante o handshake.
- A criptografia simétrica é mais rápida e eficiente para a transmissão contínua de dados.

TLS 1.2 Handshake



TLS 1.3 Handshake



Tipos de certificado

O Que é um Certificado SSL/TLS?

Um **certificado SSL/TLS** é um **objeto digital** que autentica a identidade de um site e estabelece uma conexão criptografada entre um servidor web e um navegador. Esses certificados são emitidos por **Autoridades Certificadoras (CAs)** confiáveis e desempenham um papel crucial na segurança online, protegendo dados sensíveis como informações de login, detalhes de pagamento e outras comunicações privadas.

Gerar e Validar um Certificado SSL/TLS

1. **Escolher uma Autoridade Certificadora (CA)***
2. Gerar uma Solicitação de Assinatura de Certificado (CSR)
3. **Enviar a CSR para a CA***
4. Verificação de Propriedade do Domínio
5. **Emissão do Certificado***
6. Instalar o Certificado no Servidor
7. Configurar o Servidor para Usar o Certificado
8. **Renovação do Certificado***
9. Configurar Automação de Renovação (Opcional)

Tópicos que podem ter custo financeiro ao realizar

Tipos de Certificados Digitais SSL/TLS

1. Comunicação Unificada (UCC)
2. Multi-Domínio (SAN)
3. Wildcard
4. Validação Estendida (EV)
5. Validação de Organização (OV)
6. **Validação de Domínio (DV)**

Mais rigoroso e burocrático

Menos rigoroso e burocrático

Tipos de Certificados Digitais SSL/TLS

Validação de Domínio (DV)

- Valida apenas o controle do domínio.
- Rápido e simples, ideal para blogs e pequenas empresas.
- Exemplo: Let's Encrypt (gratuito).

Os certificados **DV** são os mais rápidos e fáceis de obter, ideais para a segurança básica de sites pequenos. Outros tipos, como OV, EV, Wildcard, Multi-Domínio (SAN) e UCC, **oferecem níveis mais altos de verificação e abrangem diferentes necessidades de segurança e escopo.**

Let's Encrypt

O que é Let's Encrypt?

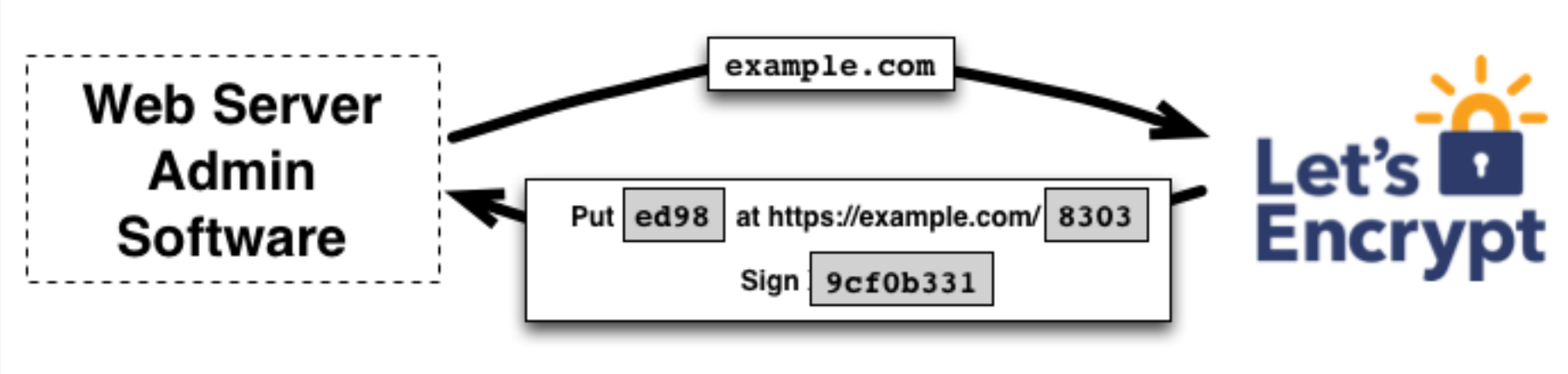
Autoridade certificadora gratuita, automatizada e aberta. Emite certificados SSL/TLS para criptografar a comunicação entre servidores e navegadores.

Principais Benefícios:

- **Gratuito:** Elimina o custo associado aos certificados SSL/TLS.
- **Automatizado:** Facilita a obtenção, renovação e gerenciamento de certificados.
- **Seguro:** Melhora a segurança do site com criptografia HTTPS.
- **Amplamente Aceito:** Reconhecido por todos os principais navegadores e dispositivos.

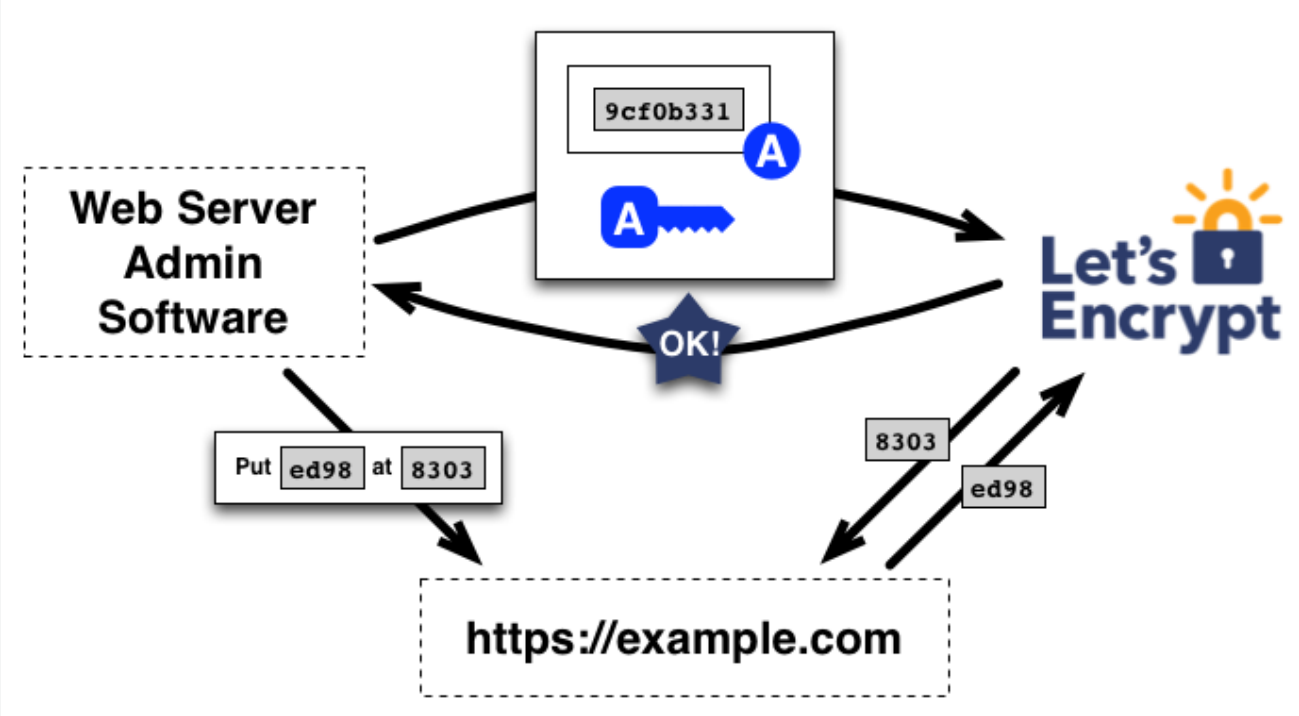
Como funciona ?

Desafio e Resposta: Verifica a propriedade do domínio através de desafios (HTTP-01, DNS-01, TLS-ALPN-01).



Como funciona ?

Desafio e Resposta: Verifica a propriedade do domínio através de desafios (HTTP-01, DNS-01, TLS-ALPN-01).



Impacto:

Acessibilidade: Democratiza a segurança da web, permitindo que qualquer pessoa use HTTPS.

Adoção Massiva: Aumentou significativamente o uso de HTTPS na internet, contribuindo para uma web mais segura.

Mais informações, **clique aqui.**

Agradeço
a sua atenção!

Eduardo Verri

eduardo.verri@sptech.school

SÃO PAULO TECH SCHOOL