VoteSystem

Uma biblioteca feita para garantir a segurança na comunicação de uma votação em uma rede Wi-Fi

Nicholas Henrique Justino Ferreira
Rafael Sutil Pereira

Sistema de Votação Seguro em uma Rede Wi-Fi não confiável

O que é ?

Motivo

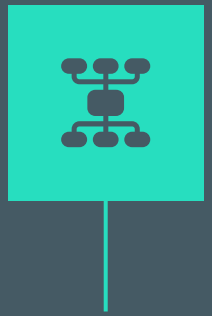
Decisões Arquiteturais

C#

Linguagem de programação desenvolvida pela Microsoft

Windows 10

Sistema Operacional da Microsoft



Cliente-Servidor

Modelo de comunicação que vincula vários clientes a um servidor

Objetivos

Confidencialidade

Capacidade de garantir o sigilo da mensagem.

Autenticidade

Capacidade de garantir que a mensagem provém da fonte anunciada.

Integridade

Capacidade de garantir que a mensagem não foi alterada.

Integridade de Entrega

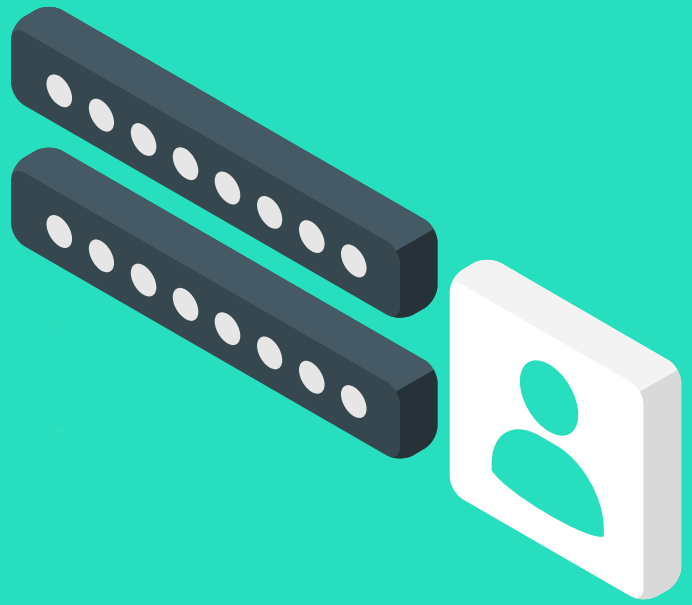
Garantir que todos os dados enviados chegarão realmente ao lado receptor.

Confidencialidade

Enviar a mensagem criptografada com a chave pública do destinatário.

Kc+(Mensagem + Nonce)

Ks+(Mensagem + Nonce)



Integridade e Autenticidade

HMAC, um código de autenticação de mensagem que usa uma chave criptográfica secreta

```
Kc+(Mensagem + Nonce)+
HMAC(Kc+(Mensagem + Nonce))
```

```
Ks+(Mensagem + Nonce)+
HMAC(Ks+(Mensagem + Nonce))
```

Características Extras

- **Truncation Attack**

```
Kc+(Tipo + Mensagem + Nonce) +
HMAC(Kc+(Tipo + Mensagem + Nonce))
```

- **Reordenação das mensagens**

```
Kc+(#seq + Tipo + Mensagem + Nonce) +
HMAC(Kc+(#seq + Tipo + Mensagem + Nonce))
```

Estratégia

Passo 1

Conectar o Socket

Passo 2

Realizar o Handshake

Passo 3

Fazer Login

Passo 4

Realizar a Votação

Handshake

Server

Hello

Certificado do Servidor

Certificado do Cliente

Kc+(Chave Secreta)

Kc+HMAC(Solicita o Login)

Bob

Possíveis Problemas

Alice

Server

Bob

Hello

SCertificado

CCertificado

Kc+(Chave Secreta)

Hello

SCertificado

CCertificado

Kc+(Chave Secreta)

Simulando um Ataque

Trudy

Hello

Hello

ServerCertificate

ServerCertificate

ClientCertificate

TrudyCertificate

Kc+(SecretKey)

Kt+(SecretKey)

[Kc+HMAC(SolicitaLogin)]

[Kt+HMAC(SolicitaLogin)]

[Ks+HMAC(LoginSenha)]

[Ks+HMAC(LoginSenha)]

CPF Diferente

Muito Obrigado!