# TLS - Attacks



- Message replays: Este ataque consiste em repetir (replay) uma mensagem enviada anteriormente.

Exemplo (aplicado a um protocolo):

A Alice autoriza uma transferência bancária da sua conta para outra, cifrando o pedido de transferência com uma chave secreta.

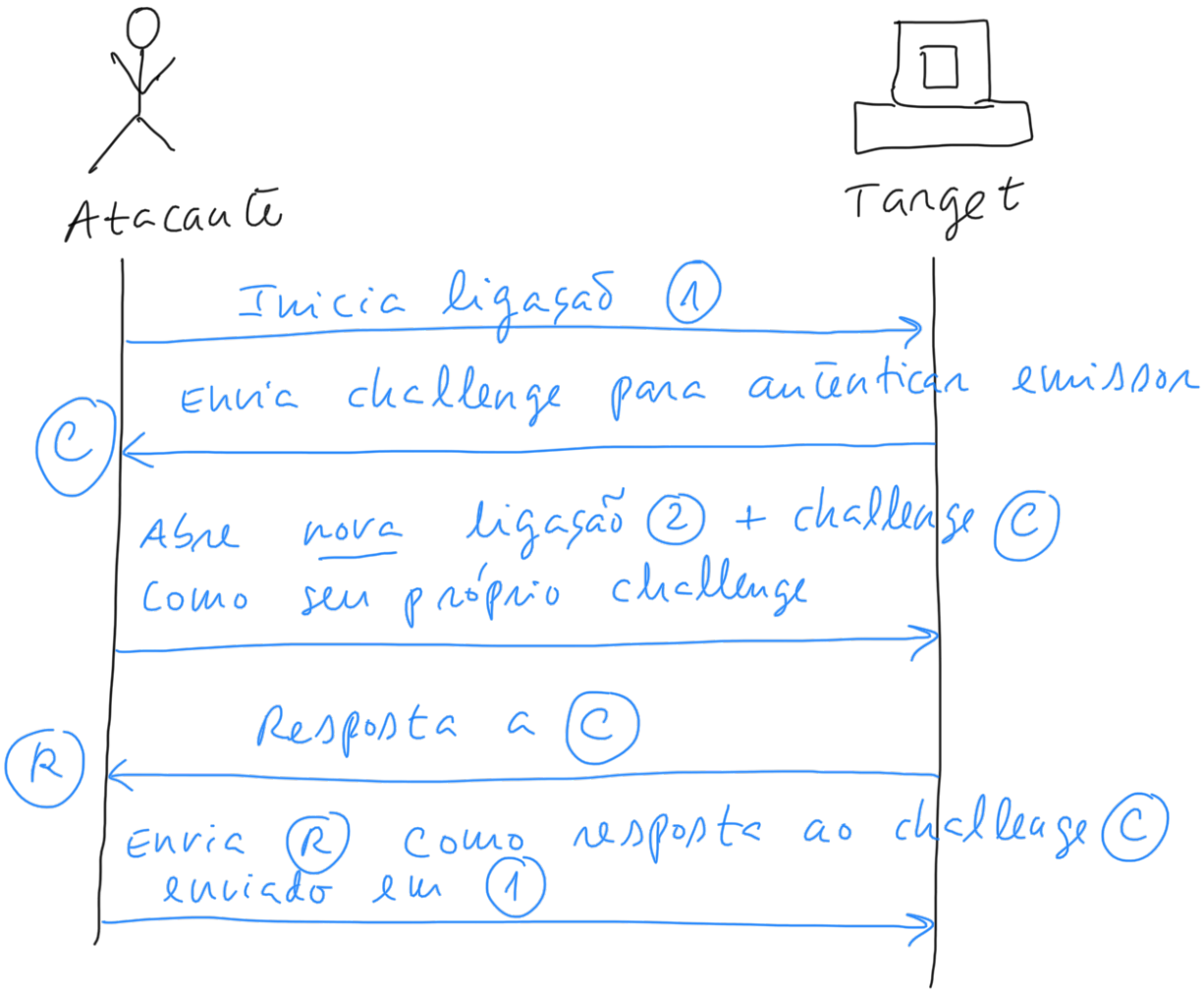
O pedido é enviado a uma máquina que verifica a identidade de Alice (p. ex., conhece a chave secreta) e realiza a transferência.

Ataque: um atacante pode capturar a mensagem cifrada e repetir o pedido junto da máquina.

Nota: no TLS este ataque é evitado devido ao uso de números de sequência. 2.

- Message Reflection: Consiste em atacar um sistema de autenticação Challenge-Response que usa o mesmo protocolo em ambas as direções.

Família de protocolos em que o emissor envia um challenge e receptor envia resposta válida ao challenge para ser autenticado (ex: senha + contra-senha)



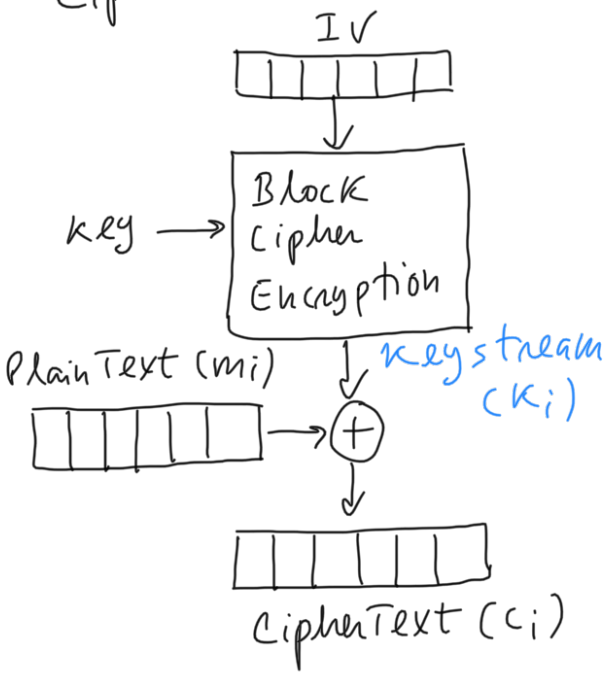

Nota: No TLS, poderia ser possível a um atacante reenviar (refletir) trama recebida do servidor, caso seja mantido o mesmo número de sequência (do cliente). Para evitar este ataque de reflexão, o TLS usa chaves cifra/MAC diferentes em cada direção.

# Ataque de keystream reuse
## (stream based symmetric encryption)

↳ Solução: no TLS são usadas chaves simétricas + IV diferentes em cada direção

Explicação:

Cipher Feedback (CFB) Mode




- Sempre que se usa o mesmo IV e key, é produzido o mesmo keystream.

Para duas mensagens

$m^0 = m_0^0\ m_1^0 \ldots$

$m^1 = m_0^1\ m_1^1 \ldots$

Cifrado: $c_i^0 = m_i^0 \oplus k_i$

$c_i^1 = m_i^1 \oplus k_i$

Combinando o XOR dos criptogramas:

$c_i^0 \oplus c_i^1 = m_i^0 \oplus m_i^1$

Assim, no TLS, usando um stream cipher e repetindo a chave + IV e captunando dois criptogramas Cliente → Servidor e servidor → Cliente, é possível obter o XOR dos plaintexts e depois descobrir os plaintexto com, por exemplo, ataques estatísticos ou ataques de dicionário.

# TLS e Perfect Forward Secrecy



Se chave privada do servidor é comprometida:

- Atacante MITM (Man-In-The-Middle) pode intersetar e decifrar a comunicação com o website
  - ↳ uma solução será revogar o certificado
- Se o atacante tiver gravado comunicações anteriores, protegidas por esta chave privada, também as pode decifrar
  - ↳ client random + server random + decifra(pre-master secret)
    - ⇓ obtém
    - master secret
    - ⇓ obtém 4 chaves MAC + cifra cliente / servidor

## Perfect Forward Secrecy

- comunicação cifrada hoje continua a ser secreta no futuro (forward secrecy) mesmo que a chave privada seja descoberta no futuro.

TLS com Perfect forward secrecy não usa o RSA para cifrar pre-master-secret, mas sim utiliza o algoritmo Diffie-Hellman para estabelecer o pre-master-secret em ambos os lados (cliente e servidor) sem comunicar esse segredo na rede.