1.Ataques criptográficos

A criptografia está presente em diversas interações diárias, protegendo dados sensíveis durante a transmissão. No entanto, a segurança dessas informações depende do algoritmo utilizado e da forma como ele é implementado. O fator essencial que diferencia dados seguros de vulneráveis é a **chave de criptografia**, que protege as informações contra acessos não autorizados. Em vez de tentar adivinhar essa chave, atacantes frequentemente exploram fraquezas na implementação dos algoritmos ou vulnerabilidades em sistemas que utilizam criptografia.

A maioria dos algoritmos criptográficos é de conhecimento público, permitindo que especialistas os testem e identifiquem possíveis falhas. Caso uma vulnerabilidade seja descoberta, o algoritmo se torna obsoleto e é substituído por alternativas mais seguras. Dessa forma, os sistemas criptográficos utilizados atualmente são aqueles que passaram por rigorosos testes e resistiram a tentativas de quebra. Entretanto, mesmo algoritmos seguros podem ser comprometidos por implementações incorretas.

Um dos ataques explorados contra funções criptográficas é o **ataque do aniversário (birthday attack)**, **que se baseia no conceito estatístico de colisão de hashes**. Em um grupo de 23 pessoas, a chance de duas delas compartilharem o mesmo dia de aniversário é de aproximadamente 50%. Da mesma forma, quando uma função de hash é aplicada a um grande número de valores, a probabilidade de duas entradas diferentes gerarem o mesmo hash aumenta significativamente. Isso pode ser explorado para falsificar assinaturas digitais ou certificados, tornando o ataque uma ameaça real. Para evitar colisões, é recomendado o uso de algoritmos de hash com saídas extensas, dificultando a repetição acidental de valores.

A fragilidade da função **MD5** exemplifica esse problema. Publicado em 1992, esse algoritmo teve suas primeiras colisões identificadas em 1996, e em 2008 pesquisadores demonstraram que era possível gerar certificados fraudulentos que pareciam autênticos ao explorarem falhas no MD5. Essa descoberta levou à rápida transição para algoritmos mais seguros, como SHA-2.

Outra técnica explorada por atacantes é o **ataque de downgrade, que força dois sistemas a utilizarem um algoritmo de criptografia mais fraco ou até mesmo a comunicação sem criptografia**. O **SSL stripping** é um exemplo desse ataque, no qual um invasor intercepta a conexão entre um usuário e um site e remove a camada de segurança HTTPS, forçando a comunicação via HTTP não criptografada. Esse ataque requer que o invasor esteja posicionado entre o usuário e o servidor, permitindo que capture informações sensíveis, como credenciais de login.

O processo de **SSL stripping** ocorre em etapas:

1. O usuário tenta acessar um site, enviando uma solicitação HTTP.
2. O servidor responde instruindo a conexão a ser feita via HTTPS.

3. O atacante intercepta essa resposta e impede que o usuário faça a migração para HTTPS.
4. O usuário continua a se comunicar via HTTP, sem perceber a manipulação.
5. O atacante captura todas as informações enviadas pelo usuário, incluindo nome de usuário e senha.
6. O atacante repassa essas credenciais ao servidor por meio de uma conexão HTTPS legítima, garantindo acesso total à conta da vítima.

Uma vez que o ataque é bem-sucedido, todas as interações futuras entre o usuário e o site passam a ser monitoradas e manipuladas pelo invasor. Essa técnica é especialmente eficaz contra usuários que não verificam se o site está utilizando HTTPS antes de inserir informações sensíveis.

Para mitigar ataques de downgrade e SSL stripping, os sites devem implementar **HSTS** (HTTP Strict Transport Security), **um mecanismo que instrui os navegadores a sempre forçarem conexões HTTPS**. Usuários, por sua vez, devem verificar a presença do cadeado de segurança nos navegadores e evitar redes Wi-Fi públicas sem o uso de VPNs.

A segurança da criptografia não depende apenas da robustez dos algoritmos, mas também da maneira como são implementados. Vulnerabilidades podem surgir de más configurações, ataques direcionados e erros de implementação, tornando essencial a adoção de práticas rigorosas de segurança para proteger dados contra acessos não autorizados.