1.Ofuscação

A ofuscação é um processo no qual informações normalmente fáceis de entender são modificadas para se tornarem mais difíceis de interpretar. Esse método pode ser utilizado de várias formas para esconder dados, tornando-os invisíveis para quem não conhece o processo de ocultação. No entanto, se alguém souber como a ofuscação foi aplicada, poderá reverter o processo e recuperar os dados originais. **Em outras palavras, a informação está escondida, mas continua acessível a quem conhece o método de ocultação**.

Uma das formas mais conhecidas de ofuscação é a esteganografia, que permite esconder informações dentro de imagens. A origem do termo vem do grego e significa "escrita oculta". **A ideia é inserir dados dentro de uma imagem sem que isso seja perceptível a olho nu**. Essa técnica é considerada um tipo de "segurança pela obscuridade", pois a informação não está protegida por criptografia, mas sim disfarçada dentro de outro conteúdo. Caso alguém descubra o método usado para ocultar os dados, poderá facilmente extraí-los. Utilizando softwares específicos, é possível inserir uma mensagem dentro de uma imagem e, posteriormente, recuperá-la. O arquivo em si não apresenta diferenças visíveis, mas contém informações embutidas em sua estrutura.

Além de imagens, a esteganografia pode ser aplicada a diferentes tipos de mídia, como tráfego de rede, onde mensagens ocultas podem ser enviadas dentro de pacotes TCP, ou até mesmo em documentos impressos. Algumas impressoras modernas, por exemplo, adicionam discretamente pequenos pontos amarelos nos documentos, conhecidos como códigos de identificação de máquina. Esses pontos são quase invisíveis a olho nu, mas, ao serem analisados corretamente, podem revelar informações sobre o dispositivo utilizado para imprimir o documento.

A técnica também pode ser aplicada em arquivos de áudio e vídeo, permitindo que dados sejam escondidos dentro dessas mídias sem alterar significativamente sua aparência ou qualidade. Esse método pode ser utilizado tanto para proteger informações quanto para fins maliciosos, como o envio de comandos ocultos em malware.

Outra forma popular de ofuscação é a tokenização, um processo que substitui informações sensíveis por valores substitutos chamados tokens. Esse método é amplamente utilizado em transações financeiras, como pagamentos via celular ou smartwatch. Em vez de transmitir o número real do cartão de crédito, o sistema gera um token temporário que é enviado ao comerciante. **Esse token não pode ser reutilizado, e mesmo que seja interceptado, não pode ser associado ao cartão original. Assim, a tokenização permite transferir dados de forma segura sem necessidade de criptografia adicional**.

O processo de tokenização ocorre em etapas. Primeiro, o usuário registra seu cartão em um dispositivo móvel, que se comunica com um servidor de tokens. Esse servidor gera tokens únicos que ficam armazenados no aparelho. No momento da compra, o dispositivo transmite um dos tokens para o terminal de pagamento via NFC. O comerciante então encaminha o token ao servidor, que faz a correspondência com o número real do cartão e autoriza a transação. Após o uso, o token é descartado, garantindo que não possa ser reutilizado.

Além da tokenização, outro método de proteção de dados amplamente utilizado é o mascaramento de dados. **Essa técnica oculta parcialmente informações sensíveis, como números de cartões de crédito, exibindo apenas os últimos quatro dígitos em recibos ou atendimentos telefônicos**. O objetivo é impedir que informações completas fiquem expostas, reduzindo o risco de fraudes. Diferentes técnicas de mascaramento podem ser aplicadas, como substituição de caracteres, reordenamento de números ou uso de símbolos, garantindo que os dados originais permaneçam protegidos.

Embora a ofuscação, a esteganografia e a tokenização não sejam substitutos da criptografia, elas complementam as práticas de segurança, tornando mais difícil o acesso não autorizado a informações sensíveis. Essas técnicas são amplamente utilizadas para proteger dados e minimizar riscos em ambientes digitais.