SSW - 2022

1.Introdução

A transmissão de dados realizada através da rede de computadores ou por outros meios, como o papel, muitas vezes podem não apresentar a segurança adequada ao valor da informação transportada. Durante décadas, várias técnicas foram desenvolvidas para que uma informação confidencial chegasse ao seu destino sem que fosse interceptada, algo que poderia causar mudanças drásticas no destino até mesmo do mundo.
Veremos algumas técnicas, algumas muito utilizadas e outras nem tanto, que possuem o intuito de aumentar a segurança das informações transmitidas ou armazenadas.

2.Esteganografia

Esteganografia é o estudo e uso das técnicas para ocultar a existência de uma mensagem dentro de outra, uma forma de segurança por obscurantismo. O primeiro uso registrado da palavra data do ano de 1499, no livro Steganographia, de Johannes Trithemius. (Wikipedia)
Uma forma bem comum utilizada atualmente para demonstrar como funciona esteganografia, é adicionar algum texto oculto em uma imagem, pdf ou outro documento, ou seja, não é possível visualizar o texto apenas abrindo a imagem ou pdf, é necessário utilizar algum outro programa para extrair essa informação.
Por exemplo: Ao utilizar um bloco de notas para abrir um arquivo de extensão jpg, bmp, pdf, gif, entre outros, que tenha um texto oculto, será exibido o código fonte do arquivo e, ao final, o texto ocultado.

3.Base64

Base64 é um método para codificação de dados para transferência na Internet (*codificação MIME para transferência de conteúdo*). É utilizado frequentemente para transmitir dados binários por meios de transmissão que lidam apenas com texto, como por exemplo para enviar arquivos anexos por e-mail.

É constituído por 64 caracteres ([A-Z],[a-z],[0-9], "/" e "+") que deram origem ao seu nome. O carácter "=" é utilizado como um sufixo especial e a especificação original (RFC 989) definiu que o símbolo "*" pode ser utilizado para delimitar dados convertidos, mas não criptografados, dentro de um *stream*.

Exemplo de codificação:

•Texto original: `Olá, mundo!`

•Texto convertido para Base64: `T2zDoSwgbXVuZG8h`

A codificação Base64 é frequentemente utilizada quando existe uma necessidade de transferência e armazenamento de dados binários para um dispositivo designado para trabalhar com dados textuais. Esta codificação é amplamente utilizada por aplicações em conjunto com a linguagem de marcação XML, possibilitando o armazenamento de dados binários em forma de texto. (Wikipedia)

Existem vários sites que permitem codificar e decodificar nesse método, por exemplo:

https://www.base64decode.org/ - para decodificar texto que está em base64

https://www.base64encode.org/ - para codificar texto em base64

4.Função Hash

Uma função hash é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. Os valores retornados por uma função hash são chamados valores hash, códigos hash, somas hash (hash sums), checksums ou simplesmente hashes.
Eles também são úteis em criptografia. Uma função hash criptográfica permite verificar facilmente alguns mapeamentos de dados de entrada para um valor hash fornecido, mas se os dados de entrada são desconhecidos, é deliberadamente difícil reconstruí-lo (ou alternativas equivalentes) conhecendo o valor do hash armazenado. Isto é usado para assegurar a integridade de dados transmitidos e é o bloco de construção para HMACs, que fornecem autenticação de mensagem.