Funções Resumo – *SHA256*

Felipe Guedes[1]

[1]Escola Politécnica – Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS)
Caixa Postal 15.064 – 91.501-970 – Porto Alegre – RS – Brazil

felipe.guedes@edu.pucrs.br

Abstract. *This paper describes the solution applied by the students on the first assessment for the systems security discipline given by the professor Avelino Zorzo. The main aspect to be explored on this paper the usage and functionalities of the SHA256 algorithm.*

Resumo. *Este artigo descreve a solução utilizada pelos alunos no primeiro trabalho da disciplina de segurança de sistemas ministrada pelo professor Avelino Zorzo. O principal aspecto a ser explorado neste artigo é o uso e funcionalidade do algoritmo SHA256.*

1. Introdução

Este é o terceiro trabalho da disciplina de segurança de sistemas, ministrada pelo professor Avelino Zorzo durante o segundo semestre de 2019. O objetivo do trabalho é a criação de um programa que permita os alunos entenderem o uso e funcionamento de funções resumo, mais especificamente o *SHA256*.

Neste artigo iremos discutir o problema proposto, em seguida abordar brevemente funções resumo, para após a solução para o problema proposto, por fim o aluno demonstra os resultados obtidos na conclusão.

2. Problema Proposto

O problema proposto aos alunos foi de utilizar uma função resumo, mais especificamente o *SHA256*, a fim de exercitar o uso desses algoritmos e por em prática os ensinamentos passados em sala de aula.

Neste trabalho os alunos tiveram que utilizar a função resumo em um arquivo mp4, simulando a forma com que o conteúdo é transmitido via internet, visando que o mesmo não seja alterado durante o caminho, nem que seu conteúdo esteja corrompido.

3. Funções Resumo

3.1 SHA256

A sigla *SHA* refere-se a algoritmo de hash seguro (*Secure Hash Algorith*). O *SHA256* é uma implementação que utiliza 256 bytes em seu hash final. Kreutz (2019), descreve que umas das principais características do *SHA-2* sendo a impossibilidade da

reversão da chave gerada para a mensagem cifrada, o que torna o algoritmo uma opção para o uso em trocas de mensagens, a fim de garantir a autenticidade do conteúdo.

4. Solução Proposta

A implementação do trabalho foi feita em Java, uma vez que é a linguagem referência do curso de Engenharia de Software da PUCRS. A *API* da linguagem já provem ao programador a função resumo *SHA256* através da biblioteca *MessageDigest*, logo não foi necessário implementar esse algoritmo.

Tendo em vista que coube ao programador apenas utilizar a implementação já provida pela linguagem, o trabalho foi focado basicamente no modo de operação, que visa garantir a integridade dos dados, quando transmitidos via internet.

As etapas implementadas foram a de leitura do arquivo em blocos de no máximo 1Kb (1024 *bytes*), podendo o último bloco ser menor. Então essa estrutura de dados, que se tratou nessa implementação de um *ArrayList* de vetores de bytes é entregue para a etapa final, a aplicação da função resumo com o modo de operação.

A função resumo então é aplicada sobre os vetores de bytes da seguinte forma, de trás para frente eles são entregues para a função resumo, sendo apenas o último encriptado sozinho, os demais possuem seus dados concatenados com o resultado da função resumo anterior, até o primeiro bloco, o qual gera o último valor encriptado que não é concatenado a nenhum valor.

Conclusão

Foi possível verificar em prática como funciona a aplicação de uma função resumo para garantir a integridade dos dados, especialmente quando transferidos via internet. A implementação é extremamente simples, no entanto muito poderosa, uma vez que garante segurança ao usuário final de que o dado que está sendo recebido está integro e é seguro executá-lo.

Referências

KREUTZ, Diego et al. Introdução à Propriedades Básicas e Avançadas de Segurança da Informação.