https://eventos.utfpr.edu.br//sicite/sicite2018

Segurança e criptografia para amostras de biometria em sistemas de identificação

Security and Encryption for Biometric Samples in Identification Systems

Gabriel Zamproni
zamproni@alunos.utfpr.edu.br
Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, Brasil

Daniel Fernando Pigatto
pigatto@utfpr.edu.br
Universidade Tecnológica Federal do Paraná, Curitiba, Paraná, Brasil

RESUMO

O crescimento do uso da biometria como fator de autenticação em diversos produtos e serviços traz consigo a necessidade de se pensar na segurança do armazenamento de informações biométricas. Um ponto crucial da necessidade da implementação de um armazenamento seguro é a imutabilidade da biometria, ou seja, caso as informações da mesma tenham sido roubadas, não há como recuperar a segurança na autenticação biométrica. Neste trabalho foi desenvolvido um modelo de armazenamento em um sistema embarcado que além de visar a ampliação da segurança das amostras de biometria guardadas, foca no baixo custo e na independência de conexões externas para seu funcionamento. O desenvolvimento foi realizado em linguagem Python 2.7 e utilizou as técnicas de criptografia *One Time Password*, banco de dados e *Hash* para realizar a segurança das informações contidas na memória de uma Raspberry Pi 3 Modelo B.

PALAVRAS-CHAVE: Biometria. Criptografia. One-time password. Raspberry Pi3.

ABSTRACT

The growth of the use of biometrics as an authentication factor in several products and services brings with it the need to think about the security in the storage of biometric information. A crucial point of the need to implement a secure storage is the immutability of biometrics, that is, if the information has been stolen, there is no way to recover security in biometric authentication. In this work a storage model was developed in an embedded system that besides aiming to extend the security of the stored biometrics samples, focuses on the low cost and the independence of external connections for its operation. The development was performed in Python 2.7 language and used the encryption techniques, One -Time Password, Database and Hash to perform the security of the information contained in the memory of a Raspberry Pi 3 Model B.

KEYWORDS: Biometrics. Cryptography. One-time password. Raspberry Pi3.

Recebido: 30 ago 2018
Aprovado: 04 out 2018

INTRODUÇÃO

Nos últimos anos o aumento da automação e do uso de redes interligando sistemas criou a necessidade de novas ferramentas que permitam manter a segurança e o pleno funcionamento desses serviços. Um recurso muito utilizado em dispositivos móveis e de autenticação é a biometria, porém, caso a segurança no armazenamento dessa informação seja comprometida, a mesma pode ser roubada. Um agravante do caso do vazamento de dados de biometria é a imutabilidade, ou seja, os danos além de irreversíveis, outros serviços que façam o uso de biometria acabariam sendo prejudicados.

Este trabalho faz a apresentação de um modelo de armazenamento que amplie a segurança de amostras de biometria salvas em um dispositivo Raspberry Pi3 Modelo B.

METODOLOGIA

Primeiramente foram obtidas as amostras de biometrias por meio de um repositório aberto disponível em http://bias.csr.unibo.it/fvc2006/. Na intenção de limpar as distorções e manchas sobre as imagens de impressões digitais foi realizado um processo de binarização das mesmas.

No objetivo de otimizar o desempenho e comparar as bibliotecas de processamento de imagens Pillow e OpenCV, foi realizado um estudo comparando o tempo de execução de um *script* de binarização escrito em Python 2.7, baseado em *Threshold* (limiar). Por apresentar melhor desempenho, a biblioteca utilizada de forma definitiva para a binarização das amostras foi a Pillow.

Após a primeira etapa do trabalho ser realizada, as amostras foram armazenadas em um banco de dados MySQL. Visando a segurança do conteúdo, o banco foi criptografado usando o algoritmo AES 128 bits.

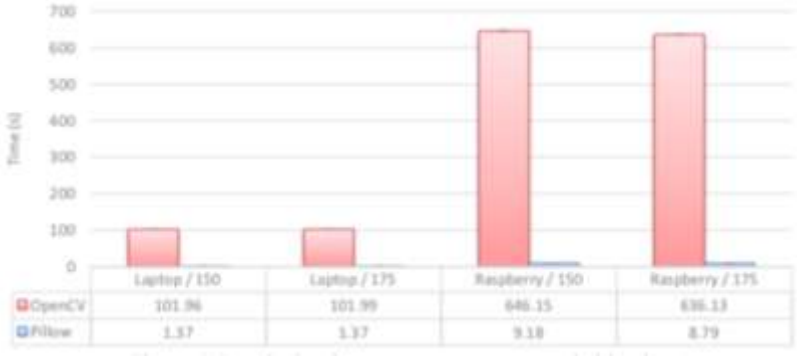
De forma a garantir que cada amostra tivesse uma única e exclusiva chave de criptografia, uma biblioteca de *One Time Password* foi usada. Baseada no identificador (ID) no banco de dados de cada amostra, essa, por sua vez, gera uma sequência de caracteres para ser usada como chave exclusiva e diferente das demais para cada uma das amostras.

O processo de recuperação das amostras criptografadas no banco de dados foi realizado por meio da inserção do identificador da amostra que se deseja obter novamente. Por questões de segurança, os dados de biometria não podem ser expostos, portanto, uma *Hash* do tipo SHA256 foi implementada como retorno. Assim, em nenhum momento após a inserção no banco de dados ocorre a exposição direta com o exterior.

RESULTADOS

O teste de comparação resultou em um melhor desempenho da biblioteca Pillow. Na Figura 1 é apresentada a comparação entre os desempenhos das bibliotecas.

Figura 1 – Comparação de desempenho



Fonte: elaborada pelo autor.

A implementação final permitiu instalar em uma Raspberry Pi3 Modelo B o sistema planejado, onde o armazenamento e recuperação dos dados em forma de *Hash* obteve seu funcionando adequadamente.

CONCLUSÃO

O trabalho desenvolvido permitiu oferecer uma solução de armazenamento em um sistema embarcado de forma independente de conexões externas e de complexidade reduzida. Em trabalhos futuros novas soluções de segurança podem ser implementadas, por exemplo, verificação em duas etapas.

REFERÊNCIAS

OpenCV (2018). **OpenCV: Introduction to OpenCV-Python Tutorials**. Disponível: https://docs.opencv.org/3.4.0/d0/de3/tutorial{_}py{_ }intro.html.

Python Pillow (2018). **Pillow: the friendly PIL fork**. Disponível: http:// python-pillow.org/.

Jain, R. (1991). **The art of computer systems performance analysis: techniques for experimental design, measurement, simulation, and modeling**. Wiley professional computing. Wiley.

PyOTP (2018). **PyOTP - The Python One-Time Password Library**. Disponível: https://pyotp.readthedocs.io/en/latest/.