Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 160 (2019) 235–240

Procedia Computer Science

www.elsevier.com/locate/procedia

The 10th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2019)
November 4-7, 2019, Coimbra, Portugal

Convolutional Neural Network Biometric Cryptosystem for the Protection of the Blockchain's Private Key

Alfaisal Albakri, Chafic Mokbel*

University of Balamand, Kelhat, AlKoura, P.O.Box 100 Tripoli, Lebanon

Abstract

Blockchain technology has attracted a lot of attention in the previous years as a secure way to protect transactions in different processes. It has been particularly used to define cryptocurrencies. While inherently secure against classical single node attacks, the blockchain cryptocurrencies have recently been subject to attacks by malwares able to capture a single user wallet and its included keys. In this work we propose the use of biometric cryptosystems to control the access to the wallets on single machines. After a brief description of the blockchain, the cryptocurrencies and the possible attacks, the paper describes the use of convolutional neural network face recognition as a tool to extract biometric features that help in a key binding approach to protect the personal data in the wallet. Experiments have been conducted on three independent face datasets and the results obtained are satisfactory. The equal error rate between false acceptance and false rejection is negligible when testing on images from the same dataset used for the training of the convolutional neural network. This generalizes well when experimenting on two other independent datasets. These results prove that face cryptosystems can be used to protect the access on sensitive data existing in the wallets of many cryptocurrencies.

Keywords: Blockchain; Biometric Cryptosystem; Face recognition; Convolutional Neural Networks;

* Corresponding author. Tel.: +961-6-930250; fax: +961-6-930278.
E-mail address: chafic.mokbel@balamand.edu.lb

1877-0509
10.1016/j.procs.2019.09.462

1. Introduction

Blockchain is a popular technology for managing digital transactions in several sectors including healthcare [1], supply chain, manufacturing [2], energy [3] and finance [4]. This emerging technology has been at the core of the definition of cryptocurrencies, bitcoin [4] being generally considered as the first one. To illustrate the rate of adoption of blockchain cryptocurrencies we note that the average number of confirmed bitcoin transactions per day was about 370.000 in May 2019 compared to about 60.000 and 215.000 in May 2014 and 2016 respectively [5].

Blockchain is a distributed ledger technology with no central administration. In this context, system vulnerability would have harmful consequences, e.g. allowing an attacker to have access to all information in the ledger. Thus security issues are very critical for blockchain based systems. According to [6] $950 million worth of cryptocurrency were stolen from exchanges and infrastructure in 2018. More critically this number is 3.6 times as much as in 2017.

Blockchain in general and cryptocurrency in particular have been lately subject to different forms of cyberattacks. Among the popular attacks is the miner malware which is spread by an attacker to use the available resources on different computers over the network in order to mine a bitcoin for example. Transfer trojans are also harmful cyberattacks. They monitor the processes running on a machine in order to detect a string similar to a crypto-currency account number, which is assumed to be the destination account of a transaction. Once detected, they replace it with a malicious account number making it the destination of the transfer transaction.

One popular cyberattack exploits existing vulnerabilities in exchanges and wallets. Wallets are the stores of cryptocurrencies. They also store the wallet private keys. Attackers try to intercept the password users employ to access their wallets or to find unencrypted wallet data. By accessing the wallet of a user, the private key becomes accessible and the attacker will virtually own all of the cryptocurrency in the compromised wallet.

Biometric cryptosystems are well established techniques to protect resources on digital machines. In order to protect the users' wallets, we propose to protect the wallets and the users' private keys by biometric access control. Deep learning has permitted the achievement of state of the art performance in biometric systems [7][8]. Biometric features, in particular face features, will be extracted from a deep convolutional network and used to compute and protect the private key and thereby the wallet in a blockchain.

The paper is organized as follows. Section 2 explores wallet security issues and cyberattacks on blockchain. Biometric cryptosystems are discussed in Section 3. The approach proposed to protect the private key of a wallet is detailed in Section 4. Afterwards the face images datasets used and the experimental results obtained are provided in Sections 5 and 6 respectively. The paper ends with concluding remarks.

2. Wallet security

Blockchain technology is based on consensus of replicated, shared and synchronized digital data that is distributed on different nodes over a network. This forms a kind of distributed database controlled by blockchain algorithm. The distributed database stores all historical transactions as a digital shared ledge where transaction is recorded in a block. The blocks are arranged in chains. Each block is linked to the preceding block which is its unique parent in the chain. In contrast, a block in the chain can have multiple children. A block is identified by a cryptographic generated hash. Each block contains in its header the signed hash of its parent block. It also contains a timestamp identifying the time the transactions have been executed. Blocks are made public and must be verifiable. In order to be able to verify that no coin can be double spent, some constraints are placed on the hash of a block that require large computation, e.g. having k leading 0's. To meet this requirement the CPUs of different nodes, the miners, are put to contribution. Inherently blockchain technology resists classical single node attacks. Actually, in order to modify one block an attacker will have to modify all the subsequent blocks while satisfying the constraint on the hash signature. This is computationally non feasible especially for a fast growing chain.

In a blockchain each transaction is signed by the private key of the user. Having access to the private key corresponding to an account is sufficient to manage and use this account. The private key is stored in the user's wallet. Thus, the security of a wallet is mainly the security of the private keys that are included. Several cryptocurrency stealing malwares have been discovered in the recent years. Trickbot [9] uses webinjection to modify webpages presented to the user. Trickbot will change the destination of the purchase towards the attacker's account but will also send to the attacker a stolen copy of the user's wallet for future damage.