UDC 004.045

M.M. Demchuk, O.L. Turovskyi
(National Aviation University, Ukraine)

Cryptocurrency assets technology protection by means of the apartment key method

The article "Cryptocurrency Asset Protection Using the Apartment Key Method" focuses on the use of the apartment key method for safeguarding cryptocurrency assets. It describes the role of hardware wallets as devices specifically designed to securely store private keys.

Hardware wallets are devices specifically designed to store private keys securely. They are considered a safer alternative to PC or smartphone wallets, mainly because they do not maintain a constant connection to the Internet. Such features significantly reduce the vector of possible attacks that are available to attackers, which in turn implies that there is no possibility to remotely interfere with the operation of such a device.

A good hardware wallet ensures that private keys never leave the device. Basically, keys are stored in a special memory partition that does not allow them to be deleted.

Because hardware wallets are constantly offline, they must be used in conjunction with a computer device. Due to their design, such devices can be connected to a virus-infected PC or smartphone and bypass possible risks associated with private key leakage. This type of wallet interacts with software that allows the user to view their balance or make transactions.

Once the user creates the transaction, he sends it to the hardware wallet (1 in the diagram below). Note that the transaction is still incomplete, as it still needs to be signed with the private key that is on the device. In addition, the user will have to confirm that the recipient's address and the number of coins to be sent are correct. He then signs the transaction, thus sending it back to the software (2), which broadcasts the transaction to the cryptocurrency network (3).

Today there are biometric tokens. Using biometrics to authenticate the user. Like the Feitian BioPass FIDO U2F FIDO2 USB-A K27. (https://rozetka.com.ua/213568621/p213568621/). This is a good method of protecting your token, using fingerprint recognition

Reliable scanning doesn't just depend on the sensor. Further processing of the data is the key to successful fingerprint recognition.

In a fingerprint scanner with an optical sensing element, in factmonochrome matrix, the image comes in as a photos..

In the simplest scanners, the image is simply compared to standard. Often further processing is based on working with several .

The digital code received from the scanner in a system with a linear thermal sensor is always a different pattern. The fingerprint scan is always different, the quality of recognition depends on the angle at which the finger was swiped, the humidity of the finger or the surface of the scanner. The data supplied by such a

scanner is actually a set of dots. No matter how the finger rests on the scanner surface, these dots will always have the same curvature of lines.

It should be noted that errors are unavoidable when recognizing fingerprints with any type of sensor or algorithm. Errors are usually divided into two types - failure to recognize a correct fingerprint and recognition of an incorrect fingerprint as a correct one

Fingerprint recognition methods and implementation

Action plan:

- binarization of the acquired image
- skeletonization of the image
- point selection
- point comparison

The technology is flawless, but it still has flaws.

Disadvantages: 1. The sensor type has high environmental requirements, and humidity and cleanliness of the fingers are required. Fingerprint wear and tear will also lead to unrecognizable effects; 2. Some people may be born without fingerprints or have few fingerprint features and they cannot be mapped; 3. Fingerprint traces are easy to retain, there is the possibility of copying, and security is reduced.

Today, there is a more advantageous user identification technology. Which you can implement to protect your hardware wallet. This technology is called Face ID (facial recognition technology)

But, of course, the most popular real-world application case is Apple Face ID. To biometrically scan the shape of the face and recognize it when you unlock the iPhone, the TrueDepth camera is equipped with two infrared projectors that pick out facial points and store them in memory as a mathematical code. A combination of the camera and proximity and light sensors, the Flood Illuminator (which you can't see in the dark), and the Dot Projector create a highly accurate three-dimensional model of your face and store the pattern directly to the processor. A specially locked part of the smartphone's CPU is responsible for storing the Face ID key. According to the developers, the system is capable of self-learning and adapting to the user, without regard to clothing, glasses and age-related changes in the face. The Face ID function can be used to authorize purchases with the payment system Apple Pay. Apple claims Face ID technology verifies matches using facial structure data that cannot be read from a printed or digital two-dimensional photo. And sophisticated neural networks protect against fraud using masks or other tricks. Face ID technology can even detect your attention span. It only recognizes your face if your eyes are open and you're looking at the device. This makes it harder to unlock your device without you knowing (for example, when you're asleep). The odds of another person being able to unlock your iPhone or iPad Pro with Face ID are 1 in 1,000,000.

Liveness: how it works, the case.

But how does the system determine if the person in front of it is real and alive? There is another interesting technology for this - Liveness. It "deals" with biometric detection of a living face. Liveness Detection prevents bots and attackers from using stolen photos, embedded deepfake videos, realistic masks or other fakes to create or

access online accounts. Liveness ensures that only real people can create and access accounts. The purpose of the real-presence verification phase: to prevent fraudsters, who increasingly resort to spoofing attacks using a photo, video, or other substitution of an authorized person's biometric characteristics to gain someone's privileges or access rights. Liveness Detection implemented in the system must comply with the ISO 30107-3 attack detection standard.

Different developers provide their Liveness solutions to society (FaceTec, ID R&D, VisionLabs), but the principle of how they work is identical. Before a user provides an identity document when registering, he must reliably prove that he is a real live person. This is to prevent an attacker from being able to authenticate using a fake photo or a realistic facial mask (Deepfake). Two types of data are required for each user authentication: facial data (for matching) and "live" data (to confirm that the facial data was obtained from a live person). Live data should be time-stamped and only valid for a few minutes and then deleted. Only facial data should be stored at all times. New "live" data should be collected each time an authentication is attempted.

So, the biometric system must determine whether the data came from a living person or an inanimate artifact (an inanimate object that attempts to reproduce human biometric features). 3D Liveness analyzes your quick video selfies for the attributes of a living person: certain head and facial muscle movements in response to commands and their corresponding shadows and highlights on skin texture; micro changes in facial expression during movement and statics; and reaction speed. Once it is proven that the new account belongs to a real person, their biometric data will be stored as a reliable reference of their digital identity for subsequent authorization.

References

1. Online source - https://businesstimenow.com/selfie-biometrics-exploring-face-recognition-liveness-technologies-for-mobile-apps/
2. Online source - https://sudonull.com/post/161763-Fingerprint-recognition-methods-and-implementation-using-Python
3. Online source - https://academy.binance.com/en/articles/what-is-a-hardware-wallet
4. Online source - https://www.liveness.com/