Security Problem Definition and Security Objectives of Cryptocurrency Wallets in Common Criteria

Araştırma Makalesi/Research Article

Yasir Emre BULUT[1,2], İsa SERTKAYA[1,3]

[1]Cybersecurity Engineering, Istanbul Sehir University, Istanbul, Turkey
[2]TUBITAK BILGEM OKTEM Lab., Kocaeli, Turkey
[3]TUBITAK BILGEM MCSLabs & BCLabs, Kocaeli, Turkey
yasir.bulut@tubitak.gov.tr, isa.sertkaya@tubitak.gov.tr
(Geliş/Received:15.01.2019; Kabul/Accepted:23.03.2020)
DOI: 10.17671/gazibtd.513088

***Abstract*—** Bitcoin paper gave birth to a new era; cryptocurrencies aiming distributed trust model. Almost all the cryptocurrencies require their users individually manage their own cryptographic keys, provide or recommend use of cryptocurrency wallets. A wallet, which at least stores public-private keys and addresses, is one of the key points for end-users' security. Since the authentication of a transaction strictly depends on private keys, any adversary who gains access to a wallet may seize all the coins within. Hence, cryptocurrency wallet solutions should be carefully analyzed and better to be certified if possible. In this study, we aim to define the security problems and objectives necessary for the development of a certified product that can stand against the known attacks within the Framework of Common Criteria (CC). We believe this would be a brief source for cryptocurrency wallet Protection Profile (PP) and Security Target (ST) documents.

***Keywords*—** bitcoin, blockchain, common criteria, cryptocurrrency, wallet, security problem, objectives

Kripto Para Cüzdanlarının Ortak Kriterler'de Güvenlik Problemi Tanımı ve Güvenlik Hedefleri

***Özet*—** Bitcoin makalesi, dağıtık güven modelini amaçlayan kripto para birimlerinin ortaya çıkmasını sağlamıştır. Neredeyse tüm kripto para birimleri, kullanıcılarının kendi kriptografik anahtarlarını bireysel olarak yönetmelerini veya kripto para birimi cüzdanlarını kullanmalarını zorunlu hale getirmektedir. Açık-özel anahtar çiftlerini ve kullanıcı adreslerini saklayan cüzdanlar, son kullanıcıların güvenliği için kilit noktalardan birisidir. Bir işlemin gerçekleştirilmesi tamemen özel anahtarlara bağlı olduğundan, cüzdana erişen herhangi bir saldırgan, bu özel anahtarlara bağlı tüm paraları ele geçirebilir. Bu nedenle, kripto para cüzdanları dikkatlice analiz edilmeli ve mümkünse sertifikalandırılmalıdır. Bu çalışmada, Ortak Kriterler çerçevesinde, bilinen saldırılara karşı dayanıklı sertifikalı bir ürünün geliştirilmesi için gerekli güvenlik problemleri ve hedeflerinin tanımlanması amaçlanmaktadır. Bu çalışmanın kripto para birimi cüzdanı Koruma Profili ve Güvenlik Hedefi dokümanları için temel bir kaynak teşkil etmesi hedeflenmiştir.

***Anahtar Kelimeler*—** bitcoin, blokzincir, ortak kriterler, kripto para birimi, cüzdan, güvenlik problemi, güvenlik hedefi

1. INTRODUCTION (GİRİŞ)

Blockchain technology was born after the paper "Bitcoin: A peer-to-peer electronic cash system" published under a pseudonym Satoshi Nakamoto [1]. This study proposes to solve the double spending problem by logging all the transactions into a chain of blocks and showed that if more than half of the involved entities are honest, the system would eventually come to a consensus [23]. Blockchain, and similarly distributed ledger technology, assures integrity of validated transactions without the need of a central authority [12]. Informally, cryptocurrency is decentralized peer-to-peer, client-based distributed

payment type to transfer value. Cryptocurrencies aim to remove intermediaries, provide flexibility and usability while requiring high security concern to achieve these features [2].

In order to be able to receive and send coins, each user needs to have a digital signing private-public key pair and an address which generally created from the public key using some algorithms [38]. For frequent usage, all of the key pairs and addresses should be stored in digital cryptocurrency wallets. It should be noted that wallets hold the addresses and keys associated with them. On the other hand, end users who want to invest on cryptocurrencies may use cryptocurrency exchanges managing sensitive data on behalf of the user. The wallets provided to take custody of a user's cryptographic keys which are used by exchanges are also called as custodian wallets [15].

Cryptocurrency wallets, shortly crypto wallets, basically store public-private keys and addresses and hence crypto wallets are of utmost importance for end-users' security [3]. Connection of such device to the Internet makes it perfect target for the theft and increases potential loss [5].

In this study, we provide necessary security objectives of cryptocurrency wallets to ensure a certain level of security against defined security problems. We will follow general approach that involves all types of wallets. In this way, developers may be able to select and use the appropriate items. For this purpose, we will focus on the detailed description of the assumptions, threats and policies that construct the security problem definition by using CC framework. CC is an international evaluation methodology for information technology products. PP is a guidance document including security features for a product type while ST is the specialized security fatures document prepared for a certain product under evaluation.

We have followed the methods to develop a PP or ST defined in the Technical Report named as "ISO/IEC TR 15446:2017 Guidance for the Production of Protection Profiles and Security Targets" and published by the International Organization for Standardization (ISO) [20].

Following the goals above, Section 2 will summarize CC goals, methods, procedures. Next, crypto wallet definitions, types and solutions will be given in Section 3. Section 4 will be about importance of the wallet security. After the Security Problem Definition is provided in Section 5, we will point out the Security Objectives for the wallets and environment to counter the security problems in Section 6. Finally, Section 7 concludes the paper.

2. COMMON CRITERIA (ORTAK KRİTERLER)

CC is a security standard to assess the security levels of Information Technology products or systems and to evaluate these products in independent laboratories. The criteria are based on TCSEC, ITSEC and CTCPEC which were American, European and Canadian security standards. CC Standard is released by ISO in 1999 [21]. Evaluation consists of document examinations, functional testing and vulnerability analysis of product. It is flexible and extensible standard to enable evaluations of broad range of IT products [22]. CC can be tailored for each application type with PP documents and for each application with ST documents. These documents define the set of security requirements [43]. PPs contain general requirements, security problem definitions and security objectives about certain product types.

CC is divided into seven levels representing the depth of examination. These levels are called as Evaluation Assurance Levels (EAL) [24]. These components indicate how deep or thorough the evaluation is [25]. EAL1 provides trust for functional efficiency and lower security assurance for non-serious threats. EAL2 and EAL3 require more developer interaction and design documentation. Starting from EAL3, configuration management and development environment control are required. EAL4 is the most used level in CC evaluations. In this level, methodological testing of sub-systems is performed [21]. In each level, vulnerability analysis is performed and attack potential for every attack is calculated. Developers can choose an assurance level and extend this level with higher components [26].

CC is flexible and the scope of the evaluation context can be altered by developer. If there is no policy or requirement from an authority, developers are allowed to define the scope of the evaluation. CC Framework is the most appropriate field for independent assessment of products and thus ensures a certain level of product safety [40]. Also, the PP guides the developers on what kind of measures they should consider. As an example, the lack of the versioning system, configuration management system and test environment, which led to security flaws on wallets used by Mt.Gox exchange and as a result of the attacks exchange filed for bankruptcy could easily be solved by CC [7].

Providing security is not only related to wallet features but also related to environmental precautions as well. Users are expected to be careful about some points, wallet developers are expected to use secure software development methods and environmental applications or operating systems are expected not to compromise any failure. The CC Framework also helps to ensure the necessary protection in this regard.

3. TYPES OF CRYPTOCURRENCY WALLETS (KRİPTOPARA CÜZDAN ÇEŞİTLERİ)

Cryptocurrency wallets are storing coin addresses, private and public keys to send and receive cryptocurrencies. Users can monitor their balance by keeping track of transactions [3]. Wallets can have one or more addresses. Even though a Bitcoin transaction does not reveal the owners of the sending address or receiving address, it does not provide full privacy for the users, since the Bitcoin addresses just behave as a pseudonym of the users [11].

Primarily, crypto wallets are divided into two categories, hot and cold wallets. *Hot wallet* means there is connection to internet and transactions could be done in a much faster way. On the contrary, *cold wallet* is kept offline as much as possible. Since they are susceptible to network attacks, hot wallets have wider attack surface. Keeping wallets offline are thought to be safer but there are other relevant security problems like stealing and losing which are the main considerations about cold wallets [11].

In order to satisfy specific user requirements and processing environment, wallets can be further classified into five types namely *paper*, *mobile*, *desktop*, *online* and *hardware wallets* [10]. In figure 1, many wallet brands in each different category as well as wallets in multiple categories are shown.

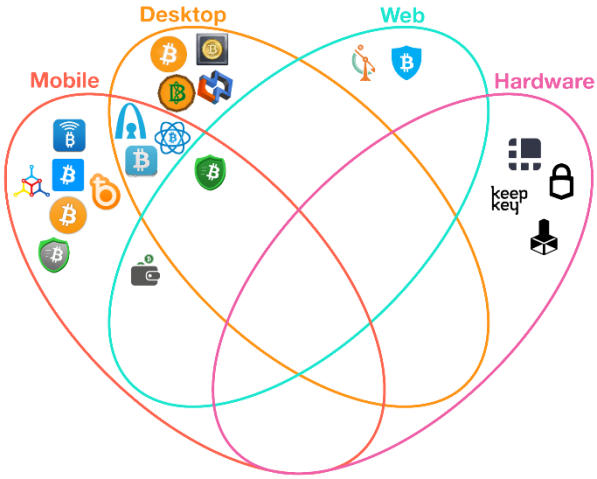

Figure 1. Taxonomy of Crypto Wallet Types
(Kripto Cüzdan Tipleri Sınıflandırması)

Mobile Wallets: Smartphones' convenience and accessibility made mobile wallets a need. These type of wallets store private keys locally, so the owner can use it almost anywhere and spend coins easily. Mobile wallets are applications running on users' phones and one advantage is having fast transaction verification mechanisms without requiring downloading entire blockchain [10].

Desktop Wallets: Desktop wallets are software running on PC or laptop. Although accessibility is restricted only to the installed computer, these wallets can offer more services than other types. If the network attacks and virus threats could be mitigated, desktop wallets offer considerable security level [10]. Armory, Electrum, Bitcoin/QT, MulitBit are in this wallet type.

Online Wallets: Online wallets are web based wallets working on cloud based systems. Despite the high availability and ubiquity providing accessibility from anywhere, keeping private keys in the cloud system is the main drawback in terms of security [10]. Coinbase, Circle, Xapo, CoinKite, ANXPro are examples of this wallet type.

Paper Wallets: These are the physical paper wallets to keep user addresses. There are two QR codes on the paper; one is for encoding user's address to receive Bitcoins, other one is for encoding user's secret key to spend Bitcoins owned by the user. To spend coins sweeping is as easy as scanning the QR code or entering private keys [10]. MyEtherWallet in figure 2 is a good example of this type.

Figure 2. MyEtherWallet Paper Wallet [35]
(MyEtherWallet Kağıt Cüzdanı)

Hardware Wallets: These are dedicated hardware products for storing private key and addresses. Physical wallets provide more security mechanisms because of the dedicated hardware storage. Since there is no connection to the outer world except connecting to a computer, attackers cannot access these devices easily. Hardware devices can be certified against certain types of attacks but users should not lose their wallets [10]. Also, one important drawback is hardware failure, if there is no recover policy, hardware failure may cause loss of everything. Against a possible failure or lose, recoverability and back-up options must be provided. Trezor, Ledger and Keepkey are well known brands of hardware wallets.

Table 1. Specifications of wallet types
(Cüzdan türlerinin özellikleri)

	Wallets (From Hot to Cold)				
Specifications	Online	Desktop	Mobile	Hardware	Paper
Physical	X	X	X	✓	✓
Always online	✓	✓	✓	X	X
Own hardware to keep keys	X	X	X	✓	✓
Need whole Blockchain to verify transaction	✓	✓	X	X	X
Prone to hardware failure or loss	X	X	X	✓	✓
Easy to support or add different coin types	✓	✓	✓	X	X

Table 1 summarized the characteristics of different wallet types. Besides above classification, according to the key generation methods, wallets can be divided into two groups, deterministic and non-deterministic. In a non-deterministic wallet, keys are generated randomly and

independently [17]. Deterministic wallets can generate whole tree of key pairs from a single key, which is root of the tree. Mnemonic sentence is a way to remember the root key or backup the wallet [18].

4. SECURITY OF CRYPTOCURRENCY WALLETS (KRİPTOPARA CÜZDANLARIN GÜVENLİĞİ)

All types of wallets provide different levels of security. Users can choose which type of wallet they will use according to their security and availability concerns. If the need is using addresses and keys always online as in exchange markets, the hardware wallets will not be the right choice or if need is to use crypto wallet in a retail store, desktop wallets will be useless.

Hardware wallets may be susceptible to hardware failures, hardware attacks and theft while software wallets are vulnerable to software failures and network attacks. Also, hardware failures of mobile, desktop or cloud platforms could affect software wallets.

We will define threats for each type of wallets in accordance with the CC terminology. Since paper wallets are not applicable to the evaluation, they are out of our scope and there will not be any threats, assumptions and organizational security policies about this type of wallets.

A wallet is a single point of failure since private keys are used for authenticating owners of the coins [14]. To enhance security, there are wallets requiring more than one signature called as multi-signature wallets (multi-sig). These wallets are mostly used by online wallets or cryptocurrency exchanges against security risks of loss or capture of private keys [41]. Coins could be accessed by using 2 or more signatures. This specification increases the difficulty of stealing coins because compromise or loss of a key will not prevent owner to access own wallet [10]. If this is enforced for exchange platforms, the attack of Bitfinex's loss resulted in $65 million and Parity's loss $30 million might be prevented [8].

A report about exchange losses specifies that cryptocurrency exchanges will be irresistible target in the near future. As this is of interest to end users as well as exchanges, end-users also seek for reliable solutions and products for securely managing their sensitive information [9]. Since cryptocurrency exchanges have to use wallets as in any blockchain application, security is based on the protection of private keys, no matter how secure the blockchain infrastructure is. Being online and having large number of users, online wallets are more prone to attacks by hackers. Due to the compromise of private keys in a multi-signature wallet hosted by BitGo, hackers achieved to stole $72m worth of bitcoin from Bitfinex, Hong Kong based cryptocurrency exchange [4].

The assets of wallets in which security is concerned could be listed as coins, protected objects, authorization data, operations, security attributes [20]. Security problems will focus on these assets and each possible situation that could create security vulnerability will be listed individually.

Each type of wallet requires user authentication so that user passwords or PINs must be strong enough [31]. Another common problem is the quality of random numbers. Since asymmetric algorithms are based on randomness, strong random numbers protect against vulnerability of cryptographic operations. Bugs and malwares are software related threats which are applicable to almost all wallet types [6].

5. SECURITY PROBLEM DEFINITION (GÜVENLİK PROBLEM TANIMI)

Security Problem Definitions are the security problems related to the product type. This section includes threats, assumptions and organizational security policies [27]. The purpose of definition is to specify the problem in a formal way because quality of the security problem definition shows the usefulness of the ST [20]. Threats are any actions performed by someone or something against assets. Assumptions are made about the environment to specify parts that cannot be tested. Organizational security policies are the ones that the users of the products have to obey to avoid any possible vulnerability while in use. These policies could be about users, physical environment, supporting software or anything else [22].

PP is the implementation independent specification document consisting of Security Problem Definitions (threats, assumptions, OSPs), security objectives, security functional and security assurance requirements [22].

To achieve the overall security of a product, every aspect needs to be considered. For this reason, threats will be supported by assumptions and policies. Threats are defined according to the possible risks related to product. Assumptions cover the environmental conditions related to the product which is called as target of evaluation (TOE) in CC framework. Also there could be policies for safe and secure use of TOE in its operational environment [22]. Figure 3 illustrates the components of security problem definition.

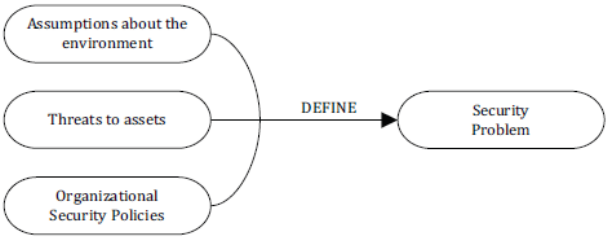

Figure 3. Components of Security Problem [20].
(Güvenlik Problemi Bileşenleri)

We generated each definition according to CC framework so that developers could easily use them in their documentation. Abbreviations at the beginning of the

definitions T, A, P, OT and OE denote Threats, Assumptions, Policies, Objectives for TOE and Objectives for Environment respectively.

5.1. Threats (Tehditler)

Here we define the threats related to the cryptocurrency wallets. During the CC Evaluation of a wallet, PP and ST documents can be created with the related threats from the following list. The definitions of the threats are in the CC format and each threat includes asset, threat agent and adverse action. Assets are data or functionality that needs to be protected. Threat agent is used to identify attackers and adverse action is any act that the attacker would capable of.

T.Compromise: An attacker may attempt to perform unauthorized actions to reveal undetected compromise of data in protected area [32].

T.UnauthorizedAccess: A malicious user or attacker may gain unauthorized access to lost or stolen wallet. Access could be granted by bypassing any PIN or fingerprint lock and attacker gain root access to reveal wallet data [31]. Attacker could take advantage of weak authentication mechanism.

T.ReverseEngineering: An attacker may obtain innate design of applications to exploit possible vulnerabilities. Vulnerabilities could be on hard-coded passwords, encryption keys or application specific information as well [31].

T.Reflashing: An attacker may be able to install unofficial firmware on the hardware wallet to gain control over device [16].

T.Replacing: An attacker may steal and replace hardware wallet with a fake one. Also, he can try to steal PIN with some ways such as placing wireless transmitter or keylogger into the fake wallet [16].

T.FakeAddress: An attacker may change the receiving address to get the coins into his own account [33].

T.WeakAuthentication: An attacker may brute force, dictionary attack or guess user password, passphrase or PIN to get access to wallet [31].

T.Eavesdropping: An attacker may listen to an existing communication between wallet and interface or any other application. With the help of replay or man-in-the-middle attacks he may capture identification and authentication data to gain access to the system [31].

T.DDoS: An attacker may cause denial of service by using tools and/or infected computers [36]. Connection quality could be degraded between wallet and Blockchain network and wallet services could be unabled consequently. Bugs or weaknesses in the software implementation let attackers to execute this type of attacks [37].

T.UnauthorizedUpdate: Malicious software and/or firmware could be used to bypass security mechanisms during update proscedures and obtain sensitive data [34].

T.InformationLeakage: An attacker may exploit information which can be leaked from the hardware wallet during its usage in order to get private key. In this attack, leakage could occur through power consumptions, electromagnetic variations, Input/Output characteristics. These type of attacks are called as side channel attacks [30].

T.Hardware: An attacker may be able to modify the hardware to get sensitive information or compromise availability and authenticity. Attacker may perform physical probing of the hardware parts and disclose security functionality data, authentication information or private keys [29].

T.Malfunction: An attacker may cause a malfunction during the normal operation by applying environmental stress. This attack could be done by applying power, clock or electromagnetic fluctuations to the hardware wallets to modify security services and functions or affect security mechanism. Especially, random number generation mechanism and quality of random numbers may be affected or the mechanism totally deactivated [29].

5.2. Assumptions (Varsayımlar)

Assumptions are expectations that must be taken by operational environment to maintain secure usage TOE. Environment means anything except wallets such as users, underlying platforms, operating systems, other applications, cloud systems or physical places. If the operational environment of wallets does not meet these assumptions, they may not be able to perform expected secure functionality.

Assumptions cannot be tested during the evaluation since evaluation of environmental components are not in the scope of CC and they are expected to be covered.

A.SecurePlatform: It is assumed that mobile platform take necessary precautions against rootkit installation, tampering or backdoor installation. Mobile operating system or security applications must have enough control over mobile device to protect wallet application against these types of attacks. System should detect untrusted applications come from untrusted servers which may have backdoor placed by a malicious user.

A.EducatedTrustedUsers: Wallet users are assumed to be aware of generic cyber attacks. They need to know how to handle with social engineering and phishing attacks. Also, users are expected to be trusted not to expose any sensitive data intentionally or unintentionally. While making a

payment, users should check correctness of receiving address [16].

A.SearchPoison: An attacker tries to poison search engine results to send users to the fake addresses. The aim is to get their private information and drain their wallets [13]. Since this is not a direct attack to the wallet, both users are assumed to know these type of attacks as stated in the previous assumption and search engines are assumed to take precautions against phishing ads and prevent fake addresses as much as possible.

A.Update: Update and recovery of environmental components assumed to be secure and will not disrupt functionality.

4.3. Organizational Security Policies (Kurumsal Güvenlik Politikaları)

Organizational Security Policies (OSP) are set of rules and constraints about TOE or its environment to protect the functionality and sensitive data. These rules could be set by an organization, policy maker or developer. Policies specify mandatory security functions inside the wallets or techniques which requires the existence of those functions [20].

P.Authentication: Wallet users will authenticate themselves before using functionality of wallets.

P.StrongAuth: Wallet PINs, passwords and passphrases will be robust and complex enough to provide the required security. This requirement could be defined by developer or customer.

Table 2. Matching Threats, Assumptions and OSPs with wallet types
(Cüzdan türleriyle Tehdit, Varsayım ve OSP'lerin Eşleştirilmesi)

Threats/Assumptions /OSPs	Hardware	Mobile	Desktop	Cloud
T.Compromise	✓	✓	✓	✓
T.UnauthorizedAccess	✓	✓		
T.ReverseEngineering		✓	✓	
T.Reflashing	✓			
T.Replacing	✓			
T.FakeAddress			✓	✓
T.WeakAuthentication	✓	✓	✓	✓
T.Eavesdropping	✓	✓	✓	✓
T.DDoS		✓	✓	✓
T.UnauthorizedUpdate	✓	✓	✓	✓
T.InformationLeakage	✓			
T.Hardware	✓			
T.Malfunction	✓			
A.MobilePlatform		✓		
A.EducatedTrustedUsers	✓	✓	✓	✓
A.SearchPoison		✓	✓	✓
A.Update	✓	✓	✓	✓
P.Authentication	✓	✓	✓	✓
P.StrongAuth	✓	✓	✓	✓
P.BackUp	✓			

P.BackUp: Hardware wallets will be designed to provide secure back up in case of a possible hardware failure or it must provide recovery.

Threats, assumptions and policies are summarized in Table 2 in regard to their applicability on specific wallet types. While software threats could be applied to all wallet types, hardware threats are matched with hardware wallets.

6. SECURITY OBJECTIVES (GÜVENLİK HEDEFLERİ)

Security Objectives are brief and discrete statement of the intended solutions of defined security problems [28]. These problems can be solved by either the product itself which is named as target of evaluation (TOE) or operational environment (OE). Objectives provide high-level, natural language solutions and combine part-wise solutions to form a complete protection [22]. According to CC, each security objective traces back to at least one security problem. Figure 4 shows the relationship between Security Problems and Security Objectives. While threats and organizational security policies can be solved by both security objectives for TOE and operational environment, assumptions can only be fulfilled by operational environment security objectives. The three role of the security objectives are listed as

- Providing high level natural language solution of problems,
- Dividing solutions into two parts so that different entities address a part of the problem,
- Demonstrating a complete solution formed by these part wise solutions [28].

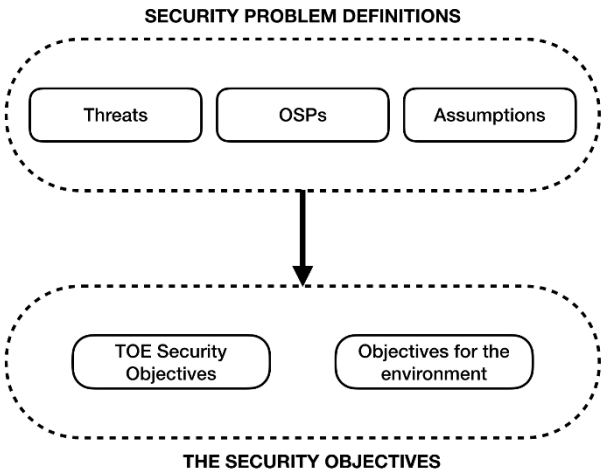

Figure 4. Role of the Security Objectives [20].
(Güvenlik Hedeflerinin Rolü)

There will be part wise solutions for cryptocurrency wallets and these solutions will consist of high-level overall solution for general security problem in the scope of the product. The details of the solutions must be given as clear and understandable for potential customers of the product under evaluation.

6.1. Security Objectives for TOE (Test altındaki Ürün için Güvenlik Hedefleri)

Following Objectives are precautions that must be satisfied by wallets.

OT.Access: The security mechanism of wallet application must provide necessary level of authorization mechanism and complexity not to let anyone bypass and gain unauthorized access to the assets. Wallet must control access to the functionalities [29]. Also two-factor or multi-factor authentication might be implied. Using two factors simply means double authenticating is more secure then using ony one password, PIN or biometric data.

OT.ReverseEngineering: Security functionality of a product must not let anyone to obtain innate design of applications to exploit possible vulnerabilities.

OT.FakeAddress: Wallets must show full address to the user to protect from receiving and sending address forgery. For hardware wallets, addresses created by device must match with the one in wallet applications running on computer.

OT.Reflashing: Hardware wallets must be designed not to let any attacker to install any firmware on it. Enclosure or case might be designed as protective and tamper resistant to protect any pin or ports [29].

OT.Replacing: Hardware wallets must be designed in a way that is easily realized in case of a replacing. If the wallet is stolen, this unique and distinctive feature must let the owner understand and take the precautions.

OT.WeakAuthentication: Any type of wallet must be robust against authentication attacks such as dictionary, brute force and guessing attacks. Authentication mechanisms must have long and complex passwords, passphrase and PINs and enforce increasing waiting times starting from a short period if authentication attempts are wrong [42].

OT.Eavesdropping: Security functionality of wallets must keep communication obfuscated and encrypted so that any attacker cannot reveal any secret data or cannot get authorization data via eavesdropping. Doing cryptographic operations in the wallets' secure boundary could be another protection mechanism for this attack [29].

OT.Storage: Secret data inside the wallets must be stored in a secure way so that in case of a compromise any information gained by the attackers will be useless.

OT.InformationLeakage: Hardware wallets must be secure against information leakage. Any kind of emanation must not give any information about sensitive data [29].

OT.Hardware: Hardware wallets must provide required mechanisms to detect and block physical attacks not to disclose sensitive information or lose control of security functionalities. This type of security could be provided by tamper mechanisms which are tamper evidence, tamper resistance and tamper response mechanisms. Tamper resistance enclosure will stop attacker or mitigate attacks. Tamper response mechanisms respond in case of an attack via shielding or deleting sensitive data against disclosure [29].

OT.Malfunction: Hardware wallets must take precautions against fault attacks in hardware and software levels. Fluctuations in power, electromagnetic and other environmental conditions must not be able to disclose any information [29].

OT.Audit: TOE must detect and provide evidences of software or hardware breaches. It is very important to have audit records to understand any situation happened.

OT.KeyCompromise: Wallets must be designed to keep the sensitive data in the secured area. Private key operations must not be done outside the wallet.

OT.FailSecure: If there is a failure, wallets must enter a secure failure mode. This objective is similar to hardware attacks tamper response mechanism. Any type of wallets could respond in case of a failure by entering failure mode [32].

OT.Integrity: Wallets must have an integrity check mechanism [32].

6.2. Security Objectives for Operational Environment (Operasyonel Çevre için Güvenlik Hedefleri)

Following Objectives are precautions that must be fulfilled by operational environment of wallets.

OE.DataImport: Sensitive Data must be generated and imported into the wallet in a secure way.

OE.SecureBlocks: Blockchain applications that will be used in wallets must be designed and implemented in a secure cryptographic way not to be solved easily.

OE.SecurePlatform: Platforms on which mobile, cloud or desktop wallet application run must be secure against misuse, installing untrusted applications, rootkit, malware or backdoor installation.

OE.TrustedUsers: Trusted wallet users must be educated and know how to handle well-known cyber attacks [16].

OE.RobustComponents: Secure design must be ensured in operational environment. There must not be any information leakage or faulty operation caused by underlying components [8].

Table 3. Matching Threats and OSPs with Security Objectives for TOE
(Test Altındaki Ürün için Güvenlik Hedefleri ile Tehdit, Varsayım ve OSP'lerin Eşleştirilmesi)

Threats Assumptions OSPs	OT.Access	OT.ReverseEngineering	OT.FakeAddress	OT.Reflashing	OT.Replacing	OT.WeakAuthentication	OT.Eavesdropping	OT.Storage	OT.InformationLeakage	OT.Hardware	OT.Malfunction	OT.Audit	OT.KeyCompromise	OT.FailSecure	OT.Integrity
T.Compromise	✓	✓				✓		✓		✓		✓			
T.UnauthorizedAccess	✓				✓	✓		✓				✓			
T.ReverseEngineering		✓						✓						✓	✓
T.Reflashing				✓								✓			
T.Replacing					✓										
T.FakeAddress	✓		✓								✓				
T.WeakAuthentication	✓					✓					✓				
T.Eavesdropping							✓				✓		✓		
T.DDoS							✓				✓		✓		
T.UnauthorizedUpdate	✓			✓				✓				✓			✓
T.InformationLeakage									✓						
T.Hardware								✓		✓	✓			✓	✓
T.Malfunction											✓			✓	✓
P.Authentication	✓														
P.StrongAuth	✓					✓									
P.BackUp													✓		

Table 4. Matching Threats, Assumptions and OSPs with Security Objectives for Operational Environment
(Operasyonel Çevre için Güvenlik Hedefleri ile Tehdit, Varsayım ve OSP'lerin Eşleştirilmesi)

Threats Assumptions OSPs	OE.DataImport	OE.SecureBlocks	OE.Platform	OE.Users	OE.Components	OE. StrongAuth	OE.SafeSeed	OE.FakeAddress	OE.Update
T.Compromise						✓			
T.UnauthorizedAccess				✓			✓		
T.ReverseEngineering		✓							
T.Reflashing			✓		✓				
T.Replacing				✓					
T.FakeAddress			✓	✓	✓				
T.WeakAuthentication						✓			
T.Eavesdropping				✓		✓			
T.DDoS				✓		✓			
T.UnauthorizedUpdate					✓				
T.InformationLeakage					✓				
T.Hardware									
T.Malfunction									
A.MobilePlatform	✓		✓		✓				
A.EducatedTrustedUsers				✓					
A.SearchPoison				✓				✓	
A.Update									✓
P.Authentication									
P.StrongAuth						✓			
P.BackUp									

OE.StrongAuth: Simple and predictable PINs, passwords and passphrases must not be chosen. Instead of any series of repeated or sequenced numbers, letters or words users must choose random and robust ones [8].

OE.SafeSeed: Users are expected to keep recovery seed or passphrase physically secure. Since the recovery seed or passphrase is used for recovery, the coins can be accessed easily without the real wallet using a different one [19].

OE.SeachEngine: Users are expected to realize the fake addresses in search engine results. Also, search engine experts are expected to extract these misleading results.

OE.ReliableUpdate: Environmental components are expected to keep security during and after the update and recovery processes.

Table 2 and table 3 show mapping between security problem definitions and security objectives. Tables demonstrate that each threat is countered by least one security objective for TOE, each OSP is enforced by at least one security objective for TOE or environment and each assumption is uphold by at least one security objective for operational environment. Assumptions could be covered only by environmental objectives.

7. CONCLUSION (SONUÇ)

We defined security problem definition and security objectives of cryptocurrency wallets according to CC Framework. These definitions are aimed to cover all possible vulnerabilities against cryptocurrency wallets since they are expected as single point of failure. To explain the importance of security and certification, we identified security breaches in the recent history. The fact that we receive news of a new vulnerability every day shows us the lack of confidence and guarantee that certification provides. For this reason, we described CC and mentioned about wallets in terms of security. Threats and related objectives will cover the required security mechanisms in a typical wallet while assumptions, OSPs and related environmental security objectives will cover requirements about users, platforms and other applications.

Since blockchain is an emerging technology, while researches pursued on alternative currency solutions and their further applications, not enough effort is put on usability and security certification concerns of by products. As best of our knowledge this paper is the first study in the CC field for Cryptocurrency wallets, our aim is to attract developers, users, and CC evaluation labs to put more focus on standardized framework for this evolving era. We believe CC framework and evaluation processes would surely contribute developments of more secure cryptocurrency wallet applications and devices. As most known formal evaluation methodology CC is the best suitable way of evaluating information technology products and systems. Whether or not they apply for certification, crypto wallet manufacturers can benefit from

this paper if they apply the defined security features correctly and completely. Furthermore, if international or national technical committees are established related to these products in user groups of CC, this study will be very useful for them.

As a future work, we are planning to define security functional requirements compatible to the security objectives given in this study.

REFERENCES (KAYNAKLAR)

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.

[2] S. Guler, **Secure Bitcoin Wallet,** Master's Thesis, KTH, School of Information and Communication Technology, Stockholm, Sweden, 2015.

[3] S. Eskandari, D. Barrera, E. Stobert, J. Clark," A First Look at the Usability of Bitcoin Key Management", *Internet Society*, doi:10.14722/usec.2015.23015, 2015.

[4] O. Boireau, "Securing the blockchain against hackers", *Network Security*, 2018(1), 8-11. doi:10.1016/S1353-4858(18)30006-0, 2018.

[5] T. Bamert, C. Decker, R. Wattenhofer, S. Welten, "BlueWallet: The secure Bitcoin wallet", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8743*, 65–80, 2014.

[6] J. H. Mosakheil, "Security Threats Classification in Blockchains", *Culminating Projects in Information Assurance*, 2018.

[7] Internet: A. Rosic, 5 high profile cryptocurrency hacks. https://blockgeeks.com/guides/cryptocurrency-hacks/, 2017.

[8] R. Juzenaite, "Security vulnerabilities of cryptocurrency exchanges", *Infosec Instittute*, 2018.

[9] Internet: J. Kirk, Cryptocurrency exchanges lost 882 million to hackers. https://www.bankinfosecurity.com/ cryptocurrency-exchanges-lost-882-million-to-hackers-a-11624, October 2018.

[10] G. Karame, E. Androulaki, **Bitcoin and blockchain security**, Boston: Artech House, 2016.

[11] M. Conti, E. S. Kumar, C. Lal, S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin", *IEEE Communications Surveys & Tutorials*, 20(4). doi: 10.1109/COMST.2018.2842460, 2018.

[12] M. Tanriverdi, M. Uysal, M. Üstündağ, "Blokzinciri Teknolojisi Nedir? Ne Değildir?: Alanyazın İncelemesi", *Bilişim Teknolojileri Dergisi*. 203-217. 10.17671/gazibtd.547122, 2019.

[13] Internet: J. Weiczner, Hackers Stole $50 Million in Cryptocurrency Using 'Poison' Google Ads. http://fortune.com, 14 February 2018.

[14] T. Volety, S. Saini, T. Mcghin, C. Z. Liu, K.-K. R. Choo, "Cracking Bitcoin wallets: I want what you have in the wallets", *Future Generation Computer Systems*, 91, 136–143. doi: 10.1016/j.future.2018.08.029, 2019.

[15] R. Houben, A. Snyers, **Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion**, Brussels: European Parliament, 2018.

[16] Internet: Security: Threats, https://wiki.trezor.io/Security:Threats#Hacking_SatoshiLabs_servers.

[17] Internet: P. Marek, R. Pavol, V. Aaron, B. Sean, Mnemonic code for generating deterministic keys, https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki, 10 September 2013.

[18] A. M. Antonopoulos, **Mastering Bitcoin: Unlocking Digital Crypto-Currencies,** California, USA: O'Reilly Media Inc., 2014.

[19] N. Courtois, P. Emirdag, F. Valsorda, "Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events", *IACR Cryptology ePrint Archive*, 2014, 848, 2014.

[20] Technical Committee ISO/IEC JTC 1 SC 27, **ISO/IEC TR 15446:2017 Information technology - Security techniques - Guidance for the production of protection profiles and security targets**, Geneva, Switzerland, 2017.

[21] M. Gregg, **CISSP Exam Cram**, Fourth Edition. USA: Pearson IT Certification, 29 August 2016.

[22] Common Criteria Development Board, **Common Criteria for Information Technology Security Evaluation Part 1**, 2017.

[23] E. Karataş, "Developing Ethereum Blockchain-Based Document Verification Smart Contract for Moodle Learning Management System", *Bilişim Teknolojileri Dergisi*, 11(4), 399-406, DOI: 10.17671/gazibtd.452686, 2018.

[24] S. Y. Kang, J. H. Park, M. K. Khan, J. Kwak, "Study on the common criteria methodology for secure ubiquitous environment construction", *Journal of Intelligent Manufacturing*, 23(4), 933-939, 2009.

[25] S. P. Kaluvuri, M. Bezzi, Y. Roudier, "A Quantitative Analysis of Common Criteria Certification Practice", *Trust, Privacy, and Security in Digital Business Lecture Notes in Computer Science*, 132-143, 2014.

[26] Bundesamt für Sicherheit in der Informations technik (BSI), **Guidelines for Developer Documentation according to Common Criteria Version 3.1.**, 2007.

[27] A. Bialas, "Ontology-Based Security Problem Definition and Solution for the Common Criteria Compliant Development Process", **2009 Fourth International Conference on Dependability of Computer Systems**, 3-10. Brunow, Poland, 2009.

[28] Common Criteria Development Board, **Common Criteria for Information Technology Security Evaluation Part 3**, 2017.

[29] Bundesamt für Sicherheit in der Informations technik (BSI), **Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014**, 2014.

[30] F. X. Standaert, "Introduction to side-channel attacks", **Secure integrated circuits and systems**, 27-42. Springer, 2010.

[31] R. Sachova, M. M. Marcos, S. H. Revetti, **Security of Mobile Payments and Digital Wallets**, European Union Agency for Network and Information Security, 2016.

[32] Trusted Computing Group, **Protection Profile PC Client Specific TPM**, 2014.

[33] A. Garba, Z. Guan, A. Li, Z. Chen, "Analysis of Man-In-The-Middle of Attack on Bitcoin Address", **ICETE 2018**, 388-395. 10.5220/0006864003880395, 2018.

[34] Full Drive Encryption International Technical Community, **Collaborative Protection Profile for Full Drive Encrytion Authorization Acquisition**, 1 February 2019.

[35] Internet: A. Rosic, Paper Wallet Guide: How to Protect Your Cryptocurrency, https://blockgeeks.com/guides/paper-wallet-guide/, 2017.

[36] C. H. Kateraas, **Threats to Bitcoin Software**, Master's Thesis, Norwegian University of Science and Technology Department of Computer and Information Science, 2014.

[37] Internet: L. King, Bitcoin Hit by Massive DDoS Attack as Tensions Rise. www.forbes.com, 12 February 2014.

[38] K. Fanning, D. P. Centers, "Blockchain and Its Coming Impact on Financial Services", *J. Corp. Acct. Fin*, 27(5), 53-57. doi:10.1002/jcaf.22179, 2016.

[39] D. Dasgupta, J. Shrein, K. D. Gupta, "A survey of blockchain from security perspective", *Journal of Banking and Financial Technology*, 10.1007/s42786-018-00002-6, 2019.

[40] D. Mellado, E. Fernández-Medina, M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems", *Computer Standards & Interfaces*. 29. 244-253. 10.1016/j.csi.2006.04.002, 2007.

[41] O. Taş, F. Kiani, "Blok Zinciri Teknolojisine Yapılan Saldırılar Üzerine bir İnceleme", *Bilişim Teknolojileri Dergisi*, 11(4) , 369-382, 2018.

[42] I. Bashir, **Mastering blockchain distributed ledgers, decentralization, and smart contracts explained**, Birmingham: Packt Publishing, 2018.

[43] R. Richards, D. Greve, M. Wilding, W. M. Vanfleet, "The Common Criteria, Formal Methods and ACL2", **ACL2 Workshop 2004**, Texas, USA, 2004.