MA-TEECM: MUTUAL ANONYMOUS AUTHENTICATION-BASED CREDENTIAL MIGRATION TECHNOLOGY FOR MOBILE TRUSTED EXECUTION ENVIRONMENTS

[1] **Mr.M.V.Nagesh,**
Associate Professor, Department of CSE, Sreyas Institute of Engineering and Technology,Telangana, India, nagesh.vagu@sreyas.ac.in

[2] **Maada Sathvika,**
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India,sathvikareddymaada@gmail.com

[3] **Venkata Sai Swapna Pallapothu,**
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana,India, pvsaiswapna@gmail.com

[4] **Munukuntla Divya,**
Department of CSE, Sreyas Institute of Engineering and Technology,Telangana,India, divyamunukuntla15@gmail.com

[5] **Kondooru Yashwanth Reddy,**
Department of CSE, Sreyas Institute of Engineering and Technology, Telangana, India, kondooriyashwanthreddy8930@gmail.com

Abstract

ARM TrustZone is the most widely used mobile trusted execution environment (TEE) technology today. Its hardware-enabled isolated execution environment provides reliable assurance of secure storage of credentials in mobile devices. However, the research on managing credentials stored in the TEE throughout the lifecycle of mobile devices has received little attention in recent years, and the credentials in TEE generally face usability problems caused by the mobile device lifecycle events. Aiming at the risk of information disclosure caused by the third-party service providers in the traditional credential migration scheme, this paper presents a mutual anonymous authentication- based credential migration framework for mobile trusted execution environments. First, we propose a peer-to-peer credential migration model between mobile terminals based on TrustZone and SGX, which solves the single point of failure caused by attacks on trusted third parties that act as credential transfer stations and managers in traditional solutions; Second, we propose an identity authentication protocol between TEEs based on mutual anonymous authentication, and a detailed authentication process is designed based on the universal mobile TEE model; Third, we build a formal verification model using High-Level Protocol Specification Language (HLPSL). Finally, the formal and informal security

analysis indicate that the improved scheme meets the expected security requirements and is secure against several known attacks.

Keywords: *Credential migration, trusted execution environments, mutual authentication.*

I INTRODUCTION

Arm partners have shipped more than 232.4 billion Arm-based processor chips by mid-2022, which are widely used in mobile Internet devices such as mobile phones, tablet computers, and smartwatches. As mobile devices are more and more commonly used in business, finance, and information technology, the coexistence of sensitive data and normal data on mobile terminals is becoming very common. For example, Bring Your Own Device (BYOD) is a policy that allows employees to use their personal mobile devices to access office areas to process corporate data and login Intranet applications . Many enterprises accept it by creating secure containers on employees' personal mobile devices to ensure data security. However, because sensitive data, such as user credentials, are tightly coupled with mobile devices, when an user tries to migrate data to a new device due to a device's lifecycle events (such as terminal replacement or employee separation), the user usually needs to manually re-register credentials acquired in various scenarios to the new devices one by one, instead of migrating directly from the old terminal to the new. Credentials are the evidence that lets entities access privileged data and services, such as user keys, certificates, and other authentication information. As the device's usage time accumulates, a considerable amount of credentials will be stored in the trusted execution environment (TEE) of the mobile device, which poses several challenges to the credential management of the mobile terminal.

First, traditional user passwords are vulnerable to phishing and dictionary attacks, and key management software based on TEE is gradually gaining popularity to obtain more secure and convenient password management functions. For example, the Keystore system component has been introduced since Android 4.0, which makes the keys independent of the application or even the operating system. That is, the user can encrypt, decrypt and manage the key through the Keystore API without obtaining the key, which significantly improves the security of the keys. However, it also increases the cost for users to reconfigure keys. With the growth of the number of keys, it is no longer feasible to manually reconfigure keys on new terminals.

Second, with the rapid development and broad application of artificial intelligence technology, the machine learning process has been introduced in increasingly digital credentialing systems. For example, in all series of iPhone devices, the fingerprint and face print data stored in the TEE will be gradually strengthened over time, and if users cannot migrate this credential directly, it will take some

time to relearn in the new terminal.

Finally, digital assets stored as credentials are gaining popularity, such as cryptocurrencies, NFT, and digital copyright certificates. Users urgently need a solution to automatically migrate their credential files to the new terminal when replacing devices. Therefore, it is necessary to migrate the credentials between devices considering device lifecycle events.

II LITERATURE SURVEY

The TEE credential migration refers to transferring and reloading credential data between different TEEs. Credential migration services can save significant device re-initialization overhead and are critical for lifecycle events such as mobile device replacement. However, the standard TEE implementation today still cannot solve the problem of credential migration very well. The key migration issue first appeared in the research on the Trusted Platform Module (TPM), which is an essential part of TPM 1.2 and 2.0 specifications, and many researchers have proposed various methods to improve it [6]. However, research on key or credential migration for mobile TEE has not received sufficient attention. Based on a public resource known as the Open Certificate Platforms (OCP), Kari et al. proposed a trusted domain certificate migration protocol. They recommended encrypting and backing up the credentials on a trusted server with a password known only to the user and then completing the credential migration by entering the password again. The protocol framework does not require complex user interaction and authentication processes, however, all user credentials must be stored in the server in clear text, and the migration process becomes the process of reconfiguring the backup files in the server. Although a key known only by users protects the process, the architecture lacks a discussion on the identity authentication between the OCP and the two devices' TEE. There is a privacy breach due to the service provider's full access to user credentials and personal data. Arfaoui et al. propose a privacy-preserving scheme for migrating credentials between Global Platform TEEs, which requires dynamic interaction between service providers and TEE managers. Although the authors mention that the service provider must authenticate the TEE, the migration protocol does not provide a specific identity certification procedure, and the necessity of mutual authentication between the service provider and the TEE is not covered.

Similarly, Literature and implement identity authentication management between credential migration devices through a trusted service provider. Carlton et al. demonstrated the necessity of mutual authentication in the credential migration service for the first time, and used formal tools to model their proposed mutual authentication protocol, proving the security of the protocol process. Tan and Song ,proposed a key migration protocol that supports mutual authentication between trusted roots, which achieves identity binding of both migration parties by adding device attributes in the authentication process between the source and target devices to the

service provider. Nishimura et al. propose using a trusted third party to identify the owner of a personal device to prevent the sharing of authentication keys to malicious nodes. The literature mentioned above, however, all needs to assume that the third-party service provider is trusted.

"Secure authentication key sharing between personal mobile devices based on owner identity"

The public key-based Web authentication can be securely implemented using modern mobile devices with a hardware-assisted trusted environment such as the Trusted Execution Environment (TEE) as a secure storage of private keys. As a private key is strictly kept secret within the TEE and never leaves the device, there is a usability issue: the user must register the key separately on each device and Web site, which is burdensome for users who start using a new device. The aim of this research is to provide a solution with enhanced usability in key management by relaxing the restriction that the keys never leave the device and allowing the private keys to be shared among the devices while still maintaining an acceptable level of security. We introduce a third party that is responsible for supervising the key-sharing between devices in an authentication system. The third party performs the identification of the owner of each device to mitigate the risk of the keys being illegally shared to another person's device. Also, we propose a secure method for copying keys from the TEE of one device to that of another through a certificate-based mutually authenticated channel. We implemented the copying method in the ARM TrustZone-based TEE and showed that our approach is feasible on a commercially available smartphone.

" *Secure migration of WebAssembly-based mobile agents between secure enclaves"*

Cryptography and security protocols are today commonly used to protect data at- rest and in-transit. In contrast, protecting data in-use has seen only limited adoption. Secure data transfer methods employed today rarely provide guarantees regarding the trustworthiness of the software and hardware at the communication endpoints.The field of study that addresses these issues is called Trusted or Confidential Computing and relies on the use of hardware-based techniques. These techniques aim to isolate critical data and its processing from the rest of the system. More specifically, it investigates the use of hardware isolated Secure Execution Environments (SEEs) where applications cannot be tampered with during operation. Over the past few decades, several implementations of SEEs have been introduced, each based on a different hardware architecture. However, lately, the trend is to move towards architecture-independent SEEs.

III EXISTING SYSTEM

Based on a public resource known as the Open Certificate Platforms (OCP), Kari et al. proposed a trusted domain certificate migration protocol. They recommended encrypting and backing up the credentials on a trusted server with a password known only to the user and then completing the credential migration by entering the password again. The protocol framework does not require complex user interaction and authentication processes; however, all user credentials must be stored in the server in clear text, and the migration process becomes the process of reconfiguring the backup files in the server.

Disadvantages

- Although a key known only by users protects the process, the architecture lacks a discussion on the identity authentication between the OCP and the two devices' TEE.
- There is a privacy breach due to the service provider's full access to user credentials and personal data.

IV PROPOSED SYSTEM

Considering the target model, the attacker model, and the Global Platform TEE specification, this paper proposes a novel model MA-TEECM, for TEE credential migration based on mutual anonymous authentication. Specifically, a new group manager (GM) participant is introduced between the source TEE and the target TEE. GM is an enclave program running in Intel SGX, responsible for verifying the integrity of the access device's TEE, creating group signatures, and issuing group membership certificates for the source TEE and target TEE. With the assistance of the GM, a shared interaction channel is created for any legitimate TEE.

Advantages

We recommend that users implement credential migration between user devices in a peer-to-peer manner to prevent remote attackers from compromising key infrastructure.GM verifies the integrity of the TEE fingerprint of mobile devices and issues group member certificates to all nodes that pass the verification.We provide an online algorithm, named CEDC-O, based on Lyapunov optimization, to convert

the long-term optimization problem.MA-TEECM enables mutual anonymous authentication, ensuring that users' identities remain private and secure during credential migration. Secure Credential Migration facilitates secure migration of credentials between mobile trusted execution environments, protecting sensitive information from unauthorized access. MA-TEECM ensures that trust is maintained throughout the credential migration process, guaranteeing the integrity of the transaction. By utilizing trusted execution environments and anonymous authentication, MA-TEECM provides an additional layer of security for mobile transactions. The technology enables efficient credential migration, reducing the overhead and latency associated with traditional authentication methods.

MA-TEECM enables seamless communication and credential migration between different mobile trusted execution environments, promoting interoperability. The technology allows users to securely and privately migrate credentials between devices, enhancing the overall user experience. By minimizing the exposure of sensitive information, MA-TEECM reduces the risk of identity theft, fraud, and other security threats.MA-TEECM can help organizations comply with regulations and standards requiring robust security and privacy measures for mobile transactions. The technology is designed to support a large number of users and transactions, making it an ideal solution for large-scale mobile applications

V IMPLEMENTATION

Source device

when the source device's establishes a connection, the request process or even the key program itself may still use protocol vulnerabilities to transmit key request credentials to the receiver, causing the receiver to lose the ability to identify the connection to the sender Using this module source device with register with application and send request to group manager who will generate security key and send to source device which will be used to link source device information. Source device will authenticate with target device when migrating data after confirmation only data will be deleted from source device

Target Device:

Identifying whether the target device belongs to the source device owner is critical in the credential migration 1) Ensure that the root of trust of the current device is secure, that is, satisfy the integrity,

and grant it a ticket for end-toend communication; 2) Verify that the terminal contains a root of trust before credential migration

Using this module target device will send authentication to source device to get key to login then send authentication request.To group manager to get other key with this key he can view data which is stored in source device

Data Storage Server:

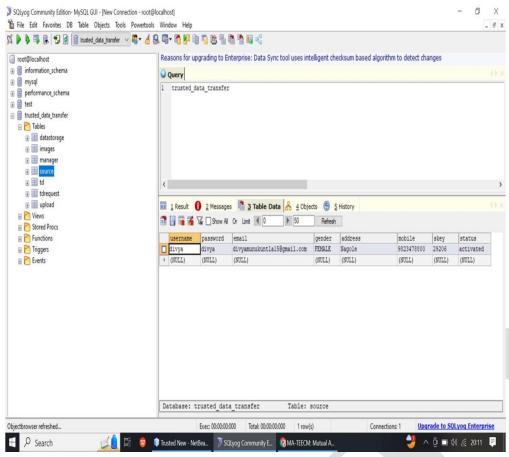
This module is used to store data from source device and target device and view information of every user

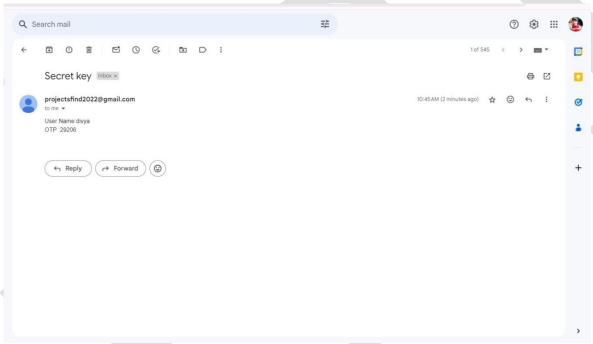
Group Manager Server:

Specifically, a new group manager (GM) participant is introduced between the source device and the target device. GM is an enclave program responsible for verifying the integrity of the access devices, creating group signatures, and issuing group membership certificates for the source device and target device. With the assistance of the GM, a shared interaction channel is created for any legitimate devices.

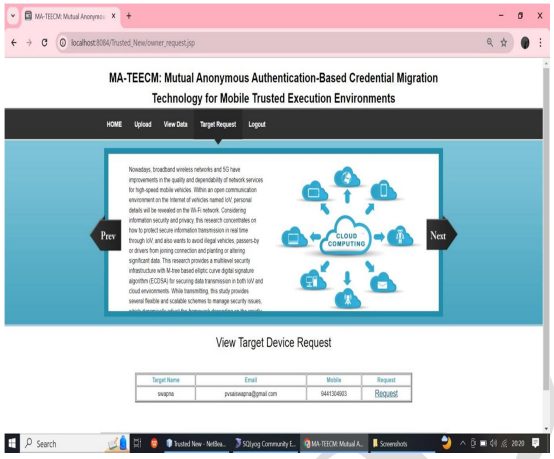
Using this module group manager will login and view requests for key generation and key request form source and target devices and send keys through mail

VI RESULTS




Search mail
Secret key
projectsfind2022@gmail.com
User Name:divya
OTP: 29206
Reply
Forward


MA-TEECM: Mutual Anonymous Authentication-Based Credential Migration
Technology for Mobile Trusted Execution Environments
HOME
View Request
View Target Device Request
Logout
Prev
Next
CLOUD COMPUTING
View Source Device Request



VII CONCLUSION

Trusted Execution Environment is emerging as a flexible mobile security mechanism that can provide enhanced security guarantees for security-critical applications, credential files, and other types of sensitive data on any mobile device. This paper proposed a model framework that enables peer-topeer credential migration between personal mobile devices to address credential availability issues caused by device lifecycle events. A third party, insulated from sensitive data, was introduced in the channel establishment process of credential migration, which is responsible for assisting two mobile devices in the local area network to establish group membership. Furthermore, a peer-to-peer credential migration protocol based on the mutual authentication scheme was designed, and the algorithm and model of credential migration in TEE were created. Security analysis showed that MA-TEECM could guarantee the confidentiality and integrity of credential data. Finally, AVISPA's back-end automated verification tools, OFMC and ATSE, were used to verify the security of the proposed protocol successfully.

REFERENCES

[1] Hideo Nishmura,Yoshihiko Omori and Takao Yamashita, "Secure Authentication key sharing between personal mobile devices based on owner identity",in proc. IEEE Truscom,vol 28 292- 301(apr.2020).

[2] M. Sabt, M. Achemlal, and A. Bouabdallah, ''Trusted execution environment: What it is, and what it is not,'' in Proc. IEEE Trustcom/BigDataSE/ISPA, vol. 1, Aug. 2015, pp.

57–64.

[3] L. Karlsson and M. Hell, ‘‘Enabling key migration between noncompatible TPM versions,’’ in Proc. Int. Conf. Trust Trustworthy Comput. Cham, Switzerland: Springer, 2016, pp. 101–118

[4] K. Kostiainen, N. Asokan, and A. Afanasyeva, ‘‘Towards user-friendly credential transfer on open credential platforms,’’ in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur. Berlin, Germany: Springer, 2011, pp. 395–412.

[5] G. Arfaoui, S. Gharout, J.-F. Lalande, and J. Traoré, ‘‘Practical and privacypreserving tee migration,’’ in Proc. IFIP Int. Conf. Inf. Secur. Theory Pract. Cham, Switzerland: Springer, 2015, pp. 153–168.

[6] H. Li, Z. Li, Z. Wang, and X. Chang, ‘‘Authorization credential migration method, terminal device, and service server,’’ U.S. Patent 16 476 988, Nov. 21, 2019. [10] N. Kumar, ‘‘Identity authentication migration between different authentication systems,’’ U.S. Patent 10 412 077, Sep. 10, 2019.

[7] C. Shepherd, R. N. Akram, and K. Markantonakis, ‘‘Remote credential management with mutual attestation for trusted execution environments,’’ in Proc. IFIP Int. Conf. Inf. Secur. Theory Pract. Cham, Switzerland: Springer, 2018, pp. 157–173.

T. Liang and S. Min, ‘‘TPM2.0 key migration-protocol based on duplication authority,’’ J. Softw., vol. 30, no. 8, pp. 2287–2313, 2019.