JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

MA-TEECM: Mutual Anonymous Authentication-Based Credential Migration Technology for Mobile Trusted Execution Environments

Mr. RAMBABU ATMAKURI - Head, Department of CSE, Anurag College of Engineering (Aushapur, Ghatkesar, Telangana 501301)

Mr. GUNDLAPALLY ESHWAR PRASAD - Student, Department of CSE, Anurag College of Engineering (Aushapur, Ghatkesar, Telangana 501301)

Mr. YALLA JASHWA - Student, Department of CSE, Anurag College of Engineering (Aushapur, Ghatkesar, Telangana 501301)

Mr. MOHAMMED AQUEEL AHMED -Student, Department of CSE, Anurag College of Engineering (Aushapur, Ghatkesar, Telangana 501301)

Mrs. BANOTH MANDIRA - Student, Department of CSE, Anurag College of Engineering (Aushapur, Ghatkesar, Telangana 501301)

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.

1. INTRODUCTION

Arm partners have shipped more than 232.4 billion Arm-based processor chips by mid-2022 [1], [2], 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 [3]. 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 a 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) [4] 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.

2. 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 [5], 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. [7] 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. [8] 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 [9] and [10] implement identity authentication management between credential migration devices through a trusted service provider. Carlton et al. [11] demonstrated the necessity of mutual authentication in the credential migration Technology for Mobile TEEs 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 [12], [13] 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. [14] propose using a trusted third party to identify the owner of a personal device to prevent the sharing of authentication keys to malicious nodes.

3. OVERVIEW OF THE SYSTEM

3.1 Existing System

a trusted domain certificate migration protocol based on the Open Certificate Platforms (OCP). This protocol involves encrypting and backing up credentials on a trusted server with a user-known password, followed by completing the credential migration by entering the password again. However, all user credentials must be stored in the server in clear text, and the migration process involves reconfiguring backup files in the server.

3.1.1 Disadvantages of Existing System

Lack of Identity Authentication: The architecture lacks a discussion on identity authentication between the OCP and the devices' TEEs.

Privacy Breach: There is a privacy breach due to the service provider having full access to user credentials and personal data.

3.2 Proposed System

The proposed system introduces a novel model called MA-TEECM for TEE credential migration based on mutual anonymous authentication. This model involves the introduction of a group manager (GM) participant between the source TEE and the target TEE. The GM, running in Intel SGX, is responsible for verifying the integrity of the access device's TEE, creating group signatures, and issuing group membership certificates for the source and target TEEs. With the assistance of the GM, a shared interaction channel is created for any legitimate TEE.

3.2.1 Advantages of Proposed System

Peer-to-Peer Credential Migration: Users can implement credential migration between user devices in a peer-to-peer manner to prevent remote attackers from compromising key infrastructure.

Integrity Verification: The GM verifies the integrity of the TEE fingerprint of mobile devices and issues group member certificates to all nodes that pass the verification.

Online Algorithm: An online algorithm named CEDC-O, based on Lyapunov optimization, is provided to convert the long-term optimization problem.

3.3 Proposed System Design

In this project work, there are four modules and each module has specific functions, they are:

1. Source device Module

2. Target Device Module

3. Data Storage Server Module

4. Group Manager Server

3.3.1 Source device Module:

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.

3.3.2 Target Device Module:

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-to-end 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.

3.3.3 Data Storage Server Module:

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

3.3.4 Group Manager Server Module:

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.

3.4 Architecture

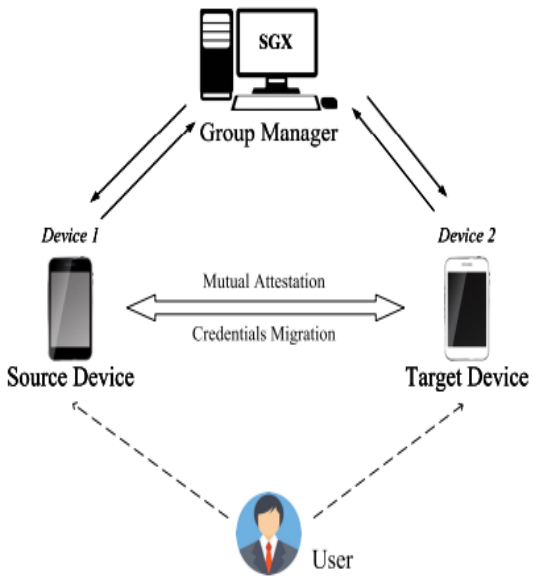
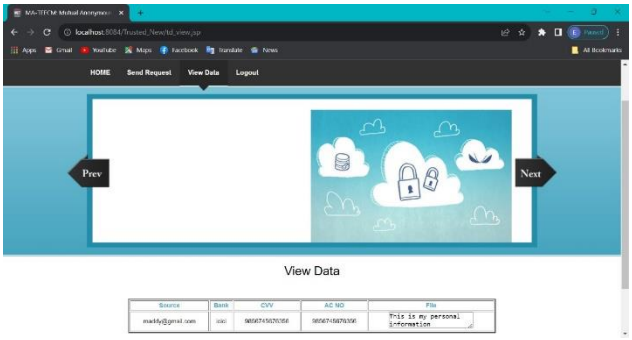
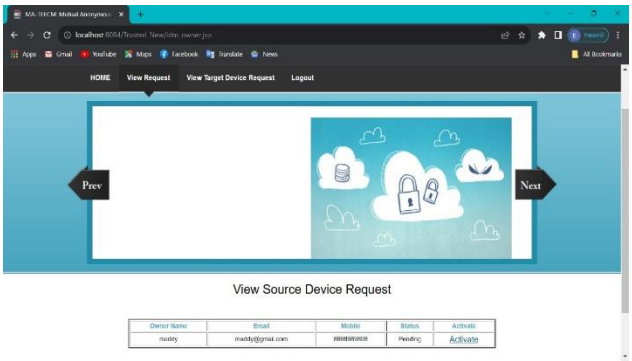
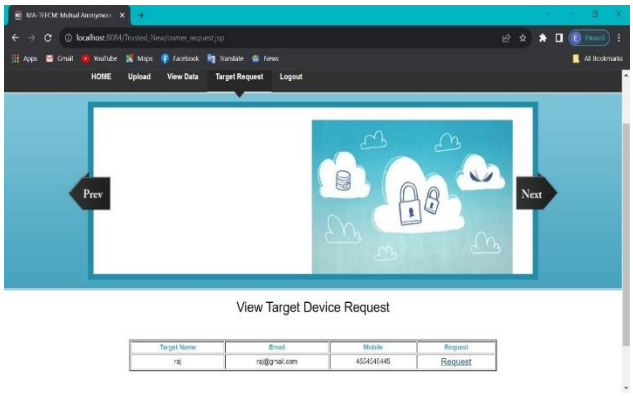


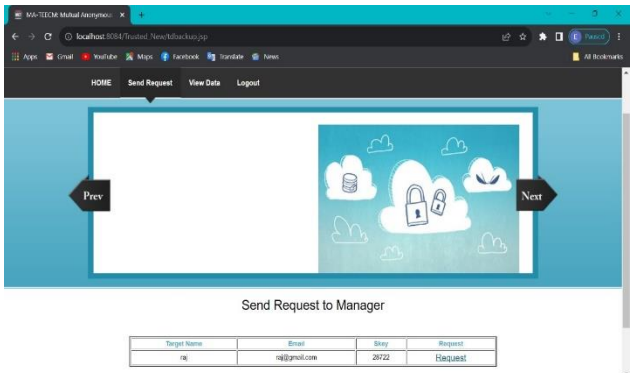
Fig 1: System Architecture

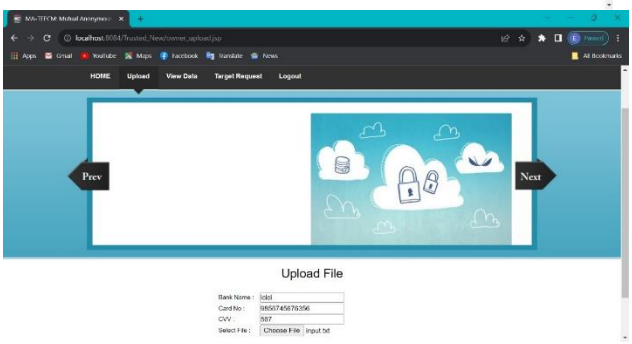
4. RESULT SCREEN SHOTS

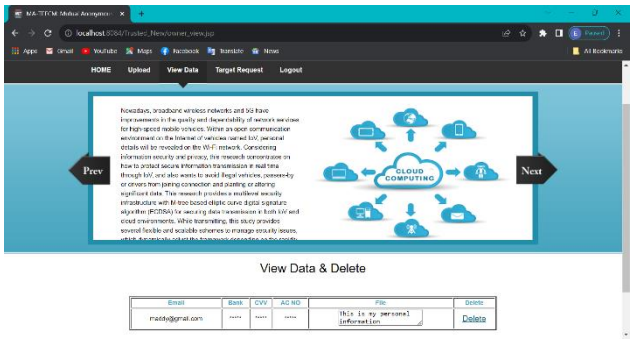












5. CONCLUSION

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

6. REFERENCES

[1] J. Bonneau, C. Herley, P. C. Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE S&P 2012, pp. 553–567.

[2] N. Huaman, S. Amft, M. Oltrogge, Y. Acar, and S. Fahl, "They would do better if they worked together: The case of interaction problems between password managers and websites," in Proc. IEEE Symp. Secur. Privacy (SP), May 2021, pp. 1367–1381.

[3] D. Pasquini, A. Gangwal, G. Ateniese, M. Bernaschi, and M. Conti, "Improving password guessing via representation learning," in Proc. IEEE Symp. Secur. Privacy (SP), May 2021, pp. 265–282.

[4] W. Li and J. Zeng, "Leet usage and its effect on password security,"

[5] IEEE Trans. Inf. Forensics Security, vol. 16, pp. 2130–2143, 2021.

[6] Have I Been PWNED. Accessed: Aug. 15, 2021. [Online]. Available: https://haveibeenpwned.com

[7] Yahoo! Data Breaches. Accessed: Aug. 15, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Yahoo!_data_breaches

[8] Yahoo Tries to Settle 3-Billion-Account Data Breach With $118 Million Payout. Accessed: Aug. 15, 2021. [Online]. Available: https:// arstechnica.com/tech-policy/2019/04/yahoo-tries-to-settle-3-billion- account-data-breach-with-118-million-payout/

[9] Z. Whittaker. (2018). Github Says Bug Exposed Some Plaintext Pass- words. [Online]. Available: https://www.zdnet.com/article/github-says- bug-exposed-account-passwords/

[10] S. M. Bellovin and M. Merritt, "Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise," in Proc. ACM CCS, 1993, pp. 244–250.

[11] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password- authenticated key exchange using Diffie–Hellman," in Proc. EURO- CRYPT. Cham, Switzerland: Springer, 2000, pp. 156–171.

[12] C. Gentry, P. MacKenzie, and Z. Ramzan, "A method for making password-based key exchange resilient to server compromise," in Proc. CRYPTO Cham, Switzerland: Springer, 2006, pp. 142–159.

[13] S. Jarecki, H. Krawczyk, and J. Xu, "OPAQUE: An asymmetric PAKE protocol secure against pre-computation attacks," in Proc. EUROCRYPT. Cham, Switzerland: Springer, 2018, pp. 456–486.