April 2021

Networkless Mobile Payments With Minimal changes in Trusted Execution Environments

Arun Samudrala

Dilip Padmanabhan

Abhijith Bera

Pankaj Gupta

Hemanth Sambrani

See next page for additional authors

Inventor(s)
Arun Samudrala, Dilip Padmanabhan, Abhijith Bera, Pankaj Gupta, Hemanth Sambrani, and Will Drewry

Networkless Mobile Payments With Minimal changes in Trusted Execution Environments

ABSTRACT

Peer-to-peer mobile digital payments can be made in the absence of a network as follows: the receiver of funds verifies the availability of on-device balance by examining the prior, authenticated, transaction records of the sender. A new transaction record including the transaction amount is created, made immutable and secure using cryptographic techniques, and is stored at both sender and receiver. When either sender or receiver regains network connectivity, the transaction is settled with the original provider of the on-device balance, e.g., a financial institution. The integrity of the records of offline transactions, e.g., made in the absence of a mobile network, is vital for offline payments to be secure and trustworthy. This disclosure describes techniques that, with minimal modifications to trusted applications (TAs) in a trusted execution environment (TEE) to securely verify transaction records and to harden them against malicious attacks.

KEYWORDS

- Mobile payment
- Peer-to-peer payment
- Networkless payment
- Double-spend attack
- Near-field Communication (NFC)
- Key pair
- Trusted execution environment (TEE)
- Trusted application (TA)
- Public-key cryptography
- Digital cash

BACKGROUND

Peer-to-peer mobile digital payments can be made in the absence of a network (or during the unavailability of a network due to a traffic spike) as follows. A user has an initial amount, referred to as the balance, that is transferred to their mobile device from a balance provider, e.g.,

a financial institution. The balance is digitally signed by both the user and the balance provider. Peer users bring their mobile devices near each other or otherwise establish peer-to-peer communication between the devices to effect a contactless payment, e.g., using Bluetooth or near-field communication (NFC). The peer devices connect, authenticate each other, and set up a secure communication channel using digitally signed user identities previously issued by a trusted third party.

With appropriate permissions, the receiver device (which is to receive funds) verifies the availability of sufficient balance at the sender to cover the transaction by examining the prior, authenticated, transaction records of the sender, e.g., going back to the initial deposit made by the balance provider. For the current transaction, a new transaction record including the present transaction amount is created on both sender and receiver. The transaction record is signed with a transaction-specific key pair generated by the secure key storage of the sender's device and attested to by the sender's device, e.g. using a hardware-backed trusted execution environment of the device; made immutable by being signed by the private keys of both parties to the transaction; and is appended to ledgers maintained at both sender and receiver device.

When either sender or receiver regains network connectivity, the transaction is settled with the balance provider. A sender can settle with all their counterparty receivers. A given receiver can settle with not only a given sender but with all the receiver-counterparties of the given sender who transacted with the given sender prior to the given receiver, without being privy to the other receivers' transactions with the sender.

The use of transaction-specific keypairs ensures that any attempt by the sender to alter or delete a transaction from the ledger, e.g., to fraudulently claim a larger running balance or to cheat a recipient of a previous transaction, results in further transactions being disabled. Since

the receiver also has a copy of the authenticated transaction record, attempts by the sender to deny a transaction fail, as the receiver can always settle with the sender's balance provider when a network connection becomes available at a later time. Double-spend attempts by the sender are forestalled by enabling a receiver to authenticate the true and current balance on a sender's device (even in the absence of a network), and by enabling the receiver to settle with the sender's balance provider on the basis of an authenticated transaction record. Cloning of the balance on another device is rendered ineffective by the user authentication and device integrity checks, and by binding the balance to the device.

Trustworthy offline payments rely on the authenticity of transaction key pairs and on the security of transaction records' storage and management. Although a trusted execution environment (TEE) is a natural medium to support offline payments, the inability to update a trusted application (TA) within a TEE, even in case of bugs, makes writing a new TA for supporting offline payments infeasible.

DESCRIPTION

Trusted execution environments (TEEs) are more secure than traditional feature-rich operating systems such as smartphone operating systems, because, by design, TEEs have a small footprint, with few lines of code. Their small size ensures thorough verifiability. Also, applications running inside TEEs, known as trusted applications (TAs), are vetted applications from well-known developers and are considered secure. Most TEEs enable only static loading of TAs and, after initial loading, are not updated during the lifetime of the device. Manufacturers typically don't send over-the-air firmware updates for TEEs. Because of all these reasons, it is difficult and time consuming to write a new TA for all the popular vendors and populating user devices with it.

This disclosure proposes making small changes to existing TAs that are widely distributed across various TEEs. The TEEs are leveraged to ensure the authenticity of key pairs, which in turn secures the ledger of transaction records. Per the techniques, a hardware-backed key store, e.g., a widely distributed and well-vetted TA, supports limited-scope, provable keys that can be verifiably destroyed after an assigned number of uses, e.g., for signing. The minimal changes, such as described herein, enable the construction of a reliable protocol on top of a TEE to ensure the integrity of transaction records and hence of the balance on the device, enabling reliable and secure offline payments.

With user permission, the techniques can leverage further features of mobile devices when available and upon permission the user. Such features include, for example:

- A hardware-backed secure key storage implemented in a trusted execution environment. Further, key material that resides on the hardware-backed secure key storage that cannot be extracted by pure software methods.
- Biometric authentication.
- A secure key storage that ensures that an application can access its own keys but not those of other applications.
- A keypair attestation that provides a reliable indicator of genuineness of the secure key storage, its capabilities, the state of the bootloader, and the integrity of the application. A secure key storage that supports keypair attestation, which in turn provides a verifiable chain of trust from the bootloader to the application.
- Security mechanisms that ensure that compromising a mobile payments app and/or operating system (OS) at runtime is relatively non-trivial.

Key material that is non-extractable from the secure key storage via software methods ensures that secret keys cannot be stolen or tampered with. Hardware security modules or secure elements provide an added benefit that hardware attacks to steal or tamper the secret keys are also non-trivial. Per the techniques, mobile devices that include the above features can perform purely offline transactions, where both sender and receiver are offline during the transaction.

Keypair attestation is a determining factor to establish trust between the two peers. Keypair attestation on hardware-backed secure key storage reliably indicates whether: the device bootloader is unlocked; the boot state is not verified; and/or the application has been modified. If the receiver finds that any of the above is true, the transaction with the sender can be declined or the device can proceed to enforce online authentication of the transaction.

If the mobile device is compromised, e.g., by a reboot of the device to unlock the bootloader and subsequent installation of a rootkit, the previously issued balance gets destroyed. The user is required to obtain a fresh balance again, triggering mobile-device integrity verification, which in turn indicates a compromised/unlocked device. The balance provider that issued the original balance can then deny issuing a new balance to the user.

Aside from peer-to-peer mobile payments, the techniques of this disclosure can also be used to enable unlocking of paid services such as transit gates, hotel rooms, self-driven or shared vehicles, etc., and to secure the communication channel between two devices.

Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs, or features described herein may enable the collection of user information (e.g., information about a user's payment app/ wallet, a user's transactions, a user's preferences, or a user's current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more

ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

CONCLUSION

The integrity of the records of offline transactions, e.g., made in the absence of a mobile network, is vital for offline payments to be secure and trustworthy. This disclosure describes techniques that, with minimal modifications to trusted applications (TAs) in a trusted execution environment (TEE) to securely verify transaction records and to harden them against malicious attacks.

REFERENCES

[1] Bera, Abhijit; Samudrala, Arun; Gupta, Pankaj; Padmanabhan, Dilip; Sambrani, Hemanth; Weng, Shuo; and Wong, Wallace, "Secure Mobile Payments Without Network Connectivity," Technical Disclosure Commons, (October 26, 2020).
https://www.tdcommons.org/dpubs_series/3700 accessed Apr. 6, 2021.