Toward A Secure and Highly Available Credit Card Payment Scheme with Trusted Execution Environments

Shintaro Hodai
The University of Tokyo
Tokyo, Japan

Takahiro Shinagawa
The University of Tokyo
Tokyo, Japan

EXTENDED ABSTRACT

With the rapid progress of digital technologies in recent years, the shift towards cashless payments is accelerating on a global scale. Among various cashless options, credit cards continue to grow remarkably due to their unparalleled convenience and versatility. In fact, the volume of credit card transactions, including cross-border transactions, is increasing annually [5], underscoring their indispensability for global payments and highlighting the need for a robust credit card payment infrastructure.

In the current credit card payment scheme, each payment transaction must go through an authorization process. This process begins with a payment terminal generating a payment message after reading the card information. The payment message is then transmitted through multiple relay centers, such as payment gateways, merchant acquirers, and international brand networks, and finally reaches the card issuer for authorization. The payment message includes essential transaction information, such as the payment amount and date, as well as necessary card details such as the card number, expiration date, and security code.

However, the current credit card payment scheme faces several challenges. First, the security of card information in the payment message during the authorization process is not sufficient; the card information is handled in plain text to route payment messages through relay centers, posing a risk of information leakage if malicious employees are present at these centers [6]. Second, the availability of the payment scheme is not sufficient, as a failure in one of the relay centers or networks connecting them would cause transaction interruptions, leading to a large-scale failure of the payment system [3]. Third, the speed of payments may be degraded due to transaction delays caused by increased network latency. Network latency is especially problematic when networks are congested due to payment transactions concentrations or when transactions cross geographically distant countries, both of which are inherently difficult to avoid. Speed and availability of payments, as well as security, are critical issues for payment systems, and their improvement are indispensable [7].

Numerous efforts have been devoted to enhancing the security of credit card payment systems. For instance, Payment Card Industry Data Security Standard (PCI DSS) compliance involves comprehensive security audits to ensure the protection of cardholder data through practices such as regular network monitoring, vulnerability scanning, and the implementation of strong access control measures. Tokenization [1] replaces some of the sensitive information in the payment messages, reducing the risk of data breaches. However, these measures cannot fully prevent unauthorized access by malicious employees at relay centers. Other studies explored solutions for improving availability of payment schemes, such as offline payment systems [2] and blockchain-based payment schemes [4]. However, these studies remain a challenge in terms of compatibility with existing financial infrastructures and handling of sensitive information.

We propose a novel credit card payment scheme that enhances security and availability by leveraging Trusted Execution Environments (TEEs). In this scheme, payment terminals, relay centers, and issuer servers all process payment messages within their respective TEEs so that card information is not exposed in plain text during authentication. Leveraging TEEs allows payment terminals and relay centers to process payment messages based on their content while preventing sensitive information in the payment messages from being disclosed to potentially malicious attackers at each site. We also offload some of the payment authorization functions from the issuer to the TEE at the relay center by exploiting a data type similar to a conflict-free data type (CRDT) [8], which allows the authorization process to be completed without a network connection to the issuer's server and without compromising consistency. By combining TEEs with distributed authentication, our scheme significantly improves security and availability compared to existing solutions, while maintaining compatibility with existing credit card payment systems.

We implemented the proposed payment scheme on Azure's Confidential Computing and evaluated it from the perspectives of security, availability, and network delay resilience. To assess network delay resilience, we compared the authorization processing time during network delays with that of existing payment schemes. Our evaluation showed that the proposed scheme achieved a maximum reduction of 72% in processing time, demonstrating its effectiveness in mitigating network delays and enhancing overall performance.

REFERENCES

[1] Ossama Al-Maliki and Hisham Al-Assam. 2022. A tokenization technique for improving the security of EMV contactless cards. *Information Security Journal: A Global Perspective* 31, 5 (2022), 511–526. https://doi.org/10.1080/19393555.2021.2001120

[2] V. Daza et al. 2016. FRoDO: Fraud Resilient Device for Off-Line Micro-Payments. *IEEE Transactions on Dependable and Secure Computing* 13, 2 (2016).

[3] eBizCharge. 2021. Credit Card Processing Outages: Why They Happen What To Do. (2021). https://ebizcharge.com/blog/credit-card-processing-outages-why-they-happen-what-to-do

[4] Yining Hu et al. 2019. A Delay-Tolerant Payment Scheme Based on the Ethereum Blockchain. *IEEE Access* 7 (2019), 33159–33172. https://doi.org/10.1109/ACCESS.2019.2903271

[5] Alberto Di Iorio et al. 2024. *Tap, click and pay: how digital payments seize the day.* Technical Report CPMI Brief No 3. Bank for International Settlements (BIS).

[6] Adnan Noor Mian et al. 2015. Enhancing Communication Adaptability Between Payment Card Processing Networks. *IEEE Communications Magazine* 53, 3 (2015), 58–64.

[7] Committee on Payments and Market Infrastructures. 2016. *Fast payments - Enhancing the speed and availability of retail payments.* Technical Report. Bank for International Settlements (BIS).

[8] Nuno Preguiça et al. 2018. *Conflict-Free Replicated Data Types CRDTs.* Springer International Publishing, Cham, 1–10. https://doi.org/10.1007/978-3-319-63962-8_185-1