Apple Pay: How different is it from other Pay solutions, what role does tokenisation play, and to what degree can Card not Present payment benefit from Apple Pay in future

Marcel Fehr

Technical Report

RHUL–ISG–2018–3

3 April 2018

Information Security Group
Royal Holloway University of London
Egham, Surrey, TW20 0EX
United Kingdom

Abstract

We are living in a world where smartphones follow us at every turn. We are used to 'bringing our own device'. Why not introduce secure mobile payments as part of our daily purchasing experience? Indeed, the trend in consumer preference for mobile wallets over physical wallets is well documented, and several recent surveys [4] indicate a mild surge in the use of mobile wallets. This surge is mainly caused by the publicity around the launch of the three 'Pay' solutions, namely Apple Pay, Samsung Pay, and Android Pay. At the same time, questions emerge about using a smartphone as a payment device. People wonder whether it is safe enough or if the sensitive cardholder information is sufficiently protected. Moreover, privacy concerns surface concerning the extensive collection of metadata.

This paper focuses on the security aspects of Apple Pay as a mobile payment solution at a point of sales (PoS) and its application of EMV tokenization and compares it to Samsung Pay and Android Pay. The aim is to provide insight into the different payment ecosystems, allow the reader to understand the deviating approaches to wallet security, and provide an understanding of what can go wrong and what Apple Pay does well concerning security.

The three wallets implement the mobile payment solution differently, but all are compatible to the EMV contactless payment specification and tokenization and are supported by the card schemes. They allow using a smartphone as a contactless credit card (near field communication device) at a PoS and are compatible to MasterCard's *PayPass* and Visa's *payWave* specification.

The project demonstrates that following the EMV tokenization specification greatly improves the security of contactless payment at a PoS irrespective of the solution. This is because the use of tokenization combined with dynamic EMV payment cryptograms *renders captured payment details mostly useless for cross-channel fraud in card not present transactions*. Additionally, using the smartphone as a payment device and its ability to provide additional metadata, facilitates enhanced fraud analytics. This comes along with robust mechanisms for cardholder identification and device authentication, applying fingerprints and one-time passwords to name a few. The new 3D-Secure 2.0 specification [80] will play a significant role in providing metadata.

The threat and vulnerability analysis of the Apple Pay ecosystem has not revealed any weaknesses but outlines that the increased number of stakeholders (e.g. TSP, wallet provider) widened the possible attack surface. The card enrolment process is an attractive target for fraudsters and must be watched to prevent enrolment of stolen credit cards. Another important aspect is the security posture of the payment device. Both, Samsung Pay with its trusted execution environment (TEE) and Apple Pay with the secure element technology follow the Security by Design approach. Android provides security with a multi-layered approach. It uses Host Card Emulation (HCE), where tokenization is employed and the limited use keys are replenished in time through a cloud connection.

Besides PoS security improvements for contactless payments, the secure remote payment path will soon experience important changes as it is expected that the Card Present fraud figures will further drop in favour of a significant rise in CNP figures. This constellation has been analysed by the Boston Reserve Bank [61]. In the UK, fraud statistics [56] show a significant 20 % increase in CNP e-commerce frauds to the year before. This is where Apple Pay's remote secure payment implementation can play an important role in the future. The option to widen the scope from mobile in-app purchase using an EMV payment token and cryptograms to third party devices sounds promising. *This facilitates the EMV cryptographic strength to the CNP environment* and would help to minimize fraud. From my point of view, the introduction of EMV at PoS in the United States could have been a strategic step to prepare the United States' outdated payment infrastructure for the new mobile payment environment, including secure remote payment.

Overall, mobile payment solutions have a lot to offer regarding providing metadata for advanced fraud analytics and prevention, strong cardholder identification or the small effort it needs to manage the tokenized credit cards compared to the physical replacement tasks due to fraud, loss or theft. All three 'Pay' solutions will have their share in the mobile payment market.