A study on the security aspects and limitations of mobile payments using Host Card Emulation (HCE) with Near Field Communication (NFC)

Shana Micallef

Technical Report

RHUL–ISG–2018–6

5 April 2018

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

Executive Summary

The payments industry has evolved from magnetic stripe cards to smart cards and eventually to contactless cards payments. Now the industry is making another step in its evolution by replacing the card with a mobile phone. Initially a solution based on a secure element in the mobile phone was proposed but Issuers did not like the reliance on MNOs and eventually HCE was proposed as a solution. In HCE, an App, termed a wallet is responsible for communication with a POS during a transaction and for storing the payment credentials. To limit risk in HCE, payment credentials are exchanged for tokens that have limited use, a process known as tokenization.

In recent years, a number of wallet applications have been introduced by different stakeholders, including Android Pay deployed by Google and Microsoft Wallet deployed by Microsoft. However, Issuers can also develop their own wallet app. Other than for some minor specifics, such as exchanging credentials with tokens, HCE uses the same infrastructure used by contactless cards. A transaction executed by a contactless card is nearly identical to a transaction done through HCE. Most card schemes support payments with HCE and also provide services such as tokenization.

HCE is attractive to consumers because it allows for quick and convenient way to make a payment. It is faster as cardholder verification can be done on the mobile device using biometrics instead of PINs. It is also more user interactive and HCE wallet can provide other services that a physical card cannot, e.g. providing a history of payments. The benefits of HCE is not only limited to cardholders but also to merchants and Issuers. Issuers can deploy loyalty programs through HCE without possible additional marketing costs.

While convenience is a necessity in today's world, HCE comes with its own set of risks. Given the use of mobile devices, HCE could be exposed to a number of threats and vulnerabilities such as malicious attacks from malware running on the mobile device. Thus the industry needs to be more pro-active to ensure that the same level of security provided by a Secure Element is achieved.

In this regard, the aim of this project was to evaluate current implementations from a security perspective. To achieve this, a finite state machine model of an HCE wallet application, based on the requirements provided by VISA and in line with EMV's specifications was developed. The model was then studied for security risks with particular emphasis on customer verification and authentication methods, tokenization and the impact in operating cryptographic functions and storing cryptographic keys, required during an HCE payment process. Other generic issues in the use of mobile phones for payments when employed in HCE payments were also outlined.

As a result of the risks identified, the main findings of this project can be summarized into the following points:

- A safe storage for limited use keys and other sensitive data is required on the mobile device. Shifting the data to the cloud does not necessarily eliminate the risk of theft of such keys.
- The generation of tokens (i.e. LUKs) should occur on the mobile device rather than on the cloud. Considering all the risks involved between doing this process in the cloud and on the mobile device, the latter is a safer approach.
- There is a strong need for a method/technique that can be used to uniquely identify a mobile device. The technique should be difficult to tamper with.
- A supply and demand synchronization mechanism between token generation and token usage is required. While tokens are of limited use, a better way of managing them is required.