Digital Payments Security Discussion Secure Element (SE) vs Host Card Emulation (HCE)

15 October 2014

Frazier D. Evans
Evans_Frazier@bah.com

Booz | Allen | Hamilton

There are four key areas that need to be investigated when talking about Mobile Digital Payments

- Complexity
  - —With the use of Host Card Emulation, the complexity moves from the device to the issuer which will then bear the burden of all security measures in it back-end, application and processes
- Cost
  - —There are impacts on both solutions, the cost for implement HCE is currently unknown, while hardware Secure Elements needs significant investment by the multi-player infrastructure with costs distributed between the players
- Usability
  - —Requires the provisioning of temporary tokens on handset to authorize the transactions and performing regular security updates that require the user to re-authenticate
- Auditability
  - —Requires formal processes for the testing, certification and security evaluation of the hardware SE, which exist today. Similar processes for the HCE do not exist as there is no “Standard” way of implementation and the actual risk has to be evaluated individually.

Security is part of the assessment of the Risk associated with a payment system

In mobile payments there are 3 parts to security

- Physical Security

  Is to safeguard (protect) the physical or hardware elements by means of tamper-proof hardware that elements where sensitive data (Card Holder information) is stored and crucial operations are executed

- Logical Security

  What software safeguards are placed in the system. Software needs access to the hardware elements to operate but logical security does not use the HE provide the security.

- Procedural Security

  Provides security based on safeguarding sensitive data through organizational procedures. This type of security has to be evaluated on a case by case basis.

What are the security objectives we are trying to meet

The goal of security is to protect the device owner’s information from threads in terms of confidentiality, integrity and availability.

- Assets

  This includes the Primary Account Number (PAN), use keys and tokens, also included in this is the Device PAN that is a unique PAN for the device. These assets can be captured by attackers such as fraudulent users, merchants and attackers.

- Threats

  A system is open to attack at different locations or points of vulnerability. Vulnerabilities are attacked when the assets are of value to the attacker.

- Security Measures

  Are applied to mitigate the rick of a threat to a valuable asses.   They may not be used, or reduces, to accelerate deployments or reduce costs

Security in mobile payments

Issuing banks work with sensitive payment data on a daily basis and these risks they understand. When introducing mobile payments additional risks are introduced and they are in forms that the banks are not used to dealing with.

Issuer have the challenge of authenticating the user and their device, as well as securing storing an account number (PAN or pseudo PAN), use keys and cryptograms on the device. The risk should remain manageable for the issuers when implementing a secure mobile payments solution.

Current solutions for storing the secure data are:

- Secure Element either UICC or a device specific Secure Element(SE)
- Trusted Execution Environment (TEE) – Applications run in a separate space that restricts access to the secure data and requires a TSM to deploy the applications that run on the device
- Host Card Emulation – Sensitive data is managed on network server in the cloud. The device must make a secure connection to obtain the data

Potential vulnerabilities that need to be looked at

Note these are only examples and is not extensive

Cloud-based system

- Interception of sensitive data by spoofing the identity of a user
- The biggest challenges are secure access and authentication of the user to the cloud

Mobile payment application

- Reverse engineering of the application to get to the data
- Compromise by tampering with the data

Mobile Handset

- The OS may have vulnerabilities
- Use of a screen logger
- The use of Offline pin

Secure element

- The critical point is the access to the SE and could be based on certificate access improving the security

Point of sale – NFC Interface

- Potential for relay attacks for low-value payments. Tampering with the data could also be done by an attaker collecting use keys. The impact of such attacks can be reduces by implementing security mechanisms such as tokenization or Point to Point Encryption P2PE

A comparison of risks between solutions

Security Aspect	Impact	
	Hardware Based Solution	Software Based Solutions
Security	Provides a well understood level of security	Levels of security can be achieved, the concern is the what are the risks that are currently unknown
Usability	The challenge is the provisioning of the user	Will be based on the implementation and could add costs for the issuer
Costs	Involvement of many parties like TSMs and MNOs to provision the payment product will raise costs	Tokenization and cryptography measures are required. The back-end system of an issuing bank should be adapted which is a cost factor
Auditability	Formal processes in place today and accepted by the brands	Needs to be developed and accepted by the card brands
Complexity	Complexity lies in the multi-party ecosystem	Complexity lies within the issuing bank or processor (wallet)

Apple Pay and what I have learned so far

Available on the iPhone 6 & 6+, iWatch (it is assumed to be on the new iPads be announced October 16)

- Uses EMV NFC contactless specification version 2.4 updated 4/2014
- Issuers have implemented EMV Payment Tokenization version 1.0 issued 3/2014
- iWatch requires an iPhone 5s/ 6 / 6+ and potentially the latest iPads to perform the biometrics operations (think enabling the NFC radio for transactions on the iWatch)
- Each device will have a unique Device specific Personal Account Number (DPAN) (***assumption***)
- Issuers are assuming all liability for any fraudulent purchases that might occur. Customers and merchants will face zero 0 liability for fraudulent transactions. This applies to both Face-to-Face and “in-app” purchases.
- It is rumored that fraudulent transactions may be charged back to Apple but is only speculation at this time
- Appears to support up to 8 cards per device

Is there a perfect mobile payments solution?

It is to early to tell if one actually exists:

A solution that brings the following components together:

- ✓Biometrics authentication of the User (movement in that direction)
- ✓Hardware Secure Element in the device (could be part of the TEE)
- ✓Trusted Execution Environment (or secure enclave iOS)
- ✓Device specific PAN with unique cryptogram (keys)
- ✓NFC connectivity
- ✓Second Factor of authentication means that acquirers should evaluate if the interchange rate should be treated as Card Present vs Card Not Present
- ✓Support of both online and offline transaction
- ✓Taking advantage of EMV specifications that are already defined

The challenge is that there is not a common set of components that exists across all devices