10-2019

Host Card Emulation with Tokenisation: Security Risk Assessment

Luís Pereira da Fonte

Valentim Vieira de Oliveira

João Paulo Barros

Host Card Emulation with Tokenisation: Security Risk Assessment

Luís Pereira da Fonte, Instituto Politécnico de Beja (IPBeja), Portugal, luispereiradafonte@gmail.com

Valentim Vieira de Oliveira, SIBS, S.A., Portugal, valentim.oliveira@sibs.com

João Paulo Barros, Instituto Politécnico de Beja (IPBeja), Beja, and UNINOVA-CTS, Monte de Caparica, Portugal, joao.barros@ipbeja.pt

Abstract

Host Card Emulation (HCE) is an architecture that provides virtual representation of contactless cards, enabling transactional communication for mobile devices with Near-Field Communication *(NFC) support without the need of Secure Element (SE) hardware.*

Performing the card emulation mainly by software, usually in wallet-like applications which store payment tokens for enabling transactions, creates several risks that need to be properly evaluated in order to be able to materialise a risk-based implementation.

This paper describes the HCEt and proposes the identification and assessment of its risks through a survey conducted to specialists in the subject matter, analysing the model from the point of view of a wallet application on a mobile device that stores payment tokens to be able to perform contactless transactions.

Despite the increasing complexity and specialisation of software, hardware, and the respective technical cyberattacks we conclude that the human nature remains the easiest to exploit, with greater gains.

Keywords: *Host Card Emulation; Tokenisation; Risk Assessment; Near-Field Communication; Mobile Device.*

1. INTRODUCTION

Host Card Emulation along with Tokenisation has become a game changer for the mobile payments' ecosystem, combining the virtualisation of payment, loyalty and ticketing contactless cards on mobile devices, enabling them to be used through NFC. Along with the capabilities of this technology, many threats have emerged and the work here presented assesses the risks.

The usage of payment cards as a universal payment method, and in particular the Europay, Mastercard and VISA (EMV) card[1] (EMVCo, 2018), which has greatly enhanced the security of card payments, along with the development of the contactless card[2] technology has created a slew of new use cases based on portability and convenience for the users. Similarly, the growth in the

[1] Represents more than 50% of the cards in the world
[2] Taking advantage of the NFC technology

usage (Statista, 2018) and in the capabilities of smartphones (Wang, 2012) has also made it possible to virtualise essential physical objects in people's lives, such as banking cards, likewise the mobile banking services already accessible through smartphones for several years.

The emulation of cards in mobile devices has been used by financial entities and to this day various forms of emulation have been used (see next section). All of the emulation methods have advantages and disadvantages at the business and operability level, as well as associated risks. One of these implementations is Host Card Emulation based on Tokenisation (HCEt), in which the emulation of the banking card is made by software in a mobile application, storing cryptographic keys inside (tokens) derived from the original keys of the physical cards. Thus, the processes of key provisioning and management for the execution of payments (via NFC) is simpler, compared to implementations based on SE, which by design has a high level of security[3] (Taherdoost, 2011).

Emulating a secure microprocessor chip with cryptographic keys on an application that can authenticate financial transactions in a general-purpose device, places a challenge in keeping the risks at acceptable levels.

Performing and managing the emulation of chip cards by software, storing the keys (tokens) in the application as well as other critical data, necessarily creates dependency on the security levels of the application, the mobile device, the service support infrastructure, as well as the level of awareness in information security of the user. All these dependency factors, which are also points of failure, represent exposure to several threats that pose different risks to the security of the solution and its assets. Although some controls have been implemented, a clearer view of subsisting risks should be evaluated.

This paper, resulting from a master thesis (Fonte, 2019), seeks to perform a risk assessment regarding the HCEt model, in which card cryptographic keys derived from the physical Universal Integrated Circuit Card (UICC) keys are stored within the application for performing the emulation of contactless cards when in communication with payment terminals through NFC. Due to the lack of scientific documentation publicly available (to the best of our knowledge, and research) regarding risk assessment of this technology, the risk estimation was achieved through an online survey directed to Information Security professionals in specific and IT professionals in general. The study was based on the threats identified in a research (Mobey Forum, 2016) performed to Mobile Financial Applications, by Mobey Forum[4], which were found to be applicable to the HCEt architecture.

[3] SEs are tamper-proof microprocessor chips
[4] https://www.mobeyforum.org

2. HOST CARD EMULATION

Host Card Emulation (HCE) is an architecture that provides virtual representation (e.g. emulation) of contactless cards[5], enabling transactional communication for mobile devices with NFC support without the need of SE hardware used in NFC payments prior to HCE, being the card emulation performed mainly by software.

Through the adoption of this technology, merchant terminals that accept contactless cards may accept payments from HCE devices with no need to change the terminal software or hardware.

2.1. NFC and Technical Aspects

Based on RFID, NFC is a specification for contactless short-range communication (Garvey, 2012). NFC uses magnetic field induction to enable communication between electronic devices up to a distance of 20 cm (but usually between 0 and 4 cm), limited to a 424 kilobits per second data transfer rate with no native encryption, and has three operation modes (Roland, 2010) represented in Figure 1:

1. **Read/Writer:**

   An active NFC device can read and write data from, or to, a tag or a smartcard3;

2. **Peer-to-Peer (P2P):**

   Two battery powered devices establish a bidirectional half duplex channel between them in order to exchange data;

3. **Card Emulation:**

   The NFC interface works as a smartcard based on industry's standard communication interfaces (this enables smartcard emulation and has as its main advantage the compatibility with the existent smartcard industry).

[5] Payment, loyalty and ticketing cards

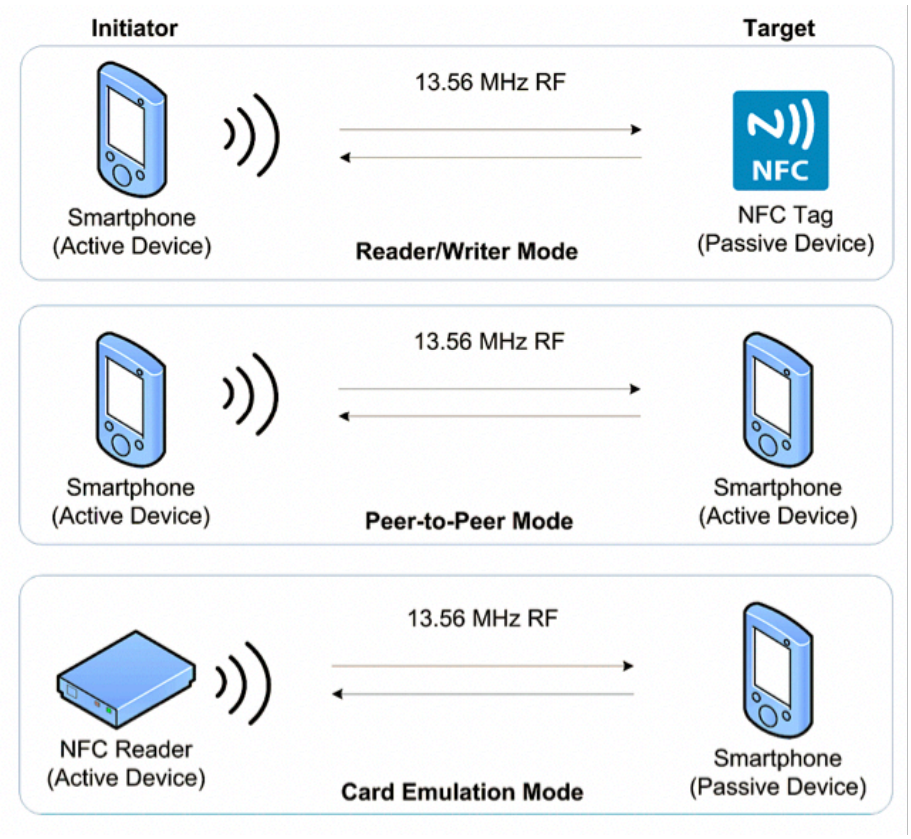

Figure 1 - NFC Operating Modes and Interactions (image from [29])

Secure Element

The first practical implementations of NFC on mobile devices consisted on having a physical SE assembled on the device, functioning exactly as a smart card when in communication with an NFC reader (ACHEMLAL, 2014). Similar to a Subscriber Identity Module (SIM) card, an SE is a secure and tamper-resistant "System on Chip" (SoC) (Jullien, 2004). The NFC reader sends and receives Application Data Unit (APDU) commands to, and from, the application inside of the SE.

There are three forms of SE implementations on handsets (UL, 2016):

1. **UICC[6]:** Making use of the traditional SIM card to embed the SE;
2. **Embedded SE:** SE based on a hardware chip assembled on the device, independent of the SIM card;
3. **SD-card:** Using an application inside the SD card as an SE.

Each of these strategies of implementing an SE on a handset has advantages and disadvantages, depending on the participating party:

- The UICC strategy was most favoured by the Mobile Network Operators (MNO) given that this would give them the opportunity to supply these critical personalisation services in the payments' arena. The advantages of this strategy were the speed of coverage of handsets

[6] Universal Integrated Circuit(s) Card

that could be obtained given that all handsets have a SIM slot, and substituting SIMs with these added features or personalising them over-the-air could be achieved at a low cost and reasonably quickly. Difficulties are related to the security of card's critical data, being provided by Issuers to MNOs;

- The Embedded SE was favoured by the handset manufacturers, however, the time necessary to migrate all users from older handsets to new handsets supporting the integrated SE was a burdensome challenge;
- The SD-card implementation was strongly limited because handsets had to support SD-card readers and because of its provisioning, done practically by only one Service Provider (SP)[7] for each SD-card, which does not allow a user to use emulated cards from multiple SP's in the same SD-card. Additionally, the NFC capable SD-cards[8] in some handsets were placed in locations where RF signals were suppressed by metallic enclosures.

Given the problems described for these three strategies, the concept of HCE emerged.

2.2. Host Card Emulation Models

In the HCE ecosystem, a card can be emulated in two different ways:

1. **Cloud-Based HCE:** a remote machine (i.e. Cloud Server) in communication with the NFC-enabled mobile device;
2. **HCE with Tokenisation:** Directly on the NFC-enabled mobile device to be presented to the acceptance terminal.

Hence two models for implementing HCE were adopted and are described in the following two sections.

Cloud-Based HCE

With the card emulation being performed "in the cloud" and both payment credentials and flow logic residing in a remote server, this is considered a full cloud HCE architecture. In this case, the app communicates with the cloud system authenticating the user and providing user interface, and then the transactional processing is done through APDU commands sent and received through a secure connection and passed to and from the NFC controller of the acceptance device. For each transaction, the server has to access to card data (keys and other data) in order to be able to perform the transaction.

[7] Bank or financial entity
[8] For handset devices without NFC antenna

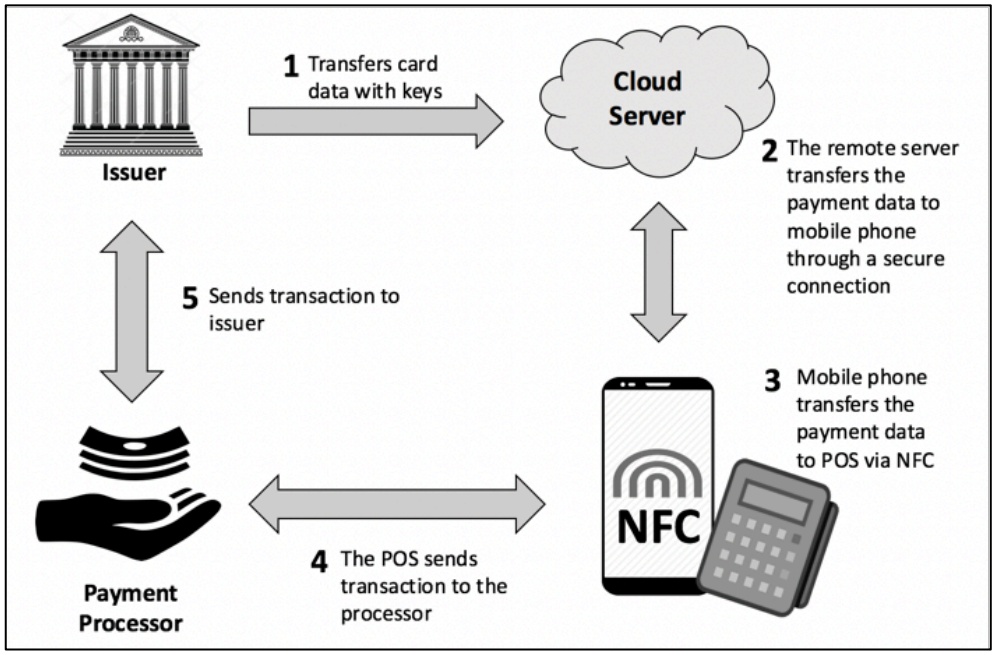

Figure 2 - Cloud-Based HCE - Transaction Flow (modified from the original figure in [38])

In comparison to the SE architecture, this architecture (Figure 2) is based on the emulation of the SE data and its behaviour on a remote server.

While not having any credentials stored locally on the device enhances security, there are challenges to consider, like the hardening of the remote server and the communication channel, as well as the need for ”going always online” combined with the possible latency of network communications, depending on the MNO service availability and other factors.

Host Card Emulation with Tokenisation

In this HCE model, instead of having the card emulation being performed by a remote server, the application performs the card emulation in its entirety. It stores the keys needed and mandatory to perform an EMV transaction. These keys are not the actual card keys stored in the UICC of the physical cards, but cryptographic keys and tokens derived from them.

Token

A token is a surrogate or alternative value that replaces the Permanent Account Number (PAN), or other sensitive card data, in the payment ecosystem. Its characteristics may vary such as its format, utilisation and applicability.

Tokenisation

The process of replacing the sensitive card data by a token for a specific or limited replacement (EMCo, 2014).

HCE with Tokenisation (represented in Figure 3) introduced innovative capabilities to NFC payments allowing the use of multiple emulated cards per device, and the capability of performing offline transactions due to the in-app generated EMV Application Cryptogram (EMV AC). Online communication through an MNO is only requested when the tokens need to be replaced (e.g. expiration) or when the implementation only performs or accepts online transactions.

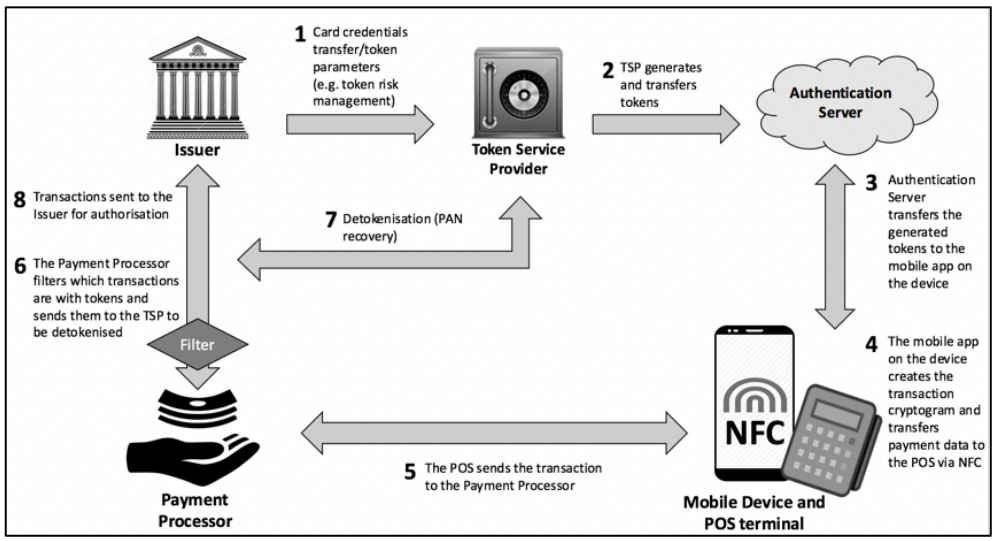

Figure 3 - HCE with Tokenisation - Transaction Flow (image modified from the original in [38])

The HCEt ecosystem is composed of the following components:

- **Mobile Application and POS terminal:**
  - Mobile app that communicates with an acceptance device (e.g. POS terminal) through APDU commands and has tokens stored for generating EMV ACs. Also communicates with the Token Service Provider for token provisioning and authenticates the user to the remote system of the mobile app provider;
  - The POS terminal is the acceptance device that establishes communication with the mobile device in order to perform the transactions generated in the mobile app;
- **Token Service Provider (TSP):**
  - Responsible for token management, namely, token issuance, provisioning and detokenisation[9];
- **Payment Processor:**
  - A payment system (e.g. VISA, MasterCard), a processor (e.g. SIBS), or another payment processing provider. The transaction data is sent to the POS via NFC and the Payment Processor verifies16 the token-based payment and sends it to the TSP to be detokenised before sending it on to the Issuer to authorise the transaction.

[9] The process of reverting tokenisation previously performed

Optionally, the Issuer may request the detokenisation instead of the Payment Processor;

- **Issuer:**
  - The Issuer's system that accepts or denies the transaction.

The next chapter will focus on the structure and methodology of the Risk Assessment presented in the next section.

3. Risk Assessment Methodology

A Risk Assessment identifies assets, applicable threats, vulnerabilities, existing controls and evidences which lead to the determination and comprehension of the inherent risks. The main factors that contribute for their classification, the likelihood and impact, are identified and ranked according to the risk evaluation criteria.

The methodology for the Risk Assessment performed to the HCEt architecture is aligned with the ISO/IEC 27005 (PCI SSC, 2015) and is restricted to the Risk Assessment process which steps are presented in Figure 4. No Risk Treatment was performed since the study is not applied to a specific implementation and/or design. It represents an assessment of the general risks that may be considered before the design and implementation of an HCEt solution, and during its life cycle.

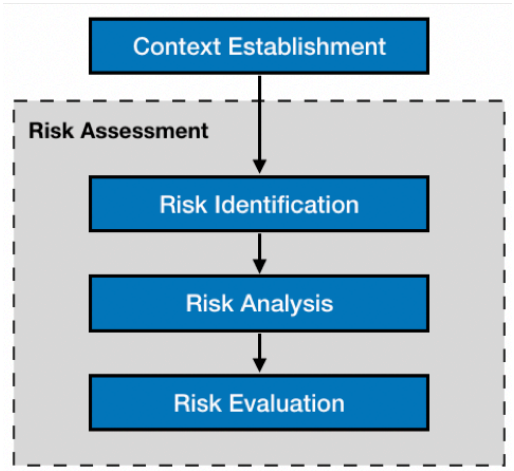

Figure 4 - ISO/IEC 27005 (2018) Risk Assessment Process (ISO / IEC, 2018)

The assessment describes the applicable threats and vulnerabilities for the identified assets and subsequently the risk for these threats in order to classify the related impact and likelihood of each one, considering the existing controls.

Based on the assigned values for Impact and Likelihood in the Risk Analysis process, the risk level for each threat is determined by calculating the Product of the two factors. It is assigned a value

between 1 and 5 for both classification variables, resulting in a matrix of values as can be seen in Table 1.

IMPACT	**Very High**	**5**	5	10	15	20	25
	High	**4**	4	8	12	16	20
	Medium	**3**	3	6	9	12	15
	Low	**2**	2	4	6	8	10
	Very Low	**1**	1	2	3	4	5
RISK DETERMINATION			**1**	**2**	**3**	**4**	**5**
			Very Low	**Low**	**Medium**	**High**	**Very High**
			LIKELIHOOD				

Table 1 - Matrix for Risk Determination

In order to obtain a consolidate risk evaluation, all risks are prioritised from the highest to the lowest and summarised.

This section described the methodology followed to perform the risk assessment on HCEt, which is presented on next section. As already mentioned, the risk assessment was performed through a survey conducted to IT and Information Security specialists.

4. Conducted Survey for Host Card Emulation with Tokenisation

After studying the available scientific documentation, it was clearly found that the lack of documentation to be able to analyse and carry out a duly supported risk analysis together with the fact that the subject matter was very specific and relatively recent, would be concrete obstacles to the execution of the study. In these cases, where documentation is scarce, the best way of assessing an opinion or reality is through an inquiry (ENISA, 2017), and as such, it was decided to classify the risk based on the opinion of IT specialists and Information Security specialists.

An online survey (Fonte, 2018) was conducted, from the 21st August 2018 to the 30th September 2018, to measure the risk levels of the threats to HCEt model, based on a recent risk analysis on mobile financial services (study conducted by Mobey Forum). This study identifies the various threats inherent to this type of mobile applications, also applicable to the HCEt model, given that it is a specific form of a mobile financial service.

4.1. Methodology, Preparation and Execution

The survey, which is based on the best practices described in the documentation consulted (Harvard University, 2013), was conducted on the Google Forms online platform from the 21st August 2018 to the 30th September 2018, and respondents were invited by email to respond. A document with

the presentation and description of the HCEt architecture was added to the survey, as well as the description of the inherent threats.

The survey, consisting of 34 questions, has the following four parts structure:

1. Personal and Professional (questions 1 to 6);
2. User Background, Experience and Trust in the Security of Smartphones, Financial Applications and HCE (questions 7 to 21);
3. Risk Classification for HCEt Threats (questions 22 to 32);
4. Suggestions for Improvement (questions 33 to 34).

4.2. Characterisation of the Reporting Sample

The survey sample corresponded to 32 respondents, which is above than expected given the special nature of the theme and the difficulty in reaching the target audience. Given the heterogeneity of positions among the respondents (although they were all or specialists in Information Security or IT professionals), it was necessary to group together (see Figure 5) the different positions/professions in order to categories the respondents by professional profile, creating groups of professional profiles.

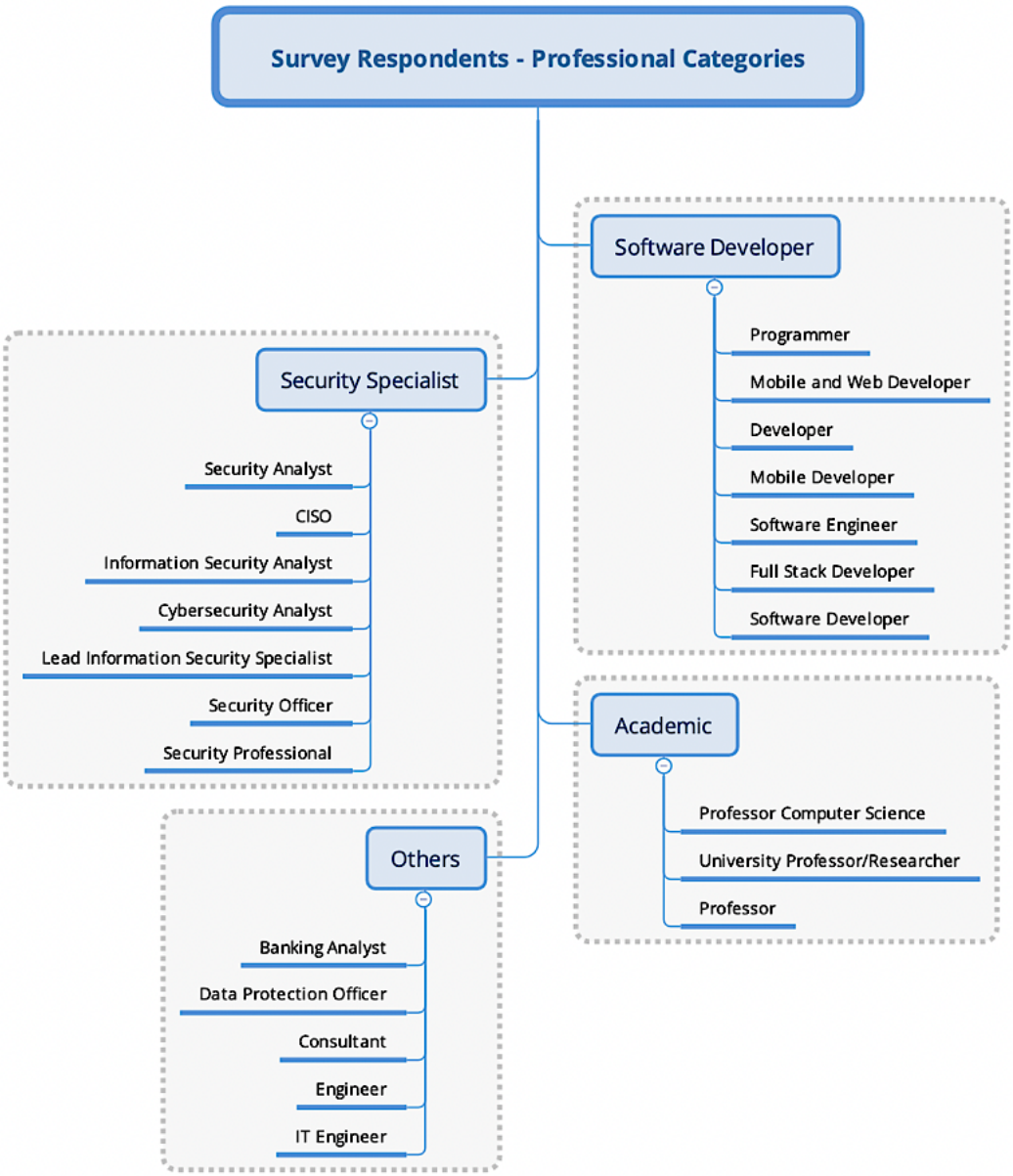

Figure 5 - Professional Categories of Survey Respondents

Through the analysis of the similarities between professions the following categories were identified:

- Software Developer;
- Security Specialist;
- Academic;
- Others (what does not fit into the rest).

4.3. Residence and Age Distribution of Respondents

Responses were obtained from, approximately, 84% residents in Portugal and 16% from other countries as can be seen in Figure 6.

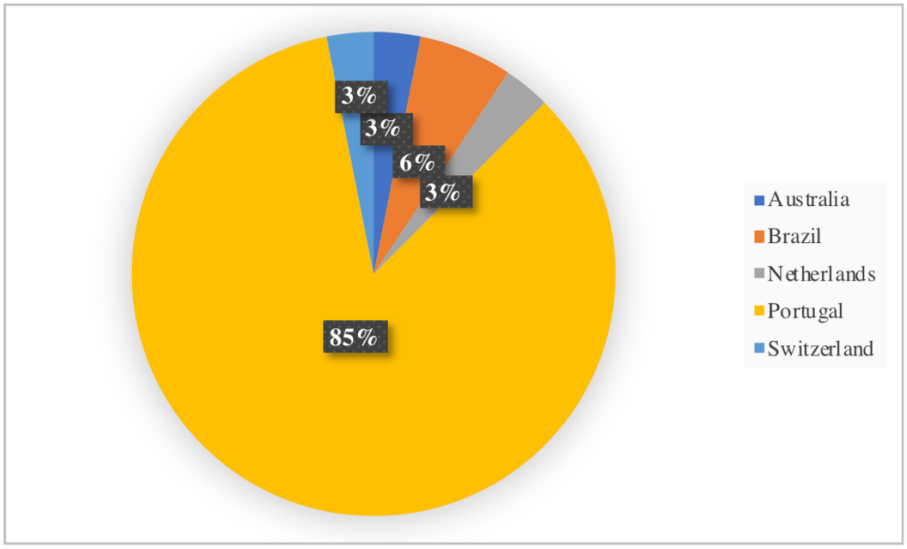

Figure 6 - Percentage of Respondents by Country Where Living

Regarding the age of the respondents, the distribution was quite uniform (Figure 7), with the prevalence of the ”21-30 years” and ”41-50 years” age groups, and there were no respondents Under 20 years and Over 60 years.

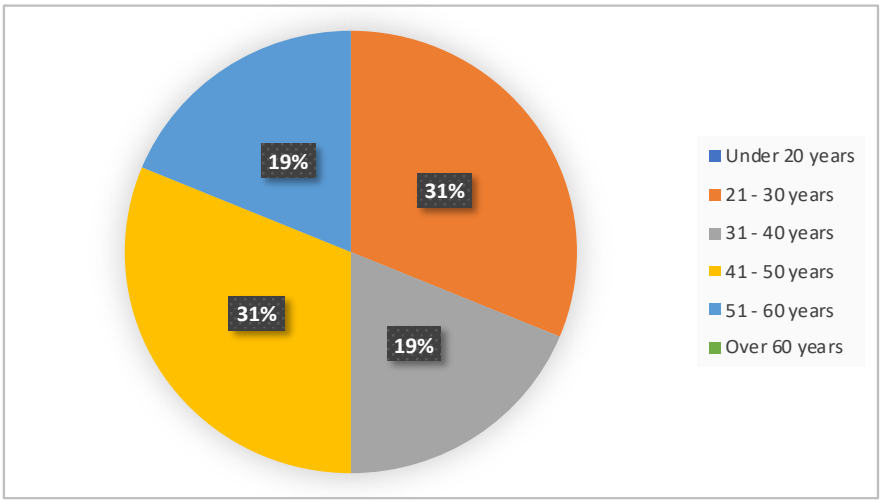

Figure 7 - Percentage of Respondents by Age Span

4.4. Experience by Professional Area

Respondents were asked about their professional experience, and the distribution (Years of Experience) can be consulted in Figure 8 and Figure 9.

Most respondents have ”10 years or more” of IT experience (Figure 8). Given that 66% of respondents have at least 7 years of experience and only 3% have less than 4 years of experience, this is an indicator that represents the good level of IT experience on the part of the respondents.

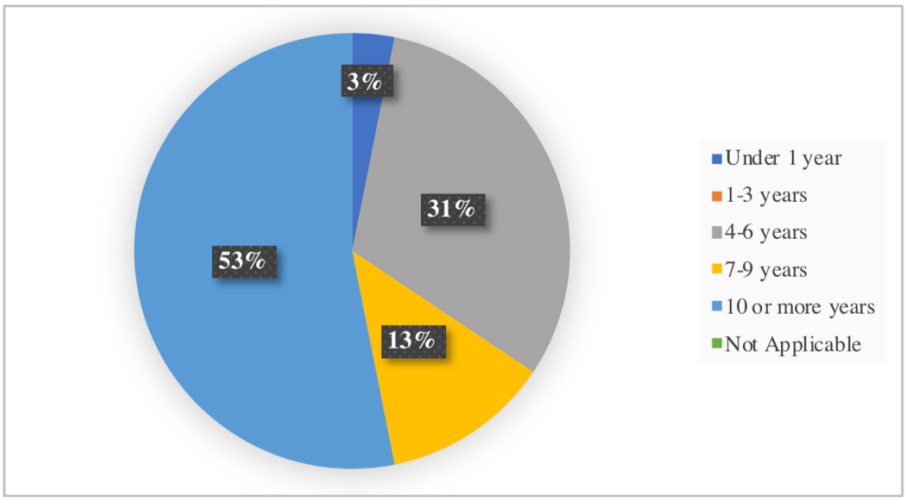

Figure 8 - Percentage of Respondents with Experience in IT by Number of Years

By analysing Figure 9, it can be concluded that only 19% of the entire sample has no experience in Information Security, which is an excellent indicator taking into account the purpose of the survey.

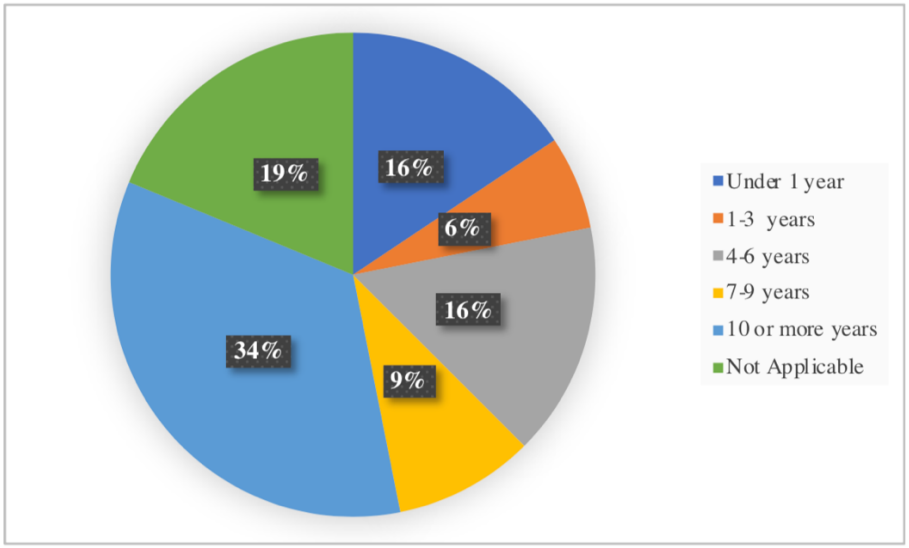

Figure 9 - Percentage of Respondents with Experience in Information Security by Number of Years

In addition, 34% of respondents have been in Information Security for “10 years or more”, representing 51.5% of all respondents with Information Security experience, which indicates a high level of experience in this area.

4.5. Data Treatment

From the group 2 of questions (see 4.1), was performed, in the original thesis from which this paper is based, data treatment on the opinion of the respondents about topics such as User Background, Experience and Trust in the Security of Smartphones, Financial Applications and HCE.

In summary, the main results from that treatment are:

- Regarding mobile operating systems, 93% of respondents have experience in Android and 43,75% in iOS;
- 75% of respondents have "7 or more years" of smartphone usage, and 47% have "10 or more years";
- From 1 to 5, the majority of the respondents classified the trust in smartphone security with 3;
- 33% of the respondents classified the security of mobile card emulation applications compared with security of contactless cards with 3 (from 1 to 5). Same percentage classified it with 4;
- 65% of the respondents are users of mobile card emulation applications, with the majority (93%) being users for less than 4 years.

In addition to these results, none of the respondents suggested other threats to HCEt, in the group 4 of questions.

5. HOST CARD EMULATION WITH TOKENISATION: SECURITY RISK ASSESSMENT

The possibility of emulating smart cards on a mobile device without the need of an SE turns the NFC payment ecosystem simpler while adds value to payment service providers by improving factors such as time-to-market and development costs. Additionally, the need to cooperate with other parties is no longer necessary given that the role of SE issuers and manufacturers is eliminated. On the other hand, payment service providers will have to accept or externalise the additional risk or put in place controls in order to mitigate or eliminate the risks.

Paradigm Shift

The paradigm has changed with HCE. Before, the security of the architecture (traditional chip card + PIN) was ensured at the hardware level with cryptographic keys being stored in tamper-proof chips (SE) embedded in physical cards, which provided a high level of security, assuring the critical data within the chip is trustworthy and the transactions authenticated by the chip are legitimate. With HCE, the critical data is stored on software and the key provisioning is performed by a Token Service

Provider and sent over-the-air, via mobile or Wi-Fi. It cannot be assumed that the data or the transaction are legitimate per se. In order to mitigate this increment in risk, further security controls should be implemented. The mobile ecosystem is increasingly complex, and plenty of security challenges where the mobile device is only the ”user facing component” of a much wider ecosystem consisting of app stores, services and content providers (Mobey Forum, 2016). For instance, entities offering these types of mobile payments need to develop applications for multiple operating systems and for many distinct device models and types. This fact requires specialised knowledge about the security threats (CSO, 2017) of each of them and that adequate risk mitigation measures be implemented. This constitutes a constant and continuous effort to maintain an acceptable risk level.

5.1. Context Establishment

This risk assessment is intended to determine the risks related to the HCEt architecture, as well as evaluating them by their severity levels.

5.2. Scope

The scope of this risk assessment is the architecture of HCEt, which comprises the following items of its groups of Assets and Processes/Phases:

Assets:

- Application;
- Communications;
- Customer;
- Data;
- Mobile Device;
- Service Infrastructure;
- Transaction.

Processes/Phases:

- App Installation;
- Provisioning (token provisioning to the mobile app);
- Mobile Transaction;
- Detokenisation;
- Issuer Authorisation.

5.3. Boundaries

The context of this risk assessment is limited to the concept of the architecture presented and the scope previously defined. It is not applied to any specific real and/or commercial implementation. For those cases, each model or implementation needs to be specifically evaluated.

5.4. Identification of Assets

Assets represent something that has value for an organisation, an entity, etc., and which therefore requires protection. Table 2 identifies the assets for HCEt model.

ASSET	DESCRIPTION
Credentials	Personal data that characterises the customer as to his individuality or that may be used as security credentials, which shall not be disclosed. Credentials can be for example, payment tokens, cell phone number, card numbers or PINs.
Data	Data related or supporting the business or personal identity that if disclosed could constitute an advantage to competitors or violate regulations (e.g., privacy requirements).
Funds	Monetary value eligible to be transacted.
Infrastructure	Continuous reliability, availability and trust of the infrastructure systems. Degradation of the correct functioning of the infrastructure systems may lead to costs.
Payment Tokens	In accordance with most known card schemes, Payment Tokens vary from the real PAN both by its numeric representation and its date expiration or purchase limit.
Reputation	Intangible and subjective global evaluation as being a trustful, reliable and credible organisation.
Services	Continuous availability and reliability of the service provided, and the inherent costs related to the failure of the service provision.

Table 2 - Identification of Assets

5.5. Identification of Threats

As mentioned, the threats identified in the study "Risk Management in Mobile Financial Services - The Risk Review" by Mobey Forum, are applied to Mobile Financial Services (MFS), in whose HCEt are included. Given this, the applied threats for HCEt environment (described bellow) to be analysed and evaluated within this risk assessment are the same as the identified in the Mobey Forum's study, except of "Man-in-the-Browser", which were not considered for this risk assessment. Plus, for the threat "Attacks on Secure Element", the mode applied to the HCEt environment is the Software SE mode.

The threats for HCEt are identified and grouped below:

- *Customer:*
  - [T1] Customer Impersonation;
- *Mobile Device:*
  - [T2] Unauthorised Physical Access to Mobile Device;
  - [T3] Attacks on Software Secure Element;
  - [T4] Attacks on Operating System;
- *Application:*
  - [T5] Application Modified in Runtime by Malware;
  - [T6] Hijack Genuine Application User Interface;
  - [T7] Static Code Analysis;
- *Communication:*
  - [T8] Man-in-the-Middle;
- *Service Infrastructure:*
  - [T9] Denial of Service (DoS);
  - [T10] Data Breach;
  - [T11] Compromised Service Provider Servers.

5.6. Identification of Existing Controls

Existing Controls (EC) (ISO / IEC, 2018) are controls that are already implemented in order to mitigate risks while avoiding unnecessary work or cost in extra mitigation measures.

The existing controls that are common for HCEt assets and contribute to mitigate the likelihood and ease of exploiting a vulnerability, or the impact of an incident are the following:

- [EC1] Mobile OS Common Security Features;
- [EC2] Communication Security in Transport (SSL / TLS) Between Financial Entities;
- [EC3] Payment Tokens Limited Utilisation for Major Contactless Payment Schemes, by Design.

The following threats are not addressed by the ECs:

- **T4 - Attacks on Operating System:** By default, mobile devices don't have built-in anti-malware software to protect them from being compromised. On the application side, there

are ways of hardening applications to self-protect from compromised or rooted devices but they are costly and it is easier for the organisations to accept the risk and chargeback the customer victim of an attack, instead of investing on the protection of the application;

- **T9 - Denial of Service (DoS):** Delaying server responses to client requests based on their volume in certain periods of time or distributing the server bandwidth load by multiple servers are good practices that should be put in place for the type of infrastructure that HCEt is. However, it depends always on the specific implementation and it is not a mandatory control.

5.7. Identification of Vulnerabilities

Vulnerabilities are related to flaws or weaknesses in the design or implementation that can be exploited by threats (intentionally or unintentionally) to adversely cause harm to an asset or group of assets. The identified vulnerabilities for the HCEt architecture are:

- [V1] Software Vulnerabilities;
- [V2] Lack of Awareness and Security Information Training;
- [V3] Lack of Code Obfuscation and/or Encryption;
- [V4] Lack of Implementation of Defensive and Preventive Mechanisms;
- [V5] No Encryption Set for Sensitive Data Inside the Wallet App;
- [V6] Server Misconfiguration;
- [V7] Use of Communication Protocols Without Encryption;
- [V8] Lack of Control in Published Apps by App Stores.

5.8. Risk Analysis

As previously mentioned, the Risk Analysis for HCEt was performed through a survey conducted specifically to Information Security and Information Technology (IT) experts. These experts estimated the likelihood and impact for the identified threats based on their knowledge and experience with HCEt[10], assigning them with values from 1 to 5, from the most to the least likely and harmful, respectively.

The estimation for the risk of HCEt threats, obtained from the answers to the survey, is presented below, as well as the answer distribution for the likelihood and impact values assigned for each threat. Empty answers were not considered for the sample. The likelihood and impact estimation are represented by the mean value from all valid answers.

[10] And information about HCEt given with the survey

Risk Estimation Summary

Based on the results of the Risk Estimation presented below in Figure 10, it is possible to observe that for the great majority of the threats, the respondents attributed a higher impact when compared to the likelihood of occurrence.

It should be noted that only one of the eleven threats (representing 9%) had an estimated value lower than 3 (Medium) for impact.

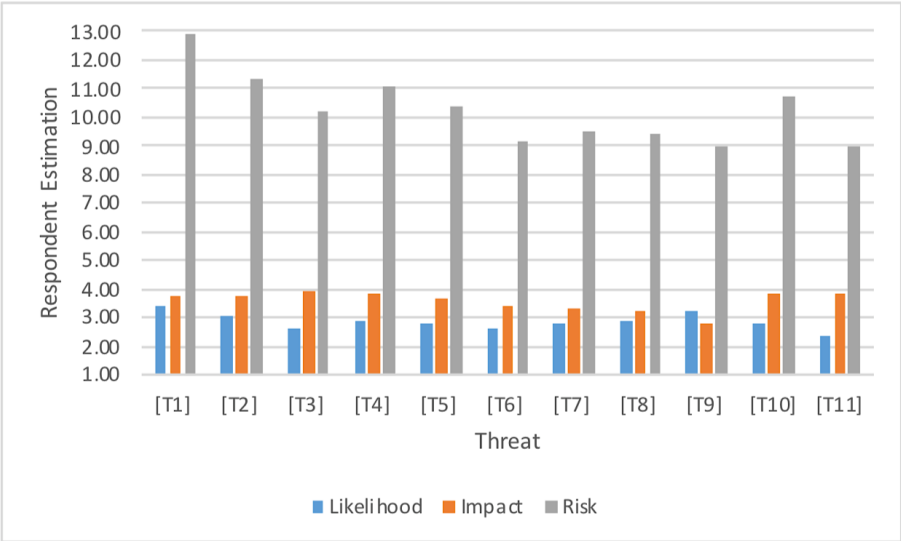

Figure 10 - Risk Estimation for HCEt Threats with Answer Distribution

The results of the classification are very linear, being all threats classified with Medium probability of being exploited (except for T11), and impact values for its exploitation varying from 3 (Medium) to 4 (High) for every threat according to the opinion of the respondents. No Low impact was identified for any threat, being the majority of the threats expected to be likely to be exploited.

From the analysis of results, and represented in the gray bar of Figure 10, it can be concluded that all threats were classified with "Medium" risk score.

5.9. Consolidated Risk Evaluation

Risk Evaluation seeks to understand and provide conclusions about the results obtained from the Risk Analysis. Figure 11 shows risks ordered by severity, from the highest to the lowest. All risks are at an average level of severity (between 8.96 and 12.89) with about 50% of risks presenting values slightly above "Medium" according to the matrix for the risk determination. The main conclusion to be drawn from the Risk Assessment is that respondents conclude that the main risks (T1 and T2) for HCEt model are based on the exploitation of the human flaws or, on the other hand, that the greatest threats lie in exploiting vulnerabilities on humans, in which the most determinant is "[V2] - Lack of Awareness and Security Information Training". Given the experience and

knowledge of the professional areas of the respondents, this risk assessment clearly portrays the perceived lack of user awareness, above any risk of technology-based attack.

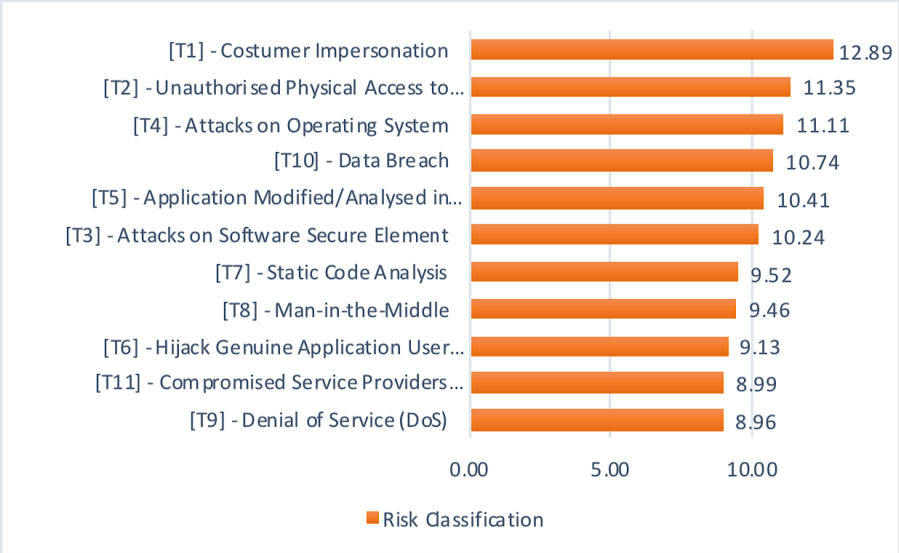

Figure 11 - Consolidated Risk Evaluation by Threat (from the highest to the lowest)

Taking into account the average value of the risk, 10.25, it is possible to name the risks that are above the average of the classification as Top risks. Denial of Service ([T9]) is considered the threat with the lowest risk, although it was considered the threat with the 2nd highest probability, as can be seen in Figure 11. It is also by far, the threat with the lowest impact attributed, which allows to conclude that the unavailability of the service is not as significant a risk as the rest.

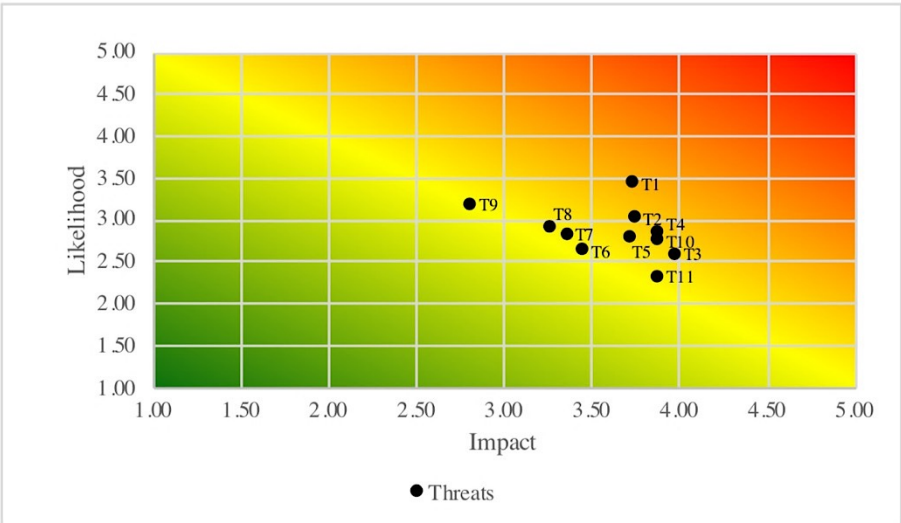

Figure 12 - Risk Evaluation Distribution

Analysing the Risk Evaluation Distribution in Figure 12, it is possible to obtain the perception of the risk severity positioning of each threat. Although the values obtained are close to each other, it

is easily verifiable that the most conspicuous risks are T1 and T9, which correspond to the threats of higher and lower risk level, respectively. T9 (DoS) is by far the threat with the lowest impact in case of exploitation and is also considered by the respondents as the second most likely to occur, only surpassed by Customer Impersonation (T1), which is the threat with the highest level of estimated risk. By transposing these facts into practical reality, respondents determined the higher risk of social engineering compared to more sophisticated attacks with respect to severity. In other words, exploiting the knowledge and awareness gap for information security is easier to exploit than for example executing a DoS attack or a Data Breach, which are typically attacks that require high technical level, unlike social engineering attacks, or even improper access to the device, as is the case of T2 that is the second threat with the highest level of risk.

Reducing the scale of the distribution of risk classification for HCEt (in Figure 13) allows a more detailed view of the results in order to perform a more detailed analysis in an attempt to find patterns that with the original scale are more difficult to visualise.

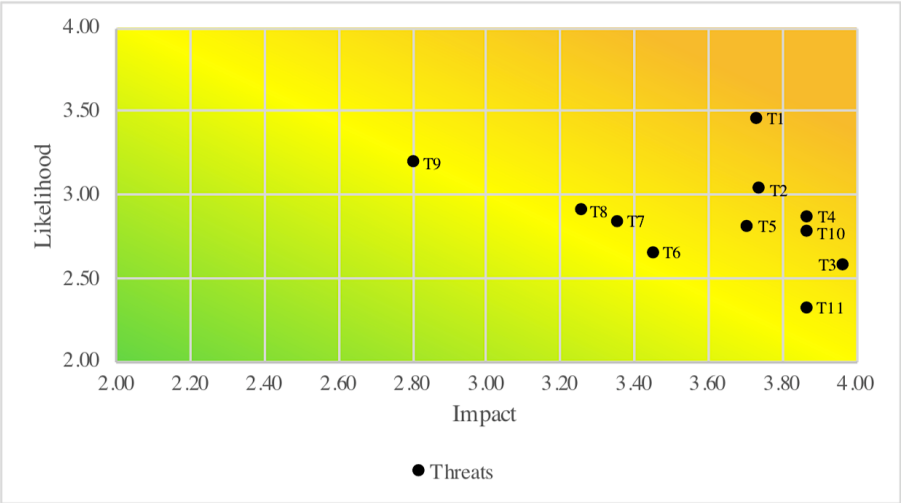

Figure 13 - Risk Evaluation Distribution with Reduced Scale

Table 3 presents the consolidated risk evaluation presenting all risks for the HCEt model ordered from the highest to the lowest. This should be the order of importance of the risks to be taken into account for this architecture.

ID	TITLE	LIKELIHOOD (L)	IMPACT (I)	RISK LEVEL (L x I)
[T1]	Customer Impersonation	3.45	3.73	12.89
[T2]	Unauthorised Physical Access to Mobile Device	3.03	3.74	11.35
[T4]	Attacks on Operating System	2.87	3.87	11.11

ID	TITLE	LIKELIHOOD (L)	IMPACT (I)	RISK LEVEL (L x I)
[T10]	Data Breach	2.77	2.87	10.74
[T5]	Application Modified/Analysed in Runtime by Malware	2.81	3.71	10.41
[T3]	Attacks on Software Secure Element	2.58	3.97	10.24
[T7]	Static Code Analysis	2.84	3.35	9.52
[T8]	Man-in-the-Middle	2.90	3.26	9.46
[T6]	Hijack Genuine Application User Interface	2.65	3.45	9.13
[T11]	Compromised Servers	2.32	3.87	8.99
[T9]	Denial of Service (DoS)	3.19	2.81	8.96

Table 3 - Consolidated Risk Evaluation

Next section presents the resume of the achievements and conclusions from the study, as well as the recommendations for future research.

6. CONCLUSIONS

The capability of migrating a universal payment method such as the EMV chip card to a mobile device with the ability to emulate and behave like one (EMV chip card contactless) at a POS terminal without the need to change its hardware or software and making it possible to have multiple cards in the same application, is undoubtedly a major breakthrough for the payment industry. Host Card Emulation has brought various new use cases based on mobility and convenience, but it has also created a space for new fraud schemes and new threats to the financial industry.

In this study, in which a risk assessment to HCEt has been performed with the collaboration of IT and Information Security specialists through a survey, where they answered based on their experience and knowledge, the results were clear about the overall severity of the risks identified, despite the small sample of results. In fact, the difficulty in having a large sample was the biggest limitation of the conducted work, due to the specificity of the subject. For future work, extending the survey for risk classification to a larger number of respondents and professional categories would increase the value of the study. Another important contribution would be the analysis and proposal of the best mitigation measures for the risks identified in this study.

None of the risks of HCEt were classified with Low severity, being all of them classified with Medium severity. This, in brief, means that none of the risks should be disregarded as to their importance. From all the risks identified and evaluated, the ones that standout as being the most severe are ”T1 - Customer Impersonation” and ”T2 – Unauthorised Physical Access to Mobile Device”. These are related to Social Engineering and leveraging on the lack of awareness and training in information security. Despite the increasing complexity and specialisation of technical

cyberattacks as well as the technical sophistication of both software and hardware, from this study it has also become clear that the human nature remains the easiest vulnerability to exploit, with greater gains. This is relevant and tells much about the human side of Information Security that should be, desirably, seen as an essential necessity in the regular training of financial services' customers, but more importantly, in school education, as part of the foundation of the technological society of today.

REFERENCES

ACHEMLAL, M. A. (2014). Host-based card emulation: Development, security, and ecosystem impact analysis. IEEE HPCC, CSS and ICESS.

CSO. (2017). Five new threats to your mobile security. Retrieved from https://www.csoonline.com/article/2157785/data-protection/five

EMCo. (2014). EMV Tokenisation Payment Specification.

EMVCo. (2018). Emvco reports over half of cards issued globally are emv-enabled. Retrieved from EMVCo, Techincal Report: https://www.emvco.com/wp-content/uploads/ 2018/04/Global-Circulation-Figures FINAL.pdf

ENISA. (2017). Risk management glossary. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory

Fonte, L. (2018). Master's dissertation survey. Retrieved from Google Forms: https://docs.google.com/forms/d/1FJZi7mI9Cv3NzTuq42pCEalHuhK0VcqW3pEXE0Fdil0

Fonte, L. (2019). Host Card Emulation with Tokenisation: Security Risk Assessment (Master's Dissertation). Beja: Instituto Politécnico de Beja (IPBeja).

Garvey, A. C. (2012). Near field communication. International Journal of Electrical and Computer Engineering (IJECE), vol. 2, no. 3.

Harvard University. (2013). Program on survey research.

ISO / IEC. (2018). International Standard ISO/IEC 27005 - Information technology — Security techniques — Information security risk management.

Jullien, W. (2004). System-on-chip for real-time applications. Kluwer International Series in Engineering and Computer Science, SECS 711.

Mobey Forum. (2016). Guide to risk management in mobile financial services - part 1. Mobey Forum.

PCI SSC. (2015). Additional Security Requirements and Assessment Procedures for Token Service Providers (EMV Payment Tokens).

Roland, J. C. (2010). Anwendungen und Techkik von Near Field Communication (NFC). Springer-Verlag Berlin Heidelberg.

Statista. (2018). Number of smartphone users worldwide from 2014 to 2020 (in billions). Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

Taherdoost, S. S. (2011). Smart card security; technology and adoption. IJS, vol.5, no.84.

UL. (2016). Hce security implications, analysing the security aspects of hce. Tech Report.

Wang, K. S. (2012). Smartphone security challenges. IEEE Computer Society.