Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 340 (2018) 137–150

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Risk Assessment Methodology For EMV Financial Transaction Systems

Mohammed Alqahtani[1] and Aad van Moorsel[2]

School of Computing
Newcastle University
Newcastle, UK

Abstract

Banks have introduced various financial transaction systems to manage money transfers between accounts, both locally and internationally. EMV (named after its inventors Europay, MasterCard, and Visa) is one of the most widely spread financial transaction systems. The aim of introducing EMV was to eliminate fraud. However, the EMV system has some vulnerabilities and it has suffered some attacks. The aim of this paper is to develop a risk assessment methodology for EMV transaction systems. The purpose of this methodology is to enhance the process of decision making by analysing, modelling and evaluating the risks that might occur during EMV payment transactions.

Keywords: Risk Assessment, Risk Management, Modelling, EMV, Financial Transaction Systems.

1 Introduction

Banks use several systems to manage, track and settle payments and money transfers between accounts. These systems are both online and offline, varying from networks of cash machines to the processing of credit cards, and bookkeeping systems [4]. Market economies benefit from financial transaction systems to ease money exchange between different parties in both domestic and international transactions [15].

With the acceleration of technology development, new financial transaction systems have been introduced. Nevertheless, financial transaction systems suffer from different vulnerabilities and flaws which increase the risk of using such systems. Financial transaction systems need to fulfil a range of requirements, such as security, acceptability, usability, and cost, and in these respects they each have a variety of strengths and weaknesses [16].

[1] Email: m.s.a.alqahtani2@newcastle.ac.uk
[2] Email: aad.vanmoorsel@newcastle.ac.uk

https://doi.org/10.1016/j.entcs.2018.09.010
1571-0661/© 2018 The Author(s). Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

EMV was introduced to reduce fraud transaction; however the reality was quite a bit more difficult than the hypothesis [3,8]. In fact, EMV also presents some new vulnerabilities and a number of attacks have been registered [3]. These attacks include card-not-present, counterfeit, lost and stolen cards, mail non-receipt, cheque fraud, ID theft, and online and phone banking attacks [3,8,21]. In the end, customers are the stakeholders with the most to lose in EMV transactions [2].

Fraud Type	**Amount(£million)**	**# of cases**	**%**
Remote Purchase (CNP)/ Of which e-commerce	432.3 / 308.8	1,437,832	70 %
Counterfeit	36.9	108,597	6 %
Lost & Stolen	96.3	231,164	16 %
Card ID Theft	40	31,756	6%
Card non-receipt	12.5	11,377	2%
Total	**618**	**1,820,726**	**100%**
UK	418	-	-
Fraud Abroad	200.1	-	-
Total	**618.1**	-	-

Table 1
Annual fraud losses and Case Volumes on UK-issued cards 2016.
All figures in millions. (source: Financial Fraud Action UK (FFA UK)).

Despite the fact that financial transaction systems have raised vulnerabilities and a number of attacks have been registered, a risk management decision still has to be made regarding which payment system to use, in order to mitigate or ignore some vulnerabilities and to maintain usability.

This paper is part of an ongoing research project designed to develop a risk management of financial transaction systems by setting up an appropriate methodology to model the risks, thereby providing managers with results to enhance their decisions. The project will apply the proposed methodology to three case studies, starting with the EMV system. This paper proposes a risk assessment methodology for EMV systems. The proposed methodology will study the EMV transaction process and identify the stakeholders. After that, a risk identification process will take place to identify the potential risks that could happen during payment transactions. Finally, we will model EMV transaction systems.

The rest of the paper is organised as follows. Section 2 presents a background review about risk assessment and risk management, EMV systems and related work. Section 3 shows the proposed methodology. Section 4 concludes the paper.

2 Background

This section will be divided into three sub-sections. The first presents general background information about risk assessment and risk management processes in general. The second section will provide a background review of EMV systems. The third section provides a background investigation of risk assessments for financial transaction systems and related work.

2.1 Risk assessment and Risk Management

Firstly, it is necessary here to clarify exactly what is meant by the term risk. Widely varying definitions of risk have emerged and these may have differing points of focus, such as how certain or uncertain outcomes are, the probability of something occurring, or other elements of risk, for example the subset of uncertainty [5]. According to ISO 31000, risk is the effect of uncertainty on objectives[24]. The ISO 31000 definition of risk focuses on the probability of an effect instead of the probability of an event [24]. A risk situation has been defined by Haimes as one where the potential outcomes or consequences of an action can be depicted in moderately well-known probability distributions[14]. However, this study examines financial transaction systems and the probability of attacks that could happen during payment transactions. Moreover, the study will examine who has liability for the lost money to answer the question who should pay? Thus, the associated cost of each attack needs to be addressed. In the present study, risk is defined as the possibility that something will go wrong during a payment transaction and the cost associated with this.

Risk management constitutes a set of processes, starting with identifying the risks and ending with a treatment action or plan. Risk assessment is part of the risk management process and it aims to identify, model and evaluate the risk. Haimes defines the risk assessment process as a set of logical, systemic, and well-defined activities that provide the decision makers with a sound of identification, measurement, quantification, and evaluation of the risk associated with certain natural phenomena or man-made activities [14]. According to Haimes [14], the risk assessment and management processes include the following:

Risk Assessment Process:

- Risk identification (what can go wrong?).
- Risk modelling, quantification (What is the likelihood that it would go wrong?).
- Risk evaluation (What are the consequences?).

Risk Management Process:

- Risk acceptance and avoidance.
- Risk management.

Moreover, according to Hessami[17], the risk assessment process includes the following: (a) Hazard Identification; (b) Causal Analysis; (c) Consequence Analysis; (d) Loss Analysis; (e) Options Analysis; (f) Impact Analysis; and (g) Demonstration

of Compliance.

According to ISO 31000:2009 [24], the risk assessment process is part of the risk management process and it consists of the following processes: (a) Risk identification; (b) Risk analysis; and (c) Risk evaluation.

This research will adopt the risk assessment process from [24] and [14] to assess and model the risks associated with financial transaction systems. The proposed methodology will combine the above mentioned risk assessment processes with some additional steps as will be mentioned in Section 3.

2.2 EMV

The EMV system supports magnetic strip authentication by a chip, which is harder to tamper with since it authenticates transactions using cryptography. The card holder is identified by a signature or by a PIN and the PIN is verified by the chip locally. This is branded as chip and PIN in some countries (e.g. the UK and Canada) since PIN verification is utilised in most point-of-sale transactions, and as chip and signature in other countries (e.g. Singapore) where signature verification is still used to authenticate customers [3,20].

EMV payment transactions consist of three processes (Figure 1), namely card authentication, cardholder verification and transaction authorisation. Firstly, card authentication is where a chip in the card validates the authenticity of the card to the terminal. Next, cardholder verification assures the terminal that the customers entered PIN or signature matches the one that is embedded on the card. Finally, transaction authorisation is where the issuing bank (card issuer) is involved in the approval of the transaction [21,20].

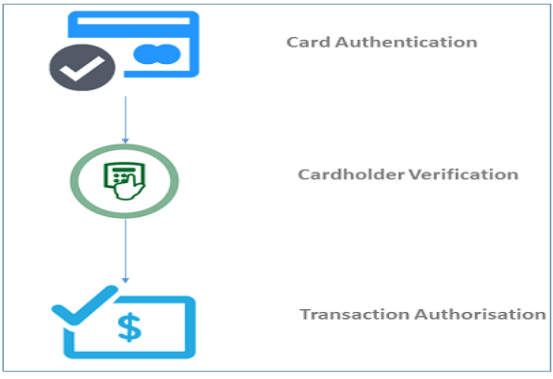

Figure 1: EMV payment transactions processes, namely card authentica-tion, cardholder verification and transaction authorisation.

According to Financial Fraud Action UK (FFA UK), during 2016 the total sum spent on both debit and credit cards totalled £904 billion, with 19.1 billion transactions. Moreover, overall card fraud losses from the money we spend on our cards reached 8.3p per £100 in 2016[1].

2.3 Risk Assessment Methodology for Financial Transaction Systems

This section will present the findings of the background investigation on risk assessment methodology for financial transaction systems. This investigation aims to identify existing research studies on risk assessment/modelling of EMV and other financial transaction systems.

In terms of a risk assessment methodology for EMV systems, the literature shows that no papers have proposed a risk assessment methodology for EMV systems. However, most research on the risk assessment and risk modelling of EMV systems has been carried out in one of three areas: testing EMV protocols [13], model-based testing to generate vulnerability test cases [22,11], or attacks [7].

In addition, a number of papers have proposed a risk assessment or modelling of other financial transaction systems. To address these papers we will adopt a high-level systematic mapping approach. It will investigate the processes and methodologies currently in use.

There are various scientific databases available, through which a search of the literature could be conducted, such as ACM Digital Library, IEEE Explore, ScienceDirect, and Scopus. However, at this point, the search focuses on Scopus databases. Moreover, terms have been selected as main keywords for the search for papers are shown in Table 2.

The search was conducted for documents with publication dates ranging from 2000 to 2017, and for all document types (articles, books, etc.). After these results were obtained, all of the papers were screened to select the related papers that had clear risk assessment/modelling processes or methodologies, excluding all others. The relevant papers either introduced a methodology or simply performed the risk assessment, modelling or analysis. The above-mentioned criteria (keywords, time range limit and screening step) were employed in order to narrow down the focus of our research.

After applying the above-mentioned search criteria, the result shows that there are papers performing risk assessment/modelling for single financial transaction systems. There are four papers on mobile payment systems [22,11,7,10], four papers on online payment and E-business [18,25,13,9], two papers on smart cards [19,23], and one paper on virtual currencies and crypto currencies [27].

Some papers assess/model the risks of financial transaction systems in general and some do so for one or more aspect of financial transaction systems. For instance, [10] proposed a risk assessment for mobile payment systems while [18] discussed the risks to third parties of online payment.

From a methodological point of view, different methodologies were utilised to assess, model, or analyse the risk of several financial transaction systems. Most papers start by analysing the business processes of the discussed financial transaction systems. For instance, [25] carries out a risk assessment approach for mobile payments starting with understanding and analysing mobile payment systems, identifying roles, and linking these roles to mobile payment flow. Moreover, some papers utilise business process diagrams to illustrate the business process. For instance, [9] used several UML diagrams to build a better understanding of the smart card pay-

Risk Assessment Payment system(s)	Risk Assessment Mobile payment / Mpayment
Risk Assessment Credit card	Risk Assessment Smart card
Risk Assessment Online banking	Risk Assessment Online payment
Risk Assessment Bitcoins	Risk Assessment EMV
Risk Assessment Blockchain	Risk Modelling Payment system(s)
Risk Modelling Mobile payment / Mpayment	Risk Modelling Credit card
Risk Modelling Smart card	Risk Modelling Online banking
Risk Modelling Online payment	Risk Modelling Bitcoins
Risk Modelling EMV	Risk Modelling Blockchain
Security Assessment Payment system(s)	Security Assessment Mobile payment / Mpayment
Security Assessment Credit card	Security Assessment Smart card
Security Assessment Online banking	Security Assessment Online payment
Security Assessment Bitcoins	Security Assessment EMV
Security Assessment Blockchain	Security Modelling Payment system(s)
Security Modelling Mobile payment / Mpayment	Security Modelling Credit card
Security Modelling Smart card	Security Modelling Online banking
Security Modelling Online payment	Security Modelling Bitcoins
Security Modelling EMV	Security Modelling Blockchain

Table 2
List of keywords used in the search for papers

ment system. Also, [10] proposed a framework for a mobile payment system that builds a transaction process model to show the business processes. In addition, some papers involved risk identification in their work [19,10,23,27,17].

To conclude, the literature clearly shows that to date no research has proposed or modelled a risk assessment methodology for EMV systems. In addition, most papers start by analysing the business processes of the discussed financial transaction systems and some involve conceptual models for business processes.

3 Methodology

This paper focuses on security and risks in EMV systems. Figure 2 shows the methodology steps undertaken in this paper to assist and model the risk. The steps undertaken in this paper adapt the risk assessment process from [24] and [14]. The proposed methodology in this paper will include risk identification and risk evaluation steps as in [24] and [14] and risk modelling steps from [14], combined with additional steps. Despite the fact that both references have a different definition of term risk, the process that both references still applicable and can be applied to any system.

The proposed risk assessment methodology will start with studying the EMV payment system. We will first identify the stakeholders and study the payment transaction process. After that, we will build a conceptual model to represent the payment transaction processes using Business Process Management Nation (BPMN) to link each process to a particular stakeholder. Then, all the potential risks that might occur during a payment transaction will be identified. The conceptual model and the identified risks will then be translated into an executable model using Performance Evaluation Process Algebra (PEPA). Finally, the risk will be evaluated and linked to each stakeholder by applying the risk expression.

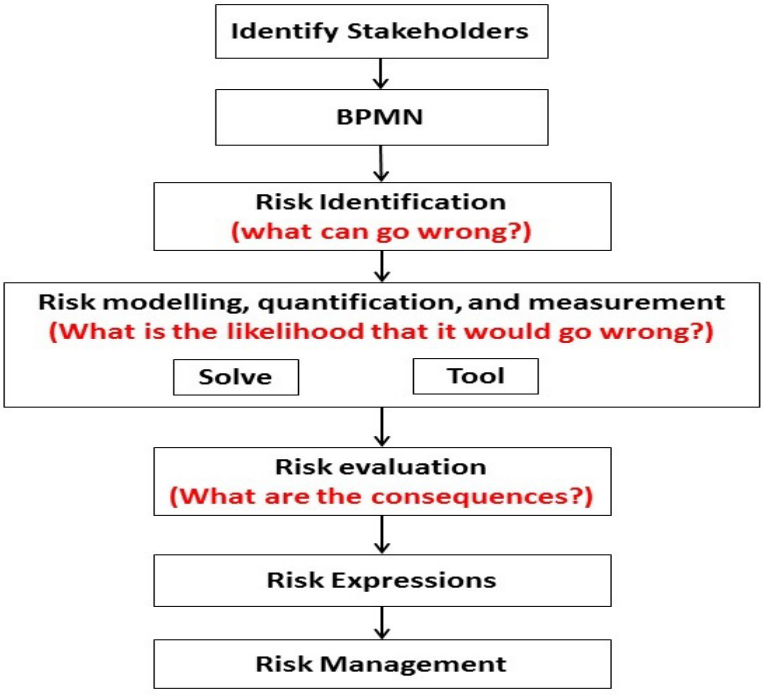

Figure 2: Risk assessment methodology for EMV transaction system

3.1 Identify Stakeholders

The first step of the proposed methodology is stakeholder identification. Stakeholders are a key element of the risk assessment and management process. Different

stakeholders are involved in different processes during payment transactions. Thus, this step will inform the business process of the payment system as well as the question who should pay? There are four main stakeholders involved in EMV payment systems: issuer banks (the cardholders bank), customers, merchants, and acquiring banks (the merchants bank) [12].

Additionally, in order to cover all of the parties involved in the transactions we add card payment networks as a stakeholder [6]. Moreover, there are two physical entities playing a significant role in EMV payment transactions; these are card and POS (point-of-sale) terminals.

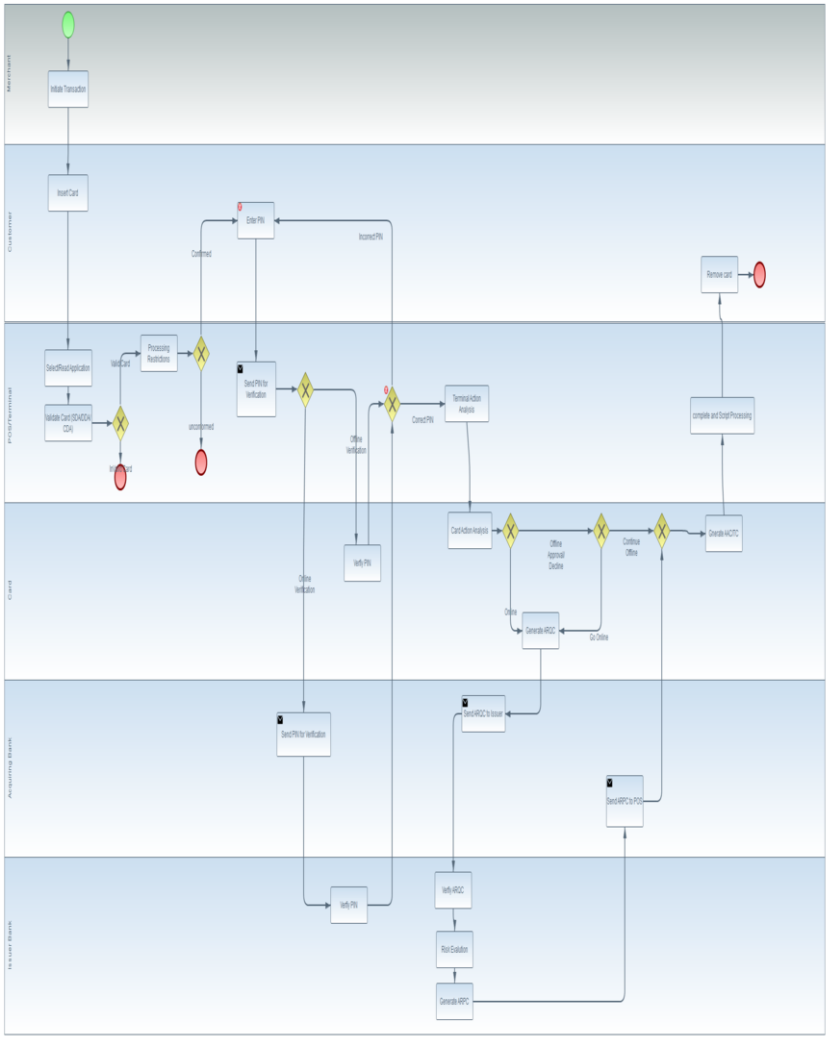

Figure 3: Business Process for EMV payment transaction system.

3.2 BPMN

BPMN (Business Process Model and Notation) is a standard notation for business process modelling. It is a very strong modelling language that can be used to model business processes and how these processes should be executed. BPMN has the advantage of using swim-lanes, which show who is performing each process.

Thus, BPMN will play a significant role in our proposed approach to gain a full understanding of financial transaction systems and link each process to particular stakeholders. Figure 3 shows the BPMN for EMV systems for contact-based transactions.

3.3 Risk Identification

According to [14], risk identification is a major step in the risk assessment process. Moreover, this step will examine the sources of failure and their causes and answer the question what can go wrong? . Table 3 presents the registered attacks, known vulnerabilities and elements that could go wrong. The attacks will be added in the future to the BPMN model and later in the executable model. Elements that could go wrong will be used in the risk expression.

What can go wrong?	**Vulnerabilities**	**Attacks**
Customers whose accounts were debited with other customers transactions	Authentication methods	Cardnotpresent
Wrong person gets money	Wrong person gets money	Counterfeit
Illegitimate payments	EMV terminals (Compatibility with magnetic strip cards)Card reader and the PIN pad are separate devices	Lost and stolen
Customers who were did not debited for their card transactions	EMV terminals (Compatibility with magnetic strip cards) PIN pads were replaced with tampered ones	Mail nonreceipt
Expired cards still work	User interface	Cheque fraud
Cross-border fraud	Stolen cards	ID theft
Money laundering	Purchase methods	Online/Phone banking

Table 3
list of the potential thing that might go wrong during EMV payment transactions, known vulnerabilities and registered attacks

3.4 Risk Modelling, Quantification, and Measurement

The maxim to manage risk, one must measure it points risk analysts in the right direction, while modelling provides the guideline for which road of risk assessment to take [14]. The main benefit of modelling is that it incorporates the processes from a variety of systems into one framework, which then constitutes a useful tool for stakeholders to carry out analyses, evaluate the outcomes and share the results [26]. It is widely believed that models will effectively enhance decision-making processes and managers will take advantage of such models [26]. Thus, the risk modelling of payment systems will help to enhance banks decision-making processes. This step will implement an executable model to investigate the likelihood of the various risks occurring. It will also establish probabilities, and model the sources of risks and their impacts.

- Tool

There are a variety of modelling tools and selecting a suitable tool will play a significant role in the risk assessment process. To begin with, Performance Evaluation Process Algebra (PEPA) will be used in this paper.

- Solve

At this stage the research will focus on EMV contact-based transactions. Continuous Time Markov Chain (CTMC) was initially chosen as the modelling approach. Firstly, EMV processes (card authentication, cardholder verification and transaction authorisation) will be modelled on PEPA and the flow of the transaction will be taken from the BPMN. The next step is to add attacks to the model. The attacks will be added to the process where they could happen, as presented in the BPMN. After that, the modelling results will be used in the following steps. At this point, we started modelling the EMV transaction processes and the code below shows the model.

```
Payment = (startTransaction, paymentRate).CardAuthentication;

// Card Authentication process

CardAuthentication= (request, rq). AuthenticationMethod;
AuthenticationMethod = (response, rs).SendPublicKeys;
SendPublicKeys = (confirm, rc).CardHolderVerification +
(cancel, rj) .TransactionCanceled;


// Cardholder Verification process
CardHolderVerification = (verify, rv). ChipPIN +
(verify, rv).ChipSignature;
ChipPIN = (response, rs).OnlineVerification +
```

```
(response, rs).OfflineVerification;

OnlineVerification = (request, rq). IssuerVerification;
IssuerVerification = (response, rs). Verification;

OfflineVerification = (request, rq). CardVerification;
CardVerification = (response, rs). Verification;

ChipSignature = (request, rq). SignatureVerification;
SignatureVerification = (response, rs). Verification;

Verification= (confirm, rc).TransactionAuthorisation +
(reject, rj).TransactionRejected;


// Transactio Authorisation process
TransactionAuthorisation= (authorise, ra).OnlineAuthorisation
+ (authorise, ra).OfflineAuthorisation;

OnlineAuthorisation = (request, rq). CardDecisions;
CardDecisions = (response, rs).SendARQC +
(decline, rj).TransactionDeclined;
SendARQC = (request, rq). SendARPC;
SendARPC = (approve, rap).TransactionApproved +
(decline, rj).TransactionDeclined;

OfflineAuthorisation = (request, rq). CardDecisions1;
CardDecisions1 = (response, rs).OnlineAuthorisation +
(approve, rap).TransactionApproved +
(decline, rj).TransactionDeclined;

TransactionRejected = (reject, rj).Payment;
TransactionCanceled = (cancel, rj).Payment;
TransactionDeclined = (decline, rj).Payment;
TransactionApproved = (approve, rap).Payment;

Payment < startTransaction > CardAuthentication
```

3.5 Risk Evaluation

Risk evaluation is the bridge between the risk assessment process and risk management. After we identify what can go wrong and the likelihood of these events occurring, we will need to determine the consequences. The aim of this step is to evaluate the modelling results and determine the cost of the attacks. This will help to apply the risk expressions based on a particular stakeholder to determine the

liability. However, this step is part of future work at this stage.

3.6 Risk Expressions

Risk expression identification will be based on particular stakeholders and for each stakeholder we will list events X cost for instance, what can go wrong? vs. cost. Different stakeholders will have different expressions but the model will be the same. Actually what can go wrong? is for the whole system and who pays? is a means risk expression for that particular stakeholder. The aim of this step is to link risk expression with the findings from the risk assessment processes so that we know what could go wrong?, who should pay?, and how much? However, this step is also part of future work at this stage.

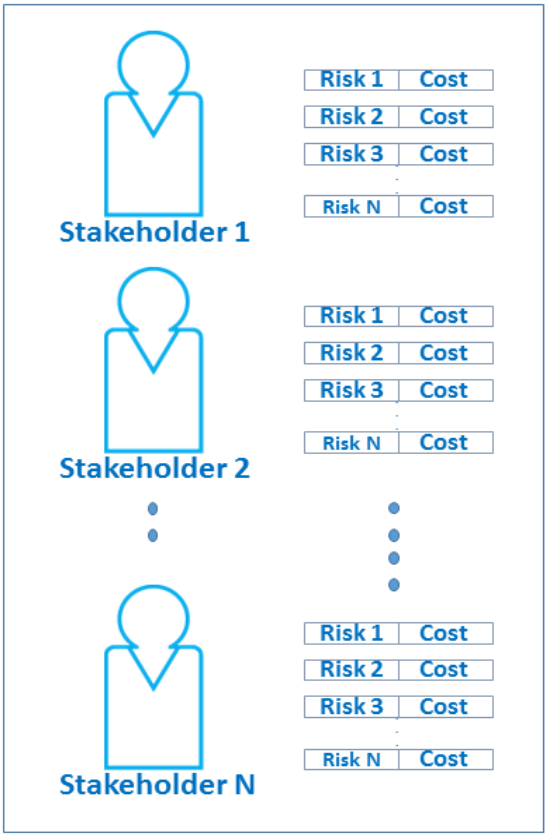

Figure 4: Risk expression will be links to each stakeholder, and for each stakeholder their will be list of risks and cost

4 Conclusion

This paper is part of ongoing research to implement a risk methodology that will be applied in different financial transaction systems. In this paper we proposed a risk assessment methodology for EMV payment systems. We adopted a high-level systematic review to examine the existing risk assessment methodology for financial transaction systems. We have started the risk assessment process and

hope to complete it in future work.

Many different steps of the proposed methodology have been left for the future. As a follow-up of this paper, we will add the attacks to the conceptual model BPMN. After that, we will use the BPMN model to implement an executable model in PEPA to model both the payment transaction processes and the potential attacks. Next, we will update both models to include contactless, online payment. Then, the risk evaluation step will use the model numbers and determine the consequences. Finally, we will apply risk expression, which is the last step in our proposed methodology.

References

[1] *Fraud the facts 2016* Available online at: https://www.financialfraudaction.org.uk/fraudfacts17/ [Accessed 08/06/2017].

[2] Anderson, R., M. Bond and S. J. Murdoch, *Chip and spin*, Computer Security Journal **22** (2006), pp. 1–6.

[3] Anderson, R. and S. J. Murdoch, *Emv: why payment systems fail*, Communications of the ACM **57** (2014), pp. 24–28.

[4] Anderson, R. J., "Security engineering: a guide to building dependable distributed systems," John Wiley & Sons, 2010.

[5] Bessis, J., "Risk management in banking," John Wiley & Sons, 2011.

[6] Blackwell, C., *Using fraud trees to analyze internet credit card fraud*, in: *IFIP International Conference on Digital Forensics*, Springer, 2014, pp. 17–29.

[7] Bond, M., M. O. Choudary, S. J. Murdoch, S. Skorobogatov and R. Anderson, *Be prepared: The emv preplay attack*, IEEE Security & Privacy **13** (2015), pp. 56–64.

[8] Bond, M., O. Choudary, S. J. Murdoch, S. Skorobogatov and R. Anderson, *Chip and skim: cloning emv cards with the pre-play attack*, in: *Security and Privacy (SP), 2014 IEEE Symposium on*, IEEE, 2014, pp. 49–64.

[9] Bushager, A. and M. Zwolinski, *Modelling smart card security protocols in systemc tlm*, in: *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, IEEE, 2010, pp. 637–643.

[10] Clarke, R., *A risk assessment framework for mobile payments*, BLED 2008 Proceedings (2008), p. 40.

[11] de Almeida Junior, R. A., *Model-based testing with a b model of the emv standard* (2012).

[12] Drimer, S., S. J. Murdoch et al., *Keep your enemies close: Distance bounding against smartcard relay attacks.*, , **312**, 2007.

[13] Emms, M., L. Freitas and A. van Moorsel, "Rigorous Design and Implementation of an Emulator for EMV Contactless Payments," Computing Science, Newcastle University, 2014.

[14] Haimes, Y. Y., "Risk modeling, assessment, and management," John Wiley & Sons, 2015.

[15] Hancock, D. and D. B. Humphrey, *Payment transactions, instruments, and systems: A survey*, Journal of Banking & Finance **21** (1997), pp. 1573–1624.

[16] Havinga, P. J., G. J. Smit and A. Helme, "Survey of electronic payment methods and systems," 1996.

[17] Hessami, A., *A systems framework for strategic approach to risk in e-business*, International Journal of Information Science and Management, Special (2010).

[18] Lao, G. and S. Jiang, *Risk analysis of third-party online payment based on pest model*, in: *Management and Service Science, 2009. MASS'09. International Conference on*, IEEE, 2009, pp. 1–5.

[19] Madlmayr, G., J. Langer, C. Kantner, J. Scharinger and I. Schaumuller-Bichl, *Risk analysis of over-the-air transactions in an nfc ecosystem*, in: *Near Field Communication, 2009. NFC'09. First International Workshop on*, IEEE, 2009, pp. 87–92.

[20] Murdoch, S. J. and R. Anderson, *Security protocols and evidence: Where many payment systems fail*, in: *International Conference on Financial Cryptography and Data Security*, Springer, 2014, pp. 21–32.

[21] Ogundele, O., P. Zavarsky, R. Ruhl and D. Lindskog, *The implementation of a full emv smartcard for a point-of-sale transaction and its impact on the pci dss*, in: *Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom)*, IEEE, 2012, pp. 797–806.

[22] Ouerdi, N., M. Azizi, J.-l. Lanet, A. Azizi and M. Ziane, *Emv card: Generation of test cases based on sysml models*, IERI Procedia **4** (2013), pp. 133–138.

[23] Peters, G. W., A. Chapelle and E. Panayi, *Opening discussion on banking sector risk exposures and vulnerabilities from virtual currencies: An operational risk perspective*, Journal of Banking Regulation **17** (2016), pp. 239–272.

[24] Purdy, G., *Iso 31000: 2009setting a new standard for risk management*, Risk analysis **30** (2010), pp. 881–886.

[25] Runtong, Z. et al., *Risk assessment management for mobile payment security*, , **2**, IEEE, 2008, pp. 1966–1970.

[26] Sawah, S. and A. Rizzoli, *Selecting among six modelling approaches for integrated environmental assessment and management* .

[27] Ummah, K., K. Mutijarsa and W. Adijarto, *System security requirement identification of electronic payment system for angkot using nist sp 800-160*, in: *Information Technology Systems and Innovation (ICITSI), 2016 International Conference on*, IEEE, 2016, pp. 1–6.