Universidade Católica Portuguesa

Faculdade de Engenharia

The power of credit card numbers and enhanced CVVs

Valentim Vieira de Oliveira

Dissertation submitted as a fulfilment for the degree of

Master of Information Systems Security

Jury

Professor Manuel José Martinho Barata Marques, PhD (President)

Professor Rui Jorge Correia Mendes Alves Pires, PhD

Professor Tito Lívio dos Santos Silva, PhD (Supervisor)

September 2013

Declaration

These studies were conducted under the supervision of Professor Tito Santos Silva. The work presented in this thesis is the result of original research carried out by myself, in collaboration with others, whilst enrolled in the *Faculdade de Engenharia da Universidade Católica Portuguesa* as a candidate for the degree of Master of Information Systems Security. This work has not been submitted for any other degree or award in any other university or educational establishment.

Valentim Oliveira
September 2013

Resumo

O roubo de informação respeitante a cartões de crédito é uma ameaça ao comércio electrónico. Os sistemas de pagamento introduziram o conceito do CVV2 como forma de mitigar o risco baseado no princípio de que estes valores não deveriam ser armazenados uma vez completa a transação. Sistemas, comunicações e bases de dados comprometidos resultam na captura ilícita desta credencial de autenticação frustrando assim o seu propósito inicial.

Este estudo propõe a criação de CVVs dinâmicos (*enhanced* CVVs) como forma de contrariar estes ataques. Desta forma, o compromisso de todos os elementos presentes numa ou mais transações não são suficientes para garantir o sucesso na autenticação de transações subsequentes.

É essencial que qualquer novo método de pagamento tome em conta os factores determinantes para que seja aceite por todas entidades participantes. Este estudo propõe dois métodos de CVVs dinâmicos: Matriz de CVVs e CVVs Longos. Os métodos propostos baseiam-se na infraestrutura atual de pagamentos baseados em cartões, com o objectivo de mitigar as maiores ameaças atuais, tendo o cuidado de manter o delicado equilíbrio dos factores determinantes para todos os participantes.

Ambos os métodos são analisados na vertente da segurança de forma a avaliar, e comparar, o nível de resistência perante situações de compromisso de transações. Questões relativas à implementação e à migração são igualmente analisadas de forma a determinar os impactos respeitantes à adoção dos métodos propostos

Palavras chave: pagamentos electrónicos, comércio electrónico, número de cartão de crédito, CVC2, CVV2, Problema do Colecionador de Cromos.

Abstract

Theft of credit card information is an increasing threat to e-commerce. Payment systems introduced CVV2 as a method to mitigate the threat based on the principle that these values would not be stored once the transaction has completed. Compromised systems, communications and databases result in the unlawful capture of this authentication credential and therefore thwart its initial purpose.

This study proposes the creation of dynamic CVVs (enhanced CVV2s) in order to counter these attacks. Thus a compromise of all the elements in one or more transactions will not be sufficient to guarantee successful authentication of subsequent payments.

It is essential for success, that any new payment scheme take into account the key factors determinant for the acceptance of each of the participating parties. Two implementation schemes of enhanced CVVs are proposed: Matrix CVVs and Long CVVs. The proposed methods build upon the current card based e-payment infrastructure with the objective of mitigating present day threats whilst maintaining the delicate equilibrium of key factors for all participating parties.

Both schemes are analysed at a security level so as to evaluate, and compare, the level of resistance function of the number of previously compromised transactions. Implementation and migration issues are equally analysed so as to determine the impacts of adoption of the proposed schemes.

Key words: e-payments, e-commerce, credit card number, CVC2, CVV2, Coupon Collectors Problem.

Acknowledgement

A realização desta tese só foi possível com o contributo e apoio de inúmeras pessoas. Gostaria de aproveitar esta oportunidade para agradecer a todos os que tornaram este estudo possível.

Agradeço ao Professor Tito Santos Silva por me dar liberdade nas linhas de pesquisa e por me desafiar a fazer melhor.

Não posso deixar de agradecer à SIBS (Sociedade Interbancária de Serviços) por proporcionar a oportunidade de aprender mais; por me dar um contexto de desafio constante e estimulante. Gostaria de agradecer ao Dr. Vítor Bento por ser um exemplo a seguir, ao Eng.º João Luís Batista por me ensinar a fazer sempre melhor e ao Dr. Francisco Roxo por ter despoletado esta viagem.

A todos os meus colegas que carinhosamente me apoiam e que juntos formam uma equipa fantástica. Aos colegas com quem tenho trabalhado diretamente, em especial à equipa atual que formam um grupo de elite; obrigado.

Ao António Teixeira, que é um exemplo como profissional mas acima de tudo como Homem, um agradecimento especial.

Acima de tudo, esta dissertação não teria sido possível sem o apoio da minha família. Dedico esta dissertação aos meus pais, Valentim e Purificação, a minha esposa Susana, que me apoiou incondicionalmente, e às minhas filhas Raquel e Carlota por me darem carinho e força ao longo destes anos.

O meu agradecimento a todos.

Table of contents

Table of tables

Table of figures

Abbreviations

Abbreviation	Description
3-D SET	Three Domain Secure Electronic Transaction protocol.
BIN	Bank Identification Number.
CAP	Chip Authentication Program.
CD	Check Digit. Protects the coherency of the PAN with the Luhn formula for modulus 10 check digit.
CID	Card Identification Number. American Express terminology for the three digit cryptogram placed on or besides the card signature panel that protects the integrity of the Card Number and the Expiry Date on card not present transactions.
CNP	Card Not Present transaction.
CVC	Card Verification Code. Also referred to as CVC1. Mastercard terminology for the three-digit cryptogram placed on the magnetic track 2 that protects the integrity of the magnetic track data namely that Card Number, the Expiry Date and the Service Code.
CVC2	Card Verification Value 2. Mastercard terminology for the three-digit cryptogram placed on or besides the card signature panel that protects the integrity of the Card Number and the Expiry Date on card not present transactions.
CVK2	Cryptographic key used in the calculation of the CVV2 cryptograms.
CVV	Card Verification Value. Also referred to as CVV1. Visa terminology for the three-digit cryptogram placed on the magnetic track 2 that protects the integrity of the magnetic track data namely that Card Number, the Expiry Date and the Service Code.
CVV2	Card Verification Code 2. Visa terminology for the three-digit cryptogram placed on or besides the card signature panel that protects the integrity of the Card Number and the Expiry Date on card not present transactions.

ECVV	Enhanced Card Verification Value. Abbreviation used in this study in order to refer to MCVVs or LCVVs indistinctly.
EMV	Chip card application on payment bank cards. EMV stands for Europay Mastercard and Visa who first developed the chip card based standards.
iCVV	Card Verification Value that is placed on the EMV chip application on payment card
IIN	Issuer Identification Number. Referred to as the BIN in the banking industry.
IPS	International Payment Systems.
LCVV	Long CVV. Refers to one of the Enhanced CVV2 techniques that constitute in a long multi-digit CVV2.
MCVV	Multiple CVV. Refers to one of the Enhanced CVV2 techniques that constitute matrix or group of CVV2s.
MOTO	Mail Order / Telephone Order payments
PAN	Primary Account Number. Also generally referred to as the Card Number.
PIN	Personal Identification Number.
PVV	PIN Verification Value. A four-digit cryptogram used to validate PINs.
TCVV	Transaction Card Verification Value. Enhanced CVV2 present in a transaction making use of the MCVV or LCVV scheme.
TCVV PC	Transaction CVV Positions Code. Indicates the position of the CVV in the Matrix CVV or the positions of the CVV digits in a Long CVV.
TPAN	Transaction PAN. Transformed PAN used in the Enhanced CVV scheme transaction.
SET	Secure Electronic Transaction.
SMS	Short Message Service.
SPA	Secure Payment Application protocol.

Chapter 1: Introduction to the study

1.1 Introduction to the Problem

The credit card and the PIN together are one of the most successful authentication mechanisms of all times. Tens of millions of transactions are authenticated daily through the combined use of cards and PINs [6] [11]. This dual factor authentication mechanism seems to have achieved a favourable balance between security and user convenience.

Throughout the years the card number and expiry date has been gradually adopted for authenticating MOTO (Mail order and Telephone Order) transactions. With the growth of the Internet, and the consequent need to perform commerce over this channel, the same authentication means was adopted for yet this CNP (Card Not Present) environment. Credit card numbers are the dominant payment method in overall e-commerce [9] [10] [27].

The anonymous nature of the Internet together with the possibility of accessing high volumes of transactions, among other factors, created a propitious context for some attack vectors to evolve. Various attempts have been made to implement a standard for secure electronic transactions over the Internet [26] [32]. SET (Secure Electronic Transaction) [2] was the first major attempt by Visa and Mastercard to establish a *de facto* standard for securing credit card transactions over the Internet. Various initiatives have followed such as 3-D SET and 3-D Secure (under the brand names "Verified by Visa" for Visa and SecureCode for Mastercard) but none have yet managed to prevail as the dominant e-payment authentication mechanism.

Meanwhile the payment systems have created an auxiliary authentication token, for CNP transactions, that consists on three digits printed on the signature panel. This Card Security Code is known as the CVV2 (Card Verification Value 2) by Visa, CVC2 (Card Verification Code 2) by Mastercard and CID (Card Identification Number) by American Express. The concept behind this code is that the cardholder, by supplying this number proves that he is, or has been, in physical possession of the card.

The CVV2 has been placed on cards since 1998. Since then the adoption by merchants has been slow and gradual. The CVV2 has been effective in deterring certain types of attacks such as card number generation and extrapolation or attacks resulting from the capture of card magnetic track data.

Recent attacks tend to capture large quantities of card transaction data [27] [28], sometimes together with the CVV2. The static nature of the CVV2 constitutes a vulnerability in these cases, given that with the compromised card number, expiration date and CVV2 a fraudster may perform subsequent transactions at ease.

1.2 Background of the Problem

1.2.1 Fraud Context

Fraud on the Internet has risen in the first years of this century in scale and in sophistication [8]. E-commerce and online banking systems have been the preferred targets for these attacks. The capture of financial services authentication credentials has been the main objective for these attacks [7]. A specialized electronic payment fraud industry has emerged covering all areas of the value chain, from the search of vulnerabilities, and malware development, through system compromises and botnet commercialization to the fraudulent use of compromised credentials and money laundering [28].

Two types of attacks have been taking place, compromising a vast number of credentials: malware [46] and data breaches [43].

Malware distributed from an ever growing fleet of compromised systems drawn into botnets [44], of unimaginable scale, have put at risk millions of users. The openness nature of the Internet and the non security aware computing techniques of the beginning have left open a vast scope of vulnerabilities that have been challenging to patch-up. The number of vulnerabilities that are disclosed yearly [47] denote a long struggle yet ahead. Botnets have made use of these weaknesses to propagate through the Internet, hijacking computers into their net and subsequently harvesting whatever data they can from the users' systems.

In recent years a number of incidents of data breaches have occurred [44] at payment processors and merchants compromising tens of millions of card detail records with authentication data, such as CVVs. The number of compromised cards has been of an unprecedented scale affecting at some times in a single incident a 100 million cards [28], corresponding to 2% of bank cards in circulation in the world.

1.2.2 Protecting Financial Services on the Internet

The simpler "bank to client" context of online banking systems makes the adoption of new authentication mechanisms a manageable task. Password matrixes, SMS or CAP are examples of the instruments that the banks have been introducing so as to authenticate their clients. The adoption of these new mechanisms has taken into account both user convenience and the security levels proportionate to the sensed threats.

Unfortunately e-commerce poses a more complex context than online banking systems. The adoption of a viable solution in this multi-sided platform environment depends on attaining critical mass over a reasonable space of time for the involved parties[30]. Thus all parties (issuers, payment systems, acquirers and namely cardholders and merchants) have to be assured enough value to embark in any proposed solution.

Various attempts have been made to implement a standard for electronic transactions over the Internet by the payment systems. SET, 3-D SET, SPA and 3-D Secure [26] are the major initiatives in this field. Some have failed whilst others struggle to achieve a widespread adoption in the market.

The lack of a generally accepted *de facto* standard for e-commerce security has given way for the credit card number and expiry date to sustain itself as one of the preferred methods for these transactions [9].

1.2.3 CVV2 Introduction

The credit card number and the expiry date were the elements that secured most of the transactions on early e-commerce sites. This method of payment was very convenient for the common shopper and the fact that most potential buyers carried credit cards with themselves guaranteed a vast base as a starting point.

Unfortunately the security level of this adopted method was not enough to resist the harsh environment of the Internet.

Attacks, such as credit card number and expiry date generation or extrapolation, are extremely simple to perform and have a success rate that cannot be ignored. Large-scale attacks, sometimes performed from jurisdictionally uncontrolled geographical regions, are relevant, if not protected.

To counter these relevant threats, payment systems introduced, as early as 1997 the CVV2 concept. The principle behind this three-digit number was that it would give some assurance that the person performing the payment had the card physically available at the moment of purchase.

1.2.4 Security Properties for CVV2

The CVV2 value is calculated through a CVV calculation algorithm that is based on several rounds of DES calculations making use of a double length (112 bit) cryptographic key. The end result are three decimal digits that are printed on or near the signature panel. In principle this value will only be printed on the card and can only be validated by the card issuer, or any delegated party, that has the cryptographic keys to validate the CVV and an HSM to perform the validate CVV function.

At the moment of purchase the merchant will prompt the customer for these three digits, along with the card number and expiry date. These values will be routed through to the issuer that will validate the correctness of the value. After the transaction has been authorized all traces of the CVV2 should be eliminated.

An attacker trying to perform a transaction by guessing a CVV2, for a known card number and expiry date, will have a one in a thousand chance of getting the right CVV2.

1.3 Statement of the Problem

Botnets spreading malware have compromised millions of computers worldwide. Customer education, antivirus developments and a whole range of other protection initiatives have not been able to deter this threat and as a consequence many attacks make use of data collected at the users' systems, including card numbers and CVV2s.

Data breaches have, during recent years, reaped hundreds of millions of records with card data [44], sometimes with CVV2 data. The payment systems have taken great efforts in establishing best practices through the Payment Card Industry - Data Security Standard [5] initiative. In this program all parties that process, transmit or store card data are only allowed to keep cardholder data if properly protected, and no sensitive authentication data, such as CVV2s, may be stored after authorization, even if encrypted. By doing so risks deriving from the compromise of databases are greatly reduced.

The lack of a robust and simultaneously convenient method for authenticating transactions on the Internet hinders the growth of e-commerce. The CVV2 is not effective to counter these major attacks.

1.4 Statement of Purpose

A new method for authenticating e-commerce transactions is required to enhance the security needed to mitigate present-day major threats. It is however crucial that the subtle balance of characteristics be maintained so as to have success.

User convenience must be maintained at an acceptable level, and user security perception must be preserved to ensure confidence in any new scheme.

Attaining critical mass on a cardholder perspective and on a merchant perspective has been behind many failures. Building upon the unprecedented existing infrastructure, minimizing impacts and guaranteeing a migration process is critical for the success of any new scheme.

1.5 Aims and Objectives of Study

This dissertation proposes and analyses two methods for securing e-commerce transactions that consists on having specific CVV2s for each transaction, thus a CVV2 of dynamic nature. In this way, the illicit capture of transaction data, including one of these new Enhanced CVVs, will not be sufficient to perform subsequent transactions. Both methods are compared so as to attain their resistance in case of a compromise of transaction data.

The proposed schemes maintain impacts on involved parties and infrastructure at a minimum and guarantee ease of migration.

1.6 Research Question

The main focus of this study is to determine the extent to which the Enhanced CVVs grant security in a case of compromise of card data.

The study will determine the probability that an attacker, that has obtained compromised data by intercepting a determined number of transactions, will have in successfully executing a fraudulent transaction.

1.7 Definition of Terms

Card Security Codes have been introduced by the payment systems to protect the integrity of certain authentication elements. The first Card Security Code introduced by the payment systems had the objective of protecting the track 2 data from being doctored. Visa named it CVV and Mastercard CVC, although both are calculated using exactly the same algorithm.

The CVV2 or CVC2 was introduced to secure the card number and the expiry date making use of the same algorithm with some variations on the input.

This study will refer to the CVV2, CVC2 and the CID as the CVV2.

1.8 Research Method

This study will announce two implementation variants for Enhanced CVV2s and will analyse their security robustness in face of a situation of compromised transactions. Impacts resulting from the effort necessary to prepare the existing card payment system infrastructure to support this new method as well as migration issues are scrutinised given the importance these factors have towards a global acceptance.

1.9 Description of Thesis Organisation

The following chapter, "Chapter 2: Review of Publications", will look into the publications pertaining to the streams of knowledge developed in this study in order to perceive the essence of current knowledge.

In "Chapter 3: Current card based payment schemes description" the current CVV2 based scheme and the 3-D Secure scheme are described. The authentication elements, the involved parties and their respective roles are described. An analysis of the flux of information during the setup and during a transaction will complement the understanding of these systems.

“Chapter 4: Key success factors for new e-payment scheme proposals” describe the factors that are determinant for the acceptance by each party and comments the changes that the proposed schemes entail.

In “Chapter 5: Enhanced CVV2 scheme proposals” the proposed solutions are described on a functional point of view.

A security analysis is conducted in "Chapter 6: Enhanced CVV2 scheme security analysis" calculating the robustness level of either of the Enhanced CVV2 implementation variants in a situation where transaction data is compromised.

Implementation issues, identifying the modifications that have to be implemented at each phase by each party and identifying the involved effort is analysed in "Chapter 7: Enhanced CVV2 scheme implementation analysis".

Finally “Chapter 8: Summary and conclusions” Summarizes the study suggests future research streams and draws final conclusions.

Chapter 2: Review of Publications

2.1 Introduction

Research into the themes covered by this study led to the compilation and analysis of an extended number of publications. The main streams of research were in the following fields:

- Electronic Payments - *key words: Electronic Payments, Card Payments, CNP, Card Not Present Payments, E-commerce Payments Security, Electronic Commerce Payments, Internet Payments, Web Payments, Payment Protocols, micropayments;*
- Bank cards - *key words: Bank card, Credit Card, Debit Card, ISO 7812;*
- CVV2 - *key words: CVV, CVV2, Card Verification Value, CVC, CVC2, Card Verification Code, CSC, CSC4, Card Secret Code;*
- Payment Fraud - *key words: Payment Fraud, Card Payment Fraud, Malware, Phishing, Skimming, Counterfeit, LSNR, Lost Stolen and not received, Key logger, Trojan, Data Breach;*
- Authentication Criteria- *key words: Authentication, Authentication: Requirements, Criteria, Effectiveness, Quality, Security;*
- User convenience - *key words: User convenience, Human Factors, Usability, Acceptability.*
- Password - *key words: Password, Password Card, Password Matrix, Password Table, Code Card, TAN, Transaction Account Number, OTP, one-time password;*
- Coupon Collectors Problem - *key words: Coupon Collectors Problem.*
- Payment systems success factors - *key words: Payment systems success factors, Critical mass, Start-ups.*

2.2 Research streams

2.2.1 Electronic Payments

A vast number of Internet payment protocol publications [14] [17] have been issued throughout the last two decades and many have been implemented [32]. Most publications refer to the credit card transactions as being the most used means to pay on the Internet [9] [10] [27], at their time, and then go on to announce or analyse yet one more protocol (ex. CAFE, CyberCash, DigiCash, iKP, MicroMint, MilliCent, MiniPay, NetBill, NetCard, NetCash, NetCents, NetCheque, NetChex, PayWord, QIPP, SEPP, SET, 3-D SET and STT).

Although credit cards have been the predominant means of payment on the Internet, a limited body of knowledge examine these payments with or without the CVV2, and even so in very broad terms.

No studies analyse the card payments in order to understand what are the fundamentals that cause to be the most popular means of payments.

2.2.2 Payment systems success factors

Many studies, some proposing new Internet payment protocols, identify the requirements that authentication mechanisms on Internet payment protocols should accomplish [6] [13] [16].

Earlier studies gave great relevance to technical criteria namely security issues, including anonymity, accountability, authentication and irrefutability. Subsequent studies [21] [22] [31] add user related criteria such as ease of use, security perception and trustworthiness. This shift results from the failed adoption of the SET protocol, backed by the major international payment systems, that had user convenience issues.

Later studies [33] [34] focus on the multi-party aspects of these systems and on the fact that all parties must perceive benefit from the adoption of these systems. If any participating party does not have their interests safeguarded then they by themselves may embargo the adoption of the new systems. Out of these studies requirements for merchants and all other participating parties have been identified.

2.2.3 Passwords

Although passwords can be considered a part of modern society's day-to-day activity, few in-depth academic studies covering the subject of passwords have been published [15] [20] [21] [29]. References to password matrixes or partial password authentication are found but studies on these mechanisms are scarce.

2.2.4 Coupon Collectors Problem

The Coupon Collectors Problem[35] determines the expected number of coupon draws, with replacement, to complete a set of a determined number of coupons. Recent studies [40] [41] [42] have researched various variations of this problem.

Having k coupons drawn at each draw, or choosing the least withdrawn coupon at each k coupon draw, completing m number of coupon sets are but some of the variations studied along these papers.

In this study two particular variations are studied that consists in determining the expected number of drawn distinct coupons after a number of *j* draws, where the draw reveals one or three coupons at a time. These variants are used to determine:

- The number of CVVs, out of a set of ***n*** CVVs, that are known to an attacker intercepting transactions with these CVVs.
- The number of digits, out of a set of ***n*** CVV digits, that are known to an attacker intercepting transactions where each transaction holds three of these CVV digits.

2.3 Conclusions

Much study on the search for an adequate Internet payment protocol has been carried out. The dominant Internet payment protocol, based on credit cards, has not been the focus of most research. The CVV2 cryptograms have contributed to elevate the security level of Internet credit card based payments however this mechanism has not been a subject of interest in academic research. Although some research has covered the properties of passwords, very little mention of partial passwords and password lists, matrixes, cards, etc., can be found. Global fraud statistics are frequently noted as lacking but regional and industry fraud trends are increasingly available.

Chapter 3: Current card based payment schemes description

3.1 Introduction

With the public adoption of the Internet came the need to develop a commerce platform that could insure security to payments. Due to the lack of an adequate e-payment protocol the credit card number and expiry date sustained itself as a *de facto* electronic payments method for the Internet from the very beginning to this date. Due to the fact that a valid card number and expiry date are easily guessable it has been vulnerable to attacks that simply generate card numbers and expiry dates in the hope that a valid pair will be accepted.

The payment systems meanwhile introduced the CVV2 [4] [23] [24]. This three-digit token, printed on or besides the signature panel on the back of the card, was introduced in order to validate that the cardholder is in possession of a genuine card in CNP transactions. Guessing valid card data became improbable given this extra authentication element.

Since 2002 the payment systems have invested further in securing e-payments through the introduction of the 3-D Secure protocol. This protocol adds an extra mechanism through which the issuer may authenticate the cardholder before the transaction is processed and thus gives guarantees that the cardholder is the legitimate one.

3.1.1 Overview

In this chapter the current CVV2 based scheme is described through the identification of the authentication elements and the involved parties in an e-commerce system and their respective roles. An overview of the infrastructure setup and of a transaction flow is described. Finally the 3-D Secure protocol is covered, equally through the description of the involved elements, parties and the flux of messages.

3.2 CVV2 scheme description

3.2.1 Authentication elements

The CVV2 based system makes use of three data elements:

- Card number;
- Expiry Date, and
- CVV2.

Card number

The card number is a series of up to 19 digits and is standardized by the ISO/IEC 7812 standard [1]. In the financial industry this number is also referred to as the Primary Account Number (PAN) and is constituted by the following elements:

- Issuer Identification Number (IIN);
- Account Identification (IAI);
- Checksum Digit (CD).

Issuer Identification Number (IIN);

In the financial industry the IIN is called the BIN (Bank Identification Number). The BIN is constituted by 6 digits and identifies the institution that issued the card to the cardholder. The BIN is used as a routing mechanism so that transactions occurring with a given card may be sent to the respective issuer.

Account Identification (IAI);

The IAI is assigned by the issuer and is of variable length however it may not have more than a maximum of 12 digits.

Checksum Digit (CD).

The last digit of the PAN is a Check Digit. This digit is calculated on all of the previous PAN digits making use of the Luhn formula for modulus 10 check digit as described in [1].

A high majority of card numbers are 16 digits long although card numbers with lengths between 12 and 19 digits can be found currently in circulation.

Expiry Date

The expiry date indicates the year and month up to which the card is valid. Following the last day of the referred month the card will be considered expired. This data element is constituted by two groups of two digits (MMYY): two for the month (MM) followed by two for the year (YY).

CVV2

This card verification element is a cryptogram that is calculated over the Card Number and the Expiry Date, and Service Code field (forced to a specific constant) making use of a secret issuer key known as the CVK2 (Card Verification Key for CVV2). This element is referred to as the CVV2 (Card Verification Value 2) by Visa and CVC2 (Card Verification Code 2) by Mastercard.

The presentation of these three data elements by the cardholder is widely used to authenticate e-commerce transactions as well as other card not present (CNP) transactions such as Mail Order and Telephone Order (MOTO) transactions.

3.2.2 Parties

In order for a cardholder to transact with an e-commerce merchant various entities will have to participate, namely the following:

- Cardholder
- Merchant
- Acquirer
- Payment system
- Issuer
- Card personalizer

Cardholder

The E-commerce cardholder will be supplied with a set of credentials that will enable him to authenticate the transaction at the e-commerce site. The cardholder shall obtain, at a time prior to the transaction, a card number, expiry date and a CVV2. These data elements are typically mailed to or directly handed to the cardholder printed or embossed on a traditional plastic credit card. Another way to be granted such information can be through the use of proxy or virtual cards. In this case the three data elements may be obtained for example at an ATM, an Internet site, via SMS or through a dedicated mobile app.

At the moment of transaction at the e-commerce site the cardholder will be prompted for the three elements: card number, expiry date and CVV2. The cardholder might still be requested the payment system (ex: Visa, Mastercard, Amex etc.).

Merchant

So that an E-commerce Merchant may accept card based transactions he must contract with one or more acquirers the ability to do so. At the moment of transaction the merchant will prompt for the card number, expiry date and CVV2. The merchant will send the authorization request to the payment system including the prompted data together with the amount and the respective currency.

Acquirer

Acquirers are payment system members that establish contractual relationships with merchants.

The acquirer shall receive transactions forwarded by the merchants and send them to the respective payment system network so that they be routed to the card issuer.

Payment system

The payment system will enrol acquirers and issuers establishing a network connecting these parties in order to route transactions between acquirers and issuers.

Issuer

The issuer shall enrol and supply the e-commerce cardholder with credentials that will enable the cardholder to authenticate the transaction at the e-commerce site.

The issuer will supply credentials in the form of physical or virtual credit cards. In either case, card data will have to be generated, and in the case of physical cards, card personalization will have to take place by a card personalizer.

The issuer shall also authenticate and authorise the transactions originated by their clients when performing transactions as e-cardholders using the supplied credentials.

Card personalizer

The card personalizer shall personalize cards with the data supplied by the issuer. The data comprises typically of magnetic card data (card number, expiry date, CVV1/CVC1, PVV, etc.), embossing card data (card number and expiry date), signature panel printing data (CVV2) and chip data for EMV cards.

3.2.3 Infrastructure setup

In order to set up the infrastructure to process transactions the various parties have to establish contractual agreements as well as establish connections between themselves. The following relationships must be established:

- Merchant to acquirer
- Acquirer to payment system
- Payment system to Issuer
- Issuer to cardholder

Furthermore the issuer must generate card data and issue the physical cards to the cardholder, through a card personalizer, so that the cardholder is able to authenticate himself during transactions.

The issuer shall generate card data to be placed on the card namely plastic card data, magnetic stripe and chip data. The plastic card data comprises in a card number and an expiry date to be embossed or infilled on the front of the card and a Card Security Code to be printed on or near the signature panel to be printed on the back of the card.

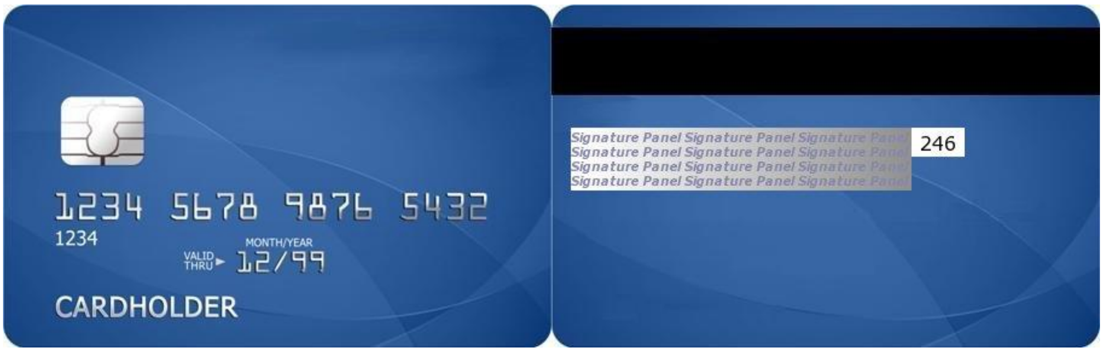


Figure 3.1– Traditional bank card

3.2.4 Transaction flow

Following is a high-level overview of the transaction flow for an e-payment based on CVV2:

0. The Issuer has issued a bank card to the consumer with a CVV2.
1. At checkout moment, in order to pay for the goods, the Cardholder inputs payment data by typing in the card number, the expiry date and the three-digit CVV2.
2. The Merchant sends payment data to the acquirer.
3. The Acquirer sends payment data to the payment system corresponding to the payment scheme
4. The Payment system sends the payment data to the issuer owner of the BIN
5. The issuer identifies the cardholder through the card number, validates the expiry date and authenticates the cardholder through the validation on an HSM of the Card Security Code.
6. After verifying additional authorisation criteria the issuer sends back an authorization to the payment system.
7. The payment system routes back the authorisation to the respective acquirer.
8. The acquirer informs the merchant of the authorisation for the transaction.
9. The merchant finalises the transaction giving the cardholder feedback on the success of the transaction.

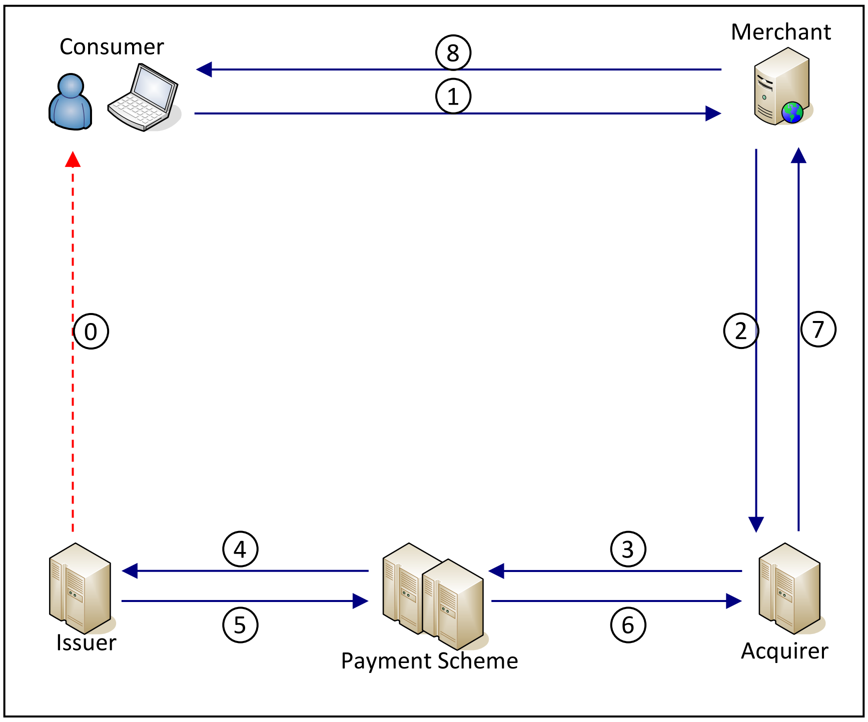


Figure 3.2– Standard payment authorisation transaction flow

3.3 3-D Secure scheme description

3.3.1 Authentication elements

The 3-D Secure protocol [3] involves a series of functionalities in order for the cardholder to be authenticated prior to the transaction. The main functionalities are the following:

- Merchant plug-in (MPI);
- Payment System Directory Server
- Access Control Server (ACS)
- Authentication History Server.

MPI

MPIs are installed on the merchant systems and will transact with the Payment System Directory Server so that the cardholder be verified prior to forwarding the standard payment authorisation transaction. Once the cardholder has introduced the card details the MPI will query the Payment System Directory Server in order to verify enrolment of the card and obtain the ACS URL. If the card is enrolled, and upon reception of the ACS URL, the merchant will send an authentication request to the ACS through the cardholder’s browser. Upon completion of the cardholder verification the MPI will receive a signed authentication confirmation from the issuer’s ACS.

Payment System Directory Server

The Payment Systems setup a Directory server that will answer to the MPI upon verification requests, indicating if the card is enlisted in the 3-D Secure protocol. So that the Directory Server is able to give an answer to the merchant, the Directory Server will contact the issuer's ACS to check the validity of the card and query its participation in the 3-D Secure scheme. The ACS will forward the ACSs URL to MPI so as to redirect the cardholder's browser so that the issuer may authenticate the cardholder.

ACS

The ACS will respond to the Payment Directory Servers queries on card 3-D Secure enlisting and provide the URL to which the cardholder be directed for issuer verification of the cardholder authenticity. When the cardholder is redirected by the MPI to the ACS, the ACS will authenticate the cardholder by whatever means he has adopted (ex. static password, SMS token, etc.). After authentication has been performed the ACS shall respond with the authentication result to the MPI and shall equally inform the Authentication History Server of the result.

Authentication History Server

The Authentication History Server shall hold the results of the authentications performed by the ACS for eventual disputes.

3.3.2 Parties

In order for a transaction to be processed via the 3-D Secure protocol various services will have to be implemented. These services may be implemented by the Issuers, Acquirers and the Payment Systems themselves or may be performed by third party service providers.

The new players that support the 3-D Secure protocol are the following:

- MPI (Merchant Plug-In) Provider
- Payment System Directory Server
- ACS (Access Control Server) Provider
- Payment System History Server

MPI Provider

Merchants will have to install the MPI in their systems. Payment systems license the software to MPI providers.

ACS Provider

Issuers will setup an ACS or contract an ACS provider so that queries from the Payment System Directory are answered and cardholder authentications executed upon authentication verification requests from MPI.

3.3.3 Infrastructure setup

In order for the 3-D Secure process to be in place various preparation activities must take place.

Issuers must setup an ACS and enrol cards to the scheme. Cardholders will be informed of the authentication mechanism to be used prior to the usage. Some issuers have opted to enrol and choose authentication mechanism at the moment of the first cardholder's 3-D Secure based transaction.

Merchants must enrol and integrate the MPI in their e-commerce systems so that prior to standard payment authorisation transaction the MPI query about the card enrolment in to the 3-D Secure and request authentication verification if enrolled.

3.3.4 Transaction flow

In a 3-D Secure transaction the following steps will take place:

0. The Issuer has enrolled the card BIN into the 3-D Secure scheme and the Merchant has enrolled into the 3-D Scheme.
1. At checkout moment, in order to pay for the goods, the Cardholder inputs payment data by typing in the card number, the expiry date and the three-digit CVV2.
2. Prior to sending payment data to process the standard payment authorisation, the MPI queries the Directory Server for card 3-D Secure enrolment.
3. The Directory Server queries the ACS to validate that the card is enrolled.
4. The ACS responds with the enrolment status of the card and with the URL that will authenticate the cardholder.
5. The Directory Server routs the card enrolment status and URL to the merchant.
6. The MPI sends an authentication request to the ACS via the Cardholders browser.
7. The ACS requests the cardholder to authenticate and the cardholder authenticates himself.
8. The ACS verifies authentication and responds to the MPI with authentication response.
9. The ACS informs the History Authentication server of the authentication result.
10. The MPI validates the response and if the authentication was successful the standard payment authorisation proceeds.

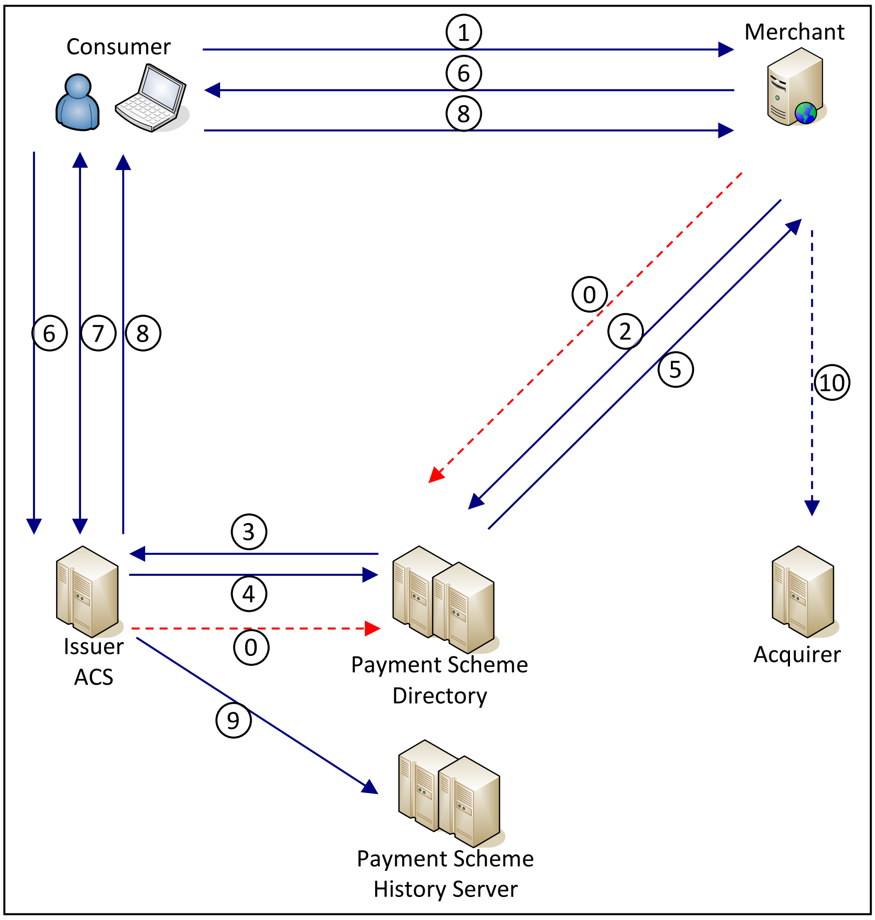


Figure 3.3 – 3-D Secure transaction flow

Chapter 4: Key success factors for new e-payment scheme proposals

4.1 Introduction

Hundreds of e-payment schemes have been proposed in the last two decades [14] [17] but very few have withstood time and have been able to declare even limited success. Meanwhile payments with bank cards on the Internet have been the preferred means of e-payment and have dominated the e-payments landscape [9]. E-payments with bank cards may be considered a crude authentication method, security wise, given the rudimentary fundamentals that are based on a sixteen digit number, an expiry date and sometimes a three digit CVV2. Frequent data breaches [28] through the last decade, and millions of virus infected PCs [43] have highlighted its vulnerabilities. However users continue to prefer this payment method.

Various studies have outline key success factors for e-payments schemes. A first phase of studies covered technical attributes that should be fulfilled by e-payment systems. These focused mainly on security issues [6] [13] [16] such as anonymity, privacy, non-repudiation, integrity, etc.

As a result of failure in adoption of IPS backed major initiatives, namely SET [2] and 3-D SET, due to user convenience issues, many subsequent studies [18] [19] [22] highlighted user related criteria. Ease of use, trust, reliability, user acceptance, are but some of the criteria that were evaluated in order for an e-payment system to succeed.

Recent studies [33] [34] have a holistic approach in regard to the criteria that an e-payments system shall withhold in a sense that all parties in the e-payment systems must have their interests attended to. Users, merchants, and all other participating parties must yield benefit from the system, given that if this isn’t guaranteed any one of these participants may embargo the adoption of a proposed scheme. Critical mass has been identified as an important characteristic that has to be overcome by any new scheme [30]. Users want to adopt schemes that are accepted at all merchants with whom they transact, and on the other hand merchants will only support payment methods that are used by a relevant number of their client base.

4.1.1 Overview

This chapter describes the factors that are important for each of the payment system participants for a new e-payments proposal to succeed. These are divided into three orders of factors:

- Key factors for user acceptance;
- Key factors for merchant acceptance;
- Key factors acceptance by other parties;

4.2 Key factors for user acceptance

Many studies have covered the characteristics that should be present in an e-payments scheme. Dennis Abrazhevich has elaborated an extensive analysis [18] of the characteristics that users deem as determinant for acceptance of an e-payment scheme. His study reveals a survey that has been conducted over a universe of 1328 respondents in order to obtain empirical evidence of the importance of the characteristics to end users for e-payments. The characteristics that have been surveyed are the following:

- Anonymity, privacy,
- Applicability (acceptability)
- Convertibility
- Efficiency
- Reliability
- Security
- Traceability
- Trust
- Usability (ease of use)

Following, an analysis of these characteristics and an interpretation of their importance for the user, resulting from the survey, will be performed. The applicability of these characteristics to the traditional bank card based payments will be commented, and finally a comment on the changes that the proposed schemes of this study have on the characteristics will be noted.

4.2.1 Characteristics analysis

Anonymity, privacy

Anonymity is the characteristic that protects the user’s identity and personal information from being known.

Although many studies have highlighted anonymity as being an essential characteristic, the survey showed that only 13.5% of respondents were concerned or very concerned that shops could register their purchases. Actually 72.9% would prefer that their purchases were registered to avoid disputes and 72.8% would never refrain from paying because of revealing identity when paying.

Bank cards do not guarantee anonymity but through the survey we may conclude that users do not give much importance to this characteristic and are ready to sacrifice it to avoid or resolve disputes.

The proposed schemes in this study maintain this characteristic intact, thus will neither augment nor hinder the level of privacy to which the user is subject.

Applicability (acceptability)

Applicability (or acceptability) of an e-payment system is the characteristic that indicates the extent to which it is accepted at e-commerce sites.

Respondents to the survey gave great importance to the fact that one single particular payment scheme be used in most places where they pay; 59.8% considered it very important and 28.3% quite important that a single mechanism be used. Furthermore 85.8% emphasised that the ability to pay with a payment system at multiple and diverse points of sale was important.

Bank cards are, indisputably, the most used payments means on the Internet and any e-merchant wanting to accept payments on the Internet cannot ignore this payment means to achieve scale.

The proposed scheme builds upon the fact that bank cards are presently widely accepted and that the installed base is global from the very beginning. The proposed schemes are readily acceptable at any 3-D Secure merchant, once the issuer adopts the payment scheme. For non-3-D Secure merchants the users may still fallback to the traditional card payment experience with or without the CVV2.

Convertibility

The ease in converting funds between payment systems is defined by the characteristic of convertibility.

The survey did not cover convertibility between bank cards and accounts or cash, however, most respondents considered that conversion between payment systems is important specially the conversions between account and cash.

Given the direct link between debit cards and accounts, and that credit cards have well established processes to convert between credit card and accounts, bank cards in general satisfy this characteristic.

The proposed mechanism does not influence any change on convertibility when compared with standard bank card e-payments.

Efficiency

Efficiency underlines characteristic of cost per transaction and is of special importance for low value transactions.

Many proposed e-payment protocols have given weight to this characteristic however few (13.4%) respondents considered it had any importance at all.

Payments with bank cards are not as efficient as could be to handle low payment values; on the other hand, millions of e-payments based on cards are performed daily and news on dissatisfaction on costs of payments on the Internet with cards is residual.

The proposed scheme does not alter the costs of transactions based on cards.

Reliability

The availability of a payment system and the capability to function as expected is translated in to the reliability characteristic.

The survey highlighted the preference of respondents for bank cards (58.1%), compared to cash and smart cards, when questioned which are more reliable.

The payment industry has established a resilient infrastructure to process traditional bank cards. This same infrastructure has been used to process e-payments capitalizing on a well-proven installed base.

The proposed schemes support themselves on the well-established systems used by the present day and no modification is necessary. No changes are necessary to current messages between the systems.

Security

The security characteristic, on a user perspective, is the level to which a user’s funds are secure when paying online.

Security is one of the most stressed characteristics on numerous studies on e-payment methods. Aligned with this concern, a very high proportion of respondents considered security as very important (84.7%) or quite important (13.7%). Conversely when questioned if the respondents would refrain from using debit cards or credit cards if thought they were insecure, 96.7% would not refrain to use debit cards and 81.2% credit cards.

Payments with bank cards have suffered various security setbacks such as large-scale data breaches and continuous news on card data collecting malware situations. Although the general public perception is that card based e-payments are not secure, it seems that the lack of viable alternatives has avoided the decrease in usage of these means.

The proposed solution will enhance security of these payments and enhance protection against the major threats to the bank cards based payments, namely data breaches and data collecting malware.

Traceability

The traceability characteristic reflects the ease with which money flows, including fund sources and fund destinations, may be traced.

45.3% of respondents are concerned that sources of their income may be known to vendors. Although respondents are not concerned with strong anonymity, responses reveal that consumers still would like to have a certain degree of privacy. 58.3% of responses indicate that users consider it important that they do not leave personal information such as name, address and bank account, to merchants.

Payments based on bank cards leave traces of transactions that are essential for dispute resolutions. Apart from the card number no other personal information is revealed in most standard payments, although some merchants require names or addresses to increment verification levels.

The proposed scheme does not reveal further information when compared to a standard card based e-payment.

Trust

The trust characteristic denotes the degree of confidence that the user places on the system so that its funds and its interests be protected.

The survey revealed that trust was considered as being very important. 97.6% would only trust a system introduced by an established organization and 94.4% would stop using a system that they felt that was not trustworthy.

Although much negative publicity on the security of cards has come to light throughout its existence, card based payments continue to be the preferred mechanism for e-payments. Given the importance that the survey result emphasises on trust it leads us to conclude that cards seem to be the most trusted means of e-payments. The fact that the user understands the mechanism and that he has a sense of control (i.e. the secret is on a plastic that he keeps in his wallet) gives him a sense of security.

The proposed scheme adds further perception of security to the user given that at each payment he will be asked for a different part of a secret, thus we will not reveal the whole secret to any one, as is the case with traditional payments.

Usability (ease of use).

The ease with which users perform the e-payments is known as the usability characteristic.

The ease of use has been indicated as one of the most importance characteristics special given some major initiatives that failed in this field such as the SET protocol backed by the main international payment systems. 81.7% of respondents referred that they feel more comfortable when using something tangible to pay.

Most respondents indicated that it was easy to pay with credit cards over the Internet (68.2% - “very easy” and 28.0% - “easy”).

The proposed solutions will impact the usability characteristic negatively. The user will be challenged to type in one of the CVVs or three digits of a long CVV. Either challenge makes use of mechanisms that have been adopted in the market and have been successful. The impacts on usability will depend on the size of the secret to be adopted but can be kept at a minimum, resulting in a residual impact.

4.3 Key factors for merchant acceptance

Millions of e-merchants make up today’s e-commerce ecosystem. Along with the users, merchants are instrumental so that a new scheme is successfully adopted. A merchant’s main requirements are that a payment scheme offers secure and reliable transactions and that the implementation and operational costs be justified by the user base that will be gained with the new payment scheme.

The following characteristics will be commented, and changes to the proposed schemes will be noted:

- Security
- Applicability
- Cost of implementation
- Cost of operation

4.3.1 Characteristics analysis

Security

The security characteristic, on a merchant perspective, is the level to which a merchant has guarantees that the payment will be honoured.

Merchants have been attacked throughout recent years, having had their systems compromised and card data being stolen. Payment systems have forced the PCI DSS program on to merchants so that systems protect against card data compromise. Implementing the PCI DSS program is costly and furthermore does not guarantee that vulnerabilities are all mitigated. In fact many data breaches have occurred at merchants that were at the time of compromise, certified as being compliant to PCI DSS.

The proposed solution is based on the adoption of dynamic CVVs. The compromise of one of these dynamic CVVs, present in a transaction, will frustrate the intentions of the attackers given that it may not be used in any subsequent transaction. With this scheme the compromised card data, namely the enhanced CVV2, has less value for the attacker and so will discourage attacks.

Applicability (acceptability)

Applicability (or acceptability) of an e-payment system on a merchant perspective reflects the user base that will be able to perform payments through the new means.

Payments based on bank cards are the most popular means of payments on the Internet. Attaining critical mass is an essential factor to justify cost in implementing any new payments system.

The fact that bank cards are widely used by most users and that a migration process may be supported in order to migrate users into the new proposed scheme, guarantees the merchant with the much-needed critical mass.

Cost of implementation

Changing millions of e-commerce sites to be able to process a new payments scheme implies a formidable investment by merchants. History has proven that there is great inertia in these kinds of changes. Simple changes such as the support for CVV2 at merchant sites has taken more than a decade and still many sites do not support payments with CVV2. The SET protocol required merchants to perform significant changes to their systems; some argue that this impact was one of the factors that crippled the adoption of this protocol. As a final example, adoption of 3-D Secure has been backed by the International Payment Systems through liability shift incentives, and although merchants require minor changes to their systems, many merchants haven’t yet migrated.

Changing a site to adopt a payment means that is uncertain to succeed and that does not have guarantees of a critical mass of customers from the very beginning discourages merchants.

The proposed schemes build upon present infrastructure. 3-D Secure merchants do not have to change their systems in order to support the proposed schemes. Non 3-D Secure merchants have the option to adopt 3-D Secure or to perform minor changes to their existing systems, to benefit from the enhanced security inherent to the proposed schemes.

Cost of operation

Operational costs are a major concern for merchants and all parties alike. Interchange fees have been a notable battlefield in the payments, as well as the e-payments, arena.

Synergies between the physical world payments and the e-payments have proven to be advantageous. The fact that billions of consumers hold a card in their wallets that can be used on the Internet and that many merchants already have systems that process payments through contracted merchants is a favourable starting point. The existence of support processes such as dispute handling, blacklist management, fraud detection and management systems, are essential to support any payment scheme.

The proposed schemes build upon this existing context with no need for changes.

4.4 Key factors acceptance by other parties

Implementing any system based on a multi-sided platform is a particularly difficult challenge. Many aspects have to be accounted for in a balance that brings benefits for all participating parties. By building upon a well-tuned existing infrastructure, all parties such as acquirers, issuers, financial institutions, network operators, processors and regulators, have their interests assured.

The proposed scheme brings on little or no changes to this context whilst augmenting protection to relevant attacks.

Chapter 5: Enhanced CVV2 scheme proposals

5.1 Introduction

This study proposes and analyses two distinct methods for securing e-commerce transactions that consist on having different CVV2s for each transaction:

- Multiple CVV method
- Long CVV method

In this way, the illicit capture of transaction data, including one of these new CVVs, will not be sufficient to perform subsequent transactions.

5.1.1 Multiple CVV method overview

The Multiple CVV scheme consists on supplying the cardholder with a matrix of three-digit CVVs, that we shall call MCVVs, printed on the credit card. At the moment of transaction the cardholder shall be prompted for one of the MCVVs thus authenticating him.

For each transaction only one of the MCVVs will be used thus maintaining the rest of the MCVVs unknown to an eventual eavesdropper or an attacker compromising a merchant's database. The MCVV used for each transaction shall be called the Transaction CVV (TCVV).

5.1.2 Long CVV method overview

The Long CVV scheme [25] consists on supplying the cardholder with a long CVV value with ***n*** digits, that we shall call LCVV, printed on the credit card. At the moment of transaction the cardholder shall be prompted for three of the LCVV digits in order to authenticate the cardholder.

For each transaction only three digits of the LCVV will be used thus maintaining the remainder of the LCVV digits unknown to an eventual eavesdropper or an attacker compromising a merchant's database. The three LCVV digits used for a transaction shall be called the Transaction CVV (TCVV).

5.1.3 Chapter overview

In this chapter we will cover a description of both methods. The implementation of these methods depends on the adherence of the merchant for 3-D Secure. If the merchant is 3-D Secure then the merchant does not have to implement anything to support the proposed schemes. If the merchant does not support 3-D Secure, and doesn't want to support 3-D Secure then minor modifications have to be implemented to support one of the proposed schemes.

Thus this chapter shall describe in the following sections the Multiple CVV and the Long CVV scheme implementations in 3-D Secure merchants. The last two sections shall describe the implementations at non 3-D Secure Merchants.

5.2 Multiple CVV implementation for 3-D Secure merchants

In this section the following phases of the Multiple CVV scheme will be described:

- Issuer card data preparation
- Card personalisation
- Merchant checkout process
- Issuer cardholder authentication process

The first two phases occur once for each card lifecycle whilst the latter two occur for each transaction.

5.2.1 Issuer card data preparation

The issuer prepares the data for card personalisation as in a traditional card data preparation with the exception that instead of generating one CVV2 the issuer will generate the CVV2 along with a set of ***n*** MCVVs. The set of MCVVs takes the form of a matrix of MCVVs with ***a*** columns and ***b*** rows ($\boldsymbol{n} = \boldsymbol{a} \times \boldsymbol{b}$):

$$MCVV\ matrix = \begin{bmatrix} MCVV_{11} & MCVV_{21} & \dots & MCVV_{a1} \\ MCVV_{12} & MCVV_{22} & \dots & MCVV_{a2} \\ \dots & \dots & \dots & \dots \\ MCVV_{1b} & MCVV_{2b} & \dots & MCVV_{ab} \end{bmatrix}$$

The issuer generates each of these MCVV values making use of the traditional HSM function for CVV generation that is used for generating the CVVs in general (e.g. CVV1 for the magnetic track, CVV2 for the signature panel and iCVV for the EMV Track 2 Equivalent Data).

The HSM *GenerateCVV* function produces a three digit CVV2 cryptogram having as inputs the cryptographic CVK2 key (Card Verification Key for CVV2s), the PAN, the Expiry Date and the Service Code.

```
CVV2 = GenerateCVV (CVK2,PAN,ED,SC)
```

Where,

```
CVK2 - Card Verification Key for CVV2s
PAN - Primary Account Number
ED - Expiration Date
SC - Service Code
```

In the case of this proposed solution, the MCVVs are calculated by forcing the Service Code to a value equal to a zero concatenated with the column number and row number of each MCVV of the matrix.

```
Service Code = 0 || x || y
Where x varies between 1 and a, and y varies between 1 and b
```

The issuer needs only to retain the CVK2 key for the card range, given that this key and the data present at the moment of transaction: PAN, Expiry Date and the row and column of chosen CVV, is sufficient for validating MCVVs.

Example

Let us assume that the MCVV matrix has 7 columns and 2 rows. The results of the 14 GenerateCVV function calls for the card with the PAN "1234 5678 9876 5432" and the expiry date "1299" could produce the following MCVV Matrix (values are merely illustrative).

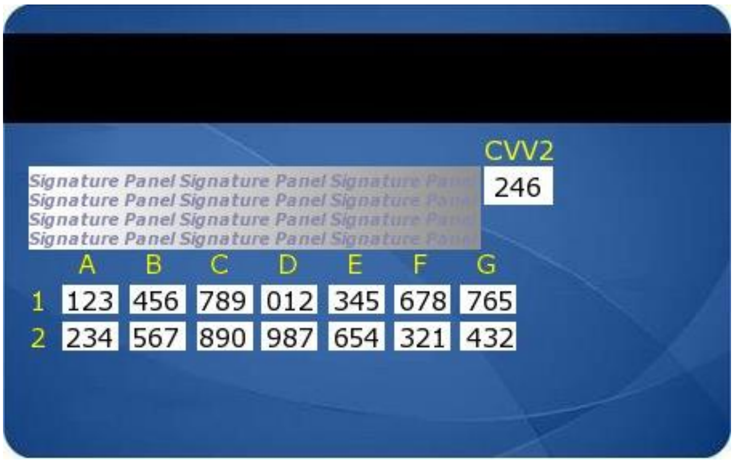
$$\text{MCVV Matrix } = \begin{bmatrix} 123 & 456 & 789 & 012 & 345 & 678 & 765 \\ 234 & 567 & 890 & 987 & 654 & 321 & 432 \end{bmatrix}$$

5.2.2 Card personalisation

Traditional cards already have the capacity for printing CVV2 values on or besides the signature panel. In the Multiple CVV scheme the card personalizer has to additionally place the MCVV Matrix values on the back of the card. A legend for the matrix has to be incorporated into the card design to help the cardholder reference the MCVV in the matrix.

Example

Let us assume a card with a MCVV matrix with 7 columns and 2 rows with the values printed below the signature panel on the back of the card as shown in the following figure.



Signature Panel Signature Panel Signature Panel
Signature Panel Signature Panel Signature Panel
Signature Panel Signature Panel Signature Panel
Signature Panel Signature Panel Signature Panel

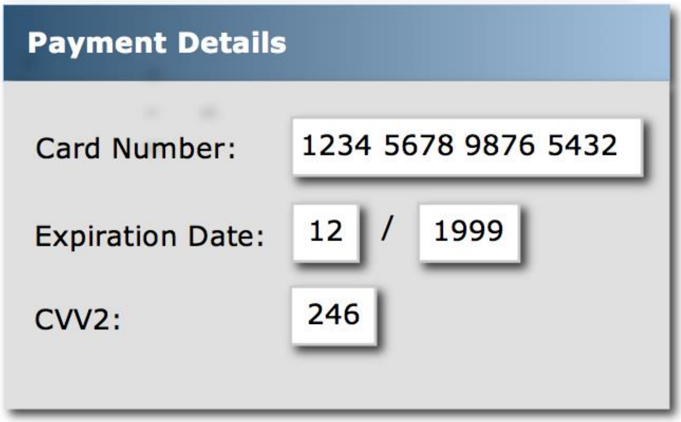
CVV2: 246

	A	B	C	D	E	F	G
1	123	456	789	012	345	678	765
2	234	567	890	987	654	321	432

Figure 5.1 – MCVV card example

5.2.3 Merchant checkout process

During the merchant checkout process the cardholder will be prompted for the card number, the expiry date and optionally for the CVV2.



Payment Details

Card Number: 1234 5678 9876 5432

Expiration Date: 12 / 1999

CVV2: 246

Figure 5.2 – Traditional checkout example

In this analysis, given that the merchant and the cardholder are both 3-D Secure the cardholder will be redirected to the issuer so that the cardholder be authenticated. If the result of the issuer authentication is positive the merchant will proceed with the standard payment transaction forwarding the payment data to the acquirer.

5.2.4 Issuer cardholder authentication

Upon redirection of the cardholder, the issuer prompts the cardholder for the three TCVV digits by requesting for the MCVV in column ***x*** and row ***y***:

TCVV = MCVV matrix[xy]

The issuer validates the MCVV through the use of the HSM *ValidateCVV* function (present on all traditional financial HSMs) using as input the cryptographic CVK2 key, the PAN, the Expiry Date and the Service Code.

The Service Code to be used in this function is obtained by concatenating a zero with the chosen column and line numbers, as in the issuer data preparation phase:

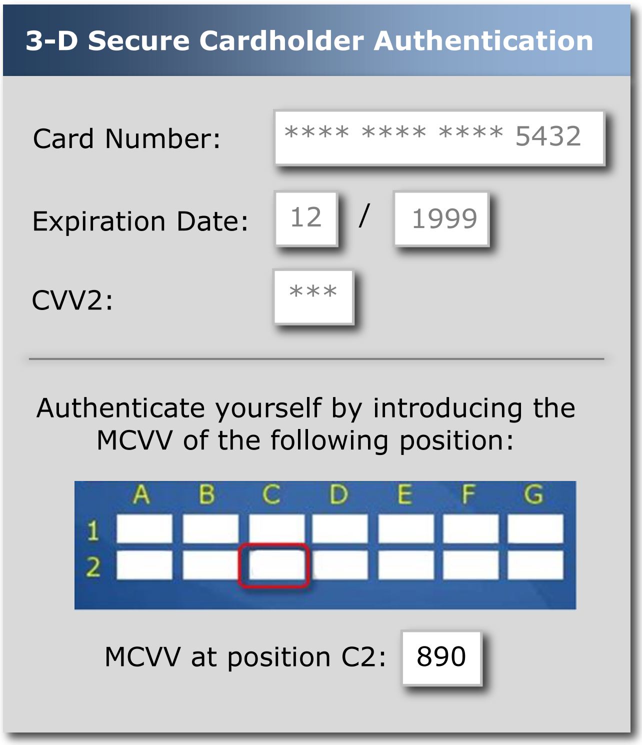
Service Code = 0 || x || y

The HSM *ValidateCVV* calculates the CVV with the input fields and if equal to the input field TCVV then it gives a positive response indicating that the TCVV is the correct one and that the cardholder has authenticated the transaction.

ValidateCVV(TCVV, CVK2, PAN, ED, SC)

Example

> *Let us assume that issuer chooses the numbers three and two for the column and row of the MCVV for this example. In this case the issuer requests for the MCVV in position C2 corresponding to the CVV in the 3rd column and 2nd row:*



3-D Secure Cardholder Authentication

Card Number: **** **** **** 5432

Expiration Date: 12 / 1999

CVV2: ***

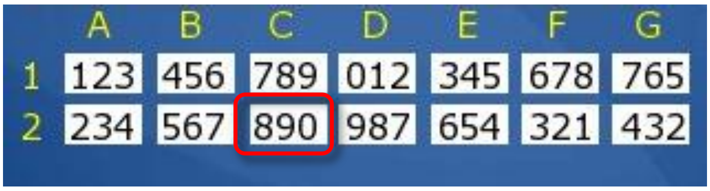
Authenticate yourself by introducing the MCVV of the following position:

	A	B	C	D	E	F	G
1							
2							

MCVV at position C2: 890

Figure 5.3 – Issuer cardholder authentication with MCVV example

The cardholder introduces the MCVV at position C2 of the MCVV thus producing a TCVV with the value 890.



	A	B	C	D	E	F	G
1	123	456	789	012	345	678	765
2	234	567	890	987	654	321	432

Figure 5.4 – MCVV example.

In this case the Service Code used for the ValidateCVV function will have the value 032:

Service Code = 0 || *x* || *y* = *032*

Finally the TCVV shall be validated through the following function call to the HSM:

ValidateCVV (CVV, CVK, PAN, Expiry Date, Service Code)
ValidateCVV (890, CVK, 1234 5678 9876 5432, 1299, 032)

5.3 Long CVV implementation for 3-D Secure merchants

In this section the following phases of the Long CVV scheme will be described:

- Issuer card data preparation
- Card personalisation
- Merchant checkout process
- Issuer cardholder authentication process

The first two phases occur once for each card lifecycle whilst the latter two occur for each transaction.

5.3.1 Issuer card data preparation

The issuer will prepare the data for card personalisation as in a traditional card personalisation with the exception that an extra field called LCVV shall be generated.

The issuer shall generate, for each card, an LCVV with ***n*** random digits:

$$LCVV = C1, C2, C3, \ldots Cn$$

The issuer must use a deterministic function of his choice to generate LCVVs during data preparation, and must use the same function during authorization. So that the issuer does not maintain a table with all the generated LCVVs, susceptible to compromise in the case of a database breach, the issuer should make use of common HSM (Hardware Security Modules) financial functions to generate the LCVV.

The issuer sends the LCVV to the card personalizer and erases this data from its systems given that the issuer holds the means to validate this data when required through HSM functions and a dedicated cryptographic key.

Example

> *Let us assume that the issuer has randomly generated a 12 digit long LCVV with the value 362 458 310 679, thus **n** is equal to 12.*
>
> $$LCVV = 362\ 458\ 310\ 679 \qquad \rightarrow n = 12$$
>
> *This value will be printed beside the signature panel on the back of the card.*

5.3.2 Card personalisation

The card personalizer will place the LCVV value on the back of the card, next to the signature panel. A legend for the LCVV will also have to be incorporated into the card design to help the cardholder reference the LCVV digits.

Example

> *With an example LCVV of 362 458 310 679, the card will have the back of the card as in the following figure:*

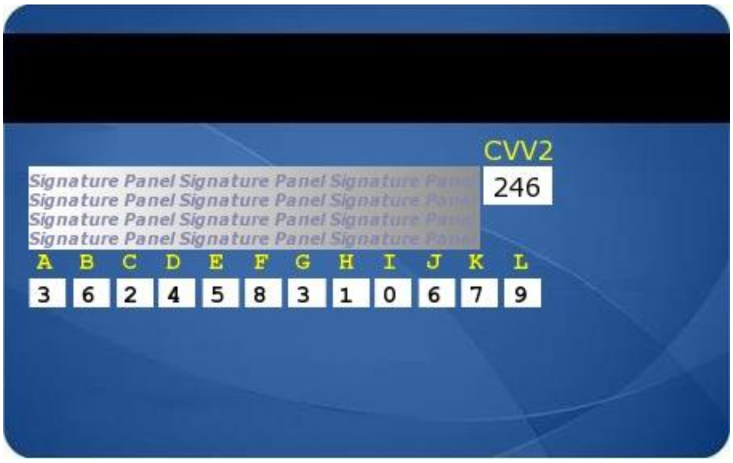
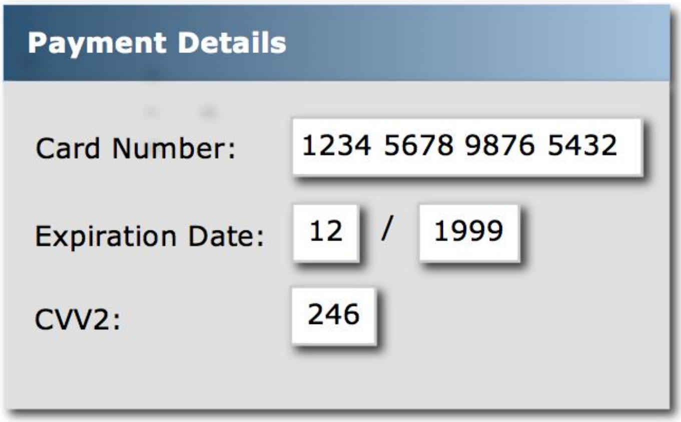


Figure 5.5 – LCVV card example

5.3.3 Merchant checkout process

During the merchant checkout process the cardholder will be prompted for the card number, the expiry date and optionally for the CVV2.



Payment Details

Card Number: 1234 5678 9876 5432

Expiration Date: 12 / 1999

CVV2: 246

Figure 5.6 – Traditional checkout example

In this analysis, given that the merchant and the cardholder are both 3-D Secure the cardholder will be redirected to the issuer so that the cardholder be authenticated. If the result of the issuer authentication is positive the merchant will proceed with the standard payment transaction forwarding the payment data to the acquirer.

5.3.4 Issuer cardholder authentication

Upon redirection of the cardholder, the issuer prompts the cardholder for three digits of the ***n*** digits that constitute the LCVV.

The issuer shall generate three non-repetitive values, ***s***, ***t*** and ***u***, between 1 and ***n***, in order to establish which three of the ***n*** positions of the LCVV will be prompted for.

The issuer shall prompt the cardholder for the three digits of the LCVV in the positions ***s***, ***t*** and ***u***. These three digits shall be the TCVV for this transaction.

$$TCVV = Cs, Ct, Cu$$

The issuer shall reproduce the LCVV value making use of a deterministic function on its HSM. The validation of the TCVV shall be performed by comparing the TCVV with the digits of the reproduced LCVV in the positions ***s***, ***t*** and ***u***.

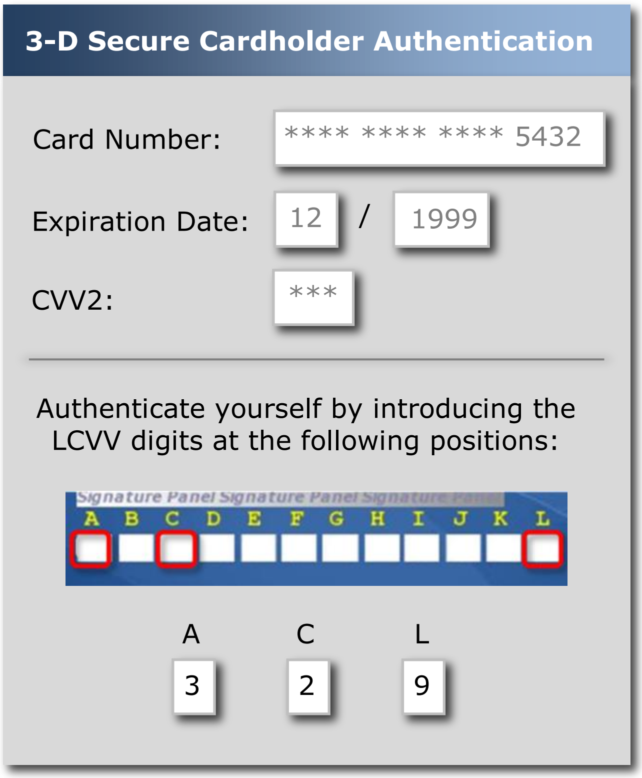
The TCVV shall be validated through the comparison of the digits in the positions ***s***, ***t*** and ***u***.

```
if (
  Reproduced LCVV[s] = TCVV[1] and
  Reproduced LCVV[t] = TCVV[2] and
  Reproduced LCVV[u] = TCVV[3]
) then TCVV ok
```

Example

At the moment of transaction the issuer shall prompt the user for three digits that will constitute the CVV for this transaction (TCVV).

Let us assume that the three randomly generated digit positions are 1, 3 and 12. The issuer shall request the digits in 1st, 3rd and 12th positions:



3-D Secure Cardholder Authentication

Card Number: **** **** **** 5432

Expiration Date: 12 / 1999

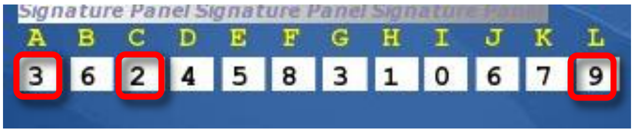
CVV2: ***

Authenticate yourself by introducing the LCVV digits at the following positions:

A	C	L
3	2	9

Figure 5.7 – Issuer cardholder authentication with LCVV example

The cardholder shall introduce the 1st, 3rd and 12th digits of the LCVV thus producing a TCVV with the value 329.



A	B	C	D	E	F	G	H	I	J	K	L
3	6	2	4	5	8	3	1	0	6	7	9

Figure 5.8 – LCVV example

The Issuer shall reproduce the LCVV making use of a deterministic function on the HSM. Let us assume that the Issuer has obtained a Reproduced LCVV value of 362458310679 for this card.

Reproduced LCVV = 362 458 310 679

Finally the TCVV shall be validated through the comparison of the 1st, 2nd and 3rd digits of the received TCVV with the 1st, 3rd and 12th digits respectively of the Reproduced LCVV.

Reproduced LCVV[2] = TCVV[1] = 3
Reproduced LCVV[3] = TCVV[2] = 2
Reproduced LCVV[8] = TCVV[3] = 9

If all digits are correct then the TCVV is correct and the cardholder is considered authenticated and the merchant is informed of a positive authentication result.

5.4 Multiple CVV implementation for non 3-D Secure Merchant

A non 3-D Secure merchant wanting to adhere to the Multiple CVV scheme may follow one of two strategies.

a) Adhere to the 3-D scheme integrating a standard MPI, benefitting of liability shifts, and no further effort is necessary.

b) If the merchant opts not to adhere to 3-D Secure he may implement minor modifications to his checkout process in order to support the Multiple CVV scheme. The issuer will have to likewise implement minor changes to the transaction authorisation process.

The Issuer card data preparation and the personalisation process is the same as described before. This section describes the modification that the non 3-D Secure merchant has to implement and that the issuer has to implement to support the Multiple CVV scheme.

- Merchant checkout process
- Issuer authorisation process

5.4.1 Merchant checkout process

At the moment of transaction the merchant generates two values ***x*** and ***y*** in accordance with the following restrictions:

$$1 \leq x \leq a \ \wedge \ 1 \leq y \leq b$$

These two values indicate the column and row (position) of the MCVV from the matrix that was chosen for the Transaction MCVV (TCVV). The merchant builds a Transaction CVV Position Code (TCVV PC) in the following way:

$$TCVV\ PC = 0 \ || \ x \ || \ y$$

Where || stands for concatenation.

It is recommended the merchant always generate the same values for each card so that in case of compromise of a merchant's systems, the attacker will know only one TCVV.

The merchant prompts the cardholder for the three TCVV digits by requesting for the MCVV in column ***x*** and row ***y***:

$$TCVV = MCVV\ matrix[xy]$$

The Merchant sends the TCVV in substitution of the CVV2 with the rest of the payment data to the issuer in the authorisation message. So that the issuer knows which MCVV is being used for this transaction it must also send the TCVV PC.

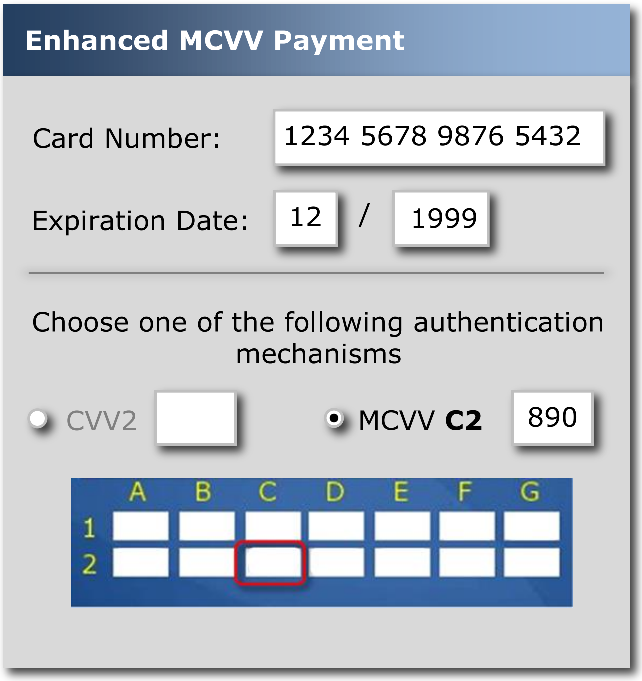
In order to pass the TCVV PC to the issuer without impacting the interlaying infrastructure, this information is packed into the PAN field of the transaction. The merchant transforms the original 16 digit long PAN into a 19 digit long Transaction PAN (TPAN) by appending the TCVV PC to the original PAN.

$$TPAN = PAN\ ||\ TCVV\ PC$$

The merchant sends the TPAN to the acquirer in order for it to be routed through to the card issuer.

Example

> *Let us assume that at the moment of transaction the merchant generates the numbers three and two for the column and row of the MCVV to be used, thus the TCVV PC has the value 32 for this example. In this case the merchant requests for the MCVV in position C2 corresponding to the CVV in the 3rd column and 2nd row:*



Enhanced MCVV Payment

Card Number: 1234 5678 9876 5432

Expiration Date: 12 / 1999

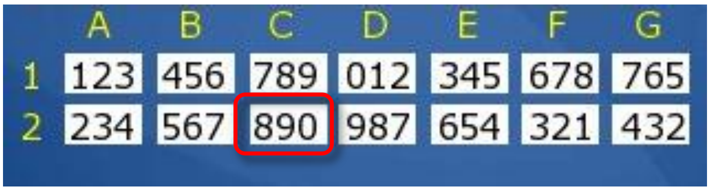
Choose one of the following authentication mechanisms

○ CVV2 ● MCVV **C2** 890

	A	B	C	D	E	F	G
1							
2							

Figure 5.9 – Checkout with MCVV example

The cardholder introduces the MCVV at position C2 of the MCVV thus producing a TCVV with the value 890.



	A	B	C	D	E	F	G
1	123	456	789	012	345	678	765
2	234	567	890	987	654	321	432

Figure 5.10 – MCVV example.

The merchant communicates to the issuer the TCVV with the value 890 in the CVV2 field and communicates the TCVV PC with the value 32 incorporated in the PAN.

Let us assume a card with PAN equal to 1234 5678 9876 5432.

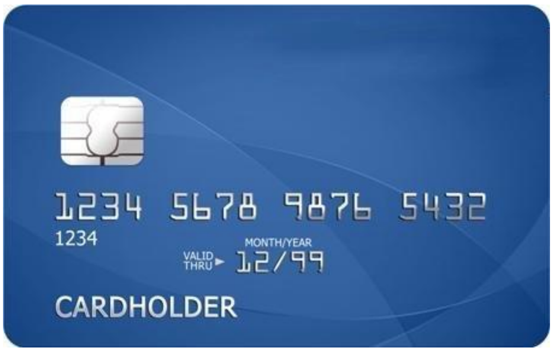


Figure 5.11 – ECVV card front example

Inputs

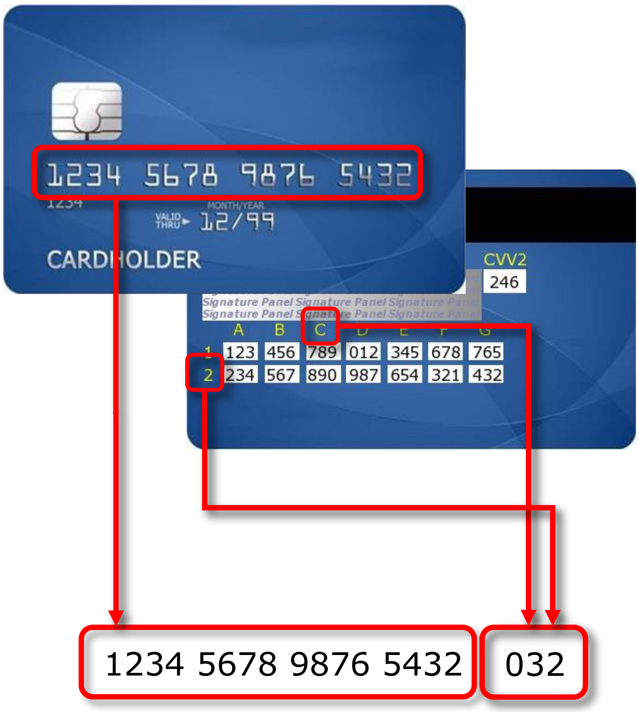
PAN = 1234 5678 9876 5432

TCVV PC = 032

TPAN construction

TPAN[19] = PAN[16] || TCVV PC[3]

TPAN = 1234 5678 9876 5432 032


1234 5678 9876 5432
1234
MONTH/YEAR
VALID THRU
12/99
CARDHOLDER
CVV2
246
Signature Panel Signature Panel Signature Panel
Signature Panel Signature Panel Signature Panel
1234 5678 9876 5432
032

	A	B	C	D	E	F	G
1	123	456	789	012	345	678	765
2	234	567	890	987	654	321	432

Figure 5.12 – TPAN construction example

5.4.2 Issuer authorisation process

The issuer, upon reception of a 19 digit long PAN for a BIN that holds 16 digit long PANs, will have knowledge that the transaction was performed by an Enhanced CVV capable merchant and therefore is in presence of an Enhanced CVV transaction. The issuer may strip the TCVV PC from the TPAN obtaining the original PAN.

The HSM *ValidateCVV* function receives as an input the cryptographic CVK2 key, the PAN, the Expiry Date and the Service Code. With these fields the HSM calculates the expected CVV and if equal to the input field TCVV then it gives a positive response indicating that the TCVV is the correct one.

ValidateCVV(TCVV, CVK2, PAN, ED, SC)

The Service Code to be used in this function is obtained from TCVV PC stripped from the TPAN, as in the issuer data preparation phase:

Service Code = TCVV PC = 0 || x || y

The remainder of the transaction processing continues as in a normal CVV2 transaction with the result being returned to the merchant with no extra changes.

Example

Let us assume that the issuer receives a transaction with the following values:

Transaction Data

TPAN = 1234 5678 9876 5432 032
Expiry Date = 1299
TCVV = 890

Given the fact that the BIN 123456 has 16 digit long PANs and that the received PAN is 19 digits long the Issuer will know that this is an Enhanced CVV transaction and that the received PAN is a transformed TPAN.

The TCVV PC will be obtained by extracting the 16th, 17th and 18th digits of the TPAN. By stripping the TPAN of the last three digits the issuer will be left with the 16 digits that constitute the original PAN.

TPAN = PAN || TCVV PC
TPAN = 1234 5678 9876 5432 032
PAN = 1234 5678 9876 5432
TCVV PC = 032

In this case the Service Code used for the ValidateCVV function will have the value 032:

Service Code = TCVV PC = 032

Finally the TCVV shall be validated through the following function call:

ValidateCVV (CVV, CVK, PAN, Expiry Date, Service Code)
ValidateCVV (890, CVK, 1234 5678 9876 5432, 1299, 032)

5.5 Long CVV implementation for non 3-D Secure Merchant

A non 3-D Secure merchant wanting to adhere to the Long CVV scheme may follow one of two strategies.

a) Adhere to the 3-D scheme integrating a standard MPI, benefitting of liability shifts, and no further effort is necessary.

b) If the merchant opts not to adhere to 3-D Secure he may implement minor modifications to his checkout process in order to support the Long CVV scheme. The issuer will have to likewise implement minor changes to the transaction authorisation process.

The Issuer card data preparation and the personalisation process is the same as described before. This section describes the modification the non 3-D Secure merchant has to implement and that the issuer has to implement to support the Long CVV scheme.

- Merchant checkout process
- Issuer authorisation process

5.5.1 Merchant checkout process

The merchant, at the moment of transaction, shall prompt the cardholder for three digits of the ***n*** digits that constitute the LCVV. The number of possible permutations of three positions out of a possible ***n*,** that the merchant can request for, can be calculated as follows:

$$P_3^n = \frac{n!}{3!(n-3)!}$$

For each transaction the merchant shall generate a random value between 1 and P_3^n in order to determine which permutation of the LCVV digits will be used for the transaction. Let us call this generated number, the Transaction CVV Positions Code (TCVV PC). This value shall represent a determined permutation that can be looked up in a permutations table. A permutation of the three positions of the LCVV that will be requested, can be represented by the values ***s***, ***t*** and ***u*** and these values shall be in accordance with the following restrictions:

$$1 \leq s < t < u \leq n$$

The permutations table shall have a TCVV PC that varies from 1 to P_3^n with the corresponding permutation of ***s***, ***t*** and ***u*** values.

It is recommended the merchant always generate the same values for each card so that in case of compromise of a merchant’s systems, the attackers will know only one TCVV.

The merchant shall prompt the cardholder for the three digits of the LCVV in the positions ***s***, ***t*** and ***u***. Theses three digits shall be the TCVV for this transaction.

$$TCVV = Cs, Ct, Cu$$

The Merchant shall send the TCVV in substitution of the CVV2 along with the rest of the payment data to the issuer. So that the issuer knows which CVV is being used for this transaction it must also send the TCVV PC.

The same technique used for the MCVV implementation will be used thus the TCVV PC shall be incorporated into the PAN thus forming a TPAN:

TPAN[19] = PAN[16] || TCVV PC[3]

The merchant shall send this value to the acquirer in order for it to be forwarded to the card issuer.

Note that if the number of LCVV digits is 20, the number of permutations is higher than 1000 and therefor the three digits of the TCVV PC are insufficient. If in fact 20 or more digits are chosen for the size of the LCVV then the number of permutations may be reduced. As an example permutations where the 1st and 2nd digits are consecutive may be excluded, taking care however to maintain an equal probability of each number occurring.

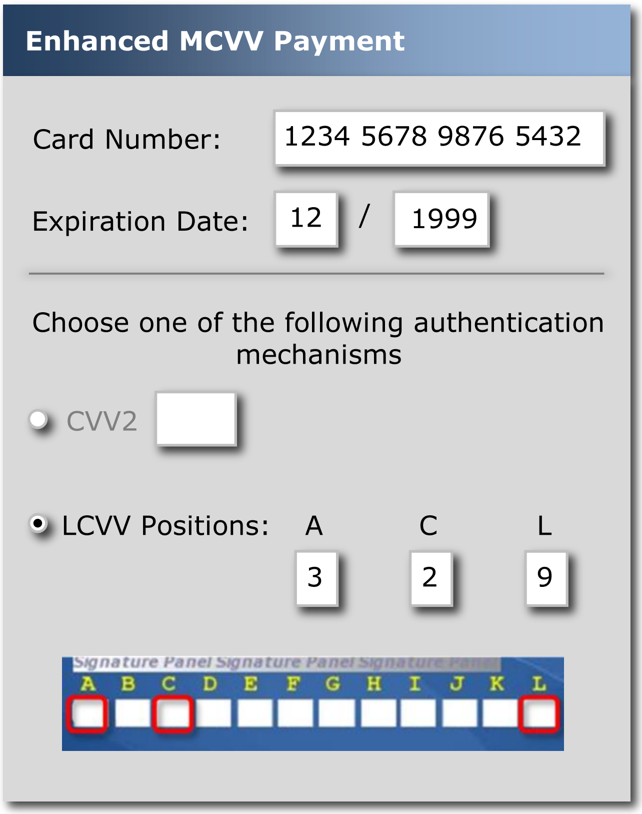
Example

At the moment of transaction the merchant shall prompt the user for three digits that will constitute the CVV for this transaction (TCVV). Given the fact that there are 220 possible permutations of three digits out of a possible 12, the merchant shall generate a random number between 1 and 220 that represents the TCVV PC and will index the following permutations table in order to know what digit positions to request the cardholder:

TCVV PC	*s*	*t*	*u*
001	1	2	3
002	1	2	4
003	1	2	5
004	1	2	6
005	1	2	7
006	1	2	8
007	1	2	9
008	1	2	10
009	1	2	11
010	1	2	12
011	1	3	4
012	1	3	5
013	1	3	6
014	1	3	7
015	1	3	8
016	1	3	9
017	1	3	10
018	1	3	11
019	1	3	12
020	1	4	5
021	1	4	6
022	1	4	7
023	1	4	8
024	1	4	9
025	1	4	10
026	1	4	11
027	1	4	12
028	1	5	6
029	1	5	7
030	1	5	8
…			
214	8	10	11
215	8	10	12
216	8	11	12
217	9	10	11
218	9	10	12
219	9	11	12
220	10	11	12

Table 5.1 – TCVV PC table and respective permutation example

Let us assume that the generated TCVV PC is 19. In this case the merchant shall request the digits in positions 1, 3 and 12:



Enhanced MCVV Payment

Card Number: 1234 5678 9876 5432

Expiration Date: 12 / 1999

Choose one of the following authentication mechanisms

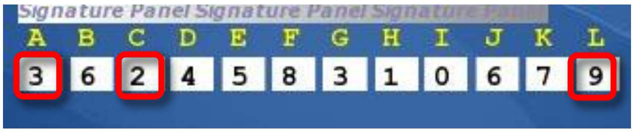
○ CVV2

● LCVV Positions:

A	C	L
3	2	9

Figure 5.13 – Checkout with LCVV example

The cardholder shall introduce the 1st, 3rd and 12th digits of the LCVV thus producing a TCVV with the value 329.



A	B	C	D	E	F	G	H	I	J	K	L
3	6	2	4	5	8	3	1	0	6	7	9

Figure 5.14 – LCVV example

The merchant shall incorporate the TCVV PC into the PAN producing the following TPAN.

Let us assume a card with PAN equal to 1234 5678 9876 5432.

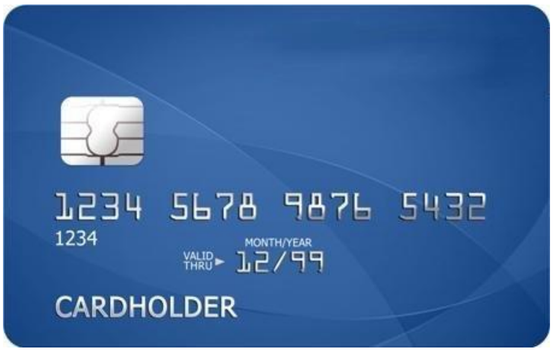


Figure 5.15 – ECVV card front example

Inputs

PAN = 1234 5678 9876 5432
TCVV PC = 019

TPAN construction

TPAN[19] = PAN[16] || TCVV PC[3]
TPAN =1234 5678 9876 5432 || 019

5.5.2 Issuer authorisation

The issuer upon reception of a 19 digit long PAN for a BIN that holds 16 digit long PANs will have knowledge that the transaction was performed by an Enhanced CVV capable merchant and therefore is in presence of an Enhanced CVV transaction. The issuer may strip the TCVV PC from the TPAN obtaining the original PAN.

If the card number is an Enhanced CVV prepared card, the issuer will validate the TCVV by validating it in accordance with the information identified in the TCVV PC otherwise it will perform a traditional CVV2 validation.

The validation of the TCVV shall be performed by comparing the TCVV with the digits of the LCVV in the positions coded by the TCVV PC.

The issuer will have to lookup the permutations table at the row indicated by the TCVV PC thus obtaining the values ***s***, ***t*** and ***u***.

s = Permutations Table [TCVV PC].s

t = Permutations Table [TCVV PC].t

u = Permutations Table [TCVV PC].u

The issuer shall reproduce the LCVV through an HSM deterministic function. The TCVV shall be validated through the comparison of the digits in the positions ***s***, ***t*** and ***u***.

```
if (
  Reproduced LCVV[s] = TCVV[1] and
  Reproduced LCVV[t] = TCVV[2] and
  Reproduced LCVV[u] = TCVV[3]
) then TCVV ok
```

The remainder of the transaction processing shall continue as in a normal CVV2 transaction with the result being returned to the merchant with no further changes.

Example

Let us assume that the issuer receives a transaction with the following values:

Transaction Data

TPAN = 1234 5678 9876 5432 019
Expiry Date = 1299
TCVV = 329

Given the fact that the BIN 123456 has 16 digit long PANs and that the received PAN is 19 digits long the Issuer will know that this is an Enhanced CVV transaction and that the received PAN is a transformed TPAN.

The TCVV PC will be obtained by extracting the 16th, 17th and 18th digits of the TPAN. By stripping the TPAN of the last three digits the issuer will be left with the 16 digits that constitute the original PAN.

TPAN = PAN || TCVV PC
TPAN = 1234 5678 9876 5432 019
PAN = 1234 5678 9876 5432
TCVV PC = 019

*The issuer shall look up the permutations table at row indicated by the TCVV PC and will find the values of 1, 3 and 12 for **s**, **t** and **u**.*

TCVV PC	*s*	*t*	*u*
019	1	3	12

Table 5.2 – LCVV PC table entry example

s = Permutations Table [TCVV PC].s = 1
t = Permutations Table [TCVV PC].t = 3
u = Permutations Table [TCVV PC].u = 12

The issuer shall reproduce the LCVV for this card through the use of a deterministic HSM function. Finally the TCVV shall be validated through the comparison of the 1st

2nd and 3rd digits of the received TCVV with the 1st, 3rd and 12th digits respectively of the Reproduced LCVV.

Reproduced LCVV[2] = TCVV[1] = 3
Reproduced LCVV[3] = TCVV[2] = 2
Reproduced LCVV[8] = TCVV[3] = 9

Chapter 6: Enhanced CVV2 scheme security analysis

6.1 Introduction

Card based e-payments have suffered due to cyber attacks that have threatened the security of this means of payments. Card data compromises have occurred through the penetration of merchant systems and processors systems. Likewise millions of end user systems have been compromised through malware exploiting the constant disclosure of vulnerabilities on popular software. Theses compromises have led to the theft of hundreds of millions of card data elements and have led to billions of dollars in fraud.

The proposed scheme’s main contribution is to maintain the essential balance of characteristics, enhancing however security in order to mitigate threats resulting from card data compromise.

6.1.1 Chapter overview

In this section the two implementations of Enhanced CVV2s are analysed on a security level so as to attain the resistance to data compromise attacks.

We firstly describe actual relevant attacks, and then give an introduction to the Coupon Collectors Problem that serves as a basis for an analysis to the security level. Finally the probability of guessing a TCVV function of the number of compromised transactions is formulated for each of the proposed methods and the security robustness of the methods are compared.

6.2 Attack scenarios

In recent years a vast quantity of card transaction data has been compromised through compromised computers hijacked into botnets, merchant, acquirer and service providers database compromises and communication interceptions. Many of these attacks have compromised card numbers, expiration dates and CVV2s. With these captured elements, the attackers may perform fraudulent payments on the majority of Card Not Present payment accepting merchants.

These types of attacks are the most severe on card payments history resulting in many hundreds of millions of cards having been compromised (1).

The international payment schemes have mandated PCI DSS certification towards processors and merchants storing, processing or communicating card data in order to protect against these types of attacks. Although these data protection requirements are a valuable set of principles, some of the attacked parties were at the time of attack PCI DSS certified. These facts suggest that although PCI DSS certification holds a basis for protecting data it is by no means enough given that the static CVV2 mechanism, once compromised, offers no resistance to these types of attacks.

6.2.1 Data Breaches

Compromising data at merchant, acquirer or payment processing systems usually results in the collection of large numbers of records. The state in which data existed at the moment of compromise may be summarized into: stored, transmitted or processed. Investigation reports [7] reveal that compromise of card data in transit seems to be uncommon and that most intrusions make use of stored data and, at a lesser degree, whilst being processed.

Avoiding storage of card data, or storing data in encrypted form, in line with the PCI DSS principles, contributes towards minimizing the probability of compromising data. Many PCI DSS certified organizations, however, have seen their data at rest compromised due to deficient implementations or storage of data on secondary support systems. When databases are compromised these may hold data prior to the date of intrusion and may expose large quantities of data. Given that most cards are valid for a couple of years, historical data in databases may still hold considerable quantities of valid data.

Compromise of data during processing will normally imply that the transaction is taking place. In this case the scope of compromised data will grow with the period of compromise although the rate of growth will decrease given that returning cards will not increment the number of distinct compromised cards.

Compromise actions take efforts to avoid detection and tend to use compromised data only after reeking a number of records rendered sufficient by the attackers. When fraudulent usage takes place, fraud detection systems detect abnormal spending patterns and are quick to determine the common point of purchase.

Given the static nature of traditional payment credentials the harvested data will be useful for subsequent fraudulent payments having as a limiting factor the lifetime of the card defined by the card expiry date. Payments at 3-D Secure merchants are however protected from the fraudulent usage of this compromised data given that the cardholder authentication credentials are collected directly by the issuer through a different channel. Fraudsters avoid performing transactions at 3-D Secure merchants and so choose on of the many merchants not adhering to the 3-D Secure protocol.

As a conclusion data breaches continue to occur exploiting an everlasting stream of vulnerabilities, and fraudulent usage is facilitated given the low adoption of the 3-D Secure protocol.

6.2.2 Botnets

Compromises of end-user systems reveal the credentials of payments performed through the user's computer; usually a single card is compromised. The cyber crime industry has evolved in recent years and is a well-tuned industry covering all aspects of a sophisticated value chain.

The search for zero-day vulnerabilities is constant and organized groups pay for these disclosures in order to circumvent anti-virus protections that are unaware of these exploits. Malware packages have grown in sophistication and little knowledge is necessary to incorporate an exploit into these malware packages. Millions of computers are hijacked into botnets and thus are under total control of cybercriminals. Botnets are commercialized via the sale or rental of botnet controlled systems. Botnets search the Internet for vulnerable systems harvesting evermore systems into the botnets. Simultaneously these malware-infected systems reek any valuable at the end users systems, such as card numbers and 3-D secure passwords. Botnet command and control systems collect vast quantities of harvested data and proceed to filtering and subsequent sale of batches of information at chat rooms or other forum. Finally actors spread out at a global level acquire these batches of card credentials and make fraudulent usage of these cards at e-merchants.

Given the massive number of botnet-hijacked [45] computers and the sophistication of tools to manage these enormous fleets and corresponding harvested data millions of cards are presently compromised through these means. The malware may collect card numbers, expiry dates and CVVs but it may also collect 3-D Secure credentials such as passwords. By doing so the fraudster may perform payments at any card-accepting merchant be it 3-D Secure or not. In the case where the issuer has adopted an authentication of dynamic nature such as SMS tokens or one-time-password calculators the fraudster will have to make use of the card credentials at non 3-D Secure merchants given that the 3-D Secure credentials expire after usage.

As a conclusion compromise through botnet controlled end-user systems continues to occur revealing vast quantity of credentials. 3-D secure adoption with static passwords is ineffective in these cases and permits the criminals to make use of the stolen credentials at merchants with or without 3-D Secure adoption. If the 3-D Secure protected cards use dynamic credentials, the fraudulent usage of the card details will have to be carried out on non 3-D Secure merchants.

6.3 Mathematical background

The classical Coupon Collector’s Problem determines the expected number of trials to collect a complete set of ***n*** coupons [35].

Many studies have since developed upon this initial problem [37] [38] [39] [40] such as determining the number of ***m*** complete sets of ***n*** coupons [36] or determining the number of trials given ***d*** coupons at each trial and choosing the one that has been drawn the least times so far [41].

In this security analysis we are equally in a presence of a Coupon Collector's Problem. The cardholder will be in possession of a set of secrets (coupons) and for each transaction (trial) a request for a randomly chosen secret will be made. We will calculate the probability that an attacker has in performing a valid transaction after he has knowledge of a set of previous transactions and therefore has information on part of the secret.

6.3.1 MCVV Coupon Collectors Problem

The security analysis of the MCVV scheme makes use of the Coupon Collector's Problem with the particularity that each coupon has a three digit random number written on it. After a certain number of trials, where one random coupon is drawn in each trial, we calculate the probability that the collector may guess the three digits of a randomly queried coupon.

Mapping the Coupons Collector problem to the MCVV scheme we have that the ***n*** coupons (number of CVVs in the MCVV matrix), constitute the collection and at each trial (transaction) a sample (***d=1***) will be drawn. A collector (attacker) will have knowledge of the contents of the drawn coupons during the ***t*** trials (compromised transactions). We will then calculate the probabilities that in a subsequent trial (the attack transaction) the collector will have in drawing a coupon in which: 1) the coupon has already been collected, 2) the coupon hasn’t been collected and therefore is unknown to the collector. With the probabilities calculated for these two situations, we finally have the basis to calculate the probability that an attacker will have in guessing the TCVV. If the attacker has knowledge of the MCVV position’s CVV he will authenticate the transaction otherwise he has a one in a thousand chance to correctly guess the three-digit TCVV.

6.3.2 LCVV Coupon Collectors Problem

The security analysis of the LCVV scheme is supported on the Coupon Collector's Problem with the particularity that at each trial three random coupons without repetition are drawn. Four situations may arise in respect to the number of drawn coupons that coincide with previously drawn coupons: none, one, two or all three of the drawn coupons may coincide, thus be already known to the collector. The objective is to determine the probability of each situation after a given number of ***t*** trials have occurred and subsequent trial is to take place.

Mapping the Coupons Collector problem to the LCVV scheme we have that the ***n*** coupons (number of positions of the LCVV), constitute the collection and at each trial (transaction) a sample of three coupons (***d=3***) will be drawn. A collector (attacker) will have knowledge of the contents of each of the drawn coupons during the ***t*** trials (compromised transactions). We will then calculate the probabilities that in a subsequent trial (the attack transaction) the collector will have in drawing three coupons in which: 1) all three have already been collected, 2) two have been collected, 3) only one has been collected or 4) none are yet known to the collector.

With the probabilities calculated for each of these four situations, we finally have the basis to calculate the probability that an attacker will have in guessing the three decimal digits of a TCVV, having knowledge of the known positions and having a one in ten chance of correctly guessing each position still unknown to him.

6.4 Multiple CVV guessing probability

The objective of this security analysis is to determine, for each MCVV matrix size, the probability that an attacker has in successfully guessing the TCVV after having had access to a number of compromised transactions of the same bank card at different merchants.

The proposed MCVV implementation introduces a dynamic nature to the authentication of CNP transactions reducing the probability of success for subsequent fraudulent transactions. In this section we will calculate the probability that an attacker will guess the right TCVV after having compromised ***t*** transactions.

In a MCVV implementation ***n*** represents the number of MCVV matrix positions. After a number ***t*** of compromised transactions of the same bank card at different merchants, the attacker has knowledge of a number of positions of the matrix (hereafter referred to as MCVV positions) and corresponding values.

6.4.1 Expected number of known MCVV positions after *t* transactions

Let X denote the number of different MCVV positions in the set of $\boldsymbol{t}$ transactions. The expected number of different MCVV positions can be presented by *E[X]*.

Let X_i be the variable that indicates that the *i*th position of the MCVV matrix was eavesdropped in any of the previous ***t*** transactions.

$$\boldsymbol{X_i} = \begin{cases} \mathbf{0}, & \boldsymbol{if\ the\ MCVV\ at\ position\ i\ hasn't\ been\ used} \\ & \boldsymbol{in\ any\ of\ the\ t\ compromised\ transactions} \\ \mathbf{1}, & \boldsymbol{otherwise} \end{cases} \qquad (1)$$

Therefore

$$\boldsymbol{E}[\boldsymbol{X_i}] = \boldsymbol{P}\{\boldsymbol{X_i} = \mathbf{1}\} = \mathbf{1} - \boldsymbol{P}\{\boldsymbol{X_i} = \mathbf{0}\}\,. \qquad (2)$$

Given that, at each compromised transaction, the probability for *i*th position not to be used is $\frac{\mathrm{n}-1}{\mathrm{n}}$, and assuming independency on transactions, then

$$\boldsymbol{P}\{\boldsymbol{X_i} = \mathbf{0}\} = \left(\frac{\boldsymbol{n}-\mathbf{1}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} \qquad (3)$$

therefore

$$\boldsymbol{E}[\boldsymbol{X_i}] = \mathbf{1} - \left(\frac{\boldsymbol{n}-\mathbf{1}}{\boldsymbol{n}}\right)^{\boldsymbol{t}}. \qquad (4)$$

Note that,

$$\boldsymbol{X} \;=\; \boldsymbol{X_1} + \boldsymbol{X_2} + \cdots + \boldsymbol{X_n} \qquad (5)$$

and therefore

$$\boldsymbol{E}[\boldsymbol{X}] = \boldsymbol{E}[\boldsymbol{X_1}] + \boldsymbol{E}[\boldsymbol{X_2}] + \cdots + \boldsymbol{E}[\boldsymbol{X_n}] \qquad (6)$$

$$\boldsymbol{E}[\boldsymbol{X}] = \boldsymbol{n}\left[\mathbf{1} - \left(\frac{\boldsymbol{n}-\mathbf{1}}{\boldsymbol{n}}\right)^{\boldsymbol{t}}\right]. \qquad (7)$$

The following table gives the average number of known MCVV positions after ***t*** transactions.

	n	MCVV matrix size										
t		10	11	12	13	14	15	16	17	18	19	20
Number of transactions	1	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00
	2	1,90	1,91	1,92	1,92	1,93	1,93	1,94	1,94	1,94	1,95	1,95
	3	2,71	2,74	2,76	2,78	2,79	2,80	2,82	2,83	2,84	2,84	2,85
	4	3,44	3,49	3,53	3,56	3,59	3,62	3,64	3,66	3,68	3,70	3,71
	5	4,10	4,17	4,23	4,29	4,33	4,38	4,41	4,45	4,47	4,50	4,52
	6	4,69	4,79	4,88	4,96	5,03	5,08	5,14	5,18	5,23	5,26	5,30
	7	5,22	5,36	5,47	5,58	5,67	5,75	5,82	5,88	5,94	5,99	6,03
	8	5,70	5,87	6,02	6,15	6,26	6,36	6,45	6,53	6,61	6,67	6,73
	9	6,13	6,33	6,52	6,67	6,81	6,94	7,05	7,15	7,24	7,32	7,40
	10	6,51	6,76	6,97	7,16	7,33	7,48	7,61	7,73	7,84	7,94	8,03

Table 6.1 – Average number of known MCVV matrix positions after *t* transactions

The following figure shows a graphical evolution of the average number of known MCVV positions after ***t*** transactions for matrix sizes of 10 to 20.

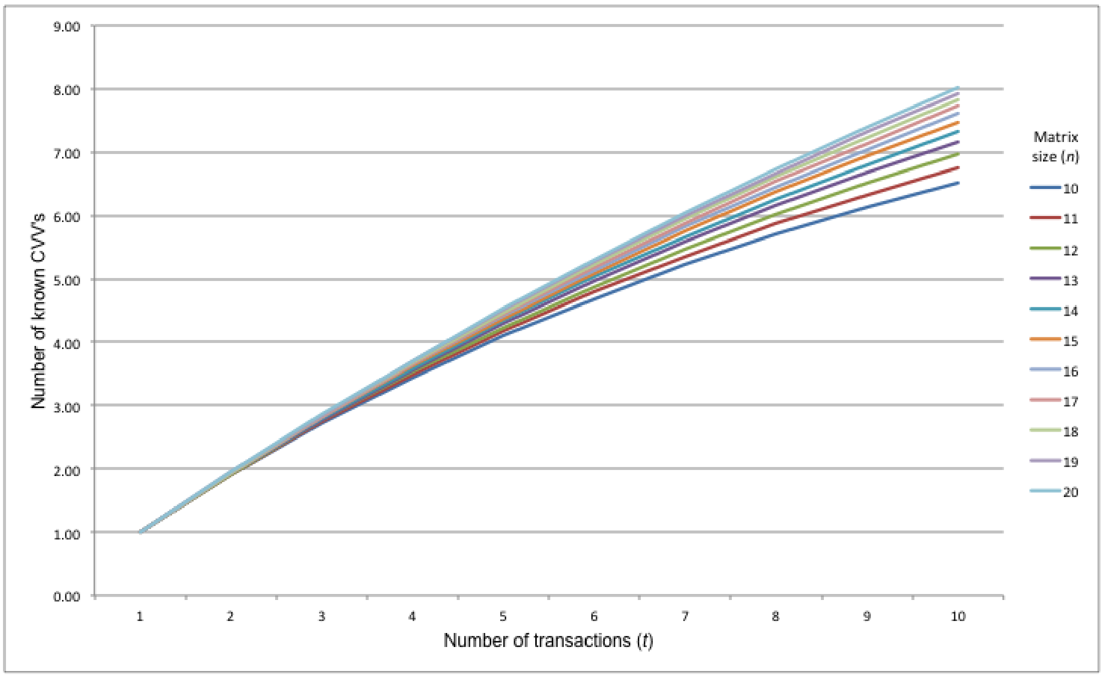


Figure 6.1 – Average number of known MCVV positions after *t* transactions

6.4.2 Probability of occurrence of situations of coinciding positions

After eavesdropping ***t*** transactions the attacker will try to guess the prompted MCVV position. Two situations may occur at this point: the prompted MCVV position is that of a known position $(\mathrm{y}=1)$, or the prompted MCVV position is unknown to the attacker $(y=0)$.

The probability of the prompted MCVV position being known is equal to the average number of known MCVV positions over the total number of MCVV positions.

$$\boldsymbol{P}_{\boldsymbol{O}(\boldsymbol{y}=\mathbf{1})}=\frac{\boldsymbol{E}[\boldsymbol{X}]}{\boldsymbol{n}} \tag{8}$$

$$\boldsymbol{P}_{\boldsymbol{O}(\boldsymbol{y}=\mathbf{1})}=\mathbf{1}-\left(\frac{\boldsymbol{n}-\mathbf{1}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} \tag{9}$$

The probability of the MCVV position not being known is:

$$\boldsymbol{P}_{\boldsymbol{O}(\boldsymbol{y}=\mathbf{0})}=\left(\frac{\boldsymbol{n}-\mathbf{1}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} \tag{10}$$

Following is a table with the probability of the drawn MCVV position being a known $(y=1)$ or unkown $(y=0)$ position, function of the number of transactions and the size ($\boldsymbol{n}$) of the MCVV matrix.

			n	MCVV matrix size										
y		t		10	11	12	13	14	15	16	17	18	19	20
Coinciding CVV	1	Number of transactions	1	10,0%	9,1%	8,3%	7,7%	7,1%	6,7%	6,3%	5,9%	5,6%	5,3%	5,0%
			2	19,0%	17,4%	16,0%	14,8%	13,8%	12,9%	12,1%	11,4%	10,8%	10,2%	9,8%
			3	27,1%	24,9%	23,0%	21,3%	19,9%	18,7%	17,6%	16,6%	15,8%	15,0%	14,3%
			4	34,4%	31,7%	29,4%	27,4%	25,7%	24,1%	22,8%	21,5%	20,4%	19,4%	18,5%
			5	41,0%	37,9%	35,3%	33,0%	31,0%	29,2%	27,6%	26,1%	24,9%	23,7%	22,6%
			6	46,9%	43,6%	40,7%	38,1%	35,9%	33,9%	32,1%	30,5%	29,0%	27,7%	26,5%
			7	52,2%	48,7%	45,6%	42,9%	40,5%	38,3%	36,3%	34,6%	33,0%	31,5%	30,2%
			8	57,0%	53,3%	50,1%	47,3%	44,7%	42,4%	40,3%	38,4%	36,7%	35,1%	33,7%
			9	61,3%	57,6%	54,3%	51,3%	48,7%	46,3%	44,1%	42,1%	40,2%	38,5%	37,0%
			10	65,1%	61,4%	58,1%	55,1%	52,3%	49,8%	47,6%	45,5%	43,5%	41,8%	40,1%
	0	Number of transactions	1	90,0%	90,9%	91,7%	92,3%	92,9%	93,3%	93,8%	94,1%	94,4%	94,7%	95,0%
			2	81,0%	82,6%	84,0%	85,2%	86,2%	87,1%	87,9%	88,6%	89,2%	89,8%	90,3%
			3	72,9%	75,1%	77,0%	78,7%	80,1%	81,3%	82,4%	83,4%	84,2%	85,0%	85,7%
			4	65,6%	68,3%	70,6%	72,6%	74,3%	75,9%	77,2%	78,5%	79,6%	80,6%	81,5%
			5	59,0%	62,1%	64,7%	67,0%	69,0%	70,8%	72,4%	73,9%	75,1%	76,3%	77,4%
			6	53,1%	56,4%	59,3%	61,9%	64,1%	66,1%	67,9%	69,5%	71,0%	72,3%	73,5%
			7	47,8%	51,3%	54,4%	57,1%	59,5%	61,7%	63,7%	65,4%	67,0%	68,5%	69,8%
			8	43,0%	46,7%	49,9%	52,7%	55,3%	57,6%	59,7%	61,6%	63,3%	64,9%	66,3%
			9	38,7%	42,4%	45,7%	48,7%	51,3%	53,7%	55,9%	57,9%	59,8%	61,5%	63,0%
			10	34,9%	38,6%	41,9%	44,9%	47,7%	50,2%	52,4%	54,5%	56,5%	58,2%	59,9%

Table 6.2 – Probability of occurrences of coinciding MCVV positions

The following figure shows the probability of a coinciding MCVV matrix position being drawn function of the matrix size after a given number of ***t*** transactions being compromised.

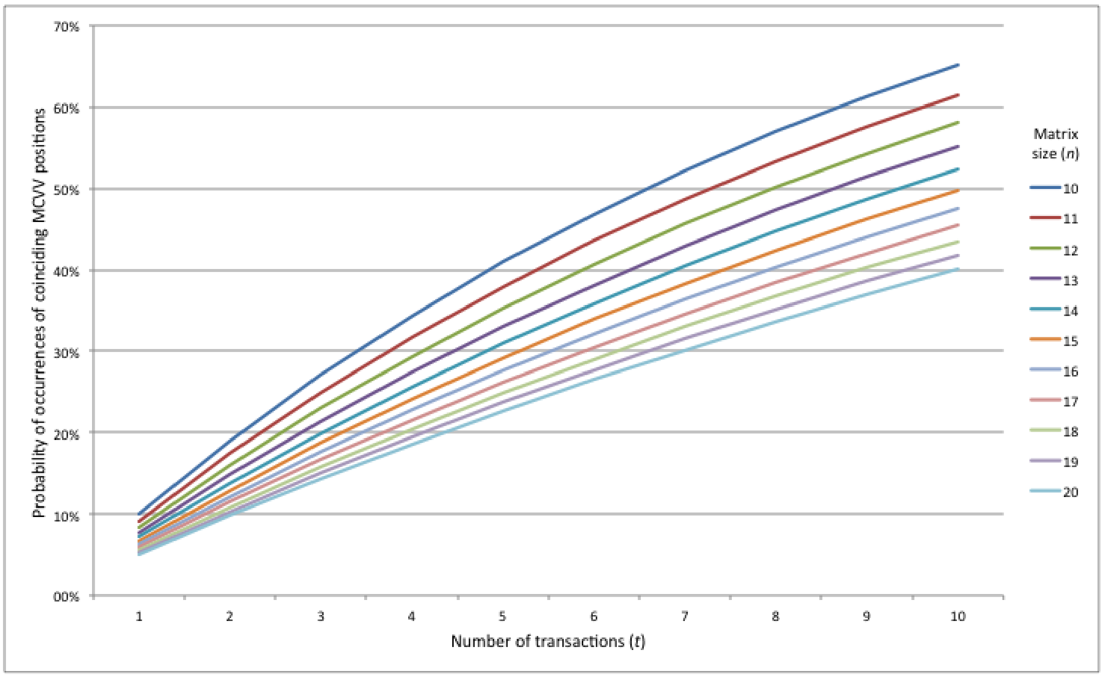


Figure 6.2 – Probability of occurrences of coinciding MCVV positions

6.4.3 Guessing probability for situations of coinciding positions

Having calculated the probability of occurrence of each situation let us now calculate the probability of guessing the correct TCVV in each of the situations.

The probability of successfully guessing the correct TCVV is absolute if the attacker knows the MCVV position:

$$\boldsymbol{P_{G(y=1)} = 1} \tag{11}$$

On the other hand if the prompted MCVV position is unknown to the attacker the probability in successfully guessing the correct TCVV, and given that the TCVV is a three decimal digit number, is:

$$\boldsymbol{P_{G(y=0)} = 10^{-3}} \tag{12}$$

6.4.4 TCVV guessing probability

We may conclude that the probability that an attacker has in successfully guessing the TCVV ($P_{G(T=t)}$) after having had access to $\boldsymbol{t}$ compromised transactions with CVVs from a MCVV matrix with $\boldsymbol{n}$ positions is given by the following formula:

$$\boldsymbol{P_{G(T=t)}} = \left(\boldsymbol{P_{O(y=1)}} \times \boldsymbol{P_{G(y=1)}}\right) + \left(\boldsymbol{P_{O(y=0)}} \times \boldsymbol{P_{G(y=0)}}\right) \tag{13}$$

$$P_{G(T=t)} = 1 - 0.999\left(\frac{n-1}{n}\right)^{t} \tag{14}$$

The following table shows the guessing probability after t transactions for MCVV matrixes with n CVVs:

	n	MCVV matrix size										
t		10	11	12	13	14	15	16	17	18	19	20
Number of transactions	1	10,09%	9,18%	8,43%	7,78%	7,24%	6,76%	6,34%	5,98%	5,65%	5,36%	5,10%
	2	19,08%	17,44%	16,06%	14,88%	13,86%	12,98%	12,20%	11,51%	10,89%	10,34%	9,84%
	3	27,17%	24,94%	23,05%	21,43%	20,01%	18,78%	17,68%	16,71%	15,84%	15,06%	14,35%
	4	34,46%	31,77%	29,46%	27,47%	25,73%	24,19%	22,83%	21,61%	20,52%	19,53%	18,63%
	5	41,01%	37,97%	35,34%	33,05%	31,03%	29,25%	27,65%	26,22%	24,93%	23,76%	22,70%
	6	46,91%	43,61%	40,73%	38,20%	35,96%	33,96%	32,17%	30,56%	29,10%	27,78%	26,56%
	7	52,22%	48,74%	45,67%	42,95%	40,53%	38,37%	36,41%	34,65%	33,04%	31,58%	30,24%
	8	57,00%	53,40%	50,20%	47,34%	44,78%	42,47%	40,39%	38,49%	36,76%	35,18%	33,72%
	9	61,30%	57,63%	54,35%	51,39%	48,73%	46,31%	44,11%	42,11%	40,28%	38,59%	37,04%
	10	65,17%	61,48%	58,15%	55,13%	52,39%	49,89%	47,61%	45,52%	43,59%	41,82%	40,19%

Table 6.3 – MCVV guessing probability $\left(P_{G(\mathrm{T=t})}\right)$

The following graph compares the strength of the various n sized matrix tables towards a guessing attack after t compromised transactions.

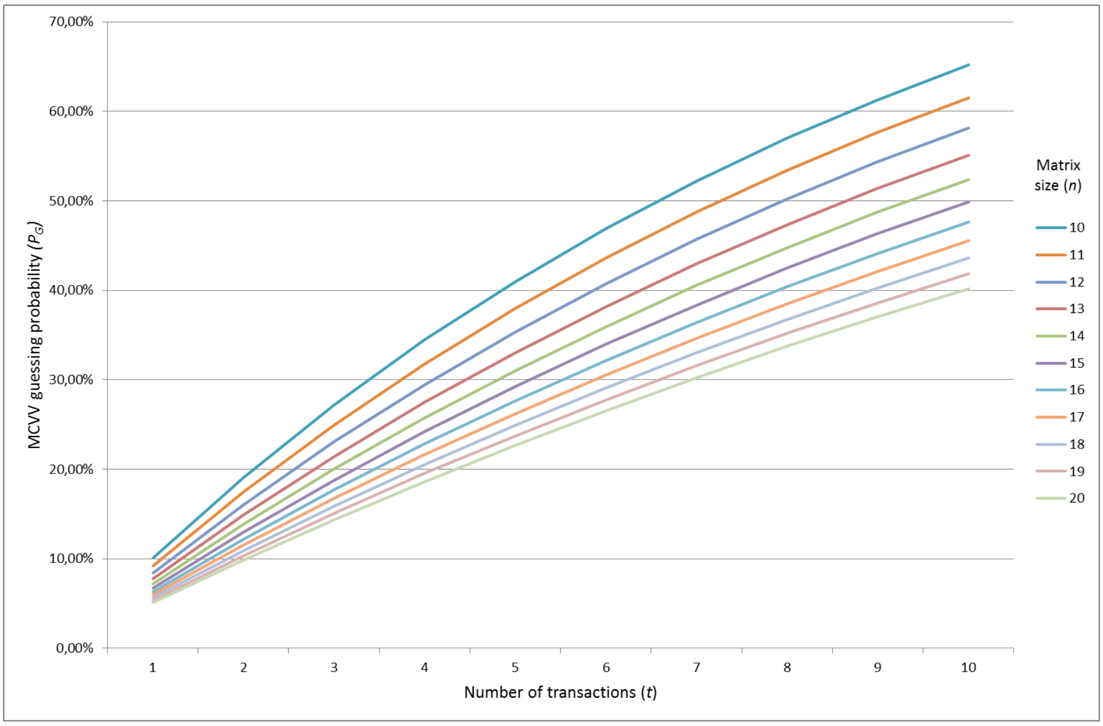


Figure 6.3 – MCVV guessing probability $\left(P_{G(\mathrm{T=t})}\right)$

6.5 Long CVV guessing probability

The objective of this security analysis is to determine, for each LCVV length, the probability that an attacker has in successfully guessing the TCVV after having compromised a number of transactions of the same card at different merchants.

The proposed LCVV introduces a dynamic nature to the authentication of CNP transactions reducing the probability of success for subsequent fraudulent transactions. In this section we will calculate the probability that an attacker will guess the right TCVV after having compromised ***t*** transactions.

In a LCVV implementation ***n*** represents the length of LCVV. After a number of ***t*** compromised transactions of the same credit card performed at different merchants, the attacker has knowledge of a certain number of positions of the LCVV (hereafter referred to as LCVV positions) and corresponding values.

6.5.1 Expected number of known LCVV positions after *t* transactions

Let *X* denote the number of distinct LCVV positions in the set of ***t*** transactions. The expected number of distinct LCVV positions can be presented by *E[X]*.

Let X_i be the variable that indicates that the i^{th} position of the LCVV was eavesdropped in any of the previous ***t*** transactions.

$$\boldsymbol{X_i} = \begin{cases} \mathbf{0}, & \boldsymbol{if\ the\ i^{th}\ position\ of\ the\ LCVV\ hasn't\ been\ used} \\ & \boldsymbol{in\ any\ of\ the\ t\ compromised\ transactions} \\ \mathbf{1}, & \boldsymbol{otherwise} \end{cases} \tag{15}$$

Therefore

$$\boldsymbol{E}[\boldsymbol{X_i}] = \boldsymbol{P}\{\boldsymbol{X_i} = \mathbf{1}\} = \mathbf{1} - \boldsymbol{P}\{\boldsymbol{X_i} = \mathbf{0}\} \tag{16}$$

Given that, for each compromised transaction three distinct positions will be drawn, the probability for i^{th} position not to be drawn is $\frac{\mathrm{n}-3}{\mathrm{n}}$, and assuming independency on transactions, then

$$\boldsymbol{P}\{\boldsymbol{X_i} = \mathbf{0}\} = \left(\frac{\boldsymbol{n} - \mathbf{3}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} \tag{17}$$

therefore

$$\boldsymbol{E}[\boldsymbol{X_i}] = \mathbf{1} - \left(\frac{\boldsymbol{n}-\mathbf{3}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} \tag{18}$$

Note that,

$$\boldsymbol{X} \;=\; \boldsymbol{X_1} + \boldsymbol{X_2} + \cdots + \boldsymbol{X_n} \tag{19}$$

and therefore

$$\boldsymbol{E}[\boldsymbol{X}] = \boldsymbol{E}[\boldsymbol{X_1}] + \boldsymbol{E}[\boldsymbol{X_2}] + \cdots + \boldsymbol{E}[\boldsymbol{X_n}] \tag{20}$$

$$\boldsymbol{E}[\boldsymbol{X}] = \boldsymbol{n}\left[\mathbf{1} - \left(\frac{\boldsymbol{n}-\mathbf{3}}{\boldsymbol{n}}\right)^{\boldsymbol{t}}\right] \tag{21}$$

The following table gives the average number of known LCVV digits after ***t*** transactions.

	n	LCVV length										
t		10	11	12	13	14	15	16	17	18	19	20
Number of transactions	1	3,00	3,00	3,00	3,00	3,00	3,00	3,00	3,00	3,00	3,00	3,00
	2	5,10	5,18	5,25	5,31	5,36	5,40	5,44	5,47	5,50	5,53	5,55
	3	6,57	6,77	6,94	7,08	7,21	7,32	7,42	7,51	7,58	7,65	7,72
	4	7,60	7,92	8,20	8,45	8,66	8,86	9,03	9,18	9,32	9,45	9,56
	5	8,32	8,76	9,15	9,50	9,81	10,08	10,33	10,56	10,77	10,95	11,13
	6	8,82	9,37	9,86	10,31	10,71	11,07	11,40	11,70	11,97	12,22	12,46
	7	9,18	9,82	10,40	10,93	11,41	11,85	12,26	12,63	12,98	13,29	13,59
	8	9,42	10,14	10,80	11,41	11,97	12,48	12,96	13,40	13,81	14,20	14,55
	9	9,60	10,37	11,10	11,77	12,40	12,99	13,53	14,04	14,51	14,95	15,37
	10	9,72	10,54	11,32	12,06	12,74	13,39	13,99	14,56	15,09	15,59	16,06

Table 6.4 – Average number of known LCVV digits after *t* transactions

The following figure shows a graphical evolution of the number of known LCVV digits after ***t*** transactions for LCVV lengths of 10 to 20.

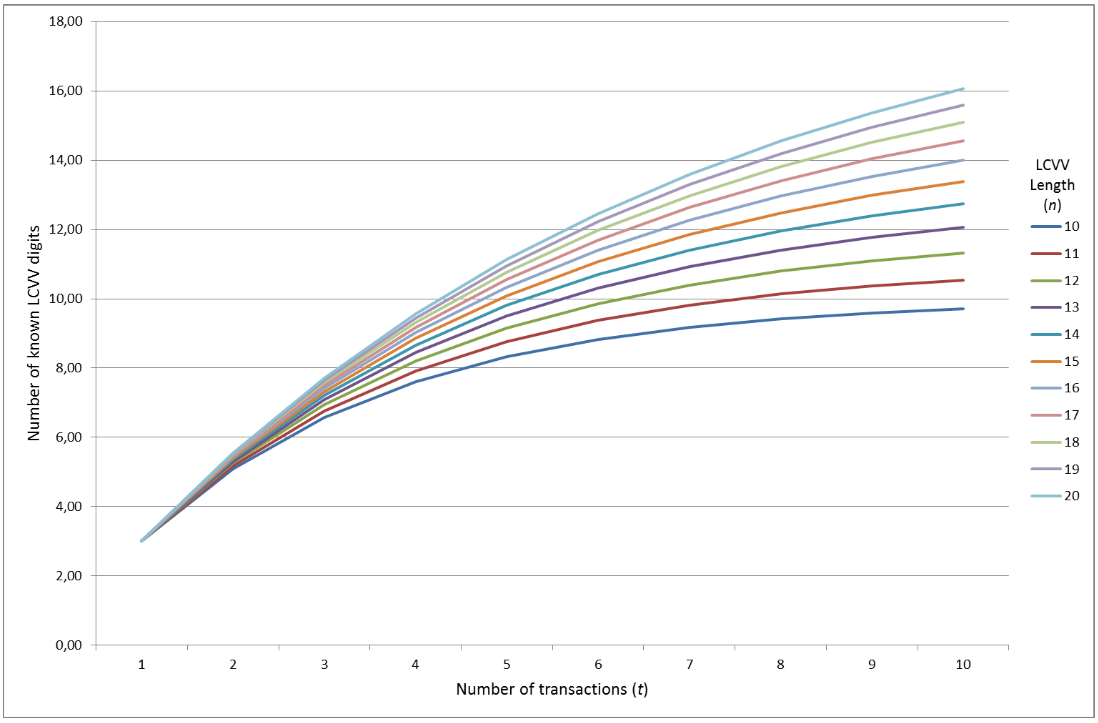


Figure 6.4 – Average number of known LCVV digits after *t* transactions

6.5.2 Probability of occurrence of situations of coinciding positions

After eavesdropping ***t*** transactions the attacker will try to guess the prompted LCVV position in a subsequent transaction. Four situations may occur at this point in respect to the three prompted LCVV positions: None ($y = 0$), one ($y = 1$), two ($y = 2$) or all ($y = 3$) of the requested positions are known to the attacker.

Let $\mathrm{P}_{\mathrm{O(Y=y)}}$ be the probability of occurrence of the situation in which ***y*** positions are known to the attacker.

y=0: None of the digits coincide

$$\boldsymbol{P_{O(Y=0)}} = \left(\frac{\boldsymbol{n - E[X]}}{\boldsymbol{n}}\right) \times \left(\frac{\boldsymbol{n - E[X] - 1}}{\boldsymbol{n - 1}}\right) \times \left(\frac{\boldsymbol{n - E[X] - 2}}{\boldsymbol{n - 2}}\right) \qquad (22)$$

$$\boldsymbol{P_{O(Y=0)}} = \frac{\boldsymbol{(n - E[X]) \times (n - E[X] - 1) \times (n - E[X] - 2)}}{\boldsymbol{n(n - 1)(n - 2)}} \qquad (23)$$

y=1: One digit coincides

$$\begin{aligned}\boldsymbol{P_{O(Y=1)}} = &\left[\left(\frac{\boldsymbol{n-E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{n-E[X]-1}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n-2}}\right)\right]\\ &+\left[\left(\frac{\boldsymbol{n-E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{n-E[X]-1}}{\boldsymbol{n-2}}\right)\right]\\ &+\left[\left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{n-E[X]}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{n-E[X]-1}}{\boldsymbol{n-2}}\right)\right]\end{aligned} \tag{24}$$

$$\boldsymbol{P_{O(Y=1)}} = \boldsymbol{3}\ \frac{\boldsymbol{E[X]\times(n-E[X])\times(n-E[X]-1)}}{\boldsymbol{n(n-1)(n-2)}} \tag{25}$$

y=2: Two digits coincide

$$\begin{aligned}\boldsymbol{P_{O(Y=2)}} = &\left[\left(\frac{\boldsymbol{n-E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{E[X]-1}}{\boldsymbol{n-2}}\right)\right]\\ &+\left[\left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{n-E[X]}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{E[X]-1}}{\boldsymbol{n-2}}\right)\right]\\ &+\left[\left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{E[X]-1}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{n-E[X]}}{\boldsymbol{n-2}}\right)\right]\end{aligned} \tag{26}$$

$$\boldsymbol{P_{O(Y=2)}} = \boldsymbol{3}\ \frac{\boldsymbol{E[X]\times(E[X]-1)\times(n-E[X])}}{\boldsymbol{n(n-1)(n-2)}} \tag{27}$$

y=3: Three digits coincide

$$\boldsymbol{P_{O(Y=3)}} = \left(\frac{\boldsymbol{E[X]}}{\boldsymbol{n}}\right)\times\left(\frac{\boldsymbol{E[X]-1}}{\boldsymbol{n-1}}\right)\times\left(\frac{\boldsymbol{E[X]-2}}{\boldsymbol{n-2}}\right) \tag{28}$$

$$\boldsymbol{P_{O(Y=3)}} = \frac{\boldsymbol{E[X]\times(E[X]-1)\times(E[X]-2)}}{\boldsymbol{n(n-1)(n-2)}} \tag{29}$$

The following formula is a general expression in order to calculate the probability of occurrence of each situation of ***y*** coinciding digits after ***t*** trials have taken place.

$$\begin{gathered}\boldsymbol{P_{O(Y=y)}} = \binom{\boldsymbol{3}}{\boldsymbol{y}}\frac{\prod_{\boldsymbol{i=0}}^{\boldsymbol{y-1}}(\boldsymbol{E[X]-i})\times\prod_{\boldsymbol{i=0}}^{\boldsymbol{3-y-1}}(\boldsymbol{n-i-E[X]})}{\prod_{\boldsymbol{i=0}}^{\boldsymbol{3-1}}(\boldsymbol{n-i})}\\ \boldsymbol{with}\prod_{\boldsymbol{i=x}}^{\boldsymbol{x\prime}} = \boldsymbol{1\,for\,x'<x}\end{gathered} \tag{30}$$

With **(21)** the general expression for the probability of occurrence of each situation is:

$$\boldsymbol{P_{O(Y=y)}} = \binom{\boldsymbol{3}}{\boldsymbol{y}} \times \frac{\prod_{i=0}^{y-1}\left[\boldsymbol{n} - \boldsymbol{n}\left(\frac{\boldsymbol{n}-\boldsymbol{3}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} - \boldsymbol{i}\right] \times \prod_{i=0}^{3-y-1}\left[\boldsymbol{n}\left(\frac{\boldsymbol{n}-\boldsymbol{3}}{\boldsymbol{n}}\right)^{\boldsymbol{t}} - \boldsymbol{i}\right]}{\prod_{i=0}^{3-1}(\boldsymbol{n}-\boldsymbol{i})} \tag{31}$$

$$\boldsymbol{with} \prod_{i=x}^{x'} = \boldsymbol{1}\ \boldsymbol{for}\ \boldsymbol{x' < x}$$

Following is a table with the probability of the drawn TCVV having three of known LCVV digits, function of the number of transactions and the length (***n***) of the LCVV.

			n	LCVV length										
y		*t*		10	11	12	13	14	15	16	17	18	19	20
Coinciding CVV digits	3	Number of transactions	1	0,8%	0,6%	0,5%	0,3%	0,3%	0,2%	0,2%	0,1%	0,1%	0,1%	0,1%
			2	9,0%	7,0%	5,5%	4,4%	3,6%	3,0%	2,5%	2,1%	1,8%	1,5%	1,3%
			3	23,2%	18,8%	15,4%	12,8%	10,7%	9,0%	7,7%	6,6%	5,7%	5,0%	4,3%
			4	39,0%	32,8%	27,8%	23,6%	20,3%	17,5%	15,2%	13,2%	11,6%	10,2%	9,0%
			5	53,4%	46,5%	40,4%	35,3%	30,9%	27,1%	23,9%	21,2%	18,8%	16,8%	15,0%
			6	65,4%	58,4%	52,1%	46,4%	41,4%	37,0%	33,1%	29,7%	26,8%	24,1%	21,8%
			7	74,8%	68,3%	62,2%	56,5%	51,2%	46,4%	42,2%	38,3%	34,8%	31,7%	29,0%
			8	81,8%	76,2%	70,5%	65,1%	59,9%	55,0%	50,6%	46,5%	42,7%	39,3%	36,2%
			9	87,0%	82,3%	77,3%	72,3%	67,4%	62,6%	58,2%	54,0%	50,1%	46,5%	43,2%
			10	90,8%	86,9%	82,6%	78,1%	73,6%	69,2%	64,9%	60,8%	56,9%	53,2%	49,7%

Table 6.5 – Probability of occurrences of three coinciding LCVV digits $\mathbf{P_{O(Y=3)}}$

The following figure shows the probability of the drawn TCVV having three of known LCVV digits function of the matrix size after a given number of ***t*** transactions being compromised.

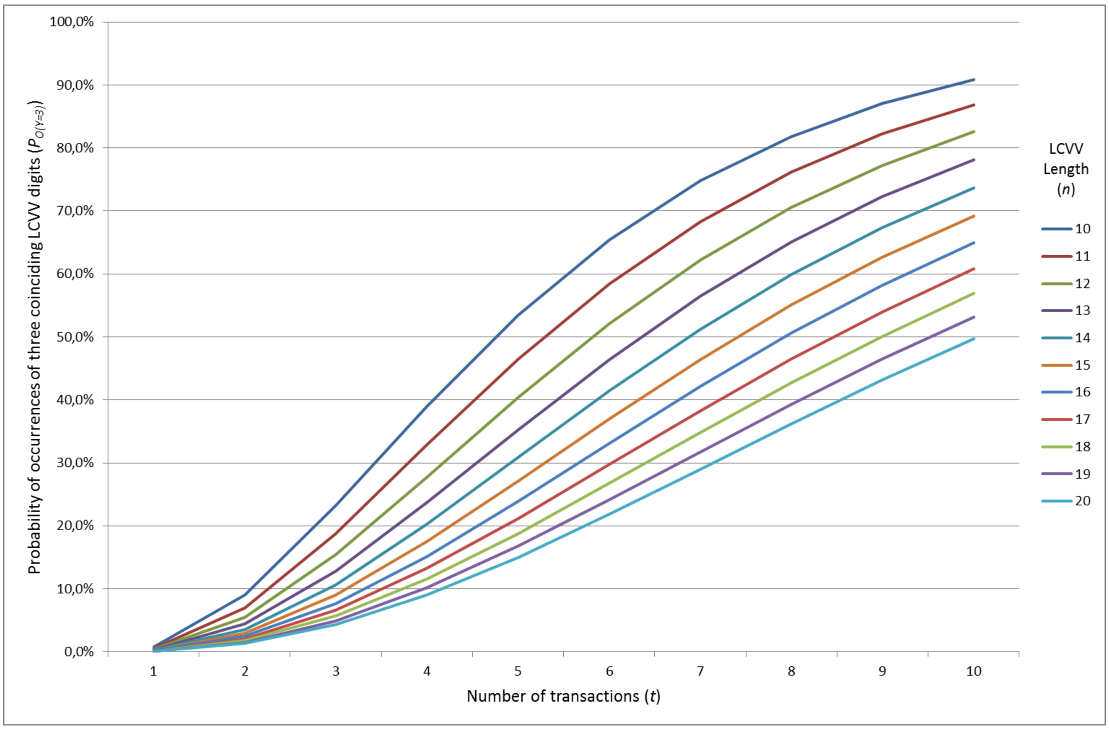


Figure 6.5 – Probability of occurrences of three coinciding LCVV digits $(P_{O(Y=3)})$

6.5.3 Guessing probability for situations of coinciding positions

Having calculated the probability of occurrence of each situation let us now calculate the probability of guessing the correct TCVV in each of the situations.

The probability of successfully guessing the correct three digit TCVV depends on the number of requested LCVV positions that are known to the attacker. If all three TCVV positions are known, the attacker will know the correct TCVV; if two positions are known and one is unknown, the attacker will have a one in ten chance of guessing the TCVV correctly. The generally expression is given by the following formula:

$$P_{G(Y=y)} = 10^{y-3} \qquad (32)$$

6.5.4 TCVV guessing probability

We may conclude that the probability that an attacker has in successfully guessing the TCVV ($P_{G(T=t)}$) after having had access to ***t*** compromised transactions with TCVVs from an LCVV with ***n*** positions is given by the following formula:

$$P_{G(T=t)} = \sum_{y=0}^{3}\left(P_{O(Y=y)} \times P_{G(Y=y)}\right) \tag{33}$$

Finally the following formula represents the probability that an attacker will have in guessing the correct TCVV at trial ***t+1***:

$$P_{G(T=t)} = \sum_{y=0}^{k}\left\{\frac{\prod_{i=0}^{y-1}\left[n - n\left(\frac{n-3}{n}\right)^{t} - i\right] \times \prod_{i=0}^{3-y-1}\left[n\left(\frac{n-3}{n}\right)^{t} - i\right]}{\prod_{i=0}^{3-1}(n-i)} \times \binom{3}{y} \times 10^{y-3}\right\} \tag{34}$$

$$with \prod_{i=x}^{x\prime} = 1\, for\; x' < x$$

The following table shows the guessing probability after ***t*** compromised transactions for LCVVs with lengths of ***n*** digits.

	n	LCVV length										
t		10	11	12	13	14	15	16	17	18	19	20
Number of transactions	1	3,14%	2,60%	2,21%	1,91%	1,68%	1,49%	1,34%	1,22%	1,12%	1,03%	0,95%
	2	13,69%	11,24%	9,39%	7,98%	6,87%	5,98%	5,26%	4,67%	4,18%	3,77%	3,42%
	3	28,69%	24,10%	20,48%	17,59%	15,25%	13,34%	11,77%	10,46%	9,35%	8,42%	7,62%
	4	44,12%	38,08%	33,07%	28,89%	25,41%	22,48%	20,01%	17,90%	16,10%	14,56%	13,22%
	5	57,75%	51,14%	45,37%	40,36%	36,04%	32,30%	29,06%	26,24%	23,79%	21,65%	19,76%
	6	68,81%	62,33%	56,39%	51,03%	46,24%	41,97%	38,18%	34,81%	31,83%	29,18%	26,81%
	7	77,35%	71,44%	65,76%	60,42%	55,49%	50,98%	46,88%	43,15%	39,79%	36,75%	34,00%
	8	83,74%	78,59%	73,43%	68,39%	63,59%	59,07%	54,85%	50,96%	47,36%	44,07%	41,04%
	9	88,42%	84,09%	79,56%	74,98%	70,47%	66,12%	61,97%	58,05%	54,37%	50,94%	47,75%
	10	91,79%	88,25%	84,38%	80,33%	76,23%	72,16%	68,19%	64,37%	60,72%	57,26%	54,00%

Table 6.6 – LCVV guessing probability $\left(\mathbf{P_{G(T=t)}}\right)$

The following graph compares the strength of the various ***n*** sized LCVVs after ***t*** compromised transactions.

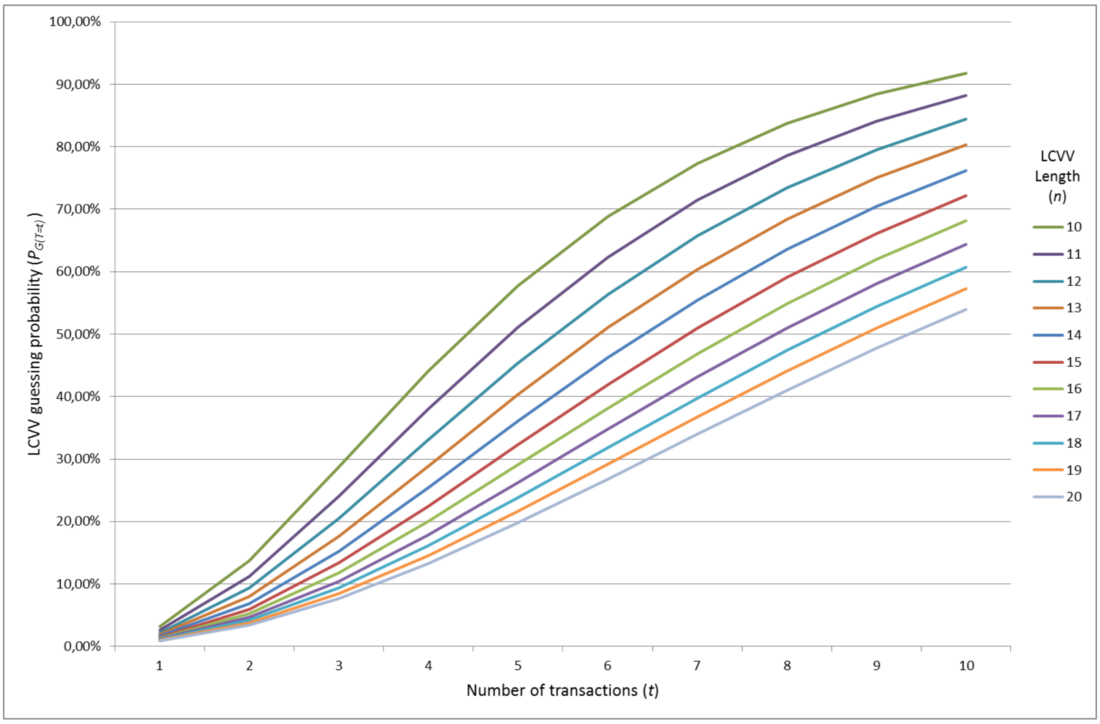


Figure 6.6 – LCVV guessing probability $\left(\mathbf{P}_{\mathbf{G(T=t)}}\right)$

6.6 Multiple CVV *vs.* Long CVV analysis

The nature of usage of either method is considerably different on a users point of view. Prompting a user for a CVV in a table or prompting for three digits out of a long CVV implies different complexity levels. User convenience surveys will have to be carried out to determine optimal sizes for both MCVV matrixes and LCVV lengths.

Smaller secrets (i.e. MCVV matrixes and LCVV lengths) are desirable in order to maintain complexity levels low, on the other hand the larger the secret the more resistance it will offer against guessing attacks after compromise of a certain number of compromised transactions.

In this section we will compare both methods in order to perceive the resistance to attacks function of the number of compromised TCVVs assuming secret sizes that will be in an acceptable range for users.

6.6.1 Comparing ECVV sizes function of number of compromised TCVVs

The following graph shows probability of success in guessing a subsequent transaction's TCVV, function of the number of compromised transactions and the size of the secrets for each method. The LCVV method offers a higher level of protection in situations where few TCVVs are compromised. The MCVV in contrast although it does not prove so efficient with a low number of compromised TCVVs it resists well to a higher number of compromised TCVVs.

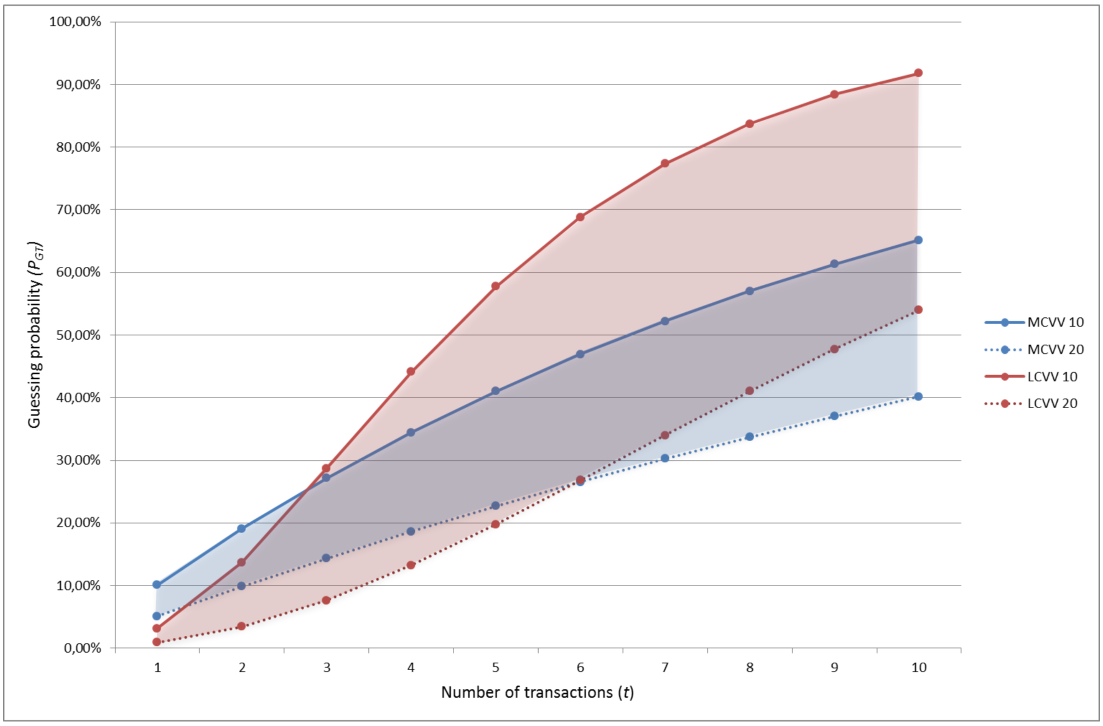


Figure 6.7 – Guessing probability $(P_{G(T=t)})$ function of the number of compromised TCVVs

As can be observed an LCVV with ten digits will have a guessing probability that varies between 3.14% for one compromised TCVV, to 91.79% for 10 compromised TCVVs. On the other hand an MCVV with ten positions will have the guessing probability varying between 10.09% and 65.17% for one to ten compromised TCVVs.

Similarly a 20 digit LCVV will have a guessing probability vary from 0.95% till 54.00% whilst a 20 position MCVV will vary from 5.10% till 40.19%, for one to 10 comprised TCVVs.

LCVV with small sizes seem to degrade quickly, function of the number of compromised TCVVs and as a result after five compromised TCVVs the guessing probability for a 10 digit LCVV is nearly 60%.

6.6.2 Comparing ECVV sizes for one compromised TCVV

The probability of success for an attacker to guess a TCVV depends on the number of transactions with distinct TCVVs that have been compromised for each card. It is proposed that a card at a certain merchant use the same secret for all transactions. By doing so a compromise of the merchant's systems will reveal one TCVV for each card, independent of the number of compromised transactions for the card.

Similarly, system compromise at an acquirer will lead to revealing a number of TCVVs for each card function of the number of merchants where the card has transacted and not to the number of transactions that has been processed for the card.

A scenario where data compromises occur on the user's system, through malware, will equally benefit from this strategy. The number of compromised TCVVs will be function of the number of distinct merchants where the user has paid independent of having made many payments.

In this section we will analyse the resistance to attacks given the compromise of one TCVV.

The following graphs show the robustness of the methods function of the size of the secret for a scenario of a single TCVV compromise.

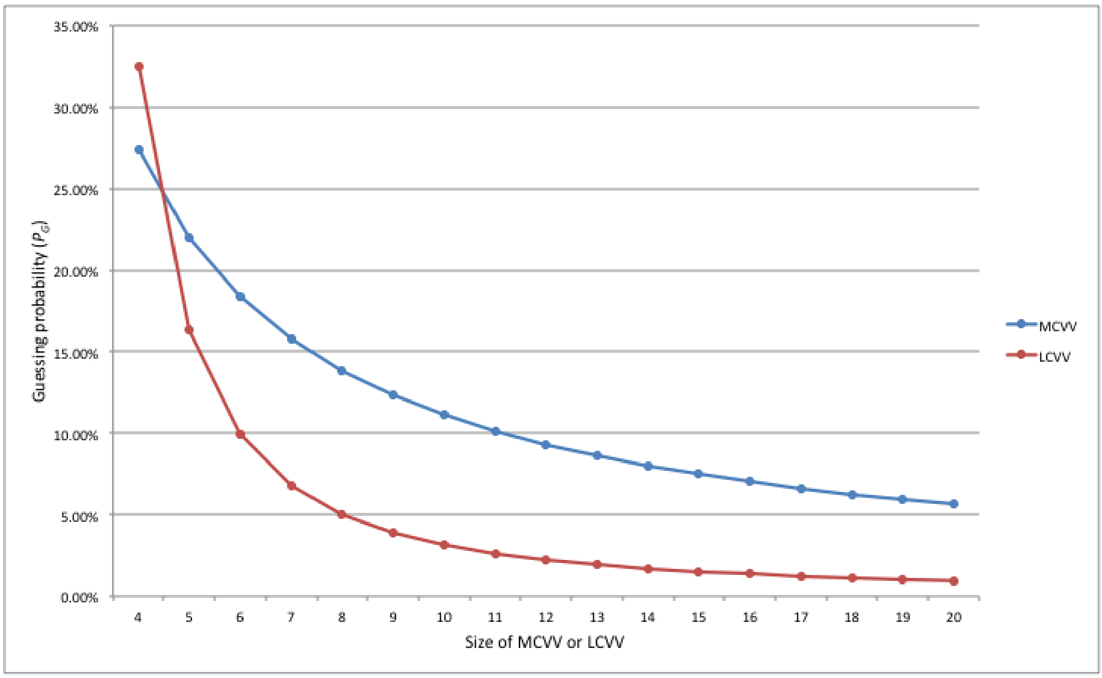


Figure 6.8 – Guessing probability $\left(P_{G(\mathrm{T=t})}\right)$ for one compromised TCVV, function of the ECVV size

For cases where one TCVV is compromised the LCVV proves to be more resistant than the MCVV implementation. Only for an extremely small secret size of four or less is the MCVV more robust than the LCVV.

It can also be observed that an MCVV with 20 positions offers less resistance than an 8 digit LCVV, thus the LCVV proves to be very effective for a single TCVV compromise even with small sizes of secrets.

For cases where ten transactions were compromised the MCVV holds lower guessing probabilities for sizes of four or higher, and so proves more robust in these scenarios as can be seen through the following graph.

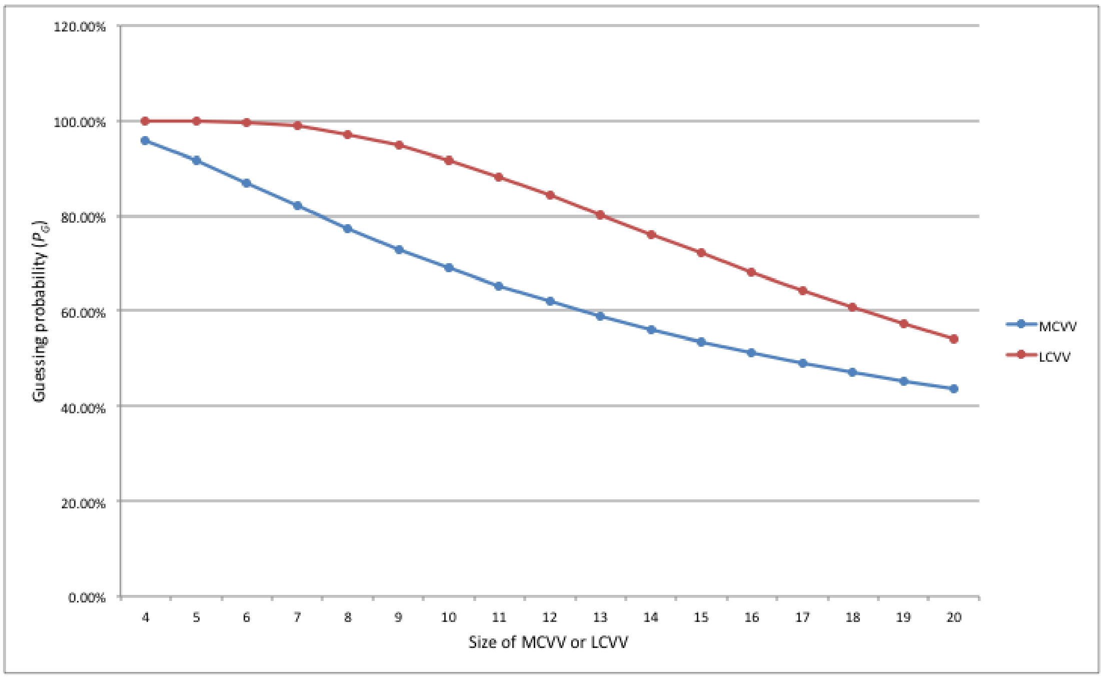


Figure 6.9 – Guessing probability $\left(P_{G(\mathrm{T=t})}\right)$ for ten compromised TCVVs, function of the ECVV size

Chapter 7: Enhanced CVV2 scheme implementation analysis

7.1 Introduction

As covered in “Chapter 4: Key success factors for new e-payment scheme proposals” it is crucial for any e-payments proposal that all parties have their main requirements met.

The proposed schemes benefit from the fact that they build upon the undisputed most adopted e-payments scheme and that migration is non-disruptive.

Issuers may migrate to the proposed schemes by producing cards that contain the traditional authentication elements as well as one of the proposed scheme enhanced CVVs. By enrolling the cards into the 3-D Secure scheme and preparing the ACS to perform 3-D Secure authentication, the cards will automatically be accepted at all 3-D Secure merchants without the merchant having to perform any changes to their systems. Non 3-D Secure merchants will either have to prepare for 3-D Secure or perform minor changes to existing systems to support the proposed schemes. All other parties such as Acquirers and Payment systems need not perform any changes given that the transaction messages remain unchanged.

Finally the users will have a slight difference in the payment experience having to introduce a CVV chosen out of the CVV Matrix or three digits from a Long CVV. Either of these tasks is simple and will maintain user convenience at an acceptable level whilst simultaneously giving an enhanced perception of security.

From day one of implementing the scheme the issuer and cardholder will benefit from all the 3-D Secure merchants accepting the enhanced scheme and offers a fallback for the rest of the merchants.

7.1.1 Chapter overview

In this chapter we shall detail the modifications that have to be implemented to setup and operate the proposed payment schemes taking into account migration issues.

7.2 Issuer

Issuers are the drivers for the adoption of the proposed scheme and will have to perform modifications to their processes in the following areas:

- Issuer card data preparation
- Card personalisation

- 3-D Secure cardholder authentication
- Card payment authorisation

By performing these changes, payments with the enhanced security of the proposed schemes will occur automatically from payments performed at 3-D Secure merchants. In this section we will analyse the modifications that the issuer has to perform.

7.2.1 Card data preparation

Traditional card data preparation produces a set of cryptographic elements such as the PVV and the CVV1 for the magnetic stripe, and the CVV2 for the signature panel. If the card is an EMV card, for each EMV application an iCVV, a Card Application Cryptogram Key and two Card Secure Messaging keys for integrity and confidentiality, will have to be produced. Apart from the symmetric keys based cryptographic elements, Static Application Data will have to be signed with the Issuer Public Key. If the card is a DDA (Dynamic Data Authentication) card an extra Card Public Key must be generated and a certificate of this key signed by the Issuer Public Key must be calculated. In the proposed schemes, along with the elements produced in the traditional card data preparation, the enhanced CVVs must be also calculated.

MCVV implementation

In this implementation the issuer will have to invoke the HSM CVV Generation function, present in traditional financial HSMs, as many times as the number of values in the matrix, for each card. As with other CVVs, no data has to be stored and therefore a compromise of the card database will not reveal the CVVs for these cards. No special HSM function is necessary although, a specially designed HSM function for the bulk generation of CVVs for MCVV matrixes may significantly optimize the effort necessary for these calculations.

LCVV implementation

The issuer will have to store the LCVV ***n*** digit long values for each produced card for later authorizations. This implementation poses the disadvantage of having to store extra data for each card and that the compromise of this data would have severe implications for these cards. An alternative is to produce the LCVV using an existing function of the HSM such as encrypting the card number by a given key and decimalizing the result in order to obtain the LCVV. This same function would have to be used in order reproduce the LCVV so as to validate the TCVV during the cardholder 3-D Secure authentication or the transaction authorisation.

7.2.2 Card personalisation

Recent card designs have reduced the signature panel and the CVV2 location placing it out of the area where the chip is placed so that damage to the chip is avoided.

For the proposed schemes, the card personalizer will have to place the enhanced CVV values on the back of the card. Card personalizers already have the capacity of printing on the back of the card and print CVV2s, secondary PANs for combo cards or other account information.

Printing a matrix of CVV values or a long CVV will not pose difficulty. Card designs will have to include legends so as to assist the user to choose the queried CVV or CVV digits.

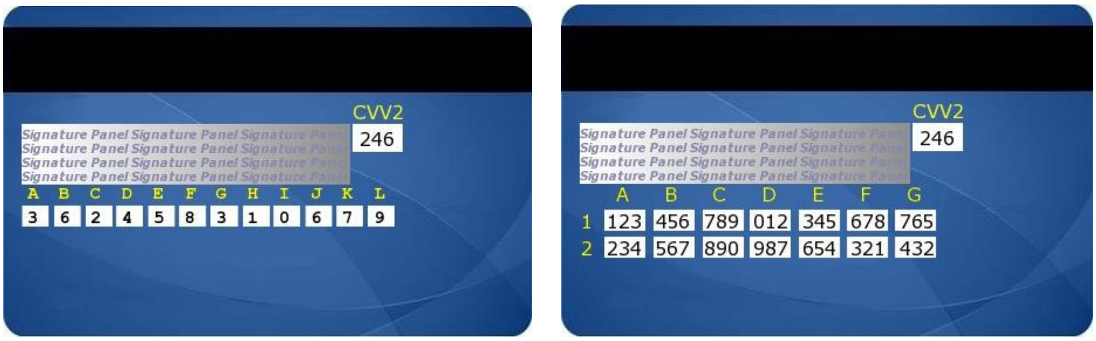


Figure 7.1 – Card personalisation examples

7.2.3 3-D Secure cardholder authentication

So that Issuers support transactions performed at 3-D Secure merchants, two modifications have to be performed:

- The issuer ACS will have to modify the authentication pop-up so as to prompt the user for the CVV of a matrix position or for three digits of the Long CVV.
- The ACS will have to validate the queried TCVV and to do so will make use of the HSM functions used for traditional card payment authorisations.

Modification of the authentication pop-up is straightforward but care should be taken so that for a given card transacting at a given merchant the same secret should be prompted for, for each transaction. By doing so, malware collecting secrets on the user's computer will only have part of the secret independent of the number of transactions performed at the merchant.

The ACS and the authorisation system are connected so that the ACS may inform the authorisation system that the cardholder has authenticated the transaction. If the Issuer ACS and the payment authorisation system are integrated then validating the queried TCVV is trivial. Otherwise the ACS must use the authorisation systems services to validate the TCVV.

7.2.4 Card payment authorisation

So that Issuers support transactions performed at non 3-D Secure merchants, the authorisation system must be modified. If the TPAN is 19 digits long, for a BIN that only holds up to 16 digits, the Issuer in the authorization process will have an extra task related to unpacking the TPAN and will modify the CVV validation function accordingly.

Unpacking the TPAN

The issuer shall obtain the original PAN by stripping the TPAN of its last 3 digits. The TPAN's 16th, 17th and 18th digits constitute the TCVV PC.

ECVV Validation

In an MCVV implementation the TCVV validation must be performed through the traditional HSM CVV validation function having the TCVV PC substitute the Service Code field in the function. This poses a minor change in respect to the current CVV2 validation.

In an LCVV implementation, the TCVV validation must be performed by reproducing the LCVV and then comparing the digits indicated by the TCVV PC.

Reproducing the LCVV may be performed through the usage of an HSM function, such as encrypting the PAN and decimalising the result.

7.2.5 Merchants

3-D merchants need not perform any changes to support the proposed schemes. Non 3-D Secure merchants may either adhere to 3-D Secure, and benefit of liability shifts, or perform the following modifications to their checkout process:

- ECVV PC generation
- ECVV prompting
- TPAN packing

7.2.6 Non 3-D Secure merchant checkout process

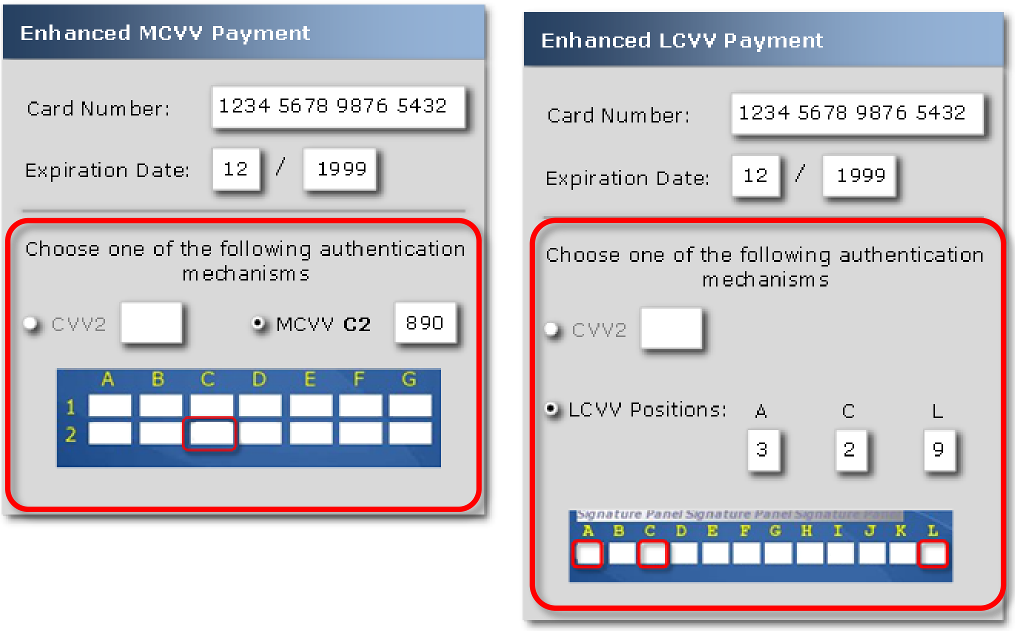
TCVV PC generation

The TCVV PC value shall be generated by each merchant in a deterministic form for each card, so as to limit the number of secrets processed by a merchant for each card.

- For MCVV implementation two values shall be generated: a column value ***x*** between 1 and ***a*** and a row value ***y*** between 1 and ***b***;
- In the case of LCVV the ECVV PC shall be a value between 1 and the number of permutations for 3 out of ***n*** digits (P_3^n);

ECVV prompting

The merchant shall modify the checkout screen so as to mention in the CVV input field, the ECVV elements that are required as highlighted in the following figure:



Enhanced MCVV Payment

Card Number: 1234 5678 9876 5432

Expiration Date: 12 / 1999

Choose one of the following authentication mechanisms

○ CVV2 ● MCVV **C2** 890

Enhanced LCVV Payment

Card Number: 1234 5678 9876 5432

Expiration Date: 12 / 1999

Choose one of the following authentication mechanisms

○ CVV2

● LCVV Positions: A 3 C 2 L 9

Figure 7.2 – Checkout modifications

TPAN packing

The merchant shall concatenate the prompted PAN (typically 16 digits) with the three digits of the TCVV PC.

7.3 Cardholders

The complexity of any of the proposed schemes is kept low whilst the security and perception of security is heightened. Cardholders, however should be educated on the new payment experience with the proposed scheme. Cardholders will have to be warned to: never reveal all of their secrets through phishing attacks, and alert of any attempt to do so.

7.4 Migration considerations

The migration process is critical to the viability of any proposed solution in order to maintain the attained critical mass. Issuers may migrate at their own will without having to depend on any other party. Cards will be processed with the proposed enhanced scheme at any 3-D Secure merchant.

Cardholders will use traditional elements at non 3-D Secure merchants that do not support the enhanced scheme. Merchants may migrate their systems to support 3-D Secure or to support the enhanced scheme at any time. By doing so the impacts resulting from a compromise of their systems is greatly reduced. As can be seen in the previous chapter, the probability of an attacker succeeding with an authenticated transaction is greatly reduced.

Chapter 8: Summary and conclusions

8.1 Summary of Findings

In this dissertation two methods have been proposed to secure e-payments based on bank cards against the present major attacks.

8.1.1 Payment systems success factors

The characteristics that should be inherent to a payments system on the Internet have been analysed. We have gone through the various studies that analyse these characteristics and the trends that were observed throughout time. From essentially technical criteria we have seen a user related criteria being added and more recently criteria referring to all parties being taken into account.

We have witnessed, for nearly two decades, the huge success of bank cards as the dominant method for payments on the Internet. No study was found that clearly substantiates this phenomenon. In this study we have covered the criteria that should be found in a payments system for all participating parties.

We have analysed criteria that is important for users based on a survey [18] performed by Dennis Abrazhevich. Contrary to the emphasis found in numerous studies anonymity seems not to have high importance for the respondents. Respondents find cards very easy to use and trust seems to be highly valued. Using a long number printed on a plastic card that is securely kept in the users wallet, conveys a perception of security that is easily perceived by the cardholders.

Payments with bank cards satisfy the conclusions drawn from the respondents, however other parties interests have to be attended to in order for a payment system to succeed. Little analysis has gone into understanding the needs for merchants. Merchants essentially want to have profit with any system they embark into. On one hand we have the costs of implementing and running a new system, and on the other hand the number of customers that may be maintained or captured into the merchant’s business. Security will ultimately define the risk on not receiving the transacted funds, and so complements the previous characteristics.

All other parties such as payments systems, financial institutions, issuers acquirers, processors will have to have their interests guaranteed by any new system.

The proposed schemes try not to alter the balance of characteristics that are present in the card based payment systems. They propose to solve current major threats at the expense of a new challenge, for the cardholders, that is deemed of residual complexity. Furthermore the implementation of the proposed schemes may be achieved with a very low investment, benefitting from a global infrastructure and a tremendous user base.

8.1.2 Security

The capture of card data is by far the most relevant attack vector that threatens Internet payments. Data breaches at merchants, processors or service providers and malware ridden end user systems are responsible for the great majority of fraudulent activity pertaining to card payments.

In this study we have analysed the level to which the value of card data may be reduced in case of a compromise. In the traditional card payments, a compromise of transaction data gives an attacker full credentials to perform subsequent fraudulent payments.

3-D Secure implementations have helped solve some of these security issues however some vulnerabilities sustain. Many 3-D Secure implementations are based on static credentials, namely passwords. These implementations protect against data breaches however are ineffective in face of malware such as key loggers. 3-D Secure implementations based on dynamic credentials usually make use of SMS tokens. In the case of SMS tokens three issues hinder a generalized adoption:

- A rise in costs related to the transmission of SMS tokens can have to be accounted for;
- User convenience is affected to a certain degree given that the user will have to have a mobile phone present in order to fulfil the transaction;
- E-payments performed on mobile phones that are infected by malware, given that the malware may perform fraudulent payments, intercept the SMS tokens and authenticate the transaction, without user interaction.

The proposed schemes have greatly reduced the ability of an attacker performing fraudulent payments with captured card data.

Data breaches

In the case of a 3-D Secure merchant data breach, the attacker will not have access to the enhanced CVV secret given that only the issuer validates the enhanced CVV and the merchant does not receive this element. In the case of non 3-D Secure merchant, the merchants will have knowledge of part of the enhanced CVV secret, per card, pertaining to one transaction independent of the number of transactions performed by the same card.

The analysis conducted in this study demonstrates that the LCVV is more effective than the MCVV solution for a single transaction secret compromise. An attacker will have a probability of successfully authenticating a subsequent transaction between 3.14% and 0.95% for LCVVs ranging from 10 to 20 digits respectively. The MCVV presents an attacker guessing probability of 10.09% and 5.10% for MCVV with 10 to 20 positions respectively.

As a result a compromise of a 3-D secure merchants systems will not reveal the enhanced CVV secret. A compromise of a non 3-D Secure merchant will enable the attacker to perform attacks on all compromised LCVV cards with a success ratio of approximately one to 32 or one to 105 for LCVV with 10 or 20 digits.

Malware

Transactions performed on user systems infected by malware may collect card data, pertaining to the user, including the enhanced CVV secrets independent of the usage of 3-D Secure protocol or not.

The amount of the enhanced CVV secret that may be captured is proportional to the number of distinct merchants with whom the user has transacted.

Whilst the LCVV is much more secure than the MCVV for a single compromised transaction, for more compromised transactions the MCVV proves to be better than the LCVV. As a result the number of merchants with whom a user transacts influences the adoption for the LCVV or for the MCVV scheme.

Conclusions

A decision on what method to adopt will have to be based on evaluating what threat causes higher losses, data breaches or malware on end user systems. The adoption of 3-D Secure will eventually mitigate risks inherent to data breaches so it is expected that malware infected end-user systems be the most relevant threat in the future. This factor should be taken in to account. Equally important is a survey on user convenience relating to choosing a MCVV out of a set of ***n*** MCVVs or choosing three digits out of a LCVV with ***n*** digits. The higher the ***n*** the more secure the system, however user convenience will establish the limit to which these secrets may grow.

8.2 Directions for future work

There are various directions of research that can be investigated in future:

Key factors for e-payment systems

A survey should be conducted on the key determinant factors for adoption in new payment systems involving all parties to better understand the drivers for each participant. Payment systems involve multiple parties with different interests and most studies fail to take them all into account. One vector of analysis would be to analyse and understand why an apparently security-wise weak system, such as the card based e-payments, has managed to dominate for the e-payments arena for so long. Despite the frequent security incidents users still trust this means of payments.

The perception of security on behalf of the user should be subject of research. The user clearly understands the security inherent to a long number that is printed on a plastic card that is secretly kept in his wallet. On the other hand, as an example, the level of security intrinsic to “a 4096 bit long Eliptic Curve cryptographic key stored in a Trusted Platform Module on a computer” may not be easily understood by the common user, and invokes a sentiment of distrust.

Surveys should be carefully prepared in order to get a better perception of the value of criteria. As an example if a user is questioned about the importance of anonymity intrinsic to payments, most will respond that it is highly important. On the other hand, when asked if the user prefers to sacrifice anonymity in order to avoid disputes surveys show that anonymity is of less importance [18].

Subjective criteria such as trust, perception of security, sense of control, etc., should be further scrutinized and evaluated.

Merchants are an important participant in a payments system given that global acceptance can only be achieved if the millions of merchants are driven to embark on any new scheme. Merchants will only be ready to adopt a new scheme if a sufficient user base is available to pay with the new mechanisms. Users will adopt new payment mechanisms, only if wide acceptance by merchants is available. This chicken and egg problem is covered in many studies however a strategy of migration of existing systems could be better understood to minimize these kind of interdependency problems.

Partial secrets

Common authentication mechanisms based on partial secrets, such as those presented in this paper (code matrixes and parts of codes) have not been covered in published academic works, as far as the research for this dissertation was able to identify. This study has contributed to the better understanding of the probabilities related to partial secrets. A survey on user convenience would be of great value in order to configure these often used mechanisms. A perception of how user acceptance is affected by the number of codes that a matrix holds, should be understood. Likewise the number of digits queried from a secret with a determined number of digits should be analysed to perceive the impact on user convenience criteria.

A variant of the MCVV scheme, presented in this paper, would be to have chronological CVVs. The card would hold 12 CVVs, each one corresponding to a month. The user would make use of the CVV for the month in which the payment is being performed. This scheme has the benefit on the fact that merchants do not have to perform any changes to accept these enhanced CVVs.

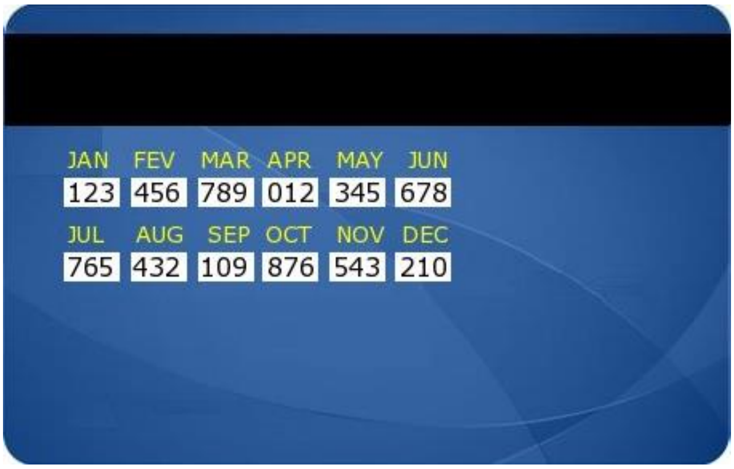


Figure 8.1 – Chronological CVV card example

This scheme would greatly frustrate the attackers intentions given that they would have to use the captured data on the same month in which it was transacted. A study of data breach incidents, namely the time span of compromised data and the time between compromise and fraudulent usage, would be of great value to evaluate this proposed method and other similar methods.

8.3 Conclusion

Card based payments are the most well succeeded payments means on the Internet. Many attempts to substitute this payments means have been made, but none has yet succeeded.

This study has stressed the importance of the factors that should be valued in a payments scheme for all participating parties. The proposed solutions build upon the current card payment schemes and scrutinize the impacts of implementation and migration issues.

Card payments currently suffer major impacts consequence of card data captures from frequent data breaches and unprecedented number of malware infected end user systems. This study has proposed two methods that, with low implementation costs and residually affecting ease of use, greatly enhance the security of the traditional e-payment scheme to better resist against these attacks.

Bibliography

[1] ISO/IEC 7812-1:2006. Identification cards – Identification of issuers – Part 1: Numbering system. Year: 2006.

[2] "SETCo. SET Secure Electronic Transaction 1.0 Specification - The Formal Protocol Definition". http://www.cl.cam.ac.uk/research/security/resources/SET/. Year: 1997.

[3] "3-D Secure Protocol Specification: System Overview". Visa International Service Association http://international.visa.com/fb/paytech/secure/main.jsp, Year: 2003.

[4] "VISA Card Verification Value (CVV2) Merchant Guide". Visa. U.S.A inc, Year: 2002.

[5] "PCI DSS - Requirements and Security Assessment Procedures, Version 1.2" Payment Card Industry. Year: 2008.

[6] "The Nilson Report" Issue 947 and 949. Year 2010.

[7] "2013 Data Breach Investigation Report" by Verizon RISK Team in cooperation with the United States Secret Service. Year: 2013.

[8] "Security Threat Report: 2010" by Sophos. Year: 2010.

[9] "2005/2006 Study of Consumer Payment Preferences", Americans Bankers Association and Dove Consulting. Year: 2006.

[10] The Economic and Social Role of Internet Intermediaries" by OECD. Year: 2010.

[11] "Credit card incidents and control systems" by Pavía, Jose M. ; Veres-Ferrer, Ernesto J. ; Foix-Escura, Gabriel. International Journal of Information Management, Vol.32(6), pp.501-503 Year: 2012.

[12] iKP -- A Family of Secure Electronic Payment Protocols (Extended Abstract)" by Mihir Bellare, Juan A. Garay, Ralf Hauser, Amir Herzberg, Hugo Krawczyk, Michael Steiner, Gene Tsudik, Michael Waidner. Year: 1995.

[13] "Requirements for Network Payment: The NetCheque Perspective" by B. Clifford Neuman, B. Cli, Gennady Medvinsky. Year: 1995.

[14] "On two Proposals for On-line Bankcard Payments using Open Networks - Problems and Solutions" by Wenbo Mao. In IEEE Symposium on Security and Privacy. Year: 1996

[15] "Independent One-Time Passwords" by Aviel D. Rubin. USENIX Journal of Computer Systems. Year: 1996.

[16] "Effectiveness Criteria for Internet Payment Systems" by Tae Hwan Shon, Paula M.C. Swatman. Year: 1996.

[17] "NetCents: A Lightweight Protocol for Secure Micropayments" by Tomi Poutanen, Heather Hinton, Heather Hinton, Michael Stumm. In Proceedings of the Third USENIX Workshop on Electronic Commerce. Year: 1998.

[18] "Electronic Payment Systems: a User-Centered Perspective and Interaction Design" by Dennis Abrazhevich. Eindhoven : Technische Universiteit Eindhoven. Year: 2004.

[19] "Electronic Payment Systems: Issues of User Acceptance" by Dennis Abrazhevich. In B.Stanford-Smith and E.Chiozza (Eds.), E-work and E-commerce. Year: 2001.

[20] "Passwords: Use and Abuse" by Peter Yapp. Computer Fraud &amp; Security, Issue 9, 1 September 2001, Pages 14–16. Year: 2001.

[21] "Quantifying the Quality of Web Authentication Mechanisms. A Usability Perspective" by Renaud, K. Journal of Web Engineering, Riton Press. Year: 2003.

[22] "Security and Usability: The Case of the User Authentication Methods" by Christina Braz and Jean-Marc Robert. Year: 2006

[23] "Comprehensive study on methods of fraud prevention in credit card e-payment system" by Dr. Saleh Al-Furiah and Lamia AL-Braheem. iiWAS 2009 ERPAS. Year:2009.

[24] "Dynamic Virtual Credit Card Numbers" by Ian Molloy, Jiangtao Li, Ninghui Li. In Financial Cryptography and Data Security (FC'07), Scarborough, Trinidad and Tobago Year: 2007.

[25] "The power of credit card numbers and long CVVs" by Valentim Oliveira and Tito Silva. 2011 5th International Conference on Network and System Security. Year: 2011

[26] "Secure Card Payments On The Internet - TR410 Version 1.0" by European Committee for Banking Standards. Year: 2002

[27] "A Survey of Payment Card Industry Data Security Standard" by Jing Liu, Yang Xiao, Hui Chen, Suat Ozdemir, Srinivas Dodle and Vikas Singh. IEEE Communications Surveys & Tutorials, Vol. 12, No. 3, Third Quarter, 2010. pp. 287-303.

[28] "The changing nature of U.S. card payment fraud " by Richard Sullivan. Year 2010. Presentation at the 2010 Workshop on the Economics of Information Security - Harvard University, Year: 2010.

[29] "Password Disclosure Matrix" Computer Fraud & Security, Vol.2003(7), pp.4-5 SciVerse ScienceDirect Journals. Year: 2003.

[30] "How Catalysts Ignite: The Economics Of Platform-Based Start-Ups" by David S. Evans. Platforms, Markets and Innovation. Cheltenham, UK and Northampton, MA, US : Edward Elgar.,Year: 2008.

[31] "Electronic Payment Market: a non-optimal equilibrium" by Malgorzata Galuszewska and Jean-Michel Sahut. Year: 2004.

[32] "European Commission ePayment Systems Database – Trends and Analysis – Electronic Payment Systems Observatory (ePSO)", by Gérard Carat. Year: 2002.

[33] "A Stakeholder Perspective on Successful Electronic Payment Systems" by Sangjo Oh, Heejin Lee, Sherah Kurnia, Robert B. Johnston, and Ben Lim. Year: 2006.

[34] "Emergence of payment systems in the age of electronic commerce: The state of art" by Sumanjeet, Singh. s.l. : First Asian Himalayas International Conference on Internet (AH-ICI 2009). Year: 2009.

[35] "An Introduction to Probability Theory" by Feller, W. New York. Year:1950.

[36] "The Collector's Brotherhood Problem Using the Newman-Shepp Symbolic Method" by Foata, D. and Zeilberger, D. Algebra Universalis, 49(4):387-395. Year: 2003.

[37] "Extreme Value Distributions for Random Coupon Collector and Birthday Problems" by Holst, L.. Extremes, 4:129-145. Year: 2001.

[38] "Martingale Approach to the Coupon Collection Problem" by Kan, N. Journal of Mathematical Sciences, 127(1):1737-1744. Year: 2005.

[39] "Some New Aspects of the Coupon-Collector's Problem" by Myers, A. and Wilf, H.. SIAM, Journal on Discrete Mathematics, 17(1):1-17. Year: 2003.

[40] "The generalised coupon collector problem" by Neal, P.. Journal of Applied Probability,45(3): 621-629. Year: 2008.

[41] "A generalized coupon collector problem" by Weiyu Xu and A. Kevin Tang, Applied Probability Trust, Year: 2010.

[42] "A Survey of the Coupon Collector's Problem with Random Sample Sizes" by John E. Kobza, Sheldon H. Jacobson , Diane E. Vaughan. pp. 573-584. Year: 2007.

[43] "Data Breaches: What The Underground World of "Carding" " by Peretti, Kimberly Kiefer. Santa Clara Computer and High Technology Law Journal, Vol. 25, No. 2, pages 375-413. Year: 2009.

[44] "Are Large Scale Data Breaches Inevitable?" by Salane, Douglas E. . Cyber Infrastructure Protection '09, 2009.

[45] "A Wide Scale Survey on Botnet" by Amit Kumar Tyagi and G. Aghila. International Journal of Computer Applications, 2011, Vol.34(9), p.10. Year: 2011.

[46] "Botnet-A Network Threat" by Sonal P.patil ; Swatantra Kumar. International Journal of Computer Applications, 2012, Vol.icrtitcs. Year 2012.

[47] "Trend Analysis of the CVE for Software Vulnerability Management" Chang, Yung-Yu; Zavarsky, Pavol ; Ruhl, Ron ; Lindskog, Dale. 2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing, Oct. 2011, pp.1290-1293. Year: 2011.